UNIVERSIDADE DO VALE DO RIO DOS SINOS (UNISINOS)
GRADUAÇÃO EM DIREITO

FRANCIS TAINÁ SILVA SCHAEDLER

DIREITO AERONÁUTICO E A CIBERSEGURANÇA NA AVIAÇÃO CIVIL: Análise da Necessidade de Regulamentação Específica no Ordenamento Jurídico Brasileiro

São Leopoldo
2024

FRANCIS TAINÁ SILVA SCHAEDLER

DIREITO AERONÁUTICO E A CIBERSEGURANÇA NA AVIAÇÃO CIVIL: Análise da Necessidade de Regulamentação Específica no Ordenamento Jurídico Brasileiro

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito da Universidade do Vale do Rio dos Sinos (UNISINOS).

Orientador: Prof. Dr. Gustavo André Olsson

São Leopoldo

2024

À minha avó, Maria Ildes Berwanger Schaedler (in memoriam), que me criou e me ensinou que “a caneta é mais leve que a enxada”, cujas palavras, sabedoria e exemplo de dedicação moldaram quem sou hoje. E ao meu fiel companheiro de quatro patas, Migo (in memoriam), que me acompanhou por 18 anos, até o penúltimo semestre desta jornada. Ele esteve presente em todas as fases da minha vida, inclusive nas noites de estudo que marcaram o início desta monografia.

AGRADECIMENTOS

A Deus, por ser minha força constante e iluminar meu caminho ao longo desta trajetória acadêmica.

Ao meu pai, Ricardo Luís Schaedler, meu maior alicerce, pelo amor incondicional e por acreditar em meus sonhos, mesmo nos momentos de incerteza.

À minha tia, Maria Lizete Schaedler, que sempre me incentivou a estudar e ficou imensamente contente com o tema da minha monografia, partilhando o entusiasmo pela aviação que tanto admiramos. Seu apoio constante e amor incondicional foram fundamentais em minha caminhada.

Às minhas amigas de faculdade, Mayara Beck Zanotto e Monique Schneider, que conheci em 2019, no meu primeiro ano de graduação na Unisinos. Desde então, nunca mais nos separamos. Nossa amizade é um vínculo que foi se fortalecendo com os anos e tornou-se indispensável em todos os momentos, tornando essa caminhada mais leve e especial.

Ao meu orientador, professor Dr. Gustavo André Olsson, que foi meu primeiro professor na graduação, em 2019, na disciplina "Conhecendo o Direito". Sua promessa de “não soltar a mão de ninguém” se manteve durante toda a minha trajetória acadêmica. Com um cuidado humano que transcendeu qualquer expectativa e um profissionalismo admirável, ele me guiou com dedicação ímpar, assegurando que cada capítulo desta monografia fosse minuciosamente lapidado. Agradeço por ter embarcado nesta jornada comigo.

A todos vocês, meu mais profundo e sincero agradecimento perene.

“Inventar é imaginar o que ninguém pensou; é acreditar no que ninguém jurou; é arriscar o que ninguém ousou; é realizar o que ninguém tentou. Inventar é transcender”[1].

[1] DIA DO nascimento de Alberto Santos-Dumont. *In*: LABORATÓRIO químico-farmacêutico da aeronáutica. Brasília, DF, [2024?]. Disponível em: https://www2.fab.mil.br/laqfa/index.php/2014-12-11-17-51-57. Acesso em: 08 nov. 2024.

RESUMO

A aviação civil desempenha um papel essencial na economia global e é fundamental para o transporte de passageiros e mercadorias no Brasil. Contudo, com o avanço tecnológico, o setor enfrenta desafios crescentes, como os ataques cibernéticos, que ameaçam tanto as infraestruturas críticas quanto a segurança dos dados pessoais dos usuários. A presente monografia busca analisar a eficácia das normas e estruturas regulatórias brasileiras, com foco no direito aeronáutico e digital, na mitigação dessas ameaças e avaliar a aplicação das legislações já existentes no setor da aviação civil. O estudo aborda inicialmente, uma análise do desenvolvimento histórico da aviação e do direito aeronáutico, seguido de uma definição abrangente de cibersegurança e de uma discussão sobre os principais incidentes cibernéticos que afetaram o setor, incluindo o ataque à SITA em 2021 e o Apagão Cibernético de 2024. A análise normativa abrange legislações, como a Lei Federal nº 7.565/1986 (Código Brasileiro de Aeronáutica), a Lei Federal nº 11.182/2005 (que cria a ANAC), a Lei Federal nº 12.965/2014 (Marco Civil da Internet), a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados), o Decreto nº 11.856/2023 (Política Nacional de Cibersegurança) e o Decreto nº 11.491/2023 (Convenção de Budapeste). Além disso, são examinadas as diretrizes de cibersegurança da ANAC e discutida a competência constitucional para processar e julgar questões envolvendo cibersegurança na aviação. Na conclusão, identificam-se três vertentes principais para a análise: (1) a responsabilidade contratual das empresas aéreas e aeroportuárias com fornecedores de tecnologia; (2) violações cibernéticas internas por funcionários; e (3) os riscos aos passageiros ao usar redes públicas. Conclui-se, portanto, que não há falta de regulamentação específica, mas sim a necessidade de uma aplicação eficaz das normas já existentes. Defende-se, ainda, que o poder público invista na educação digital, promovendo a conscientização sobre os riscos cibernéticos, bem como, faz-se igualmente necessário incentivar o contínuo estudo e aprofundamento em pesquisas acadêmicas, a fim de promover um senso crítico pelos operadores do Direito, frente aos desafios impostos pelo avanço tecnológico.

Palavras-chave: aviação; cibersegurança; direito aeronáutico; direito digital; segurança cibernética.

ABSTRACT

Civil aviation plays an essential role in the global economy and is key to the transportation of passengers and goods in Brazil. However, with technological advances, the sector faces growing challenges, such as cyber attacks, which threaten both critical infrastructure and the security of users' personal data. This monograph seeks to analyze the effectiveness of Brazilian regulatory standards and structures, with a focus on aviation and digital law, in mitigating these threats and evaluating the application of existing legislation in the civil aviation sector. The study initially covers an analysis of the historical development of aviation and aviation law, followed by a comprehensive definition of cybersecurity and a discussion of the main cyber incidents that have affected the sector, including the attack on SITA in 2021 and the Cyber Blackout of 2024. The normative analysis covers legislation such as Federal Law No. 7,565/1986 (Brazilian Aeronautics Code), Federal Law No. 11,182/2005 (which creates ANAC), the Federal Law No. 12,965/2014 (Marco Civil da Internet), the Federal Law No. 13,709/2018 (General Data Protection Law), Decree No. 11,856/2023 (National Cybersecurity Policy) and Decree No. 11,491/2023 (Budapest Convention). In addition, ANAC's cybersecurity guidelines are examined and the constitutional competence to prosecute and judge issues involving aviation cybersecurity is discussed. In the conclusion, three main strands are identified for analysis: (1) the contractual responsibility of airlines and airport companies with technology suppliers; (2) internal cyber breaches by employees; and (3) the risks to passengers when using public networks. It can therefore be concluded that there is no lack of specific regulation, but rather the need for effective enforcement of existing rules. It is also advocated that public authorities invest in digital education, promoting awareness of cyber risks, and it is also necessary to encourage the continuous study and deepening of academic research, in order to promote a critical sense on the part of legal operators, in the face of the challenges posed by technological advances.

Key-words: aviation; cybersecurity; aeronautical law; digital law.

LISTA DE FIGURAS

LISTA DE QUADROS

LISTA DE SIGLAS

ANAC	Agência Nacional de Aviação Civil
ANPD	Autoridade Nacional de Proteção de Dados
Art.	Artigo
ATAERO	Adicional de Tarifas Aeronáuticas
CBA	Código Brasileiro de Aeronáutico
CF	Constituição Federal de 1988
CGI	Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação
CIA	Confidentiality, Integrity and Availability
CINA	Comissão Internacional de Navegação Aérea
CISA	Agência Americana de Cibersegurança e Infraestrutura
CNCiber	Comitê Nacional de Cibersegurança
CRE	Comissão de Relações Exteriores e Defesa Nacional
DDoS	Distributed Denial of Service
DOU	Diário Oficial da União
EASA	Agência da União Europeia para a Segurança da Aviação
EUA	Estados Unidos da América
FAB	Força Aérea Brasileira
FTL	Ferrovia Transnordestina Logística S.A.
GPS	Global Positioning System
GSI/PR	Gabinete de Segurança Institucional da Presidência da República
IBM	International Business Machines Corporation
IEC	Comissão Eletrotécnica Internacional
IoT	Sigla em Inglês para Internet das Coisas
ISO	Organização Internacional de Normalização
LGPD	Lei Geral de Proteção de Dados
MH370	Malaysia Airlines MH370
OACI	Organização de Aviação Civil Internacional
ONU	Organização das Nações Unidas
PNCiber	Política Nacional de Cibersegurança
PSS	Passenger Service System

SGSI	Gestão de Segurança da Informação
TI	Tecnologia da Informação
TIC	Tecnologias da Informação e das Comunicações
TRF5	Tribunal Regional Federal da 5ª Região
UIT	União Internacional de Telecomunicações
USB	Universal Serial Bus
WEF	Fórum Econômico Mundial

SUMÁRIO

1 INTRODUÇÃO

A aviação civil representa um dos pilares fundamentais da economia brasileira, sendo responsável por uma parcela significativa do transporte de passageiros e mercadorias. Diante dessa relevância, a presente monografia tem por objetivo analisar as normas e estruturas regulatórias que visam à proteção desse setor frente a uma ameaça contemporânea: os ataques cibernéticos. O problema de pesquisa que norteia este estudo busca responder até que ponto as normas e estruturas regulatórias brasileiras, como o direito aeronáutico e o direito digital, são de fato eficazes para mitigar e enfrentar as ameaças cibernéticas que afetam a aviação civil e as infraestruturas aeroportuárias no Brasil? Além disso, questiona-se como o Estado pode atuar na criação e implementação de políticas mais eficazes de prevenção cibernética para o setor aéreo brasileiro.

O objetivo geral consiste em abordar as definições, primórdios e aspectos históricos que moldaram a aviação, além das características do direito aeronáutico e a evolução da legislação aeronáutica brasileira. Não obstante, será analisada o conceito de cibersegurança e sua aplicação na aviação civil, conforme as diretrizes da ANAC em 2023. Para isso, realizar-se-á uma análise das principais legislações e regulamentações vigentes no país.

O objetivo específico é examinar as legislações vigentes no Brasil que abordam o direito digital, aeronáutico e cibernético. Para tanto, pretende-se: (i) estudar a aplicabilidade e a eficácia das legislações, tais como a Lei Federal nº 7.565/1986 (Código Brasileiro de Aeronáutica), a Lei Federal nº 11.182/2005 (Cria a Agência Nacional de Aviação Civil – ANAC, e dá outras providências), a Lei Federal nº 12.965/2014 (Marco Civil da Internet), a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais), Decreto nº 11.856/2023 (Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança), o Decreto nº 11.491/2023 (Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001) e as diretrizes da ANAC; (ii) apresentar estudos de casos concretos de ataques cibernéticos que afetaram companhias aéreas e infraestruturas aeroportuárias, como o vazamento de dados de passageiros da Latam Airlines em 2021 e o Apagão Cibernético ocorrido em 2024.

A metodologia adotada será de caráter sistêmico, visando analisar as interações entre a cibersegurança, o direito digital e a segurança da aviação no Brasil.

Justifica-se o estudo ora apresentado pela possível ausência de regulamentação específica e consolidada que trate de forma adequada os riscos cibernéticos na aviação civil brasileira. Com o Brasil ocupando uma posição de destaque no cenário aeronáutico mundial, torna-se imperativo estudar o impacto de tais vulnerabilidades e propor medidas que possam mitigar os riscos, garantindo, assim, a segurança e a integridade tanto das infraestruturas aeroportuárias quanto dos dados sensíveis de passageiros e clientes.

Ainda, o presente estudo visa proporcionar uma reflexão sobre o papel do Estado na criação e implementação de políticas de prevenção eficaz, que sejam capazes de acompanhar a velocidade dos avanços tecnológicos e garantir a proteção das infraestruturas críticas. A escolha do tema reflete, portanto, a curiosidade genuína de uma acadêmica do curso de Direito, apaixonada pela aviação e inquieta com as possíveis consequências catastróficas na aviação que podem advir da possível ausência de regulamentação adequada. Assim, busca-se contribuir para a prevenção de tais riscos em um campo que, embora recente, moderno e ainda pouco dialogado, destaca a importância de discutir a segurança da aviação civil sob a ótica da cibersegurança, trazendo à tona um debate fundamental e atual para os operadores do Direito.

Não obstante, embora o tema seja contemporâneo no ordenamento jurídico brasileiro, Danilo Donela[2], jurista brasileiro e especialista em privacidade e proteção de dados, ressalta a necessidade de que o ordenamento jurídico estabeleça critérios proporcionais para a tutela da pessoa. Ele observa que essa área está intimamente ligada ao desenvolvimento da tecnologia e, muitas vezes, as tentativas de regulação são superadas por essa dinâmica. Donela, também enfatiza que o tratamento de dados pessoais envolve implicações complexas, que não podem ser abordadas apenas por meio do controle individual sobre os dados. Tendo em vista que a intensidade do fluxo de dados pessoais e a dificuldade em identificar quem os detém e como são utilizados tornam essa tarefa bastante desafiadora.

---

[2] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Revista dos Tribunais, 2021. p. 6.

À medida em que estudos conduzidos pela ANAC[3] mostram uma tendência global de aeroportos adotando arquiteturas centralizadas para otimizar o compartilhamento de informações e serviços, essas evoluções tecnológicas, enquanto aprimoram a eficiência no setor aéreo, infelizmente, também expõem os sistemas a potenciais vulnerabilidades que podem vir a serem exploradas por *crackers*[4], sendo possível trazer à baila o incidente que ocorreu em 2021, onde os clientes do Latam Pass têm dados vazados após ataque de *cracker* em um servidor na cidade de Atlanta, nos Estados Unidos da América (EUA), e afetou empresas que utilizam o sistema de PSS[5].

Ademais, em julho de 2024, um apagão cibernético global causou grandes transtornos no setor aéreo, resultando no cancelamento de centenas de voos. O ataque afetou não apenas sistemas de gestão de companhias aéreas, mas também comprometeu serviços bancários e de emergência em diversos países[6]. Ainda, cumpre salientar que com o mesmo estudo realizado pela ANAC, supracitado, dispõe de informações fornecidas pelo Diretor de Estratégia e Gerenciamento de Segurança da Agência Europeia de Segurança da Aviação (EASA) e revelam que, em média, ocorrem aproximadamente 1.000 ciberataques por mês a aeroportos em escala global[7].

Portanto, o presente estudo se justifica pela necessidade de aprofundar o conhecimento sobre as ameaças cibernéticas no setor da aviação e as medidas regulatórias aplicáveis. A pesquisa contemplará a revisão de literatura acadêmica, incluindo livros e publicações especializadas, para entender a evolução do direito aeronáutico e da cibersegurança. Casos concretos de ataques cibernéticos que

---

[3] ANAC. **Manual de Conscientização de Segurança Cibernética da Aviação Civil**. Brasília: Agência Nacional de Aviação Civil, [2023]. Disponível em: https://www.anac.gov.br/manual-conscientizacao. Acesso em: 08 nov. 2024.

[4] O termo "hacker" refere-se a um indivíduo que possui habilidades avançadas em programação e sistemas computacionais, explorando essas habilidades para fins éticos, como melhorar a segurança de sistemas (hacker ético) ou desenvolver novos recursos. Ao passo que, "cracker" se refere a um indivíduo que quebra sistemas de segurança, acessando redes ou informações de maneira ilegal e geralmente com a intenção de causar danos ou roubar dados. DIFERENÇA entre hacker e cracker. *In*: HUGE networks. [*S. l.*], [2024?]. Disponível em: https://www.huge-networks.com/blog/ciberseguranca/diferenca-hacker-e-cracker. Acesso em: 08 nov. 2024.

[5] LAURANCE, Felipe. Clientes do Latam Pass têm dados vazados após ataque de hacker. *In*: CNN Brasil. São Paulo, 25 ago. 2022. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/clientes-do-latam-pass-tem-dados-vazados-apos-ataque-de-hacker/. Acesso em: 08 nov. 2024.

[6] APAGÃO cibernético afeta setor aéreo e voos são cancelados. *In*: CNN Brasil. São Paulo, 27 jul. 2024. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/apagao-cibernetico-afeta-setor-aereo-e-voos-sao-cancelados/. Acesso em: 08 nov. 2024.

[7] ANAC, *op. cit*.

impactaram companhias aéreas e infraestruturas aeroportuárias também serão estudados com intuito de compreender com exatidão os tipos de ataques cibernéticos que ocorrem no mundo da aviação. Desta forma, este estudo, especificamente focado no vazamento de dados e ataques cibernéticos no setor aéreo, fora escolhido por tratar de um dos pilares essenciais da economia nacional. Ademais, cumpre mencionar que pouco se debate sobre os ataques cibernéticos nesse contexto, seus riscos, consequências, danos e responsabilidades. Assim, espera-se que os resultados desta monografia sirvam de fomento para futuras discussões e aprimoramentos no âmbito das legislações que norteiam a cibersegurança no setor da aviação civil brasileira, incentivando o poder público a destinar investimentos em educação digital. Considerando que a temática ainda é pouco explorada tanto na seara jurídica quanto na sociedade, observa-se um desconhecimento generalizado acerca dos riscos inerentes à ataques cibernéticos na aviação. Assim, almeja-se a reflexão e provocação para que se avance em mais estudos sobre a cibersegurança na aviação.

2 COMPREENSÃO E PRIMÓRDIOS DA AVIAÇÃO E DO DIREITO AERONÁUTICO

Embora a aviação seja o mais recente dos modais de transporte, o desejo de voar acompanha a humanidade desde os tempos pré-históricos. Observando os pássaros, os homens das cavernas retratavam esse anseio por meio de pinturas rupestres[8].

Para Gusmão[9], a maioria das pessoas acreditavam que fosse impossível voar e que era um dom muito além da capacidade humana. No entanto, ainda assim o desejo persistiu com o passar dos séculos. Há registros históricos de que há milhares de anos os chineses haviam confeccionado um balão, um artefato confeccionado em papel de seda e propulsado com ar quente e, a partir disso, foi possível concluir que, através de registros que estão presentes em toda civilização antiga, tais como sumérios, os maias, os incas e os astecas, bem como nas mitologias egípcias, nórdica, grega e romana que a ideia de voar vem dos tempos antigos[10].

Ao passo que, inúmeros pioneiros contribuíram de forma decisiva para o desenvolvimento da aviação, seja por meio de experimentos aeronáuticos, seja por realizarem feitos extraordinários, como Leonardo Da Vinci, os irmãos Wilbur e Orville Wright e Alberto Santos Dumont.

Com base no artigo de Silva e Santos[11], Leonardo Da Vinci, no século XV, já realizava estudos e projetos de máquinas voadoras, sendo um dos pioneiros a imaginar a possibilidade de voo. No entanto, foi no início do século XX que esse sonho começou a se concretizar, com as iniciativas dos irmãos Wilbur e Orville Wright, nos Estados Unidos, que são reconhecidos por realizarem o primeiro voo controlado com uma aeronave motorizada. Não obstante, Gusmão[12] destaca que em 1906, Santos Dumont realizou o primeiro voo com uma aeronave motorizada mais pesada que o ar, o "14-bis", percorrendo 60 metros em sete segundos. Esse feito

---

[8] GUSMÃO, Roberto José Faria de. História da aviação. *In*: LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (org.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 19.

[9] *Ibid*., p. 19.

[10] *Ibid*., p. 19.

[11] SILVA, Odair Vieira da; SANTOS, Rosiane Cristina dos. Trajetória histórica da aviação mundial. **Revista Científica Eletrônica de Turismo**, Garça, v. 6, n. 1, jun. 2009. Disponível em: https://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/WydybjUDpYtjIL4_2013-5-23-10-51-57.pdf. Acesso em: 08 nov. 2024.

[12] GUSMÃO, *op. cit*., p. 20.

fora testemunhado por uma comissão oficial e marcou o início de uma era de avanços aeronáuticos, principalmente no desenvolvimento de motores mais potentes e confiáveis, que evoluíram rapidamente no período que antecedeu a Primeira Guerra Mundial.

Em 21 de julho de 1914 teve início a Primeira Guerra Mundial (1914-1918), conflito em que o avião fez sua estreia como uma inovadora e poderosa ferramenta de combate. Em um cenário em que predominava a chamada “guerra de trincheiras”, onde o avanço das tropas durava dias, semanas e, em alguns casos, meses, a aviação militar fez toda a diferença nos campos de batalha, seja combatendo as tropas inimigas entrincheiradas, seja nos combates aéreos com as forças adversárias buscando a supremacia aérea. Ao passo que, o avião consolidou sua posição como uma força essencial nas forças armadas de diversos países, primeiro integrando os exércitos e, posteriormente, com a criação de forças aéreas independentes, que surgiram como conhecemos atualmente. Inicialmente, a aviação militar era apenas uma das armas dos exércitos, assim como a infantaria, cavalaria, artilharia, engenharia e intendência[13].

À medida em que a trajetória histórica da aviação ganhou destaque a partir da Primeira Guerra Mundial, o setor aéreo passou a desempenhar um papel fundamental no desenvolvimento econômico global, sendo hoje uma das principais alavancas da economia brasileira. Conforme Silva e Santos[14], o transporte aéreo é um dos elementos mais dinâmicos para o turismo e a economia mundial, proporcionando uma conectividade global que tem sido importante para o crescimento do setor de turismo no Brasil, uma vez que facilita o deslocamento de turistas e estimula o desenvolvimento de novos destinos. No entanto, com esse crescimento exponencial, entende-se que surge a necessidade de enfrentar novos desafios, como a proteção dos dados dos passageiros e a segurança cibernética das infraestruturas aeroportuárias e das companhias aéreas. Por este motivo, no próximo capítulo será abordado brevemente a evolução da aviação e o Impacto das Convenções Internacionais no Desenvolvimento da Aviação no Brasil.

---

[13] GUSMÃO, Roberto José Faria de. História da aviação. *In*: LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 21-22.

[14] SILVA, Odair Vieira da; SANTOS, Rosiane Cristina dos. Trajetória histórica da aviação mundial. **Revista Científica Eletrônica de Turismo**, Garça, v. 6, n. 1, jun. 2009. Disponível em: https://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/WydybjUDpYtjIL4_2013-5-23-10-51-57.pdf. Acesso em: 08 nov. 2024.

2.1 O impacto das Convenções Internacionais na Aviação

As Convenções Internacionais foram importantes para normatizar, padronizar e regularizar a atividades aéreas, fornecendo as bases para a formação do Direito Aeronáutico tanto no Brasil quanto em diversos outros países. Convém esclarecer que os termos “Convenção” e “Tratado” são sinônimos, embora, historicamente, a Convenção fosse usada para acordos econômicos, comerciais ou administrativos, enquanto o Tratado indicava acordos de caráter político[15]. Com o tempo, essa distinção deixou de ser aplicada. Não obstante, o longo dos anos, ocorreram várias convenções importantes, como a de Paris (1919), Havana (1928), Varsóvia (1929), Roma (1933), Chicago (1944) e Tóquio (1963)[16]. Na presente monografia, apenas as Convenções de Paris, Varsóvia e Chicago serão abordadas, considerando o contexto histórico das Guerras Mundiais e destacando o indispensável para a compreensão do desenvolvimento do Direito Aeronáutico.

A Convenção de Paris, realizada em 1919, foi a primeira com o objetivo de criar normas globais para as atividades aéreas. Gusmão,[17] menciona que nesse evento, foi criada a Comissão Internacional de Navegação Aérea (CINA), visando ao desenvolvimento seguro da aviação civil internacional, com o entendimento de que seu crescimento poderia promover a amizade entre as nações, mas também poderia representar um perigo para a segurança geral se mal utilizada. Os países signatários concordaram que a aviação civil deveria se desenvolver de forma segura e sistemática, garantindo igualdade de oportunidades no transporte aéreo internacional. Ao passo que, a convenção trouxe princípios importantes, como a nacionalidade das aeronaves, certificados de aptidão, normas para navegação sobre território estrangeiro e a criação de uma comissão internacional para supervisionar a aviação. Essa regulamentação foi baseada em leis marítimas, adotando procedimentos semelhantes aos da marinha mercante.

Não obstante, entre a Primeira e a Segunda Guerras Mundiais, a aviação teve um desenvolvimento expressivo, com a criação de aeronaves maiores e mais eficientes, muitas das quais originadas do excedente da Primeira Guerra. Diversas

---

[15] GUSMÃO, Roberto José Faria de. História da aviação. *In*: LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 21.

[16] *Ibid*., p. 21.

[17] *Ibid*., p. 22-23.

empresas aéreas surgiram nesse período, incluindo no Brasil, com a fundação de companhias como a Cruzeiro do Sul (1927), Varig (1927), Panair (1930) e Vasp (1933). Essas empresas cresceram e se consolidaram, muitas vezes se fundindo com outras para formar grandes companhias aéreas durante o século XX e início do XXI[18].

Outro marco importante foi a Convenção de Varsóvia, realizada em 1929, tinha como principal objetivo estabelecer normas e procedimentos claros sobre os direitos e deveres dos passageiros do transporte aéreo, além de regulamentar o transporte de bagagens e cargas. Foi a partir dessa convenção que o bilhete de passagem aérea se consolidou como o contrato entre a companhia aérea e o passageiro, detalhando as responsabilidades de ambas as partes. Além disso, foi criado o conhecimento de bagagem, que vinculava a bagagem despachada ao seu proprietário, e estabelecia a responsabilidade civil da companhia aérea pelo transporte seguro dos pertences[19].

Dessa forma, a Convenção de Varsóvia estabeleceu as bases e garantias jurídicas para os passageiros do transporte aéreo, assegurando-lhes a proteção jurídica necessária para realizar viagens aéreas, tanto no que diz respeito à sua integridade pessoal quanto aos seus pertences. Em que pese, Gusmão também mencione:

> Tal Convenção, ainda que não contemplasse diversos outros aspectos técnicos e de padronização da atividade aérea, representou um grande salto para a indústria do transporte aéreo em todo o mundo. Não foi sem razão que a maioria das empresas de aviação comercial surgiram em tal período, algumas das quais continuam voando até os dias atuais[20].

Por conseguinte, durante a Segunda Guerra Mundial, a aviação desempenhou um papel importantíssimo. Em 1941, o Brasil, sob o governo de Getúlio Vargas, criou o Ministério da Aeronáutica e a Força Aérea Brasileira (FAB), com Joaquim Pedro Salgado Filho como ministro. A aviação, já consolidada em muitos países, foi largamente utilizada durante o conflito, tanto pelos Aliados quanto pelos países do Eixo. O Brasil declarou guerra à Alemanha e seus aliados em 1942, e em 1944 enviou tropas e aviadores para lutar na Itália. Ao passo que, o 1º Grupo

---

[18] GUSMÃO, Roberto José Faria de. História da aviação. *In*: LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 23.

[19] *Ibid*., p. 23-24.

[20] *Ibid*., p. 24.

de Aviação de Caça da FAB, treinado pela Força Aérea dos Estados Unidos, operou com grande sucesso nas missões de combate, integrando-se às operações aliadas[21].

À vista disso, a Convenção de Chicago, realizada em 1944, antecipando o fim da Segunda Guerra Mundial, tinha como objetivo organizar a aviação civil global, dado o enorme excedente de aeronaves e equipamentos gerados pela guerra. Durante essa convenção, foi criada a Organização de Aviação Civil Internacional (OACI), que substituiu a Comissão Internacional de Navegação Aérea (CINA), com a missão de padronizar normas que tornassem a aviação mais segura e eficiente[22]. Gusmão dispõe que:

> Esta convenção foi promulgada no Brasil pelo decreto 21.713, de 27/08/1946. Pelo artigo 37 da referida convenção, os estados contratantes se obrigaram a colaborar a fim de atingir a maior uniformidade possível em seus regulamentos, normas e procedimentos, sempre que isto trouxesse vantagens para a atividade aérea[23].

Por fim, após a Segunda Guerra Mundial, o mundo passou por um novo reordenamento geopolítico, com a criação da Organização das Nações Unidas (ONU) em 1945, substituindo a Liga das Nações. A OACI foi integrada à ONU e passou a ter um papel central na padronização das normas e procedimentos da aviação civil mundial. O Brasil, como signatário da Convenção de Chicago e dos anexos estabelecidos, continuou a ser um participante ativo nas discussões e assembleias da OACI, firmando-se como um dos países com uma aviação desenvolvida, possuindo uma grande frota de aeronaves, tripulantes treinados e uma infraestrutura aeroportuária moderna[24]. Ao cabo, no próximo capítulo, abordar-se-á a caracterização e os aspectos do Direito Aeronáutico, destacando sua autonomia como um ramo jurídico especializado, imprescindível para a regulação eficaz da aviação civil.

---

21 GUSMÃO, Roberto José Faria de. História da aviação. *In*: LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 24-25.

22 *Ibid*., p. 25.

23 *Ibid*., p. 24-25.

24 *Ibid*., p 25-26.

2.2 Caracterização e aspectos do Direito Aeronáutico e sua autonomia

Nas palavras de Leite e Silva[25], a definição de um conceito no Direito é sempre uma matéria “espinhosa”, pois envolve uma operação lógica que demanda tanto a delimitação rigorosa do que está sendo definido quanto a diferenciação em relação a outros conceitos próximos, revelando assim sua essência. No caso do Direito Aeronáutico, a definição não se restringe apenas à descrição de suas características, mas também à determinação dos limites de sua abrangência, o que implica analisar seu objeto e sua natureza jurídica.

Ao passo que, como já exposto no capítulo anterior, nos primórdios do Direito Aeronáutico, notadamente quando da Convenção de Paris de 1919, utilizou-se como referência a legislação marítima vigente, a fim de estabelecer princípios gerais da aviação e normas de navegação aérea. Como o Direito Marítimo estava fortemente atrelado ao Direito Comercial, muitos acreditavam, à época da elaboração do Tratado de Versalhes, que o Direito Aeronáutico fosse um sub-ramo do Direito Comercial. No entanto, conforme a aviação evoluía, com o surgimento de novos problemas e particularidades da nova tecnologia, percebeu-se que esse ramo jurídico demandava estudo e regulamentação específicos, com capacidade para abarcar a crescente atividade econômica e seus reflexos sociais, que tanto contribuíam para o desenvolvimento humano[26].

Assim, surgiu um novo ramo da ciência jurídica, em pleno desenvolvimento, cuja autonomia ainda está em construção. Quanto ao nome a ser atribuído a este ramo do Direito, várias possibilidades foram cogitadas: Direito Espacial, Direito Astronáutico, Direito Aéreo, Direito Aviatório ou Direito de Aviação, entre outras. Todavia, no Brasil, prevaleceu a denominação Direito Aeronáutico, como consagrado no artigo 1º do Código Brasileiro de Aeronáutica (CBA), referindo-se especificamente ao transporte aéreo dentro da atmosfera terrestre, às regras de navegação e aos meios utilizados para esse fim[27]. “Art. 1° O Direito Aeronáutico é

---

[25] LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 33.

[26] *Ibid*., p. 33.

[27] *Ibid*., p. 33.

regulado pelos Tratados, Convenções e Atos Internacionais de que o Brasil seja parte, por este Código e pela legislação complementar”[28].

Ainda sobre o nome adotado, Ricardo Alvarenga[29] leciona que o Direito Aeronáutico se refere ao conjunto de injunções jurídicas concernentes à navegação aérea ou aeroespacial. Essa expressão, segundo ele, indica com maior precisão o verdadeiro conteúdo da matéria, uma vez que se trata do direito relacionado à navegação aérea, apesar da forte tradição doutrinária francesa usar a expressão “*droit aérien*”, na tradução “direito aéreo”.

Ao passo que, Leite e Silva[30], reforça em esclarecer que o Direito Aeronáutico não se restringe ao transporte aéreo, aeronaves e regras de navegação. Sendo o objeto do Direito Aeronáutico incluir: regras nacionais e internacionais de transporte, tráfego e navegação aéreos; serviços aéreos; proteção e segurança de voo; registro de aeronaves; investigação e prevenção de acidentes aeronáuticos; indústria aeronáutica; infraestrutura aeroportuária; relações de trabalho e treinamento dos operadores (aeronautas e aeroviários); tripulação; aviação experimental e aerodesportiva; responsabilidade civil do transportador aéreo, entre outros.

Por conseguinte, Ronaldo Poletti[31], dispõe que o Direito Aeronáutico tem caráter eminentemente público, uma vez que protege interesses e bens coletivos e regula relações jurídicas de subordinação, baseadas na ideia de justiça distributiva. Assim, para ele, esse caráter normativo não poderia ser diferente, dado que o Direito Aeronáutico busca subordinar os interesses individuais aos valores coletivos, a fim de garantir o uso seguro da técnica de navegação aérea em benefício da humanidade, sendo o objetivo promover a circulação rápida de pessoas, bens e serviços de maneira segura.

Nesse contexto, o Direito Aeronáutico pode ser conceituado como um ramo do Direito Internacional Público, responsável pela disciplina jurídica das atividades

---

[28] BRASIL. **Lei nº 7.565, de 19 de dezembro de 1986**. Dispõe sobre o Código Brasileiro de Aeronáutica. Brasília, DF: Presidência da República, 1986. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7565compilado.htm. Acesso em: 08 nov. 2024.

[29] ALVARENGA, Ricardo. **Direito aeronáutico**: dos contratos e garantias sobre aeronaves. Belo Horizonte: Del Rey, 1992. p. 15.

[30] LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 34.

[31] POLETTI, Ronaldo. A questão da autonomia do direito aeronáutico. **Revista de Informação Legislativa**, v. 31, n. 123, p. 103-112, jul./set. 1994. p. 112. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/176260/000491490.pdf?sequence=1&isAllowed=y. Acesso em: 08 nov. 2024.

relacionadas ao transporte aéreo, às aeronaves e às regras de navegação aérea, além de outras atividades-meio associadas. Conquanto, Alvarenga confirma esse conceito amplo:

> Entende-se como direito aeronáutico o conjunto de normas de direito público e privado que regulam a navegação aérea e especialmente o movimento de aviões e outros aparelhos que circulam no ar, nas suas relações com coisas e pessoas. Acrescente-se que o direito aeronáutico estuda os fatores essenciais à navegação aérea, abrangendo o ambiente em que ela se desenvolve (atmosfera e superfície); o meio com que atua (aeronave) e as relações jurídicas públicas e privadas, nacionais e internacionais que enseja. Compreende, pois, o conjunto de normas referentes ao estatuto da aeronave e da sua tribulação organização da infraestrutura terrestre que é indispensável à realização do transporte e, finalmente, a disciplina dos direitos e obrigações que deste emanam. A doutrina é pacífica no sentido de definir o direito aeronáutico como regulamentando todas as relações jurídicas, oriundas da navegação aérea, ou seja, decorrentes da circulação e da utilização das aeronaves, incluindo a sua infraestrutura e as pessoas e coisas suscetíveis de serem transportadas[32].

Portanto, o Direito Aeronáutico caracteriza-se pela interdisciplinaridade, uma vez que a atividade aérea é de grande relevância global, fomentando outras atividades econômicas, como a construção de infraestrutura e o apoio ao desenvolvimento de outras atividades econômicas[33]. Alvarenga, inclusive reforça que o Direito Aeronáutico*, latu sensu*, abrange não apenas as normas comerciais, mas também normas de outros ramos do Direito, como o Direito Trabalhista, Tributário e Administrativo[34].

Definido o conceito, se faz necessário abordar a questão da autonomia do Direito Aeronáutico. Para Poletti[35], "[...] a autonomia de uma disciplina jurídica pode ser visualizada em três níveis: a política legislativa; a de fins acadêmicos e didáticos; e a científica". Ele defende que, no nível da política legislativa, basta observar a previsão constitucional de leis especiais para disciplinar a matéria, bem como a existência de normas específicas, independentemente de codificação formal.

---

[32] ALVARENGA, Ricardo. **Direito aeronáutico**: dos contratos e garantias sobre aeronaves. Belo Horizonte: Del Rey, 1992. p. 17.

[33] LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 35.

[34] *Ibid*., p. 17.

[35] POLETTI, Ronaldo. A questão da autonomia do direito aeronáutico. **Revista de Informação Legislativa**, v. 31, n. 123, p. 103-112, jul./set. 1994. p. 105. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/176260/000491490.pdf?sequence=1&isAllowed=y. Acesso em: 08 nov. 2024.

No caso do Direito Aeronáutico, a reunião de todas as normas importantes, de forma sistematizada e lógica, em um só diploma consolidado, enfrentaria o desafio de integrar normas de origem internacional ainda não incorporadas ao ordenamento jurídico brasileiro. Para Leite e Silva, esse é um obstáculo considerável, mas não intransponível. Embora desejável, essa sistematização enfrenta dificuldades evidentes[36]. Entende-se que esse mesmo desafio é observado no contexto da falta de normas específicas para ataques cibernéticos na aviação. Assim como a integração de todas as normas internacionais no Direito Aeronáutico apresenta dificuldades, há também obstáculos para tratar os ataques cibernéticos de maneira clara no Brasil.

O autor, inclusive, reflete que é fato que o Código Brasileiro de Aeronáutica em vigor, como também o anteprojeto, contém regras lógicas, específicas e sistemáticas sobre estrutura aeronáutica, aeronaves e navegação aérea no Brasil, sem, todavia, esgotarem consideravelmente a matéria objeto do Direito Aeronáutico[37].

Para Leite e Silva, pode-se considerar que, quanto à política legislativa, existem leis especiais e próprias para disciplinar a matéria, independentemente do que se deve chamar de codificação. Trata-se de um conjunto de normas especialmente criadas, com a pretensão de resolução de problemas jurídicos que não encontram solução em outros ramos do Direito, haja vista a peculiaridade da navegação aérea, da aviação civil e das atividades afins[38].

Quanto à questão didática ou acadêmica, cogita Poletti que “[...] valem os critérios de conveniência, interesse e oportunidade”[39] ao se considerar pela abertura de cursos e disciplinas específicas sobre o tema. Para o autor, há uma crescente demanda nas universidades pelo ensino do Direito Aeronáutico, ainda que como disciplina meramente optativa da graduação, o que aponta para a franca construção de sua autonomia acadêmica. Outrossim, segundo ele, há um aumento significativo

---

[36] LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 34. p. 36.

[37] *Ibid*., p. 36.

[38] *Ibid*., p. 36.

[39] POLETTI, Ronaldo. A questão da autonomia do direito aeronáutico. **Revista de Informação Legislativa**, v. 31, n. 123, p. 103-112, jul./set. 1994. p. 106. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/176260/000491490.pdf?sequence=1&isAllowed=y. Acesso em: 08 nov. 2024.

nos cursos de pós-graduação em Direito Aeronáutico em todo o país, que evidentemente estimulam a construção doutrinária[40].

Para Poletti[41], a questão mais importante para a autonomia do Direito Aeronáutico está em sua autonomia científica, que abrange o conteúdo da disciplina, sua linguagem e seus métodos próprios. O Direito Aeronáutico tem um objeto específico, que pode ser ampliado para incluir as diversas atividades relacionadas à aviação civil. Sua linguagem e seus métodos próprios decorrem da particularidade dos fatos jurídicos regulados e da especialidade dos sujeitos e interesses envolvidos nas relações jurídicas que esse ramo do Direito protege. Para ele, a formulação de princípios típicos é essencial para uma disciplina jurídica, e isso ocorre com base na aplicação e desenvolvimento doutrinário da matéria.

Quanto aos princípios do Direito Aeronáutico, Poletti[42] menciona que eles se constroem em torno do interesse humano, das relações entre os povos, da segurança das pessoas e do uso pacífico dos meios de transporte aéreo. Ele cita ainda a proteção ao voo, a busca, a assistência e o salvamento, além da necessidade de registros aeronáuticos específicos. Embora a construção dos princípios do Direito Aeronáutico ainda esteja em desenvolvimento, pode-se apontar a austeridade na investigação como método de prevenção de acidentes aéreos, a responsabilidade objetiva do transportador e a imprescindibilidade dos serviços de aviação civil como princípios em formação. Contudo, “[...] fato é que a autonomia do Direito Aeronáutico, se ainda não é consenso, está em franca construção, sendo necessário o amadurecimento doutrinário por uma dogmática histórica”[43]. Assim, no próximo capítulo tratará das fontes do Direito Aeronáutico e de sua interdisciplinariedade, destacando-se a importância desse estudo para compreender a base normativa que sustenta este ramo jurídico e como ele se relaciona com outras áreas do Direito.

---

40 LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 37.

41 POLETTI, Ronaldo. A questão da autonomia do direito aeronáutico. **Revista de Informação Legislativa**, v. 31, n. 123, p. 103-112, jul./set. 1994. p. 106. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/176260/000491490.pdf?sequence=1&isAllowed=y. Acesso em: 08 nov. 2024.

42 *Ibid.*, p 111.

43 LEITE E SILVA, *op. cit*., p. 38.

2.3 Fontes e a interdisciplinariedade do Direito Aeronáutico

Para Gusmão, o conceito de "fontes do direito" é uma metáfora construída pela doutrina que faz alusão à origem ou nascente de algo, referindo-se àquilo de onde o direito surge ou se justifica. Ele explica que as fontes jurídicas podem ser vistas como a origem primária do direito ou como o fundamento de validade de uma ordem jurídica, conforme uma perspectiva kelseniana[44]. Ao passo que, Maria Helena Diniz, citando Nelson de Souza Sampaio, reforça que as fontes jurídicas são os fatores reais que condicionam o surgimento das normas, tratando-se, assim, das fontes materiais do direito. “[...] a origem primária do direito, confundindo-se com o problema da gênese do direito. Trata-se da fonte real ou material do direito, ou seja, dos fatores reais que condicionam o aparecimento de norma jurídica”[45].

Por conseguinte, no que diz respeito ao Direito Aeronáutico, Leite e Silva[46] esclarece que as fontes são divididas entre diretas e indiretas. As fontes diretas, também chamadas de formais ou primárias, são aquelas que originam a norma jurídica pura, enquanto as fontes indiretas, ou materiais, servem para interpretar e viabilizar a aplicação dessas normas, auxiliando no entendimento dos casos concretos.

Conforme a Lei Federal nº 7.565/1986, as fontes diretas do Direito Aeronáutico incluem: a) Tratados e Convenções internacionais incorporados pelo Brasil, b) o próprio Código Brasileiro de Aeronáutica, e c) a legislação complementar. Ao passo que, conforme mencionado anteriormente, no capítulo 2.2, o artigo 1º do CBA dispõe que o Direito Aeronáutico é regido por Tratados, Convenções e Atos Internacionais dos quais o Brasil seja parte, além do código e da legislação complementar.

Leite e Silva, observa que o artigo 1º do CBA determina que os documentos internacionais multilaterais, como as Convenções, se aplicam ao Brasil desde que o país seja parte no processo de elaboração. Mesmo não participando originalmente, o Brasil pode aderir posteriormente a essas convenções, sendo essa adesão uma

---

[44] LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 38.

[45] DINIZ, Maria Helena. **Compêndio de Introdução à Ciência do Direito**. São Paulo: Saraiva, 1993. 5. p. 255 *apud* SAMPAIO, Nelson de Souza. Fontes do Direito – II. *In*: ENCICLOPÉDIA Saraiva do Direito. São Paulo: Saraiva, falta ano. v. 38. p. 51; 53.

[46] LEITE E SILVA, *op. cit*., p. 38.

competência exclusiva do Presidente da República, conforme o artigo 84, inciso VIII, da Constituição Federal de 1988[47]. Contudo, para que o tratado tenha vigência no território nacional, é necessário o referendo do Congresso Nacional, nos termos do artigo 49, inciso I, da mesma constituição, por meio de Decreto Legislativo.

> Art. 49. É da competência exclusiva do Congresso Nacional:
> I - resolver definitivamente sobre tratados, acordos ou atos internacionais que acarretem encargos ou compromissos gravosos ao patrimônio nacional; [...]
> Art. 84. Compete privativamente ao Presidente da República
> [...]
> VIII - celebrar tratados, convenções e atos internacionais, sujeitos a referendo do Congresso Nacional; [...]

Gusmão adotou a classificação de Eduardo Sócrates Castanheira Sarmento, que dispõe que os tratados internacionais no Direito Aeronáutico podem ser divididos em direito geral e de caráter especial. No direito geral, incluem-se as convenções de Paris (1919), Madri (1926), Havana (1928) e Chicago (1944). Já os tratados de caráter especial são organizados em três grupos: sobre aeronaves (Bruxelas, 1938; Genebra, 1948), sobre responsabilidade civil (Varsóvia, 1929; Haia, 1955; Montreal, 1966 e 1975; Guatemala, 1971; Guadalajara, 1961; Roma, 1933 e 1952), e sobre direito penal (Tóquio, 1963; Haia, 1970; Montreal, 1971). A Convenção de Montreal de 1999 é destacada por Sarmento como uma reestruturação sistemática do transporte aéreo internacional de pessoas, bagagens e cargas, atualizando as regras estabelecidas pelas Convenções de Varsóvia e suas sucessoras[48], como analisado no capítulo 2.1.

Não obstante, às fontes indiretas, Leite e Silva menciona os costumes, a jurisprudência e a doutrina[49]. Ao passo que, os costumes, conforme expostos por Machado Paupério, citando Ferrara, dispõe:

> O costume, via de regra, tem sempre origem convencional e nunca litigiosa. Por isso, no direito comercial e no direito internacional, por exemplo, tem larga aplicação.
> Para Ferrara, o costume não é mais que um ordenamento de fatos que termina por se impor psicologicamente aos indivíduos. Consiste, assim,

---

47 BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 nov. 2024.

48 LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 39.

49 *Ibid*., p. 40.

> precipuamente, na prática constante e repetida de uma forma de comportamento pelos componentes da comunidade[50].

Neste diapasão, Norberto Bobbio considera o costume uma fonte essencial e complexa no ordenamento jurídico, especialmente em sistemas onde a lei é a fonte direta e superior, como nos ordenamentos estatais modernos. Para ele, o costume é uma forma de “fonte reconhecida”, sendo incorporado pelo legislador para preencher lacunas nas matérias não cobertas pela lei. Isso ocorre, por exemplo, na *consuetudo praeter legem*, quando o legislador aceita o costume como uma norma abundante que complementa o ordenamento, trazendo consigo um conjunto de normas de outras épocas ou de outros sistemas[51].

Segundo Bobbio, o costume representa uma fonte singular no ordenamento jurídico, pois, diferentemente das normas estabelecidas diretamente pelo legislador, ele se desenvolve "naturalmente" a partir do comportamento uniforme dos cidadãos. Embora o costume possa ser considerado uma "delegação" onde o ordenamento jurídico “[...] autoriza os cidadãos a produzir normas jurídicas através do seu comportamento uniforme”, ele distingue entre recepção e delegação: enquanto na recepção o ordenamento incorpora algo já existente e pronto, na delegação "[...] determina que seja feito, ordenando uma produção futura”. Dessa forma, para Bobbio, o costume “[...] assemelha-se mais a um produto natural”, enquanto regulamentos, decretos e sentenças, produtos do ato deliberado de magistrado, configuram "um produto artificial"[52].

Ao passo que, Leite e Silva[53], entende que não é difícil imaginar que, no Direito Aeronáutico, os costumes possam ser aplicados como regra em procedimentos necessários, especialmente relacionados à navegação aérea, ao transporte de cargas e pessoas, bem como às relações de trabalho e treinamento de aeronautas e aeroviários. Outra fonte indireta importante do Direito Aeronáutico é a jurisprudência, que pode ser entendida como o direito estabelecido por decisões reiteradas do Poder Judiciário. Contudo, o autor ressalta que a jurisprudência só

---

50 PAUPÉRIO, Artur Machado. **Introdução ao estudo do direito**. Rio de Janeiro: Forense, 1988. p. 121.

51 BOBBIO, Norberto. **Teoria geral do direito**. 3. ed. São Paulo: Martins Fontes, 2010. p. 202-203.

52 *Ibid*., p 203.

53 LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 41.

pode ser considerada fonte do direito quando preenche uma lacuna deixada por fontes diretas, ou seja, pela legislação.

Por conseguinte, Leite e Silva[54] aponta que a doutrina também é uma fonte indireta do Direito Aeronáutico, sendo composta pelo "[...] acervo de soluções trazidas pelos trabalhos dos juristas"[55], que se manifestam em livros, artigos, pareceres, monografias, dissertações e teses. A doutrina não só ajusta o direito ao caso concreto, mas também contribui para a sua evolução.

Por fim, alguns estudiosos, como Sarmento, mencionam o Direito Comparado como uma fonte indireta relevante, considerando-o como uma "[...] comparação sistemática das instituições jurídicas de diversos países, por meio da investigação e confrontação de textos legais, crítica das suas instituições, diferenças e analogias"[56]. Conquanto, Leite e Silva considera que o Direito Comparado não é uma fonte técnica do Direito Aeronáutico, mas sim uma ferramenta de interpretação e integração das normas, em suas palavras:

> Com a devida vênia, consideramos não ser esta uma fonte do Direito Aeronáutico na acepção técnica do termo, mas uma forma de hermenêutica e de integração da norma. Sem dúvida, quando tratamos de ramo jurídico cuja principal fonte direta é a normativa internacional incorporada pelo país, o direito comparado passa à condição de grande aliado quando necessário preencher as lacunas legislativas eventualmente verificadas[57].

No próximo capítulo será abordado a definição abrangente da cibersegurança com o objetivo de aprofundar o presente estudo e estabelecer a correlação entre a aviação e o Direito.

---

54 LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (orgs.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018. p. 41.

55 PAUPÉRIO, Artur Machado. **Introdução ao estudo do direito**. Rio de Janeiro: Forense, 1988, p. 159.

56 SARMENTO, Eduardo Sócrates Castanheira. Direito processual aeronáutico. **Revista brasileira de direito aeroespacial**, [*s. l.*], n. 80, 2000. Disponível em: https://sbda.org.br/wp-content/uploads/2018/10/1697.htm. Acesso em: 08 nov. 2024.

57 LEITE E SILVA, *op. cit*., p. 41.

3 DEFINIÇÃO DE CIBERSEGURANÇA E INCIDENTES CIBERNÉTICOS NA AVIAÇÃO: INFRAESTRUTURAS TECNOLÓGICAS, RISCOS PARA VIAJANTES E ATAQUES A COMPANHIAS AÉREAS

No que tange à definição de segurança cibernética, Louise Marie Hurel[58], menciona que não há um consenso global. No entanto, a ISO/IEC 27032:2012[59], por exemplo, foca na preservação da confidencialidade, integridade e disponibilidade de informações no ciberespaço. Já a União Europeia adota uma abordagem mais ampla, definindo a segurança cibernética como as atividades necessárias para proteger redes e sistemas de informação, onde os usuários e outras pessoas são afetadas por ameaças cibernéticas[60].

O Brasil, por sua vez, se refere à segurança cibernética da seguinte forma:

> Ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético capazes de comprometer a disponibilidade, integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis.[61]

---

58 Louise Marie Hurel é Pesquisadora Sênior no Centro Brasileiro de Relações Internacionais (CEBRI) e no Royal United Services Institute (RUSI), com foco em cibersegurança, resposta a incidentes e diplomacia cibernética. Mestre com distinção em Mídia e Comunicações pela London School of Economics and Political Science (LSE), onde está concluindo seu doutorado, Hurel é fundadora da Rede de Pesquisa em Cibersegurança da América Latina (LA/CS Net). Ela também atua em conselhos internacionais, como o Global Forum of Cyber Expertise (GFCE) e a Carnegie Endowment. LOUISE Marie Hurel. *In*: CENTRO brasileiro de relações internacionais. Rio de janeiro, [2024?]. Disponível em: https://www.cebri.org/br/especialista/1180/louise-marie-hurel. Acesso em: 08 nov. 2024.

59 A Norma ISO/IEC 27032:2012 estabelece diretrizes para melhorar a segurança cibernética de uma organização, enfatizando a preservação da confidencialidade, integridade e disponibilidade da informação no ciberespaço. Ela define o ciberespaço como um ambiente complexo, resultado da interação entre pessoas, softwares, serviços da Internet e dispositivos tecnológicos conectados, que não tem uma existência física. AZAMBUJA, Antonio João Gonçalves de; NETO, João Souza. Modelo de maturidade de segurança cibernética para os órgãos da Administração Pública Federal. **Revista do serviço público**, Brasília, DF, v. 71, n. 3, p. 660-712, 2020. Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/3210. Acesso em: 08 nov. 2024.

60 HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, Rio de Janeiro, p. 1-35, abr. 2021. p. 6. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 08 nov. 2024.

61 BRASIL. Agência Nacional de Telecomunicações. **Segurança Cibernética**. Brasília, DF: Agência Nacional de Telecomunicações, [2024?]. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/politicas-publicas#:~:text=Seguran%C3%A7a%20Cibern%C3%A9tica%20%C3%A9%20definida%20como,a%20autenticidade%20dos%20dados%20armazenados%2C. Acesso em: 08 nov. 2024.

Não obstante, para Hurel[62], a definição reitera os chamados "princípios CIA" (*Confidentiality, Integrity and Availability*)[63], amplamente aceitos na comunidade de segurança da informação. Ademais, destaca-se o foco na resiliência dos sistemas e na proteção dos dados “[...] armazenados, processados ou transmitidos”, refletindo a influência direta da Lei Federal nº 13.709/2018 (LGPD). Diferentemente da Colômbia ou da União Europeia, a definição brasileira de segurança cibernética não menciona explicitamente o papel do indivíduo.

Não obstante, cumpre mencionar que o Manual de Conscientização em Segurança Cibernética na Aviação Civil da ANAC[64], dispõe do conceito de cibernética, sendo originado nos anos 1950 e refere-se ao estudo do controle e movimento das máquinas e dos seres vivos. Com o tempo, o termo “ciber” passou a ser usado como um sufixo para conceitos relacionados a computadores e, nos anos 1990, o termo “ciberespaço” surgiu para descrever o espaço virtual por trás das atividades eletrônicas dos dispositivos computacionais. Atualmente, "ciber" é amplamente utilizado para introduzir termos relacionados à segurança da informação. O manual define ameaças cibernéticas como ações que visam sistemas de Tecnologia da Informação e Comunicação (TIC) por meio do ciberespaço com o objetivo de obter acesso ilegal, enquanto ataques cibernéticos são caracterizados como ações direcionadas a sistemas TIC, utilizando o ciberespaço como meio de execução.

Ao passo que, assim como o artigo de Hurel, o documento da ANAC conceitua a importância da autenticidade, confidencialidade, integridade e disponibilidade de dados, que são os pilares de um ambiente seguro no setor da aviação. A ANAC entende e conceitua diferentes tipos de ameaças, como *malwares*[65], *ransomware*[66], *botnets*[67], além “autenticação” e “contramedidas” para

---

62 HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, Rio de Janeiro, p. 1-35, abr. 2021. p. 6. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 08 nov. 2024.

63 Confidencialidade, Integridade e Disponibilidade.

64 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

65 Malware é um software malicioso projetado para causar danos, invadir ou comprometer sistemas de computadores. Ele pode assumir várias formas, como vírus, worms, cavalos de Troia, ransomware e spyware. Esses programas são frequentemente usados por criminosos cibernéticos para roubar dados ou prejudicar operações. GARRET, Filipe. O que é malware? Veja significado, tipos e saiba remover. *In*: TECHTUDO. [*S. l.*], 27 mar. 2021. Disponível em:

mitigar vulnerabilidades e proteger infraestruturas críticas, cujo comprometimento pode causar graves instabilidades socioeconômicas e políticas. Também trata da segurança de sistemas críticos de Tecnologia da Informação e Comunicações (TIC), essenciais para a continuidade dos serviços à sociedade e ao setor aéreo, e também faz referência ao impacto das novas tecnologias, como a Internet das Coisas[68] (IoT), destacando a necessidade de proteção desses sistemas[69].

Além dos conceitos de segurança da informação apresentados pela ANAC e por Hurel, Baars[70] *et al*.[71] [72] [73], mencionam a importância de entender e combater

---

https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em: 08 nov. 2024.

66 Ransomware é um tipo de malware que sequestra os dados de uma vítima, bloqueando o acesso a eles, e exige um pagamento de resgate para restaurar o acesso. O ataque geralmente se espalha por e-mails maliciosos ou downloads comprometidos, criptografando arquivos essenciais. É possível remover o ransomware com ferramentas especializadas de segurança, mas em alguns casos, a recuperação total dos dados pode não ser garantida. O QUE É ransomware? Entenda como funciona e como remover o malware. *In*: TECHTUDO. [*S. l.*], 27 mar. 2021. Disponível em: https://www.techtudo.com.br/guia/2023/05/o-que-e-ransomware-entenda-como-funciona-e-como-remover-o-malware-edsoftwares.ghtml. Acesso em: 08 nov. 2024.

67 Botnets são redes de dispositivos infectados por malware, controladas remotamente por um cibercriminoso. Esses dispositivos podem ser usados para realizar ataques em larga escala, como negação de serviço (DDoS), roubo de informações, e campanhas de spam ou phishing. Os botnets permitem a execução coordenada de atividades maliciosas sem o conhecimento dos proprietários dos dispositivos infectados. O QUE É um botnet? *In*: AKAMAI. [*S. l.*], c2024. Disponível em: https://www.akamai.com/pt/glossary/what-is-a-botnet. Acesso em: 08 nov. 2024.

68 A Internet das Coisas (IoT) refere-se à rede de dispositivos físicos que estão conectados à internet, como sensores, câmeras e outros sistemas tecnológicos, permitindo que eles coletem, compartilhem e processem dados em tempo real. Esses dispositivos podem ser usados em diversas áreas, como casas inteligentes, cidades conectadas, veículos autônomos e até mesmo no monitoramento de saúde. A IoT possibilita que os dados capturados pelos dispositivos sejam analisados para informar e automatizar decisões e ações, otimizando processos em vários setores da sociedade. **O que é Internet das Coisas? IoT explicada**. SAP, 2023. Disponível em: https://www.sap.com/brazil/products/artificial-intelligence/what-is-iot.html. Acesso em: 25 set. 2024.

69 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Cibersegurança.pdf. Acesso em: 08 nov. 2024.

70 **Hans Baars**, CISSP, CISM, trabalhou como oficial de segurança da informação e auditor EDP na Polícia Nacional holandesa de 1999 a 2002. Em 2002 se tornou consultor de segurança na Agência Nacional de Serviços de Polícia da Holanda. Nessa função, participou da formulação da política de segurança da informação da polícia holandesa. A partir de 2006 ele trabalhou como consultor de segurança, período em que aconselhou o governo e empresas comerciais sobre como conceber a sua segurança física e da informação. A partir de 2009, ele foi o Chefe da Segurança da Informação na Enexis BV, uma empresa de gás e energia elétrica na Holanda. Atualmente ele trabalha como consultor de segurança cibernética na DNV GL, uma empresa especializada de consultoria voltada para serviços públicos com foco particular na segurança dos sistemas de controle industrial.

71 **Kees Hintzbergen** é consultor sênior, autônomo, de segurança da informação. Kees possui mais de 30 anos de experiência em TI e no provisionamento de informações, e trabalha na área de segurança da informação desde 1999. Em sua vida cotidiana Kees é um consultor, instrutor e "exemplo", onde emprega o "método de senso comum". Desde 2012 ele está envolvido no desenvolvimento de uma Base para Segurança da Informação, com base na ISO/IEC. 27001 e na ISO/IEC 27002 (versões de 2005 e 2013), para municípios holandeses. Tem também prestado

ameaças específicas, como *malwares*, *phishing* e *spam*. Segundo os autores:

> *Malware* é a combinação das palavras inglesas '*malicious*' e '*software*' e se refere a softwares indesejados, tais como vírus, *worms*[74], cavalos de Troia (*trojans*) e *spyware*. Uma medida padrão contra malware é usar antivírus e firewalls. Entretanto, está ficando cada vez mais claro que um antivírus sozinho não é suficiente para parar um malware. Uma das principais razões para o surto de vírus são as ações humanas. Uma infecção de vírus pode muitas vezes ocorrer através de um usuário que abre um anexo em um e-mail, que contém mais do que apenas o jogo, documento ou imagem prometidos, mas também contém um vírus. Portanto, é recomendável não abrir nenhum e-mail suspeito, ou e-mails de remetentes desconhecidos[75].

Além disso, de acordo com Baars *et al*., um *botnet* consiste em uma rede de programas interligados que se comunicam entre si por diversos canais na internet, com o intuito de executar tarefas no computador de terceiros, como o envio de *e-mails* de *spam* ou a participação em ataques distribuídos de negação de serviço (*DDoS*). A formação de um *botnet* pode ocorrer por meio de ações aparentemente inofensivas, como clicar em *links* suspeitos ou abrir anexos de *e-mails* contaminados, permitindo que *malwares* sejam baixados de forma imperceptível ao usuário. Uma vez comprometido, o dispositivo for conectado a um servidor de comando e controle, através do qual o operador do *botnet* controla todos os

---

apoio em torno da implementação de tal Base, desenvolvendo produtos adicionais para apoiar a sua implementação e montando uma equipe de suporte que fornece respostas de segurança aos municípios holandeses. Ele também participou ativamente na criação de um CERT para os municípios holandeses.

72 **Jule Hintzbergen**, CISSP CEH. Depois de trabalhar inicialmente por 21 anos no Ministério da Defesa, Jule trabalha desde 1999 na Capgemini como consultor de segurança cibernética. Ele possui mais de 30 anos de experiência em TI e passa a maior parte do seu tempo lidando com segurança da informação. Trabalhou em várias funções na área de gerência de projetos, gestão da informação, segurança fisica e da informação e biometria. Desde 2003, Jule é certificado CISSP em ISC2 e desde 2013 é certificado CEH (Certified Ethical Hacker). Desde 2012 ele está envolvido no desenvolvimento de uma Base para Segurança da Informação, com base na ISO/IEC 27001 e na ISO/IEC 27002 (versões de 2005 e 2013), para municípios holandeses. Tem também prestado apoio em torno da implementação de tal Base, desenvolvendo produtos adicionais para apoiar a sua implementação e montando uma equipe de suporte que fornece respostas de segurança aos municípios holandeses.

73 **André Smulders** (CISSP) é consultor de negócios, voltado para segurança da informação e gestão de riscos, na TNO. Quando André concluiu seus estudos em Gestão de Tecnologia na Universidade de Eindhoven, ele começou a trabalhar em projetos inovadores de TIC. A partir de 2000 ele começou a se especializar na área de segurança da informação e gerenciamento de riscos. Em sua função atual, ele apoia organizações, tanto do setor público quanto do privado, no gerenciamento de riscos em ecossistemas complexos em rede. Sobre esse tema, ele é coautor do livro "Networked Risk Management: how to successfully manage risks in hyperconnected value networks".

74 "Um worm é um pequeno programa de computador que propositalmente se replica. Os resultados da replicação são cópias da propaga". BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002*.* São Paulo: Brasport, 2018. *E-book*. local. 182.

75 *Ibid*., local. 175.

computadores infectados para desempenhar determinadas tarefas. Os autores ainda destacam que em que pese estudos recentes indicam que o número de sites potencialmente perigosos cresce diariamente, com alguns *botnets* chegando a milhões de dispositivos infectados, enquanto esforços contínuos buscam desativar esses servidores de comando e controle[76].

Por conseguinte, conforme descrito no Manual de Conscientização em Segurança Cibernética na Aviação Civil, aeroportos ao redor do mundo estão adotando uma arquitetura centralizada, ou seja, em infraestrutura tecnológica mais avançada, visando o compartilhamento mais eficiente de informações e o fornecimento de serviços. Assim, ao buscar constantemente aprimoramento em suas infraestruturas tecnológicas, com o objetivo de oferecer uma experiência contínua e confortável aos passageiros, essa modernização, que inclui a integração de plataformas mais abertas para facilitar o compartilhamento de informações e a colaboração entre parceiros e colaboradores, também expõe o setor a crescentes ameaças cibernéticas. Isso implica que ativos físicos, como *scanners* de bilhetes e painéis informativos, estarão conectados aos sistemas do aeroporto, tornando-os vulneráveis a ataques cibernéticos. Dessa forma, *Crackers* podem explorar essas conexões para acessar sistemas internos[77].

Como referido na introdução, de acordo com o Diretor de Estratégia e Gerenciamento de Segurança da Agência Europeia de Segurança da Aviação (EASA), aeroportos ao redor do mundo sofrem cerca de 1.000 ciberataques por mês. Para exemplificar a gravidade dessas ameaças, o Manual da ANAC menciona a Cathay Pacific Airways, de Hong Kong, enfrentou, em 2018, um dos maiores incidentes de cibersegurança do setor, com o vazamento de 9,4 milhões de registros de dados[78].

Contudo, além dos ativos físicos mencionados acima, de acordo com um relatório da empresa de segurança cibernética Coronet, milhões de viajantes que se conectam a redes de Wi-Fi públicas nos aeroportos também correm o risco de terem

---

[76] BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018. *E-book*. local. 188.

[77] BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

[78] *Ibid*.

seus dispositivos *hackeados*. A facilidade e conveniência de conexão oferecidas por essas redes muitas vezes ocultam o perigo, já que muitas delas não possuem criptografia[79] adequada, o que as torna vulneráveis e inseguras para navegação. Nesses casos, os *crackers* podem explorar as falhas de segurança para invadir os dispositivos conectados, instalar *softwares* maliciosos, roubar informações sensíveis, como senhas e credenciais de *login*, e obter outros dados pessoais de forma clandestina. De acordo com Dror Liwer, diretor de segurança e cofundador da Coronet, destacou que o principal fator de risco é que muitas pessoas priorizam a conveniência ao invés da segurança em suas conexões[80]. Para culminar, no capítulo 3.2, será brevemente analisado os problemas de segurança cibernética relacionados ao uso de Wi-Fi a bordo.

Assim, neste sentido, Hurel destaca que a segurança de dados, sistemas, redes e infraestruturas digitais é uma prioridade em uma sociedade conectada em contexto geral, visto que esses ataques cibernéticos ocorrem diariamente ao redor do mundo, enquanto, no Brasil, aproximadamente 70% da população está conectada à internet, e entre as classes D e E, 85% acessam a rede exclusivamente por meio de dispositivos móveis, com planos de dados limitados[81].

Ainda, cumpre aferir que de acordo com a pesquisa TIC Domicílios 2022, realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação, a maior parte dos usuários de Internet no Brasil, representando 62%, acessa a rede exclusivamente por meio de dispositivos móveis, o que corresponde a mais de 92 milhões de pessoas. Segundo o artigo, esse padrão de uso é mais predominante entre as mulheres (64%), entre indivíduos pretos (63%) e pardos

---

79 A criptografia é uma técnica de segurança que transforma informações em um formato ilegível, conhecido como texto cifrado, que só pode ser decodificado por quem possuir a chave correta. Existem dois tipos principais de criptografia: simétrica e assimétrica. Na criptografia simétrica, a mesma chave é usada tanto para criptografar quanto para descriptografar os dados. Já na criptografia assimétrica, são usadas duas chaves diferentes: uma pública, para criptografar, e outra privada, para descriptografar, garantindo que apenas o destinatário consiga acessar as informações. O uso de criptografia é essencial para proteger dados sensíveis contra acessos não autorizados, especialmente em ambientes digitais, onde ciberataques são uma ameaça constante. O QUE É criptografia de dados? Definição e explicação. *In*: KASPERSKY. [*S. l.*], c2024. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em: 08 nov. 2024.

80 CEDEÑO, Karina. Veja os 10 aeroportos com maior risco de ataque de hackers nos EUA. *In*: PANROTAS. [*S. l.*], 23 jul. 2018. Disponível em: https://www.panrotas.com.br/viagens-corporativas/seguranca/2018/07/veja-os-10-aeroportos-com-maior-risco-de-ataque-de-hackers-nos-eua_157329.html. Acesso em: 08 nov. 2024.

81 HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, Rio de Janeiro, p. 1-35, abr. 2021. p. 3. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 08 nov. 2024.

(67%), bem como nas classes sociais D e E, onde 84% dos usuários acessam a Internet apenas pelo celular, conforme dados divulgados pelo Comitê Gestor da Internet no Brasil (CGI)[82].

Por conseguinte, autora Hurel, aponta que o Brasil ocupa a 70ª posição no Índice Global de Segurança Cibernética da União Internacional de Telecomunicações (UIT) e o 6º lugar na América Latina, sendo superado por Uruguai, México e Paraguai. O país, desde 2015, tem enfrentado uma crise social e econômica, agravada pela pandemia de *Covid-19*[83], o que aumenta a dependência de redes digitais para transações, serviços e comunicações, sem o devido investimento em segurança cibernética[84].

Contudo, houve um avanço significativo do Brasil no UIT. De acordo com os dados divulgados pelo Ministério da Economia e atualizado em outubro de 2022, o Brasil subiu 53 posições, passando do 71º lugar para o 18º no *ranking* de 2020, consolidando-se na 3ª posição entre os países das Américas, atrás apenas dos Estados Unidos e do Canadá[85].

Baars et al., ressaltam diversas medidas essenciais para a segurança da informação no combate a ameaças cibernéticas. Entre essas, destacam-se a atualização constante dos *softwares* utilizados no ambiente de trabalho e o uso de *scanners* especializados, que examinam o registro do *Windows* em busca de chaves suspeitas e verificam os *softwares* instalados em busca de *worms*. Em alguns casos, os programas antivírus também desempenham esse papel de detecção de

---

82 COMITÊ GESTOR DA INTERNET NO BRASIL. **TIC Domicílios 2022:** pesquisa do uso da Internet no Brasil. São Paulo: Comitê Gestor da Internet, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20230825143348/resumo_executivo_tic_domicilios_2022.pdf. Acesso em: 08 nov. 2024.

83 A pandemia de Covid-19 é uma infecção respiratória aguda causada pelo coronavírus SARS-CoV-2, reconhecida pela Organização Mundial da Saúde em março de 2020. Caracterizada por sua alta transmissibilidade e impacto global, a doença teve início em dezembro de 2019, na cidade de Wuhan, China. O vírus, um betacoronavírus pertencente à família Coronaviridae, foi identificado em pacientes com pneumonia de causa desconhecida. Desde então, a Covid-19 causou uma crise sanitária mundial, levando a medidas como vacinação em massa, uso de máscaras e distanciamento social para conter a propagação do vírus. COVID-19. *In*: GOV.BR. Brasília, DF, [2024?]. Disponível em: https://www.gov.br/saude/pt-br/assuntos/covid-19. Acesso em: 08 nov. 2024.

84 HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, Rio de Janeiro, p. 1-35, abr. 2021. p. 4. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 08 nov. 2024.

85 BRASIL. **Brasil sobe 53 posições no Índice Global de Segurança Cibernética.** Disponível em: https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/07/brasil-sobe-53-posicoes-no-indice-global-de-seguranca-cibernetica. Acesso em: 25 set. 2024.

atividades maliciosas. Os autores recomendam ainda a adoção de *firewalls*[86] pessoais, que monitoram o tráfego de rede em busca de comportamentos suspeitos, além do uso de ferramentas de monitoramento de rede para detectar *worms*. Baars et al. enfatizam a importância de incluir o tema "*botnet*" em campanhas de conscientização de segurança, de modo que a equipe esteja atenta a e-mails com solicitações duvidosas e a sites suspeitos, utilizando *softwares* que indicam, diretamente no navegador, quando uma página da *web* apresenta riscos de segurança. Dessa forma, segundo eles a políticas de segurança da informação da organização devem incorporar essas diretrizes, e é fundamental assegurar canais eficazes para o reporte de incidentes e procedimentos de acompanhamento que garantam a resolução adequada dos problemas identificados[87].

É, portanto, possível afirmar que, de acordo com o Manual de Conscientização em Segurança Cibernética da Aviação Civil da ANAC, os estudos de Dror Liwer, da empresa de segurança cibernética Coronet, bem como os dados do Comitê Gestor da Internet (CGI.br), as análises de Louise Marie Hurel e as orientações de Baars *et al*., demonstram a crescente complexidade do uso de redes *Wi-Fi* abertas em aeroportos. Essas redes, embora convenientes, apresentam riscos significativos para a segurança digital, especialmente devido à falta de criptografia e proteção adequada, o que as torna vulneráveis a possíveis ataques cibernéticos. Posto isso, no próximo capítulo serão analisados os principais alvos e agentes em consonância com a ANAC, além de casos concretos de ataques cibernéticos ocorridos na aviação nos últimos anos.

---

86 Um firewall é uma barreira de segurança para redes de computadores, projetada para impedir o acesso não autorizado, protegendo os dispositivos contra possíveis ataques e monitorando o tráfego que entra e sai da rede. Ele age como uma barreira entre uma rede confiável e uma rede não confiável, como a internet, permitindo ou bloqueando o tráfego com base em um conjunto de regras de segurança predeterminadas. O firewall pode ser um dispositivo de hardware, um software ou uma combinação dos dois, ajudando a proteger informações sensíveis contra acesso não autorizado ou mal-intencionado. O QUE É um firewall? *In*: MICROSOFT. [*S. l.*], c2024. Disponível em: https://support.microsoft.com/pt-br/office/o-que-%C3%A9-um-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603. Acesso em: 08 nov. 2024.

87 BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018. *E-book*. local. 188.

3.1 Principais alvos e agentes, bem como casos concretos segundo a ANAC em 2023

Em 2023 a ANAC enfrentou desafios e alcançou conquistas importantes no campo da segurança cibernética, que reconheceu a necessidade de proteger o setor da aviação civil brasileiro contra-ataques cibernéticos e interferências que pudessem comprometer tanto a segurança (*safety*)[88] quanto a proteção (*security*)[89] dos voos e passageiros[90].

No capítulo anterior, foi mencionado que a ANAC reconheceu os riscos e vulnerabilidades emergentes devido ao uso crescente da Tecnologia da Informação e das Comunicações (TIC)[91] no setor da aviação. Agora, neste capítulo, traz-se a notícia divulgada pelo Ministério de Portos e Aeroportos, que reforça esse mesmo entendimento. Ambas as entidades apontam que o avanço tecnológico trouxe novos desafios de cibersegurança e para prevenir e combater esses riscos, a ANAC implementou diversas ações[92].

Entre essas, destacam-se a orientação ao setor, a cooperação internacional, a governança, a gestão de incidentes, bem como a conscientização e capacitação. A ANAC ainda divulgou dois manuais, sendo eles: o Manual de Conscientização de Segurança Cibernética da Aviação Civil, destinado a sensibilizar profissionais quanto aos conceitos e boas práticas de segurança cibernética; e o Manual de Avaliação de

---

88 Na aviação, “Safety” refere-se à segurança operacional, ou seja, a prevenção de acidentes e incidentes que possam colocar em risco a vida dos passageiros, tripulantes e a integridade da aeronave. Envolve práticas, procedimentos e regulamentações que garantem operações seguras, reduzindo ao máximo os riscos operacionais. BOTELHO, José Ricardo. Segurança operacional na aviação nasce da cooperação. *In*: AEROFLAP. [*S. l.*], 22 abr. 2022. Disponível em: https://www.aeroflap.com.br/seguranca-operacional-na-aviacao-nasce-da-cooperacao/. Acesso em: 08 nov. 2024.

89 Já o “Security” refere-se à proteção contra atos ilícitos e ameaças externas, como terrorismo, sabotagem e acesso não autorizado a aeronaves e aeroportos. Ele visa garantir que as infraestruturas aeroportuárias e os voos estejam protegidos contra intenções maliciosas. *Ibid*.

90 ANAC investe em segurança cibernética na aviação civil. *In*: AGÊNCIA nacional de aviação civil. Brasília, DF, 21 dez. 2023. Disponível em: https://www.gov.br/anac/pt-br/noticias/2023/anac-investe-em-seguranca-cibernetica-na-aviacao-civil. Acesso em: 08 nov. 2024.

91 Os sistemas de Tecnologia da Informação e Comunicação (TIC) são um conjunto de recursos tecnológicos que integram computação e telecomunicações, permitindo a criação, armazenamento, transmissão e gerenciamento de dados e informações. Esses sistemas incluem hardware, software, redes de comunicação e aplicativos que facilitam o fluxo de dados entre diferentes usuários e sistemas. O objetivo principal das TIC é otimizar o uso das tecnologias de comunicação e processamento de dados para aprimorar a conectividade, a automação de processos e a eficiência em diversas áreas, como educação, saúde, negócios e aviação, entre outras. TECNOLOGIA da Informação e Comunicação (TIC): o que são e para que servem? *In*: ALGAR telecom. [*S. l.*], 24 ago. 2022. Disponível em: https://blog.algartelecom.com.br/significado-de-tics-entenda-de-uma-vez-por-todas/. Acesso em: 08 nov. 2024.

92 ANAC [...], *op. cit*.

Segurança Cibernética, baseado no CAP 1850 da Autoridade da Aviação Civil do Reino Unido[93], que auxilia as organizações a avaliarem seu nível de maturidade em segurança cibernética e a implementarem melhorias[94].

Por conseguinte, traz-se à baila os atores, alvos e motivações de ameaças em potencial, bem como exemplos de alguns incidentes cibernéticos ocorridos na aviação civil, conforme descrito no Manual de Conscientização em Segurança Cibernética na Aviação Civil da ANAC. Ainda, cumpre deliberar que a exposição desses fatores evidenciará a relevância e a pertinência da presente monografia ao demonstrar como as ameaças cibernéticas impactam diretamente o setor da aviação.

Portanto, conforme o Manual, as infraestruturas, os sistemas e as plataformas críticas constituem os principais alvos das ciberameaças no setor da aviação civil. Dentre esses alvos, podem ser mencionados os aeródromos (relacionados à "*safety*" e "*security*"), as instalações físicas do controle de tráfego aéreo, os sistemas de gerenciamento de passageiros e cargas de companhias aéreas, os sistemas de TIC, os sistemas de manutenção e instalações, além dos órgãos reguladores. Para ANAC, qualquer indivíduo ou entidade com uma motivação específica pode ser um potencial agente de uma ciberameaça[95]. Para melhor compreensão, elaborou-se uma tabela que categoriza esses agentes e suas motivações:

Quadro 1 - Agentes e suas motivações segundo a ANAC

Pessoas	Organizações	Estados/Nações
Terroristas; Ativistas; Criminosos; Curiosos	Organizações criminosas; Organizações terroristas; Empresas concorrentes; Empresas terceirizadas	Nações/Estados hostis; Grupos financiados por Estados.

[93] O CAP 1850 da Autoridade da Aviação Civil do Reino Unido (CAA) é um guia que fornece orientações para completar o Cyber Assessment Framework (CAF) no setor de aviação. Ele auxilia as organizações a realizarem avaliações de segurança cibernética, focando na resiliência contra ameaças digitais. O documento faz parte de um processo de supervisão da CAA que visa garantir a conformidade das empresas com as normas de segurança cibernética. CYBER security oversight. *In*: CIVIL aviation authoroty. London, c2024. Disponível em: https://www.caa.co.uk/commercial-industry/cyber-security/cyber-security-oversight/. Acesso em: 08 nov. 2024.

[94] ANAC investe em segurança cibernética na aviação civil. *In*: AGÊNCIA nacional de aviação civil. Brasília, DF, 21 dez. 2023. Disponível em: https://www.gov.br/anac/pt-br/noticias/2023/anac-investe-em-seguranca-cibernetica-na-aviacao-civil. Acesso em: 08 nov. 2024.

[95] BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

Vândalos; Funcionários internos da organização (Empregados em Geral, Superusuários de TI, etc).	(equipe de segurança física, equipe de limpeza, equipe de TI etc); Organizações ativistas.	

Fonte: ANAC[96].

Assim, segundo a ANAC, as motivações para um ataque cibernético podem ser amplas e variadas, incluindo ganho financeiro, fraude, *ransomware*[97], espionagem industrial, destruição, redução de reputação, interrupção de serviços, ativismo, questões geopolíticas e ações contrárias aos interesses de um Estado. Dessarte, como visto anteriormente, um ataque cibernético ocorre quando uma vulnerabilidade é explorada com o intuito de causar danos. Todavia, segundo a ANAC pode ser desencadeado até por alguém sem motivação explícita, como em casos de negligência ou falta de conscientização sobre práticas de segurança, como deixar um sistema logado ou conectar dispositivos não autorizados, como um *USB*[98] pessoal[99].

Por conseguinte, os agentes de ciberameaças podem ser divididos em ameaças internas (alguém das equipes do aeroporto com intenções maliciosas), passageiros ou anônimos presentes fisicamente no aeroporto, agentes remotos (não presentes fisicamente, utilizando *malwares*, limitados aos vetores de ataque disponíveis remotamente) e outras ameaças, como falhas acidentais ou ambientais em *softwares* ou equipamentos. Os alvos desses ataques cibernéticos podem incluir

---

96 *Ibid*.

97 Ransomware é um tipo de malware que sequestra os dados de uma vítima, bloqueando o acesso a eles, e exige um pagamento de resgate para restaurar o acesso. O ataque geralmente se espalha por e-mails maliciosos ou downloads comprometidos, criptografando arquivos essenciais. É possível remover o ransomware com ferramentas especializadas de segurança, mas em alguns casos, a recuperação total dos dados pode não ser garantida. QUE É ransomware? Entenda como funciona e como remover o malware. *In*: TECHTUDO. [*S. l.*], 27 mar. 2021. Disponível em: https://www.techtudo.com.br/guia/2023/05/o-que-e-ransomware-entenda-como-funciona-e-como-remover-o-malware-edsoftwares.ghtml. Acesso em: 08 nov. 2024.

98 USB (Universal Serial Bus) é um padrão de conexão que permite a transferência de dados e energia entre dispositivos como celulares, computadores e acessórios. Sua tecnologia possibilita o tráfego simultâneo de dados e alimentação elétrica, tornando-o amplamente utilizado em eletrônicos de consumo. O USB conta com diferentes tipos de conectores, como USB-A, USB-C e micro-USB, e versões que variam em capacidade de transferência e potência, como USB 2.0 e USB4. ALECRIM, Emerson; HIGA, Paulo. O que é USB? *In*: TECNOBLOG. [*S. l.*], [2023]. Disponível em: https://tecnoblog.net/responde/o-que-e-usb/. Acesso em: 16 out. 2024.

99 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

ativos de TIC, redes de comunicação *wireless*[100] e cabeadas[101], funcionários ou passageiros usados como vetores de ataque, além de ataques dinâmicos entre ativos, em que um ativo comprometido serve como base para a propagação do ataque[102].

À medida que diversos incidentes cibernéticos foram registrados na aviação civil, o acidente da Spanair em 2008, cujo sistema de monitoramento técnico foi infectado por *malware*; o ataque de *malware* aos aeroportos de Istambul Ataturk e Sabiha Gokçen em 2013, que tentou roubar dados do sistema de controle de passaportes; e o incidente em Newark, também em 2013, causado por um rastreador de *GPS*[103] ilegal que interferiu nos sinais de navegação. Outros exemplos incluem o vazamento de dados de 750 mil clientes da Japan Airways em 2013, a invasão da conta do *Twitter*[104] da Malindo Air no mesmo ano, e o *cracker* da Autoridade de Aviação Civil da Malásia em 2014, um dia após o desaparecimento do voo MH370[105]. Ainda em 2014, houve ataques de negação de serviço ao governo da

---

100 Wireless é uma tecnologia que permite a transmissão de dados sem o uso de fios, conectando dispositivos por meio de sinais de rádio, infravermelhos ou micro-ondas. Com o advento dessa tecnologia, tornou-se possível conectar dispositivos como celulares, laptops e outros gadgets a redes de internet ou entre si, sem a necessidade de conexões físicas. FURTADO, Teresa. O que é wireless. *In*: TECHTUDO. [*S. l.*], 28 dez. 2011. Disponível em: https://www.techtudo.com.br/noticias/2011/12/o-que-e-wireless.ghtml. Acesso em: 08 nov. 2024.

101 A rede cabeada é uma estrutura de conexão que utiliza cabos físicos para interligar dispositivos, como computadores e impressoras, garantindo maior estabilidade, segurança e velocidade na transmissão de dados em comparação com redes sem fio. Esse tipo de rede é amplamente utilizado em ambientes corporativos por oferecer menor interferência e alta performance, sendo uma solução eficaz para grandes volumes de dados. REDE cabeada: o que é. *In*: COMPASS soluções em tecnologia. Joinville, 09 nov. 2021. Disponível em: https://compass.srv.br/rede-cabeada-o-que-e/. Acesso em: 08 nov. 2024.

102 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

103 O GPS (Global Positioning System) é um sistema de navegação por satélite desenvolvido inicialmente para fins militares pelos Estados Unidos, mas que hoje é amplamente utilizado em várias áreas, como navegação em mapas, rastreamento de veículos e serviços de emergência. O sistema opera com 24 satélites em órbita, permitindo determinar a localização geográfica de um dispositivo com alta precisão, normalmente entre 5 e 100 metros. ALECRIM, Emerson; HIGA, Paulo. O que é GPS? *In*: TECNOBLOG. [*S. l.*], [2023]. Disponível em: https://tecnoblog.net/responde/o-que-e-gps/. Acesso em: 16 out. 2024.

104 Twitter, atualmente conhecido como "X", é uma plataforma de rede social criada em 2006, inicialmente voltada ao microblogging. Em 2023, após sua aquisição por Elon Musk, foi rebatizada com o intuito de expandir suas funcionalidades para além da comunicação, buscando transformá-la em uma “super-app”. X (TWITTER). *In*: TECNOBLOG. [*S. l.*], c2005-2024. Disponível em: https://tecnoblog.net/sobre/twitter/. Acesso em: 08 nov. 2024.

105 O voo MH370 da Malaysia Airlines desapareceu em 8 de março de 2014, enquanto seguia de Kuala Lumpur para Pequim, com 239 pessoas a bordo. O último contato ocorreu cerca de 40 minutos após a decolagem. Investigações indicam que o avião mudou de rota e provavelmente caiu no Oceano Índico, mas, apesar de extensas buscas, seus destroços não foram

Jamaica, além de uma falha no centro de controle de tráfego aéreo em Londres que resultou em grandes interrupções nos voos[106].

Ao passo que, ainda segundo a ANAC, entre 2015 e 2020, diversos outros incidentes marcaram o setor, como o *cracker* dos sistemas da LOT em 2015, que impediu a emissão de planos de voo no *hub* de Varsóvia; a falha de sistemas no aeroporto de Orly, causada pelo uso de *software* obsoleto; e o ataque de *malware* ao Aeroporto Internacional de Kiev Boryspil em 2016, cuja origem foi rastreada até a Rússia. Em 2017, a British Airways reportou um incidente envolvendo drones próximos ao aeroporto de Heathrow e, em 2018, a Cathay Pacific sofreu a maior violação de dados na aviação, com o comprometimento de mais de 860 mil passaportes e cartões de crédito. Ataques continuaram a ocorrer, como o *ransomware* que afetou o aeroporto de Bristol em 2018, deixando o serviço de informações de voo fora do ar por dois dias, e o ciberataque à SITA em 2021, que expôs dados de passageiros brasileiros[107].

O arquivo da ANAC utilizado como referência é datado de 2023 e, portanto, não inclui menção ao apagão cibernético global de 2024, que impactou voos, bancos e serviços de emergência. No entanto, esse ocorrido será abordado na presente monografia, assim como o ataque à SITA ocorrido em 2021, que expôs dados de passageiros brasileiros, ambos no próximo capítulo.

3.2 Incidentes Cibernéticos na Aviação: O Ataque à SITA em 2021 e o Apagão Cibernético em 2024

Em março de 2021, a SITA, uma das maiores fornecedoras de TI para o setor aéreo, confirmou que sofreu um ataque cibernético que comprometeu informações de passageiros de companhias aéreas em todo o mundo. O incidente envolveu o sistema de Serviço de Processamento de Passageiros (*Passenger Service System* –

completamente localizados, e o mistério persiste após 10 anos. MISTÉRIO do sumiço do voo MH370 da Malaysia Airlines completa 10 anos sem solução. *In*: CNN BRASIL. São Paulo, 08 mar. 2024. Disponível em: https://www.cnnbrasil.com.br/internacional/misterio-do-sumico-do-voo-mh370-da-malaysia-airlines-completa-10-anos-sem-solucao-veja-o-que-se-sabe/. Acesso em: 08 nov. 2024.

106 BRASIL, *op. cit*.

107 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

PSS), usado por companhias como a Latam. Dados estes, relacionados aos programas de passageiros frequentes, incluindo nomes e números de fidelidade, foram potencialmente expostos[108].

A Latam, por sua vez, afirmou que não trabalhava diretamente com os sistemas afetados da SITA, mas que, por meio de acordos comerciais com outras companhias aéreas que utilizam esses sistemas, os dados de seus clientes foram afetados. E destacou que a proteção das informações dos seus clientes é uma prioridade e criou um canal de contato para que os clientes esclareçam dúvidas sobre o vazamento[109].

Por conseguinte, em 19 de julho de 2024, um apagão cibernético global, causado pela empresa de segurança cibernética CrowdStrike[110], afetou diversas empresas brasileiras, com impacto mais significativo no setor aeroportuário e bancário. Usuários relataram dificuldades de acesso a aplicativos bancários, e voos como por exemplo da Azul sofreram atrasos devido a problemas no sistema de gestão de reservas. A companhia aérea, por sua vez, recomendou que os passageiros chegassem mais cedo aos aeroportos para realizar o *check-in* de forma manual. No Aeroporto Internacional de Brasília, cinco voos da Azul decolaram com atraso, e outros três ainda estavam atrasados até as 11h. No Aeroporto Santos Dumont, no Rio de Janeiro, também houve problemas com o sistema de *check-in*, que passaram a ser realizados manualmente[111].

Não obstante, aeroportos como Tóquio, Amsterdã, Berlim e vários terminais na Espanha também relataram problemas em seus sistemas e atrasos em voos. Nos Estados Unidos (EUA), companhias como American Airlines, Delta Airlines, United Airlines e Allegiant Air suspenderam voos devido a problemas de comunicação ocasionados pelo apagão. A United Airlines comunicou que uma falha de *software*

---

108 LAURANCE, Felipe. Clientes do Latam Pass têm dados vazados após ataque de hacker. *In*: CNN Brasil. São Paulo, 25 ago. 2022. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/clientes-do-latam-pass-tem-dados-vazados-apos-ataque-de-hacker/. Acesso em: 08 nov. 2024.

109 TUSCO, Claudio. LATAM emite nota sobre o vazamento de dados de seus clientes em ataque hacker. *In*: PONTOS pra voar. [*S. l.*], 13 mar. 2021. Disponível em: https://pontospravoar.com/latam-emite-nota-sobre-vazamento-de-dados-de-seus-clientes-em-ataque-hacker/. Acesso em: 08 nov. 2024.

110 A CrowdStrike é uma empresa de cibersegurança fundada em 2011, conhecida por sua plataforma Falcon, que oferece soluções avançadas para prevenção, detecção e resposta a ameaças digitais em endpoints. SOBRE a CrowdStrike. *In*: CROWDSTRIKE. [*S. l.*], c2024. Disponível em: https://www.crowdstrike.com.br/sobre-crowdstrike/. Acesso em: 08 nov. 2024.

111 PEDUZZI, Pedro. Apagão cibernético afetou voos da Azul e aplicativo do Bradesco: problema já foi corrigido, diz empresa de segurança cibernética. *In*: AGÊNCIA Brasil. Brasília, DF, 19 jul. 2024. Disponível em: https://agenciabrasil.ebc.com.br. Acesso em: 08 nov. 2024.

de terceiros afetou seus sistemas, o que obrigou a manutenção de aeronaves nos aeroportos de origem, enquanto os voos já em curso prosseguiram normalmente. A Ryanair, maior companhia aérea da Europa, também relatou problemas em seu sistema de reservas[112].

Ainda, cumpre deliberar que, o referido apagão afetou agências bancárias brasileiras como o Bradesco. Clientes da referida agência tiveram problemas com o aplicativo do banco, que ficou fora do ar devido ao referido apagão cibernético. O aplicativo exibia uma mensagem informando que, em virtude desse incidente, alguns canais digitais do Bradesco apresentavam indisponibilidade. O banco recomendou que seus clientes não desinstalassem o aplicativo para evitar a perda da chave de segurança. Em nota à imprensa, o Bradesco comunicou que suas equipes estavam trabalhando para resolver o problema o mais rapidamente possível e que seus terminais de autoatendimento continuavam funcionando normalmente[113].

Ao passo que, a empresa CrowdStrike, responsável pelo apagão, assumiu a responsabilidade pelo incidente. George Kurtz, CEO da CrowdStrike, explicou que o problema foi causado por uma atualização de conteúdo para computadores com o sistema operacional *Windows*[114], relacionada ao sensor *Falcon*[115], que resultou na chamada "tela azul da morte", um indicativo de falhas no sistema. Kurtz informou que o problema foi "identificado, isolado e uma correção foi implantada"[116]. Dessa forma, entende-se que a responsabilidade da empresa é objetiva pelos defeitos no serviço prestado, conforme previsto no ordenamento jurídico brasileiro,

---

112 PEDUZZI, Pedro. Apagão cibernético afetou voos da Azul e aplicativo do Bradesco: problema já foi corrigido, diz empresa de segurança cibernética. *In*: AGÊNCIA Brasil. Brasília, DF, 19 jul. 2024. Disponível em: https://agenciabrasil.ebc.com.br. Acesso em: 08 nov. 2024.

113 *Ibid*.

114 O Windows é um sistema operacional desenvolvido pela Microsoft, que permite a execução de aplicativos em computadores pessoais e corporativos. Lançado em 1985, tornou-se um dos sistemas operacionais mais populares do mundo, com versões que evoluíram para atender tanto ao uso pessoal quanto ao empresarial. HAAS, Guilherme. O que é o Windows? *In*: CANALTECH. [*S. l.*], 17 fev. 2024. Disponível em: https://canaltech.com.br/windows/o-que-e-o-windows/. Acesso em: 08 nov. 2024.

115 O sensor Falcon da CrowdStrike é uma tecnologia de segurança que monitora e protege dispositivos contra ameaças cibernéticas em tempo real. Ele detecta atividades suspeitas nos endpoints (como computadores e servidores) usando inteligência artificial e machine learning, fornecendo proteção contra malwares, ataques de dia zero, e ameaças avançadas persistentes (APT). A plataforma Falcon permite prevenção e resposta rápida a incidentes, oferecendo visibilidade completa das atividades em rede e pontos finais. O QUE É a CrowdStrike. *In*: CROWDSTRIKE. [*S. l.*], c2024. Disponível em: https://www.crowdstrike.com.br/produtos/faq/. Acesso em: 08 nov. 2024.

116 PEDUZZI, *op. cit*.

especificamente no artigo 14 do Código de Defesa do Consumidor[117], que estabelece a responsabilidade objetiva do fornecedor pelos danos causados ao consumidor decorrentes de falhas na prestação de serviços.

Embora a CrowdStrike tenha identificado e corrigido o problema relacionado ao seu sensor Falcon, que resultou na "tela azul da morte", os custos de violações de dados são altos e crescentes. Segundo a IBM[118], o custo médio de uma violação de dados em 2023 foi de USD 4,45 milhões (equivale a cerca de R$ 25,23 milhões[119]), enquanto violações relacionadas a *ransomware* atingiram USD 5,13 milhões (equivale a cerca de R$ 29,06 milhões[120]). Outrossim, o cibercrime, se fosse um país, seria a terceira maior economia mundial, ficando atrás apenas dos Estados Unidos e da China[121].

Conquanto, tenha sido analisados os casos ocorridos em território brasileiro e esses incidentes resultaram, segundo especialistas, de falhas nas atualizações dos *softwares*, o que culminou no vazamento de dados dos clientes do Latam Pass, bem como em o apagão geral e ainda, que o vazamento tenha ocorrido por falhas de terceiros, se faz necessário reiterar que ele também pode decorrer de decisões humanas e individuais, por conveniência alheia em se conectar a redes públicas, seja em aeroportos ou até mesmo a bordo de aeronaves.

Neste sentido, a matéria da Kaspersky[122], aborda os riscos associados ao uso de redes *Wi-Fi* em aeronaves, destacando que, embora as conexões a bordo ofereçam conveniência, elas podem não ser seguras. Como visto no capítulo 3,

---

117 "Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos". BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.procon.df.gov.br/wp-content/uploads/2019/08/Codigo-do-consumidor-FINAL.pdf. Acesso em: 08 nov. 2024.

118 AFSHAR, Vala. Cybercrime threatens business growth. Take these steps to mitigate your risk. *In*: ZDNET. [*S. l.*], 21 abr. 2022. Disponível em: https://www.zdnet.com/article/cybercrime-can-be-the-biggest-threat-to-business-growth/. Acesso em: 08 nov. 2024.

119 O valor de USD 4,45 milhões convertido em reais, utilizando a taxa de câmbio atual de aproximadamente 1 USD = 5,67 BRL, equivale a cerca de R$ 25,23 milhões. Essa conversão foi realizada com base na taxa de câmbio atual fornecida pela Wise e CurrencyRate em 16/10/2024. REAL brasileiro para dólar americano. *In*: WISE. [*S. l.*], c2024. Disponível em: https://wise.com/br/currency-converter/brl-to-usd-rate. Acesso em: 08 nov. 2024.

120 O valor de USD 5,13 milhões convertido em reais, utilizando a taxa de câmbio de aproximadamente 1 USD = 5,66 BRL, equivale a cerca de R$ 29,06 milhões. Essa conversão foi realizada com base na taxa de câmbio atual fornecida pela Wise e CurrencyRate em 16/10/2024. *Ibid*.

121 AFSHAR, *op. cit*.

122 DONOHUE, Brian. Wi-Fi a bordo é seguro? *In*: KASPERSKY. [S. l.], 06 dez. 2013. Disponível em: https://www.kaspersky.com.br/blog/wi-fi-a-bordo-e-seguro/1787/. Acesso em: 08 nov. 2024.

fatores como redes abertas, falta de criptografia robusta e dispositivos desatualizados aumentam exponencialmente a vulnerabilidade dos passageiros e clientes à ataques cibernéticos.

Para Kurt Baumgartner, pesquisador de segurança da Kaspersky Lab, existem diversos problemas de segurança relacionados ao uso de *Wi-Fi* a bordo. Técnicas de ataque aos pontos de acesso podem expor dispositivos conectados, permitindo o acesso a arquivos e informações por criminosos cibernéticos. Além disso, as dificuldades para atualizar rapidamente *softwares* e *hardwares* em aeronaves aumentam a vulnerabilidade, e a má conexão com redes *Wi-Fi* e portas *USB* pode impactar os serviços de bordo, como entretenimento e comunicação da tripulação[123].

Logo, assim como discutido no capítulo, 3.1, o maior perigo, segundo a análise de Baumgartner, é que especialistas em TI, pesquisadores e profissionais que frequentam grandes conferências de segurança, como a *Black Hat*[124], têm o conhecimento necessário para comprometer redes *Wi-Fi* de companhias aéreas com facilidade. Nas palavras de Baumgartner, esses profissionais, com suas habilidades, são capazes de *crackear*/*hackear* desde carros até dispositivos médicos, o que torna a tarefa de comprometer redes a bordo uma ameaça real e preocupante[125].

Deste modo, tanto o artigo da Kaspersky quanto o Manual da ANAC apontam que esses crimes são cometidos por indivíduos altamente qualificados, como *hackers* e *crackers*, especialistas em TI ou até pesquisadores. Ou seja, esses agentes utilizam da sua expertise para explorar falhas de segurança em sistemas críticos da aviação, como redes *Wi-Fi* a bordo e infraestrutura aeroportuária visando acessar dados sensíveis, realizar ataques cibernéticos ou comprometer a segurança operacional. Logo, no próximo capítulo, serão abordadas as consequências do vazamento de dados pessoais na aviação, com ênfase na consequência do vazamento de dados pessoais e quais impactos para os titulares de dados.

---

123 DONOHUE, Brian. Wi-Fi a bordo é seguro? *In*: KASPERSKY. [*S. l.*], 06 dez. 2013. Disponível em: https://www.kaspersky.com.br/blog/wi-fi-a-bordo-e-seguro/1787/. Acesso em: 08 nov. 2024.

124 "Black hat" refere-se a hackers que utilizam suas habilidades para atividades maliciosas, explorando vulnerabilidades em sistemas e redes para roubo de informações ou danos. Esses indivíduos contrastam com os "*white hats*", que atuam de forma ética para fortalecer a segurança digital. O QUE É um hacker black hat? *In*: KASPERSKY. [*S. l.*], c2024. Disponível em: https://www.kaspersky.com.br/resource-center/threats/black-hat-hacker. Acesso em: 08 nov. 2024.

125 DONOHUE, *op. cit*.

3.3 Consequências do vazamento de dados pessoais na aviação: Danos e impactos para os titulares de dados

Para a ANAC, os impactos, prejuízos e consequências potenciais de um ciberataque nos negócios e nas relações com parceiros podem incluir a perda da eficácia atual ou futura das operações devido à perda de confidencialidade dos dados, a perda de confiança em informações críticas em virtude da integridade comprometida dos sistemas e a indisponibilidade ou degradação de informações e sistemas. Essas consequências podem ser expressas de forma quantitativa ou qualitativa e escaladas como alta, média-alta, média, média-baixa e baixa, geralmente associadas a um valor numérico. Em casos com múltiplos riscos, estes são agrupados de acordo com os tipos de impactos[126].

Assim, os impactos de um ciberataque podem ser observados em diversas áreas, incluindo aspectos econômicos, reputacionais, legais, psicológicos, sociais e físicos/digitais. Para facilitar a compreensão desses impactos, elaborou-se um quadro detalhado, com fundamento no Manual de Conscientização sobre Cibersegurança da ANAC:

Quadro 2 - Aspectos e Impactos segundo a ANAC

Aspecto	Impacto
Econômico	Perdas financeiras; Roubo de informação corporativa e/ou financeira; Roubo de dinheiro; Redução dos lucros; Redução de clientes; Redução de crescimento; Redução de investimentos; Interrupção de operações online; Interrupção de vendas; Perda de negócios ou contratos; Perda de capital; Queda no preço dos estoques.
Dano à Reputação/Imagem	Perda de clientes; Perda de vendas; Redução de lucros; Redução na possibilidade de negócios; Redução de créditos; Perda de parceiros comerciais; Perda de equipe chave; Perda de certificação; Perda de fornecedores; Dificuldade de recrutar equipe desejada; Julgamento na mídia; Dano à percepção

[126] BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

Aspecto	Impacto
	pública; Multas regulatórias; Custo de investigação; Pagamento de extorsão; Pagamento de compensação; Perda de trabalho; Engano.
Legal	Perda de segurança de dados pessoais.
Psicológico	Depressão; Vergonha; Embaraço; Desconforto; Frustação; Confusão; Aborrecimento/ansiedade; Culpa; Perda de autoconfiança; Baixa satisfação; Chateação; Mudanças negativas na percepção.
Social/Societal	Mudanças negativas na Percepção pública (tecnologia); Queda na moral interna da organização; Interrupção das atividades diárias; Impacto negativo na nação.
Físico/Digital	Perda de vidas; Danos à infraestrutura; Destruição; Roubo; Infecção; Comprometimento; Exposição/ vazamento; Redução de desempenho; Ferimento corporal; Dor; Acusação; Abuso; Destrato; Roubo e identidade.

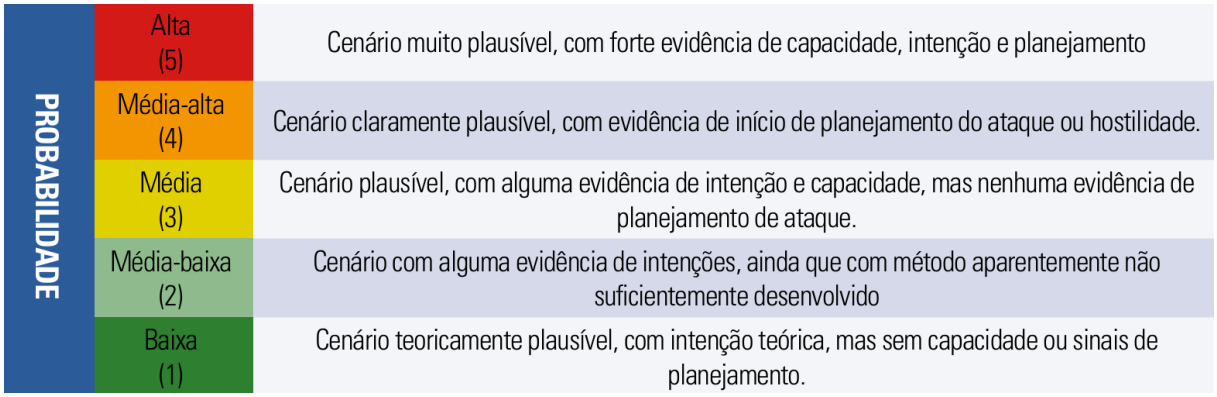
Fonte: ANAC[127].

Dessa forma, a ANAC também desenvolveu um modelo de Avaliação de Riscos que leva em consideração cenários hipotéticos de ataques cibernéticos. Entre os cenários analisados, destacam-se os ataques do tipo *DDoS*[128] em redes locais de servidores que gerenciam aeroportos, os quais têm o potencial de comprometer a operação e a segurança das infraestruturas aeroportuárias. Para melhor compreensão, foram incluídos nesta monografia o gráfico elaborado pela ANAC:

127 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

128 Um ataque DDoS (Distributed Denial of Service), ou ataque de negação de serviço distribuída, é uma tentativa maliciosa de interromper o tráfego normal de um servidor, serviço ou rede ao sobrecarregá-los com um grande volume de tráfego proveniente de várias fontes. Esse tipo de ataque visa tornar os serviços online indisponíveis para os usuários legítimos. WHAT is DDOS Attack? *In*: FORTINET. [*S. l.*], c2024. Disponível em: https://www.fortinet.com/resources/cyberglossary/ddos-attack. Acesso em: 08 nov. 2024.

Figura 1 - Gráfico de probabilidade de ataques cibernéticos na Aviação segundo a ANAC



Fonte: ANAC[129].

[129] BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

Figura 2 - Gráfico de questionário e probabilidade de ataques cibernéticos na Aviação segundo a ANAC

	PERGUNTAS	5 PONTOS	DE 1 A 4 PONTOS	0 PONTOS	PONTOS	PESO
Q1	Há histórico de paralização das atividades da organização causado por invasão de sistema causado por ataque cibernético?	Alto Potencial	Baixo Potencial	Ausência	1	1
Q2	Há histórico de invasões de algum sistema essencial de TIC para as atividades nesta organização?	Alto Potencial	Baixo Potencial	Ausência	3	1
Q3	Há relatos de perda ou vazamento de alguma informação ou banco de dados causada por ataque cibernético?	Alto Potencial	Baixo Potencial	Ausência	0	1
Q4	Há relatos de perda ou vazamento de alguma informação ou banco de dados causada por ataque cibernético em qualquer organização doméstica e/ou internacional de aviação civil?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q5	Qual é o volume de tráfego semanal de voos regulares em operação na organização?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q6	Há conhecimento de grupos "*hackers*" especializados em ataques aos sistemas da aviação civil?	Alto Potencial	Baixo Potencial	Ausência	1	1
Q7	Os usuários possuem acesso irrestrito à qualquer página / área dos sistemas?	Alto Potencial	Baixo Potencial	Ausência	1	1

Q8	Há desacordos políticos/ comerciais entre o Brasil com outras nações que propiciariam algum ataque cibernético ao Estado/Governo e serviços essenciais como os prestados por ATSP?	Alto Potencial	Baixo Potencial	Ausência	1	1
Q9	Há presença de Operadores Aéreos de países que são considerados alvos em potencial para ataques cibernético?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q10	Há informações específicas acerca da possibilidade de ocorrer um ataque através desse cenário de ameaça?	Há informações específicas de planejamento, intenção e capacidade de ataque.	Há alguma evidência de intenção e capacidade, mas nenhuma evidência de planejamento de ataque real.	Não há informações específicas ou sinais de possibilidade ou planejamento de ataque; ou há uma intenção teórica, mas sem capacidade aparente.	3	1
Q11	Um ataque cibernético tem o potencial de causar estragos em grande escala nos principais centros de transporte aéreo em todo o país e levar a um grande número de atrasos, cancelamentos de voos e alertas de segurança mais rigorosos?	Alto Potencial	Baixo Potencial	Ausência	5	1
Q12	Os dados desta organização estão registrados na nuvem?	Alto Potencial		Ausência	0	1
					Nível da situação de um ataque	30/13 = 2.3

Fonte: ANAC[130].

130 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

De acordo com o gráfico expositivo da ANAC, observa-se que as perguntas Q4, Q5, Q9 e Q11 demonstram a possibilidade de vazamento de informações ou perda de dados sensíveis em decorrência de um ataque cibernético com alto potencial, nº 5.

Baars *et al*., entendem que as redes são a espinha dorsal dos sistemas de informação e, portanto, a gestão da segurança de rede é essencial para manter elementos maliciosos afastados dos ativos críticos. Contudo, os autores alertam que apenas garantir a segurança da rede não é suficiente para proteger a informação de maneira abrangente, pois a autorização de acesso à rede não implica automaticamente o acesso a todos os sistemas de informação nela conectados. Em casos envolvendo informações confidenciais, é fundamental considerar que dispositivos conectados à rede, como impressoras multifuncionais, podem armazenar dados em seus discos rígidos, os quais podem ser acessados ou extraídos. Além disso, os autores dispõem que o estabelecimento de procedimentos e responsabilidades específicas é importante para proteger a informação contra riscos evitáveis, principalmente em contextos em que aplicações interligadas podem criar vulnerabilidades inesperadas, como ocorre em sistemas de administração e contabilidade[131].

Os autores também reforçam a necessidade de monitorar regularmente os sistemas conectados à rede, limitando o acesso de sistemas e avaliando cuidadosamente os riscos associados a conexões com outras redes, especialmente quando se lida com redes públicas ou sem fio, onde a confidencialidade e integridade dos dados podem ser comprometidas[132].

Em redes interconectadas, a gestão e manutenção por diferentes unidades ou organizações, como ocorre com provedores terceirizados, demanda coordenação precisa para garantir os requisitos e medidas de segurança apropriados. A segurança dos serviços de rede pode ser fortalecida por meio de diversas tecnologias, como o uso de certificados digitais, autenticação de usuários, firewalls, sistemas de detecção de intrusão e criptografia. *VPNs*, por exemplo, utilizam a internet para conectar redes geograficamente distantes, garantindo a integridade e

---

131 BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018. *E-book*. local. 195.

132 *Ibid*., local. 195.

autenticidade dos dados por meio de protocolos como o IPSec[133]. Os autores destacam ainda o risco de ataques quando a segurança de rede é negligenciada, como no caso de uma empresa invadida por *crackers/hackers* devido à falta de monitoramento e senhas fracas, o que resultou no vazamento de dados sigilosos. Além disso, ressaltam a importância da segregação de redes, com a distinção entre intranets – redes privadas internas – e extranets, que conectam a organização com terceiros, ampliando o alcance da rede e, consequentemente, os desafios de segurança[134].

À vista disso, demonstra-se a importância da presente monografia, pois no setor de aviação, onde há uma integração complexa de sistemas de diferentes organizações, como companhias aéreas, aeroportos e fornecedores de tecnologia, as redes interconectadas se tornam alvo preferencial para invasões e ainda que o gráfico da ANAC seja hipotético, cabe analisar se o ordenamento jurídico brasileiro está preparado para enfrentar tal situação. Cumpre, portanto, aferir que essa questão será devidamente analisada no próximo capítulo, onde se discutirá a adequação e eficácia das normas jurídicas vigentes no Brasil.

---

133 IPSec, ou Internet Protocol Security, é um conjunto de protocolos que protege e autentica pacotes de dados em uma rede IP. Ele é amplamente utilizado para configurar redes privadas virtuais (VPNs), garantindo que os dados transmitidos entre dois pontos sejam seguros e não adulterados durante o trajeto. O IPSec trabalha criptografando e autenticando cada pacote de dados, utilizando várias técnicas de criptografia para proteger a integridade e a confidencialidade das informações. CLOUDFLARE. *O que é IPSec?*. Disponível em: https://www.cloudflare.com/pt-br/learning/network-layer/what-is-ipsec/. Acesso em: 7 nov. 2024.

134 BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018. *E-book*. local. 197.

4 INTERSEÇÃO ENTRE AVIAÇÃO, CIBERSEGURANÇA E O DIREITO: ANÁLISE DAS LEIS E REGULAMENTAÇÕES APLICÁVEIS

No presente capítulo, serão analisadas as principais legislações que regulam a aviação e a cibersegurança no Brasil, com o objetivo de avaliar se o arcabouço jurídico atual está preparado para enfrentar as ameaças cibernéticas que impactam o setor aéreo. Inicia-se com a Lei Federal nº 7.565/1986 (Código Brasileiro de Aeronáutica) e a Lei Federal nº 11.182/2005 (Cria a Agência Nacional de Aviação Civil – ANAC, e dá outras providências). Em seguida, analisam-se as normas de segurança cibernética, como a Lei Federal nº 12.965/2014 (Marco Civil da Internet), a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados), o Decreto nº 11.856/2023 (Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança) e por fim o Decreto nº 11.491/2023 (Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

A partir dessas análises, busca-se responder ao problema de pesquisa que norteia este estudo, verificando se as normas e estruturas regulatórias brasileiras, como o direito aeronáutico e o direito digital, são eficazes para mitigar e enfrentar as ameaças cibernéticas que afetam a aviação civil e as infraestruturas aeroportuárias.

Portanto, cabe destacar que os capítulos anteriores trataram do conceito e dos primórdios da aviação, seguido pela análise do Direito Aeronáutico, sua autonomia, suas fontes e sua interdisciplinariedade. Também foram explorados amplamente os conceitos de cibersegurança, bem como ocorrem em específico na aviação, identificando os principais alvos e agentes na aviação, além de casos concretos como o ataque à SITA em 2021 e o apagão cibernético de 2024, conforme a ANAC. A partir deste capítulo, será abordada a interseção entre Aviação, Cibersegurança e o Direito.

4.1 Análise da Lei Federal nº 7.565/1986 e da Lei Federal nº 11.182/2005

A principal base normativa do Direito Aeronáutico no Brasil é o Código Brasileiro de Aeronáutica (CBA), instituído pela Lei Federal nº 7.565/1986 e complementado pela Lei Federal nº 11.182/2005, que criou a Agência Nacional de Aviação Civil (ANAC). Cumpre mencionar que a ANAC como agência reguladora,

possui independência administrativa e autonomia financeira, com poder normativo para regular e fiscalizar as atividades de aviação civil e infraestrutura aeroportuária no país[135]. Não obstante, o CBA reúne normas de direito público e privado e regula os diversos aspectos da aviação civil, organizados em onze títulos, que incluem desde o uso do espaço aéreo e a infraestrutura aeronáutica e aeroportuária até os contratos de transporte aéreo e responsabilidades civis[136] [137].

Dentre esses, os títulos que versam da infraestrutura aeronáutica e dos serviços aéreos são os mais relevantes para a regulação econômica do setor, constituindo o marco regulatório da aviação civil no Brasil. Contudo, a interpretação do CBA deve ser realizada à luz das disposições trazidas pela Lei Federal nº 11.182/2005, a qual, ao instituiu a ANAC, pois instituiu mudanças significativas no

---

135 "[...] Art. 4º A natureza de autarquia especial conferida à ANAC é caracterizada por independência administrativa, autonomia financeira , ausência de subordinação hierárquica e mandato fixo de seus dirigentes [...]
Art. 5º A ANAC atuará como autoridade de aviação civil, assegurando-se-lhe, nos termos desta Lei, as prerrogativas necessárias ao exercício adequado de sua competência. BRASIL. **Lei nº 11.182, de 27 de setembro de 2005.** Cria a Agência Nacional de Aviação Civil – ANAC, e dá outras providências. Brasília, DF: Presidência da República, 2005. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/Lei/L11182.htm. Acesso em: 08 nov. 2024.

136 PINTO, Victor Carvalho. **O marco regulatório da aviação civil:** elementos para a reforma do Código Brasileiro de Aeronáutica. Brasília, DF: Senado Federal, 2008. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-42-o-marco-regulatorio-da-aviacao-civil-elementos-para-a-reforma-do-codigo-brasileiro-de-aeronautica/view. Acesso em: 08 nov. 2024.

137 Título I - Disposições Preliminares (Artigos 1º ao 3º): Estabelece as disposições gerais e os princípios básicos que regem a aviação civil no Brasil. Título II - Do Uso do Espaço Aéreo Brasileiro (Artigos 4º ao 16): Regula o uso do espaço aéreo, incluindo a navegação e os direitos de tráfego aéreo, estabelecendo normas de direito público para garantir a segurança e o controle da circulação aérea no país. Título III - Da Infraestrutura Aeronáutica e Aeroportuária (Artigos 17 ao 43): Trata da organização, administração e exploração da infraestrutura aeroportuária e aeronáutica, incluindo a regulamentação de aeroportos, aeródromos e equipamentos de navegação aérea, aspectos fundamentais do direito público na aviação. Título IV - Da Aeronave (Artigos 44 ao 76): Regula a propriedade, registro e nacionalidade das aeronaves, bem como os direitos e deveres dos proprietários e operadores, aspectos que envolvem tanto direito público quanto privado. Título V - Do Pessoal Aeronáutico (Artigos 77 ao 90): Estabelece normas sobre a habilitação, os direitos e os deveres do pessoal aeronáutico, incluindo pilotos e demais profissionais da aviação, com enfoque em normas de direito público. Título VI - Do Transporte Aéreo (Artigos 91 ao 209): Regula contratos de transporte aéreo e as responsabilidades civis das empresas aéreas e operadores, abrangendo normas de direito privado e disposições relativas ao contrato de transporte, incluindo direitos e deveres dos passageiros e das companhias aéreas.Título VII - Da Responsabilidade Civil (Artigos 281 ao 317): Trata das responsabilidades civis derivadas de danos causados por aeronaves, bem como dos danos a terceiros em solo, estabelecendo critérios de indenização e responsabilidade dos operadores. Título VIII - Das Infrações e Penalidades (Artigos 289 ao 305): Disciplina as sanções aplicáveis às infrações relativas à aviação civil, com enfoque no direito público para assegurar o cumprimento das normas de segurança e regulamentação. BRASIL. **Lei nº 7.565, de 19 de dezembro de 1986.** Dispõe sobre o Código Brasileiro de Aeronáutica. Brasília, DF: Presidência da República, 1986. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7565compilado.htm. Acesso em: 08 nov. 2024.

regime econômico da aviação, garantindo às empresas aéreas maior autonomia na exploração de rotas e na definição de tarifas[138] [139].

Segundo Victor Carvalho Pinto[140], a legislação aeronáutica brasileira é composta por diversas outras normas que regulam diferentes aspectos do setor. Entre elas, destacam-se o Decreto-Lei nº 205/1967, alterado pela Lei Federal nº 5.404/1968, que trata da organização e funcionamento dos aeroclubes; a Lei Federal nº 5.332/1967, que regula o arrendamento de áreas aeroportuárias; a Lei Federal nº 6.009/1973, que dispõe sobre as tarifas aeroportuárias; e o Decreto-Lei nº 1.896/1981, que regulamenta as tarifas de uso de auxílios à navegação aérea. Outras leis complementam essas disposições, como a Lei Federal nº 7.920/1989, que criou o ATAERO[141], e a Lei Federal nº 9.825/1999, que trata da destinação de parte da Tarifa de Embarque Internacional para a amortização da dívida pública. Além disso, o Fundo Aeroviário, instituído pelo Decreto-Lei nº 270/1967, e o Plano Nacional de Viação aprovado pela Lei Federal nº 5.917/1973 que são instrumentos importantes para o planejamento e financiamento da infraestrutura aeronáutica no Brasil. Por fim, a regulação da profissão de aeronauta instituída pela Lei Federal nº 7.183/1984.

Contudo, Pinto faz uma observação importante sobre a desatualização e a falta de coesão desse conjunto de normas. Ele aponta que a CF, o CBA, a lei de criação da ANAC e a lei complementar das Forças Armadas utilizam terminologias distintas, o que dificulta a harmonização jurídica. Além disso, o autor menciona que

---

138 "Art. 48. § 1º Fica assegurada às empresas prestadoras de serviços aéreos domésticos a exploração de quaisquer linhas aéreas, mediante prévio registro na Anac, observadas exclusivamente a capacidade operacional de cada aeroporto e as normas regulamentares de prestação de serviço adequado editadas pela Anac. § 2º" BRASIL. **Lei nº 11.182, de 27 de setembro de 2005.** Cria a Agência Nacional de Aviação Civil – ANAC, e dá outras providências. Brasília, DF: Presidência da República, 2005. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/Lei/L11182.htm. Acesso em: 08 nov. 2024.

139 PINTO, Victor Carvalho. **O marco regulatório da aviação civil:** elementos para a reforma do Código Brasileiro de Aeronáutica. Brasília, DF: Senado Federal, 2008. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-42-o-marco-regulatorio-da-aviacao-civil-elementos-para-a-reforma-do-codigo-brasileiro-de-aeronautica/view. Acesso em: 08 nov. 2024.

140 *Ibid*.

141 Adicional de Tarifas Aeronáuticas. Percentual das tarifas cobradas nos embarques domésticos e internacionais e das tarifas relativas ao uso dos auxílios à navegação aérea e das telecomunicações. Os recursos arrecadados são aplicados na melhoria da infraestrutura aeroportuária. ATAERO - Adicional de Tarifas Aeronáuticas. *In*: DEPARTAMENTO de controle do espaço aéreo – DECEA. Brasília, DF, [2024?]. Disponível em: https://www.decea.mil.br/index.cfm?i=utilidades&p=glossario&single=2172. Acesso em: 09 nov. 2024.

várias disposições são antigas e incompatíveis com normas mais recentes, contudo, permanecem em vigor. Para ele há necessidade de atualização dos paradigmas legislativos, especialmente no que tange à regulação econômica, sugerindo que a criação da ANAC representou um avanço parcial, mas que o CBA ainda segue um modelo intervencionista. Para ele, a solução ideal seria a consolidação das normas e a elaboração de um novo código que adeque a legislação do setor e promova uma revisão conceitual adequada aos tempos atuais[142].

Conquanto, nos próximos capítulos, será analisado como a Lei Federal nº 13.709/2018, conhecida como Lei Geral de Proteção de Dados (LGPD), influencia na segurança cibernética na aviação. Em seguida, será estudado o papel da Convenção de Budapeste como um complemento à LGPD no combate aos crimes cibernéticos, buscando assim, compreender como tais normativas podem atuar frente ao problema de pesquisa e por fim, uma análise ao Decreto nº 11.856/2023, que institui a Política Nacional de Cibersegurança (PNCiber), proposta pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR).

4.2 Aspectos de segurança cibernética à luz da Lei Federal 12.965/2014, Lei Federal nº 13.709/2018 e do Decreto nº 11.856/2023

O ordenamento jurídico brasileiro dispõe de legislações específicas voltadas à proteção de dados e à segurança no ambiente digital, como o Marco Civil da Internet (Lei Federal nº 12.965/2014) e a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018).

O Marco Civil da Internet, estabeleceu um conjunto de princípios[143], garantias, direitos e deveres que regulam o uso da internet no país, com foco na proteção da

---

142 PINTO, Victor Carvalho. **O marco regulatório da aviação civil:** elementos para a reforma do Código Brasileiro de Aeronáutica. Brasília, DF: Senado Federal, 2008. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-42-o-marco-regulatorio-da-aviacao-civil-elementos-para-a-reforma-do-codigo-brasileiro-de-aeronautica/view. Acesso em: 08 nov. 2024.

143 "Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios: I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal; II - proteção da privacidade; III - proteção dos dados pessoais, na forma da lei; IV - preservação e garantia da neutralidade de rede; V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas; VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; VII - preservação da natureza participativa da rede; VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei". BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

privacidade dos usuários[144] e na responsabilidade dos provedores de serviços online. Esse marco legal, promulgado em abril de 2014, consolidou um avanço significativo na regulamentação da Internet ao incluir, entre suas diretrizes, a neutralidade da rede, a privacidade e a não responsabilização dos provedores por conteúdos gerados por terceiros[145], exceto em casos de descumprimento de ordens judiciais[146].

A neutralidade da rede, um dos aspectos centrais do Marco Civil, assegura que os provedores de internet tratem todos os dados de forma igualitária[147], sem discriminação quanto ao tipo de conteúdo, aplicativos ou serviços, o que é importante para garantir a liberdade de expressão e o acesso à informação[148].

A referida lei também introduziu importantes proteções à privacidade, determinando que as empresas só possam coletar e tratar dados pessoais mediante o consentimento dos usuários[149], corroborando assim com a segurança no ambiente digital. Outro ponto de destaque é a responsabilidade limitada dos provedores, que, ao seguir ordens judiciais, não são responsabilizados pelo conteúdo postado pelos usuários, contribuindo, portanto, para a manutenção da liberdade de expressão garantida pela CF. Ademais, o Marco Civil ainda estabeleceu diretrizes para que o Estado promova a inclusão digital e o acesso universal à internet[150], bem como

---

Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 nov. 2024.

144 "Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei; III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]". *Ibid*.

145 "Artigo 18º a 21º: Regulam a responsabilidade dos provedores de internet, especificando que eles não são responsáveis por conteúdos gerados por terceiros, salvo quando descumprem ordens judiciais de remoção de conteúdo". *Ibid*.

146 MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. Crimes cibernéticos. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 10, p. 109-126, out. 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/11580/5222. Acesso em: 08 nov. 2024.

147 "Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação". BRASIL, *op. cit*.

148 MAIA; COSTA, *op. cit*.

149 "[...] Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos: [...] IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; [...]" BRASIL, *op. cit*.

150 "Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção: I - do direito de acesso à internet a todos; II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos; [...]". BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em:

regulou a retenção de registros de conexão[151] [152], permitindo o acesso por autoridades em casos de investigação, desde que respeitados limites que asseguram a proteção da privacidade dos cidadãos[153].

Todavia, para Maia e Costa, o Marco Civil tornou-se uma referência internacional de legislação progressista, equilibrando a liberdade na internet com a proteção dos direitos dos usuários e empresas. Para a autora, apesar de ser considerado um exemplo global, a necessidade de aprimorar e adaptar essa legislação às inovações tecnológicas e mudanças sociais permanece um desafio contínuo[154].

Já a Lei Federal n° 13.709/2018 conhecida como Geral de Proteção de Dados Pessoais (LGPD), tem como objetivo proteger os direitos fundamentais de liberdade, privacidade e a livre formação da personalidade de cada indivíduo. A lei regula o tratamento de dados pessoais, tanto em meios físicos quanto digitais, realizado por pessoas físicas ou jurídicas de direito público ou privado, abrangendo uma série de operações que podem ser realizadas manual ou digitalmente[155].

À medida em que, o tratamento de dados é conduzido por dois agentes principais: o Controlador[156] e o Operador[157]. Além desses, há o Encarregado[158],

---

https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 nov. 2024.

151 "Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento [...]". BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 nov. 2024.

152 "Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento [...]". *Ibid*.

153 MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. Crimes cibernéticos. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 10, p. 109-126, out. 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/11580/5222. Acesso em: 08 nov. 2024.

154 *Ibid*.

155 "Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural". BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 nov. 2024.

156 "Art. 5º Para os fins desta Lei, considera-se: [...] VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais". *Ibid*.

indicado pelo Controlador, que atua como intermediário entre o Controlador, o Operador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD)[159].

A lei define o tratamento de dados como qualquer atividade que utilize dados pessoais, como a coleta, produção, recepção, classificação, armazenamento, eliminação, modificação, comunicação etc. Outrossim, o agente responsável pelo tratamento deve garantir que a finalidade[160] da operação seja clara, explícita e informada ao titular dos dados. Não obstante, ainda cumpre mencionar que, no setor público[161], o tratamento dos dados tem como principal finalidade a execução de políticas públicas, conforme estabelecido por lei ou contratos e que o descumprimento dessa exigência acarreta sérias consequências, incluindo sanções administrativas aplicadas pela ANPD, que podem variar de advertências a multas substanciais, além da publicização da infração e, em casos graves, a suspensão das atividades de tratamento de dados.

Posto a definição de ambas as leis, agora serão inseridas no contexto dos aeroportos e das empresas aéreas, sendo de extrema relevância, tanto para a prestação de serviços quanto para a segurança dessas organizações[162].

Para a ANAC, os dados pessoais sensíveis e os ativos informacionais ganharam maior relevância, não apenas em termos de segurança operacional e proteção contra interferências ilícitas, mas também em relação à privacidade dos

---

157 “Art. 5º Para os fins desta Lei, considera-se: [...] VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; [...]”. BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 nov. 2024

158 “Art. 5º Para os fins desta Lei, considera-se: [...] VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); [...]”. *Ibid*.

159 “Art. 41. O controlador deverá indicar encarregado pelo tratamento de dados pessoais”. *Ibid*.

160 “Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades; [...]”. *Ibid*.

161 “Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei; [...]”. *Ibid*.

162 BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

titulares desses dados. Porquanto, como estudado anteriormente, a violação de tais dados, segundo a LGPD, pode resultar na responsabilização dos agentes econômicos que atuam no tratamento de dados pessoais, o que inclui organizações do setor da aviação civil.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo[163].

Assim, qualquer sistema ou ferramenta voltada à segurança da informação deve incorporar as normas e princípios relativos à proteção de dados[164].

A ANAC ainda ressalta a necessidade de considerar a cibersegurança e a proteção de dados como aspectos complementares e interligados. Enquanto a cibersegurança se concentra na preservação da informação e infraestrutura dentro do ciberespaço, abrangendo ferramentas como gerenciamento de permissões, classificação de dados, controle de identidade e acesso (*logs*), estabelecimento de controles cibernéticos, uso de *firewalls*, câmeras de segurança e análise comportamental de usuários, a proteção de dados foca em direitos fundamentais, como privacidade e liberdade, com base no princípio da autodeterminação informativa[165]. Por outro lado, a proteção de dados visa a proteção dos direitos dos indivíduos, sendo que a cibersegurança, por sua vez, tem como objetivo preservar a integridade e confidencialidade das informações[166]. A ANAC ainda dispõe que:

> Com a crescente relevância e dimensão do tratamento de dados pessoais pelas organizações foi elaborada em conjunto pela Organização Internacional de Normalização (ISO) e pela Comissão Eletrotécnica Internacional (IEC) – organizações internacionais de padronização de boas práticas – a ISO/IEC 27701, norma-padrão que atualiza as ISO/IEC 27001 e ISO/IEC 27002, as quais estabelecem, respectivamente, (i) requisitos para estabelecer, implementar, manter e aprimorar um Sistema de Gestão de

---

163 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 nov. 2024.

164 BRASIL. Agência Nacional de Aviação Civil. **Manual de Conscientização em Segurança Cibernética na Aviação Civil**. Disponível em Manual_de_conscientizacao_sobre_Ciberseguranca.pdf (www.gov.br) Acesso em: 25 set. 2024.

165 *Ibid*.

166 *Ibid*.

> Segurança da Informação (SGSI) e (ii) diretrizes práticas para a implementação e gerenciamento de controles[167].

Contudo, a ANAC também alerta para o fato de que sistemas focados exclusivamente na segurança da informação podem falhar ao lidar com as fragilidades e violações dos direitos dos titulares de dados. Colaciona-se trecho neste sentido:

> Vale mencionar que algumas ameaças específicas da abordagem unicamente focada em segurança da informação podem não corresponder às fragilidades e questões a serem consideradas quando da violação dos direitos dos titulares. Além disso, a ausência dessas considerações impede que o desenho do sistema de cibersegurança possa ser adequado a respeitar os princípios da LGPD e atender aos direitos dos titulares[168].

Ademais, a ANAC dispõe que a integração da proteção de dados na cibersegurança é vastamente reconhecida, e os agentes econômicos que tratam dados pessoais devem considerar esses elementos em suas práticas. A evolução das normas e das práticas organizacionais, tanto no cenário nacional quanto internacional, consolidou uma intersecção simbiótica entre proteção de dados e cibersegurança, apesar de suas áreas distintas de enfoque. Além disso, o alinhamento das práticas de cibersegurança com os requisitos da LGPD e outras normativas de privacidade de dados proporciona sinergias que ajudam a atingir simultaneamente os objetivos de segurança da informação e de proteção de dados pessoais[169].

Outrossim, fato inconteste, é que a aplicação do princípio da responsabilidade é imprescindível quando se trata da proteção de dados sensíveis. Para Sales Sarlet e Linden Ruaro, ao abordar o tratamento de dados sensíveis no ambiente digital ou virtual, ambas entendem que é fundamental considerar, além do princípio da responsabilidade, os princípios da precaução e da prevenção, como pilares centrais na construção de uma estrutura jurídica voltada para a proteção da dignidade da pessoa humana, tanto no contexto digital quanto fora dele. Dessa forma, para as autoras, a atuação preventiva e cautelosa é imprescindível para garantir que os

---

167 BRASIL. Agência Nacional de Aviação Civil. **Manual de Conscientização em Segurança Cibernética na Aviação Civil**. Disponível em Manual_de_conscientizacao_sobre_Ciberseguranca.pdf (www.gov.br) Acesso em: 25 set. 2024.

168 *Ibid*.

169 *Ibid*.

direitos dos titulares de dados sejam resguardados[170]. Assim, no Capítulo 5.2 será tratado dos princípios da precaução e da prevenção, com ênfase em sua aplicação na cibersegurança na aviação.

Nessa perspectiva, as autoras ainda ressaltam que torna-se cada vez mais clara a proeminência da LGPD no ordenamento jurídico brasileiro, uma vez que ela visa à regulação do direito à proteção de dados pessoais, garantindo a privacidade, integridade e intimidade dos indivíduos, em consonância com a cibersegurança na preservação das informações e infraestrutura dentro do ciberespaço, gerando inúmeras possibilidades de danos decorrentes de sua manipulação inadequada ou indevida[171], (como discutidas no capítulo 3.3).

Ao cabo, se faz necessário mencionar sobre o Decreto nº 11.856, de 2023, que institui a Política Nacional de Cibersegurança (PNCiber), proposta pelo Gabinete de Segurança Institucional da Presidência da República (GSI/PR). A PNCiber estabelece um conjunto de diretrizes para fortalecer a governança cibernética no Brasil, atendendo às demandas de várias instituições e especialistas em cibersegurança, e adapta as melhores práticas internacionais à realidade e cultura institucional do País[172] [173].

Conforme mencionado pela Secretaria de Comunicação da Presidência da República a implementação da Política Nacional de Cibersegurança é considerada

---

170 SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) – l. 13.709/2018. **Revista direitos fundamentais & democracia**, [*S. l.*], v. 26, n. 2, p. 81-106, maio/ago. 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172/694. Acesso em: 08 nov. 2024.

171 *Ibid*.

172 O QUE É a Política Nacional de Cibersegurança: marco no combate aos crimes virtuais. *In*: SECRETARIA de Comunicação da Presidência da República. Brasília, DF, 29 dez. 2023. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/12/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais. Acesso em: 09 nov. 2024.

173 "Art. 2º São princípios da PNCiber: I - a soberania nacional e a priorização dos interesses nacionais; II - a garantia dos direitos fundamentais, em especial a liberdade de expressão, a proteção de dados pessoais, a proteção da privacidade e o acesso à informação; III - a prevenção de incidentes e de ataques cibernéticos, em particular aqueles dirigidos a infraestruturas críticas nacionais e a serviços essenciais prestados à sociedade; IV - a resiliência das organizações públicas e privadas a incidentes e ataques cibernéticos; V - a educação e o desenvolvimento tecnológico em segurança cibernética; VI - a cooperação entre órgãos e entidades, públicas e privadas, em matéria de segurança cibernética; e VII - a cooperação técnica internacional na área de segurança cibernética". BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança – PNCiber e dá outras providências. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 09 nov. 2024.

urgente e relevante, visto que o Brasil figura entre os países mais afetados por ataques cibernéticos. Um exemplo que é mencionado pelo artigo é o vazamento ocorrido em janeiro de 2021, no qual foram expostos dados de 220 milhões de CPFs e CNPJs[174].

Neste sentido, a PNCiber também prevê a criação do Comitê Nacional de Cibersegurança (CNCiber), composto por representantes do governo, da sociedade civil, de instituições científicas e de entidades do setor empresarial[175]. Esse comitê, com reuniões trimestrais[176], tem como função propor atualizações para a PNCiber e

---

174 Um estudo realizado pelo dfndr lab, laboratório de pesquisa de segurança da startup brasileira Psafe, revelou que houve o vazamento de dados de 220 milhões de CPFs no Brasil, um número superior à população brasileira atual, que é de 211,8 milhões de pessoas. Esse dado alarmante se deve ao fato de que, segundo auditoria realizada pelo Tribunal de Contas da União (TCU) no ano anterior, o Brasil possui 12,5 milhões de CPFs ativos a mais do que a população total. Assim, praticamente toda a população brasileira pode ter tido seus dados expostos. Conforme relatado pela Psafe, os dados acessados indevidamente incluíam informações pessoais como nome completo, data de nascimento e CPF, além de dados detalhados de ao menos 104 milhões de veículos, abrangendo número de chassi, placa, município, cor, marca, modelo e ano de fabricação. Além disso, também foram expostos dados de aproximadamente 40 milhões de empresas, contendo CNPJ, razão social, nome fantasia e data de fundação.A Psafe destacou que ainda não se sabe a origem do vazamento, ou seja, se foi causado por uma falha de segurança, tentativa de invasão ou acesso facilitado. A ausência de informações precisas sobre a forma do vazamento dificulta uma análise conclusiva sobre as causas. Além desse vazamento massivo de dados de CPF, outro incidente ocorreu em novembro do ano anterior, quando um vazamento de senhas dos sistemas do Ministério da Saúde deixou expostos, por quase um mês, dados de aproximadamente 16 milhões de brasileiros com diagnóstico suspeito ou confirmado de Covid-19. Esse vazamento foi resultado de uma lista com usuários e senhas publicada por um funcionário do Hospital Albert Einstein, de São Paulo, que tinha acesso aos dados devido a uma parceria em projeto com o Ministério da Saúde. Entre as informações expostas estavam CPF, endereço, telefone e doenças pré-existentes de diversas pessoas, incluindo políticos como o presidente Jair Bolsonaro e o governador de São Paulo, João Doria. EMPRESA afirma que vazamento expôs CPF de 220 milhões de brasileiros. *In*: CONJUR. [*S. l.*], 20 jan. 2021. Disponível em: https://www.conjur.com.br/2021-jan-20/empresa-afirma-vazamento-expos-cpf-220-milhoes/. Acesso em: 03 nov. 2024.

175 "Art. 7º O CNCiber será composto por representantes dos seguintes órgãos e entidades: I - um do Gabinete de Segurança Institucional da Presidência da República, que o presidirá; II - um da Casa Civil da Presidência da República; III - um da Controladoria-Geral da União; IV - um do Ministério da Ciência, Tecnologia e Inovação; V - um do Ministério das Comunicações; VI - um do Ministério da Defesa; VII - um do Ministério do Desenvolvimento, Indústria, Comércio e Serviços; VIII - um do Ministério da Educação; IX - um do Ministério da Fazenda; X - um do Ministério da Gestão e da Inovação em Serviços Públicos; XI - um do Ministério da Justiça e Segurança Pública; XII - um do Ministério de Minas e Energia; XIII - um do Ministério das Relações Exteriores; XIV - um do Banco Central do Brasil; XV - um da Agência Nacional de Telecomunicações - Anatel; XVI - um do Comitê Gestor da Internet no Brasil; XVII - três de entidades da sociedade civil com atuação relacionada à segurança cibernética ou à garantia de direitos fundamentais no ambiente digital; XVIII - três de instituições científicas, tecnológicas e de inovação relacionadas à área de segurança cibernética; e XIX - três de entidades representativas do setor empresarial relacionado à área de segurança cibernética [...]". BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança – PNCiber e dá outras providências. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 09 nov. 2024.

176 "[...] Art. 9º O CNCiber se reunirá, em caráter ordinário, trimestralmente e, em caráter extraordinário, mediante convocação de seu Presidente [...]". *Ibid*.

sugerir estratégias de cooperação técnica internacional, assim contribuindo para o fortalecimento de resiliência cibernética no país[177].

Da mesma forma como a ANAC dispõe em seu manual, além de Hurel (Capítulo 3.), a política da PNCiber possui como objetivos garantir a confidencialidade, a integridade, a autenticidade e a disponibilidade das soluções e dos dados utilizados para o processamento, o armazenamento e a transmissão eletrônica ou digital de informações; bem como fortalecer a atuação diligente no ciberespaço, especialmente das crianças, dos adolescentes e dos idosos, e desenvolver a educação e a capacitação técnico-profissional em segurança cibernética na sociedade[178].

Ao passo que, fundamentada nos princípios da soberania nacional e da garantia dos direitos fundamentais, para a Secretaria de Comunicação da Presidência da República, a PNCiber constitui um pilar essencial para medidas que aprimoram o combate aos crimes virtuais[179].

> O Plano Nacional de Cibersegurança desenha as ações a serem realizadas no longo, médio e curto prazo e orientam iniciativas práticas de modo que as estratégias estabelecidas sejam implementadas de maneira eficiente e alinhadas com a PNCiber

Enquanto a LGPD dispõe sobre a proteção de dados pessoais no Brasil, a Convenção de Budapeste trata da cooperação global e adequação das legislações sobre crimes cibernéticos, assim complementando a LGPD ao estender a proteção para além do território nacional. Portanto, torna-se imperativo tratar da referida convenção, o que será abordado no próximo capítulo.

4.3 O Decreto nº 11.491/2023 e a Lei Federal nº 13.709/2018: A Convenção de Budapeste como Complemento do Combate aos Crimes Cibernéticos

O Governo Federal do Brasil promulgou a Convenção sobre o Crime Cibernético, firmada em Budapeste. Com essa adesão, após convite do Conselho da

---

177 O QUE É a Política Nacional de Cibersegurança: marco no combate aos crimes virtuais. *In*: SECRETARIA de Comunicação da Presidência da República. Brasília, DF, 29 dez. 2023. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/12/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais. Acesso em: 09 nov. 2024.

178 *Ibid*.

179 *Ibid*.

Europa, onde o Brasil fortalece os laços de cooperação com parceiros estratégicos no combate aos crimes cibernéticos. O Decreto nº 11.491, que oficializa essa decisão, foi publicado no Diário Oficial da União (DOU) em 12 de abril de 2023[180].

A Convenção de Budapeste, assinada em 23 de outubro de 2001[181], oferece às autoridades brasileiras uma nova ferramenta para investigações de crimes cibernéticos e outras infrações que exigem a coleta de provas eletrônicas ou digitais armazenadas em outros países. Para o Ministério da Justiça e Segurança Pública, espera-se que essa colaboração resulte em uma atuação "[...] mais intensa, rápida e eficaz"[182].

Outrossim, os riscos decorrentes dos cibercrimes são amplamente diversificados, conforme visto no capítulo 3.1. No entanto, para Ana Maria Lumi Kamimura Murata e Paula Ritzmann Torres, a adjetivação de um delito como cibernético parece ocorrer menos pela natureza do bem jurídico protegido e mais pelo instrumento utilizado no crime. Para elas, a Convenção de Budapeste reflete essa visão, ao criminalizar uma variedade de condutas que surgiram na era digital, bem como outras já existentes que passaram a usar a internet como meio de execução, como acesso ilegal, interceptação ilícita, violação de dados, obstrução de acesso, uso indevido de aparelhagem, falsificação, fraude informática, pornografia infantil e violação de direitos autorais. Sendo o objetivo da Convenção combater a criminalidade cibernética e evitar abusos gerados por legislações menos rigorosas de determinados Estados, que podem impactar outros países[183].

Contudo, antes da adesão do Brasil à Convenção, o legislador brasileiro já havia seguido a tendência internacional, criminalizando algumas condutas mencionadas no texto da Convenção. Murata e Torres exemplificam o delito de invasão de dispositivo informático que foi incluído no Código Penal pelo art. 154-

---

180 CONVENÇÃO de Budapeste é promulgada no Brasil. *In*: MINISTÉRIO da Justiça e Segurança Pública. Brasília, DF, 17 abril 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 09 nov. 2024.

181 "Art. 1º Fica promulgada a Convenção sobre o Crime Cibernético, firmada em Budapeste, em 23 de novembro de 2001, anexa a este Decreto". BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 09 nov. 2024.

182 CONVENÇÃO [...], *op. cit*.

183 MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

A[184], por meio da Lei Federal nº 12.737/2012, também conhecida como Lei Carolina Dieckmann, e posteriormente modificado pela Lei Federal nº 14.155/2021[185].

Ao passo que, as autoras ainda exemplificam que a pornografia infantil, prevista no art. 241 do Estatuto da Criança e do Adolescente[186], foi criminalizada pela Lei Federal nº 11.829/2008. E a violação de direitos autorais, descrita no art. 184 do Código Penal, foi ajustada pela Lei Federal nº 10.695/2003[187]. Nesses casos, a Convenção de Budapeste tem aplicação imediata, pois já existem tipos penais equivalentes na legislação brasileira[188].

Não obstante, outros delitos cibernéticos, como o acesso não autorizado a redes ou sistemas, a obtenção ou divulgação indevida de dados pessoais, e a difusão de vírus, estavam inicialmente contemplados no Projeto de Lei nº 84/1999[189],

---

184 "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. § 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos". BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 09 nov. 2024.

185 MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

186 "Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa". BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 09 nov. 2024.

187 "Art. 184. Violar direitos de autor e os que lhe são conexos: Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa". BRASIL. **Lei nº 10.695, de 1º de julho de 2003**. Altera e acresce parágrafo ao art. 184 e dá nova redação ao art. 186 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal, alterado pelas Leis nos 6.895, de 17 de dezembro de 1980, e 8.635, de 16 de março de 1993, revoga o art. 185 do Decreto-Lei no 2.848, de 1940, e acrescenta dispositivos ao Decreto-Lei no 3.689, de 3 de outubro de 1941 – Código de Processo Penal. Brasília, DF: Presidência da República, 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.695.htm. Acesso em: 09 nov. 2024.

188 MURATA; TORRES, *op. cit*.

189 BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências. Autoria: Deputado Luiz Piauhylino. Brasília, DF: Câmara dos Deputados, [1999]. Disponível em:

mas não foram incluídos na Lei Federal nº 12.735/2012, também conhecida como Lei Azeredo, é uma lei que alterou o Código Penal, o Código Penal Militar e a Lei de Combate ao Racismo (Lei Federal nº 7.716/89). As autoras mencionam que ainda há projetos de lei em tramitação, como o PL 5.441/2020[190] e o PL 3.357/2015[191], que abordam cibercrimes e buscam cumprir os compromissos assumidos pelo Brasil na Convenção[192].

Para Murata e Torres, apesar do *status* de lei federal conferido à Convenção, a aplicação de algumas medidas continuam limitadas pela exigência do princípio da legalidade estrita, que demanda a complementação legal necessária para a definição precisa das condutas e penas a serem aplicadas[193].

Contudo, além da preocupação com a criação de um padrão para a criminalização dos delitos cibernéticos, a Convenção de Budapeste, em seu capítulo de Direito Penal, também estabelece formas de responsabilidade e sanções aplicáveis às pessoas jurídicas. No artigo 12 da Convenção, é prevista a responsabilidade das pessoas jurídicas por crimes cibernéticos[194].

> Art. 12. Responsabilidade Penal da Pessoa Jurídica
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que pessoas jurídicas possam ser consideradas penalmente responsáveis por crimes tipificados de acordo com esta Convenção, quando cometidos em seu benefício por qualquer pessoa física

---

https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028. Acesso em: 09 nov. 2024.

190 O Projeto de Lei 5.441/2020, de autoria do deputado David Soares, visa definir crimes cibernéticos e estabelecer suas respectivas penalidades. O projeto propõe alterações no Código Penal Brasileiro, incluindo a tipificação de condutas como a obtenção indevida de credenciais de acesso, sabotagem informática, fraude informatizada, entre outras ações relacionadas ao uso indevido de sistemas informatizados. Ele também prevê penas para a comercialização e divulgação de dados obtidos de forma ilícita, além de revogar os artigos 154-A e 154-B do Código Penal, que tratam de crimes de invasão de dispositivos informáticos. BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei nº 5.441, de 2020.** Define os crimes cibernéticos e dá outras providências. Autoria: Deputado David Soares. Brasília, DF: Câmara dos Deputados, [2020]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266423. Acesso em: 09 nov. 2024.

191 Dispõe sobre o crime de invadir dispositivo informático, sem a devida autorização, modificando conteúdo de sítio da internet. BRASIL. Congresso Nacional Câmara dos Deputados. **Projeto de Lei nº 3.357, de 2015.** Autoria: Deputado Vicentinho Junior. Brasília, DF: Câmara dos Deputados, [2015]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2024070. Acesso em: 09 nov. 2024.

192 MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

193 *Ibid*.

194 *Ibid*.

> em posição de direção, que aja individualmente ou como integrante de um órgão da própria pessoa jurídica, com base:
> a. no poder de representação da pessoa jurídica;
> b. na autoridade de tomar decisões em nome da pessoa jurídica;
> c. na autoridade de exercer controle interno na pessoa jurídica.
> 2. Além dos casos já previstos no parágrafo 1 deste Artigo, cada Parte tomará as medidas necessárias para assegurar que uma pessoa jurídica possa ser responsabilizada quando a falta de supervisão ou controle por uma pessoa natural dentre as referidas no parágrafo 1 deste Artigo tenha possibilitado o cometimento de um crime estabelecido de acordo com esta Convenção, por uma pessoa natural agindo sob autoridade dessa pessoa jurídica e em benefício dela.
> 3. Atendidos os princípios legais vigentes na Parte, a responsabilidade da pessoa jurídica pode ser civil, criminal ou administrativa.
> 4. Tal responsabilidade ocorrerá sem prejuízo da responsabilidade criminal das pessoas naturais que tenham cometido o crime[195].

No entanto, as autoras destacam que há uma diferença relevante entre o texto original em inglês, que usa o termo "*corporate liability*" sem especificar se essa responsabilidade é civil, penal ou administrativa, e a tradução adotada pelo Decreto nº 11.491/2023, que menciona a "responsabilidade penal da pessoa jurídica". Para elas, essa diferença na redação destaca uma aparente incompatibilidade entre as partes do decreto, que inicialmente fixa a responsabilidade como penal, mas posteriormente admite a possibilidade de responsabilidade civil, criminal ou administrativa, conforme a adequação aos princípios jurídicos de cada Estado-parte[196].

> Artigo 14 - Âmbito de aplicação dos dispositivos processuais
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para estabelecer os poderes e procedimentos previstos nesta seção para o fim específico de promover investigações ou processos criminais.

Assim, Murata e Torres enaltecem que a Convenção permite que cada Estado determine a forma de responsabilização que seja mais adequada ao seu ordenamento jurídico, possibilitando flexibilidade na aplicação. Além disso, estabelece dois tipos de responsabilidade para a pessoa jurídica: (i) quando um

---

195 BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 09 nov. 2024.

196 MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

crime for cometido em seu benefício por uma pessoa física em posição de direção, com base em seu poder de representação, autoridade para tomar decisões ou controle interno; e (ii) quando indivíduos, sem essas características, cometem crimes em benefício da pessoa jurídica, em razão de falha na supervisão ou controle por parte da organização. No segundo caso, o Conselho da Europa sugere que as medidas de controle esperadas devem ser avaliadas de acordo com o tipo de negócio, tamanho da empresa e melhores práticas, evitando que qualquer falha de supervisão resulte automaticamente em responsabilização[197].

Além disso, a Convenção determina que a responsabilidade da pessoa jurídica deve ocorrer sem prejuízo da responsabilidade criminal das pessoas físicas que cometeram o crime, e que as sanções aplicadas, sejam elas penais ou não, devem ser eficazes, proporcionais e dissuasivas. O modelo de responsabilidade previsto está fortemente ligado ao crime praticado pela pessoa física, o que reforça a ideia de uma responsabilidade penal, conforme previsto no decreto brasileiro[198].

> Artigo 12 - Responsabilidade penal da pessoa jurídica
> 1. Cada Parte adotará medidas legislativas e outras providências necessárias para assegurar que pessoas jurídicas possam ser consideradas penalmente responsáveis por crimes tipificados de acordo com esta Convenção, quando cometidos em seu benefício por qualquer pessoa física em posição de direção, que aja individualmente ou como integrante de um órgão da própria pessoa jurídica, com base:
> a. no poder de representação da pessoa jurídica;
> b. na autoridade de tomar decisões em nome da pessoa jurídica;
> c. na autoridade de exercer controle interno na pessoa jurídica.

Ao cabo que, para as autoras, a Convenção de Budapeste, levanta algumas considerações em relação à sua compatibilidade com o ordenamento jurídico brasileiro. Primeiramente, a Constituição Federal de 1988 prevê a responsabilidade penal da pessoa jurídica em dois dispositivos específicos. No art. 173, § 5º, a Constituição sujeita as pessoas jurídicas a punições compatíveis com sua natureza por atos praticados contra a ordem econômica e financeira, e contra a economia popular. O art. 225, § 3º, por sua vez, dispõe que condutas lesivas ao meio ambiente

---

197 MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

198 *Ibid*.

sujeitam infratores, sejam pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados[199].

> Art. 173. Ressalvados os casos previstos nesta Constituição, a exploração direta de atividade econômica pelo Estado só será permitida quando necessária aos imperativos da segurança nacional ou a relevante interesse coletivo, conforme definidos em lei. [...] § 5º A lei, sem prejuízo da responsabilidade individual dos dirigentes da pessoa jurídica, estabelecerá a responsabilidade desta, sujeitando-a às punições compatíveis com sua natureza, nos atos praticados contra a ordem econômica e financeira e contra a economia popular. [...] Art. 225. Todos têm direito ao meio ambiente ecologicamente equilibrado, bem de uso comum do povo e essencial à sadia qualidade de vida, impondo-se ao Poder Público e à coletividade o dever de defendê-lo e preservá-lo para as presentes e futuras gerações. [...] § 3º As condutas e atividades consideradas lesivas ao meio ambiente sujeitarão os infratores, pessoas físicas ou jurídicas, a sanções penais e administrativas, independentemente da obrigação de reparar os danos causados [...].

Dessa forma, para as autoras, a Constituição prevê expressamente a responsabilização penal de entes coletivos em relação a determinados bens jurídicos, o que pode abrir espaço para que condutas relacionadas a cibercrimes sejam incluídas nessa forma de responsabilidade prevista no decreto[200].

Por outro lado, as autoras entendem que o tema da responsabilidade penal da pessoa jurídica no Brasil ainda é controverso, em grande parte devido ao princípio histórico do brocardo "*societas delinquere non potest*"[201] e às dificuldades dogmáticas para compatibilizar essa responsabilidade com os princípios do Direito Penal brasileiro. Para elas, o desenvolvimento teórico dessa responsabilidade afastou a ideia de imputação por transferência ou heterorresponsabilidade, admitindo-se, conforme o princípio da culpabilidade, apenas um modelo de autorresponsabilidade[202].

No caso da Convenção de Budapeste, a responsabilidade da pessoa jurídica está atrelada aos crimes praticados por seus gestores ou diretores, mas também estabelece que o indivíduo envolvido deve ser punido. Isso cria uma responsabilidade que pode ser vista como por "ricochete" ou transferência, onde a conduta dolosa de uma pessoa física resulta na punição tanto do indivíduo quanto

---

199 MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

200 *Ibid*.

201 "*Societas delinquere non potest*": A sociedade não pode delinquir.

202 MURATA; TORRES, *op. cit*.

do ente coletivo, o que poderia incorrer em *bis in idem*[203]. Na segunda hipótese, de responsabilidade por ausência ou deficiência de controle, aproximar-se-ia de uma verdadeira responsabilidade da pessoa jurídica, porém, ainda carece de fundamentação dogmática para justificar essa exigência de controle por parte do ente coletivo[204].

Logo, entende-se as autoras Ana Maria Lumi Kamimura Murata e Paula Ritzmann Torres entendem que, embora o Brasil já tenha criminalizado várias condutas previstas na Convenção de Budapeste, ainda há lacunas que requerem complementação legislativa específica, particularmente para assegurar a definição precisa das condutas e a aplicação das sanções de acordo com o princípio da legalidade estrita. As autoras ainda observam que, apesar do *status* de lei federal conferido à Convenção, sua implementação plena demanda ajustes legais internos para ser verdadeiramente eficaz no combate à criminalidade cibernética.

Dessarte, esses aspectos indicam que o tema é passível de uma ampla discussão, envolvendo tanto questões substanciais sobre as teorias de responsabilidade penal da pessoa jurídica (em especial quanto às sanções e dosimetria) quanto processuais, relacionadas ao rito de responsabilização[205]. Contudo, é importante destacar que esta monografia não tem o intuito de abordar tais aspectos. Ainda assim, entende-se que ordenamento jurídico brasileiro já possui um conjunto significativo de legislações que possibilitam uma atuação relevante no combate aos crimes cibernéticos que assolam a aviação. Porquanto, no próximo capítulo da presente monografia, será abordada competência e o papel do Estado relacionados à aviação.

---

203 "*Bis in idem*": dupla punição pelo mesmo fato.

204 MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

205 *Ibid*.

5 DAS COMPETÊNCIAS E O PAPEL DO ESTADO

Como visto anteriormente, o poder público desempenha o papel central na prevenção e punição de crimes cibernéticos. Além disso, o governo tem a responsabilidade de promover a conscientização pública bem como fomentar recursos para a segurança cibernética e estabelecer políticas que incentivem a adoção de boas práticas. À vista disso, faz-se necessário uma análise sobre a competência para processar e julgar crimes cibernéticos cometidos a bordo de aeronaves ou em aeroportos à luz da CF de 1988, bem como a responsabilidade do Estado frente ao problema discutido na presente monografia.

5.1 Análise da competência para processar e julgar à luz da Constituição Federal de 1988

Conforme analisado nos capítulos anteriores, foram abordadas bastantes leis, decretos e regulamentações que estruturam a aviação e o direito aeronáutico no Brasil. No entanto, o presente capítulo tem como objetivo analisar a competência para processar e julgar casos que envolvam a aviação. Deste modo, observa-se que a Constituição Federal de 1988, em seus artigos 21, 22 e 178, estabelece que compete à União, de forma exclusiva, legislar e explorar as atividades relacionadas à navegação aérea e à infraestrutura aeroportuária.

> Art. 21. Compete à União: [...] XII – explorar, diretamente ou mediante autorização, concessão ou permissão; [...] c) a navegação aérea, aeroespacial e a infra-estrutura aeroportuária; [...] Art. 22. Compete privativamente à União legislar sobre: I – direito civil, comercial, penal, processual, eleitoral, agrário, marítimo, aeronáutico, espacial e do trabalho; [...] X - regime dos portos, navegação lacustre, fluvial, marítima, aérea e aeroespacial; [...] Art. 178. A lei disporá sobre a ordenação dos transportes aéreo, aquático e terrestre, devendo, quanto à ordenação do transporte internacional, observar os acordos firmados pela União, atendido o princípio da reciprocidade.

À vista disso, o texto constitucional apresenta três conceitos essenciais sobre a regulação da aviação no Brasil. Em primeiro lugar, a aviação é uma matéria de competência exclusiva da União[206], o que significa que Estados e Municípios não

---

206 "Art. 21. Compete à União: [...] XI - explorar, diretamente ou mediante autorização, concessão ou permissão, os serviços de telecomunicações, nos termos da lei, que disporá sobre a organização dos serviços, a criação de um órgão regulador e outros aspectos institucionais; [...] c) a navegação aérea, aeroespacial e a infra-estrutura aeroportuária; [...] Art. 22. Compete

possuem permissão para legislar sobre o tema, nem mesmo de forma concorrente ou supletiva. Não obstante, a União pode delegar a gestão de determinados equipamentos a Estados e Municípios, como já ocorreu com rodovias e portos, conforme autorizado pela Lei Federal nº 9.277/1996[207] [208].

Em segundo lugar, os serviços aéreos e aeroportuários podem ser regulados tanto pelo regime de direito público quanto pelo de direito privado, cabendo essa decisão ao legislador ordinário. No regime de direito público, aplicam-se os institutos da concessão ou permissão[209] [210], tratando-se de serviços públicos, enquanto no

---

privativamente à União legislar sobre: [...] X - regime dos portos, navegação lacustre, fluvial, marítima, aérea e aeroespacial; [...]". BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 nov. 2024.

207 "Art. 1º Fica a União, por intermédio do Ministério dos Transportes, autorizada a delegar, pelo prazo de até vinte e cinco anos, prorrogáveis por até mais vinte e cinco, aos municípios, estados da Federação ou ao Distrito Federal, ou a consórcio entre eles, a administração de rodovias e exploração de trechos de rodovias, ou obras rodoviárias federais". BRASIL. **Lei nº 9.277, de 10 de maio de 1996**. Autoriza a União a delegar aos municípios, estados da Federação e ao Distrito Federal a administração e exploração de rodovias e portos federais. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9277.htm. Acesso em: 09 nov. 2024.

208 PINTO, Victor Carvalho. **O marco regulatório da aviação civil:** elementos para a reforma do Código Brasileiro de Aeronáutica. Brasília, DF: Senado Federal, 2008. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-42-o-marco-regulatorio-da-aviacao-civil-elementos-para-a-reforma-do-codigo-brasileiro-de-aeronautica/view. Acesso em: 08 nov. 2024.

209 "Art. 175. Incumbe ao Poder Público, na forma da lei, diretamente ou sob regime de concessão ou permissão, sempre através de licitação, a prestação de serviços públicos. Parágrafo único. A lei disporá sobre: I - o regime das empresas concessionárias e permissionárias de serviços públicos, o caráter especial de seu contrato e de sua prorrogação, bem como as condições de caducidade, fiscalização e rescisão da concessão ou permissão; II - os direitos dos usuários; III - política tarifária; IV - a obrigação de manter serviço adequado". BRASIL. **Lei nº 8.987, de 13 de fevereiro de 1995.** Dispõe sobre o regime de concessão e permissão da prestação de serviços públicos previsto no art. 175 da Constituição Federal, e dá outras providências. Brasília, DF: Presidência da República 1995. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8987cons.htm. Acesso em: 09 nov. 2024.

210 "Art. 2º Para os fins do disposto nesta Lei, considera-se: I - poder concedente: a União, o Estado, o Distrito Federal ou o Município, em cuja competência se encontre o serviço público, precedido ou não da execução de obra pública, objeto de concessão ou permissão; II - concessão de serviço público: a delegação de sua prestação, feita pelo poder concedente, mediante licitação, na modalidade concorrência ou diálogo competitivo, a pessoa jurídica ou consórcio de empresas que demonstre capacidade para seu desempenho, por sua conta e risco e por prazo determinado; III - concessão de serviço público precedida da execução de obra pública: a construção, total ou parcial, conservação, reforma, ampliação ou melhoramento de quaisquer obras de interesse público, delegados pelo poder concedente, mediante licitação, na modalidade concorrência ou diálogo competitivo, a pessoa jurídica ou consórcio de empresas que demonstre capacidade para a sua realização, por sua conta e risco, de forma que o investimento da concessionária seja remunerado e amortizado mediante a exploração do serviço ou da obra por prazo determinado; IV - permissão de serviço público: a delegação, a título precário, mediante licitação, da prestação de serviços públicos, feita pelo poder concedente à pessoa física ou jurídica que demonstre capacidade para seu desempenho, por sua conta e risco". *Ibid*.

regime de direito privado, aplica-se o instituto da autorização, caracterizando-se como atividade econômica[211].

Em terceiro lugar, o princípio da reciprocidade deve ser observado pela União ao negociar acordos internacionais relacionados à aviação. Portanto, o Brasil não pode permitir que empresas estrangeiras operem rotas internacionais se as empresas brasileiras não receberem o mesmo tratamento no país de origem dessas empresas estrangeiras. Contudo, essa exigência de reciprocidade não se aplica ao transporte doméstico[212].

Porquanto, atribui-se à União a competência exclusiva para legislar e explorar as atividades de navegação aérea e infraestrutura aeroportuária, conforme preceitua o art. 22, inciso X[213], da Constituição Federal de 1988. Ao passo que, se faz necessário distinguir a competência jurisdicional para o ajuizamento de ações relacionadas a tais questões. Neste sentido, a Súmula 150 do Superior Tribunal de Justiça dispõe que: “Compete à Justiça Federal decidir sobre a existência de interesse jurídico que justifique a presença, no processo, da união, suas autarquias ou empresas públicas”.

Assim, entende-se que Justiça Federal é competente para julgar ações que envolvem diretamente as companhias aéreas, a ANAC como agência reguladora da administração federal indireta e outros entes federais, com base no art. 109, inciso I, da Constituição Federal, que estabelece a competência da Justiça Federal para questões envolvendo a União e suas autarquias.

> Art. 109. Aos juízes federais compete processar e julgar:
> I - as causas em que a União, entidade autárquica ou empresa pública federal forem interessadas na condição de autoras, rés, assistentes ou oponentes, exceto as de falência, as de acidentes de trabalho e as sujeitas à Justiça Eleitoral e à Justiça do Trabalho; [...]

---

211 PINTO, Victor Carvalho. **O marco regulatório da aviação civil:** elementos para a reforma do Código Brasileiro de Aeronáutica. Brasília, DF: Senado Federal, 2008. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-42-o-marco-regulatorio-da-aviacao-civil-elementos-para-a-reforma-do-codigo-brasileiro-de-aeronautica/view. Acesso em: 08 nov. 2024.

212 *Ibid*.

213 “Art. 22. Compete privativamente à União legislar sobre: [...] X - regime dos portos, navegação lacustre, fluvial, marítima, aérea e aeroespacial; [...]”. BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 nov. 2024.

Por outro lado, há um ponto importante a ser mencionado, visto que, se a ação estiver relacionada exclusivamente à administração do aeroporto, especialmente contra concessionárias privadas, como o GRU Airport, sem envolver diretamente a União ou suas autarquias, a competência poderá recair sobre a Justiça Estadual, conforme o entendimento majoritário dos tribunais[214] e o disposto no art. 109[215] da Constituição Federal, que regula a competência da Justiça Estadual.

Neste sentido, a decisão do Tribunal Regional Federal da 5ª Região (TRF-5) ao analisar um agravo de instrumento interposto pela Ferrovia Transnordestina Logística S.A. (FTL), concessionária de serviço público ferroviário, contra uma decisão que declarou a incompetência da Justiça Federal para julgar uma ação possessória. No entendimento do Tribunal, a competência da Justiça Federal não é atraída automaticamente pela participação da FTL, já que a empresa é concessionária e possuidora direta dos bens, o que a torna responsável por adotar medidas para proteger seu patrimônio sem necessidade de participação da União ou de suas autarquias, que, no caso, manifestaram desinteresse na demanda. Assim, o

---

214 BRASIL. Tribunal Regional Federal. **Agravo de instrumento 081128254.2022.4.05.0000**. Civil e processo civil. Administrativo. Ação possessória. Contrato de arrendamento [...]. 7ª Turma. Relatora: Des. Germana de Oliveira Moraes, 31 de janeiro de 2023. Disponível em: https://pje.trf5.jus.br/pjeconsulta/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?idProcessoDocumento=02772ed042ea5ab75e27c3d0298e2ccc#. Acesso em: 11 nov. 2024.

215 “Art. 109. Aos juízes federais compete processar e julgar: I - as causas em que a União, entidade autárquica ou empresa pública federal forem interessadas na condição de autoras, rés, assistentes ou oponentes, exceto as de falência, as de acidentes de trabalho e as sujeitas à Justiça Eleitoral e à Justiça do Trabalho; II - as causas entre Estado estrangeiro ou organismo internacional e Município ou pessoa domiciliada ou residente no País; III - as causas fundadas em tratado ou contrato da União com Estado estrangeiro ou organismo internacional; IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral; V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente; V - A as causas relativas a direitos humanos a que se refere o § 5º deste artigo; VI - os crimes contra a organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômico-financeira; VII - os *habeas corpus* , em matéria criminal de sua competência ou quando o constrangimento provier de autoridade cujos atos não estejam diretamente sujeitos a outra jurisdição; VIII - os mandados de segurança e os *habeas data* contra ato de autoridade federal, excetuados os casos de competência dos tribunais federais; IX - os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar; X - os crimes de ingresso ou permanência irregular de estrangeiro, a execução de carta rogatória, após o ‘exequatur’, e de sentença estrangeira, após a homologação, as causas referentes à nacionalidade, inclusive a respectiva opção, e à naturalização; XI - a disputa sobre direitos indígenas” [...]”. BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 nov. 2024.

Tribunal entende que é competência da Justiça Estadual, considerando que, em concessões de serviço público, cabe à concessionária defender a posse dos bens arrendados sem que isso, por si só, implique competência federal.

Portanto, neste sentido e embora não tenha sido encontrado um julgado específico envolvendo aeroportos, o caso citado serve como exemplo para ilustrar a competência da Justiça Estadual em situações semelhantes. No caso da Ferrovia Transnordestina Logística S.A., trata-se de uma concessionária de serviço público ferroviário em uma ação possessória, o que não envolve diretamente questões de aviação ou aeroportos. Contudo, a decisão é pertinente para demonstrar que a Justiça Federal não é automaticamente competente apenas pela natureza de concessão do serviço público, sendo possível que a competência recaia sobre a Justiça Estadual quando não há envolvimento direto da União ou de suas autarquias no litígio, como supracitado nos parágrafos anteriores.

Portanto, ressalta-se que, no contexto de cibersegurança na aviação, a competência para julgar demandas relacionadas a incidentes cibernéticos dependerá diretamente da parte envolvida e da natureza do litígio. A Justiça Federal será competente para processar e julgar ações que envolvam a União, suas autarquias, como a ANAC, ou questões reguladas pela Lei Federal nº 7.565/1986. Além de, por exemplo, casos de ciberataques que atinjam companhias aéreas, sistemas de controle de tráfego aéreo ou outras infraestruturas críticas de responsabilidade federal.

Por outro prisma, a Justiça Estadual poderá ser competente em situações em que o litígio envolva concessionárias privadas que administram aeroportos em casos em que não haja o envolvimento direto da União ou de suas autarquias, como a ANAC. Nesses casos, incidentes cibernéticos que impactem apenas a infraestrutura aeroportuária, sem afetar diretamente a navegação aérea ou questões de competência federal, poderão ser tratados pela esfera estadual.

Adiante, serão abordados os princípios da precaução e da prevenção, com ênfase na aplicação da cibersegurança na aviação civil brasileira, como possível solução do problema em questão, conforme entendimento das autoras Sales Sarlet e Linden Ruaro vistos no Capítulo 4.2.

5.2 Análise dos Princípios da Precaução e da Prevenção com ênfase na aplicação da cibersegurança na Aviação Civil Brasileira

Niklas Luhmann aborda o conceito de risco com ênfase na necessidade de compreender a complexidade inerente às decisões e suas consequências. O autor destaca que a sociedade moderna se caracteriza pela percepção de um futuro incerto, onde o risco surge justamente em função da dependência crescente das decisões humanas. Nessa perspectiva, as noções de prevenção e precaução se mostram fundamentais, uma vez que, o risco é, por definição, resultado de escolhas conscientes e está relacionado à possibilidade de danos que poderiam ser evitados caso decisões diferentes fossem tomadas[216].

Além disso, para Beck, embora a modernidade traga novas formas de ameaça que se apresentam através de complexas fórmulas científicas e diagnose médica, isso não as torna menos perigosas. Pelo contrário, as ameaças contemporâneas são difíceis de compreender e antecipar, escapando da percepção comum e exigindo conhecimento especializado[217]. Nas palavras dele:

> Intencionalmente ou não, por acidente ou catástrofe, em paz ou guerra, entram nas casas de um amplo setor da população calamidades e destruições diante das quais nos fogem as palavras, fracassa a imaginação e falha todo e qualquer conceito médico e moral[218].

Para Beck, a suscetibilidade às ameaças modernas é fundamentalmente diferente das antigas vulnerabilidades de classe. No passado, a consciência era determinada pelo ser, ou seja, pela experiência direta da miséria e das condições materiais que marcavam a vida dos indivíduos desde a juventude até a velhice, vinculando-se inevitavelmente ao destino de classe. Ele exemplifica dispondo que nas situações de classe, o potencial ameaçador, como a perda do emprego, é evidente para os afetados, dispensando instrumentos cognitivos especiais ou amostragens estatísticas. Contudo, na contemporaneidade, alguém que descobre DDT em seu chá ou formaldeído em sua cozinha não consegue, com seus próprios

---

216 DAVID, Marília Luz. Sobre os conceitos de risco em Luhmann e Giddens. **Em tese**, Florianópolis, v. 8, n. 1, p. 30-47, jan./jul. 2011. Disponível em: https://periodicos.ufsc.br/index.php/emtese/article/view/1806-5023.2011v8n1p30. Acesso em: 09 nov. 2024.

217 BECK, Ulrich. **Sociedade de risco**: rumo a uma Outra Modernidade. 2. ed. São Paulo: Editora 34, 2011. p. 62.

218 *Ibid*., p. 62.

meios cognitivos, decidir se e em que concentrações isso é perigoso, tornando-se dependente de conhecimentos externos para compreender sua própria vulnerabilidade[219].

E, portanto, para Beck, os indivíduos perdem soberania sobre sua capacidade de julgamento e se tornam incompetentes para avaliar suas próprias vulnerabilidades, submetendo-se às controvérsias e métodos dos produtores de conhecimento. Assim, a percepção de riscos transforma objetos cotidianos em "cavalos de Troia", carregando perigos que apenas os especialistas podem anunciar ou mitigar, o que evidencia a complexidade das ameaças modernas e a dificuldade de escapar à dependência cognitiva[220]. Em suas palavras:

> Em situações de ameaça, consequentemente, as coisas da vida cotidiana convertem-se, praticamente da noite pro dia, em 'cavalo de Troia', do qual se precipitam os perigos, e com eles os especialistas do risco, para anunciar, em meio a pelejas mútuas, do que é que se deve ter medo e do que não[221].

Luhmann explica que, em vez de buscar uma seguridade absoluta, a sociedade deve reconhecer a impossibilidade de eliminar completamente os riscos, mesmo com o aprimoramento das informações e das ferramentas de cálculo. Isso ocorre porque, quanto mais se desenvolvem métodos de gestão do risco, mais aumentam as incertezas, visto que surgem novos aspectos e vulnerabilidades não previstas. Dessa forma, a busca pela seguridade acaba revelando ainda mais riscos[222].

Ao passo que, o autor diferencia entre risco e perigo, enfatizando que a prevenção e a precaução devem ser aplicadas principalmente em situações de risco, onde há uma consciência clara do possível dano decorrente das ações humanas. Já os perigos são entendidos como danos que provêm de causas externas e incontroláveis. Essa distinção sublinha a responsabilidade de quem toma decisões,

---

219 BECK, Ulrich. **Sociedade de risco**: rumo a uma Outra Modernidade. 2. ed. São Paulo: Editora 34, 2011. p. 64.

220 *Ibid*., p. 64.

221 *Ibid*., p. 64.

222 DAVID, Marília Luz. Sobre os conceitos de risco em Luhmann e Giddens. **Em tese**, Florianópolis, v. 8, n. 1, p. 30-47, jan./jul. 2011. Disponível em: https://periodicos.ufsc.br/index.php/emtese/article/view/1806-5023.2011v8n1p30. Acesso em: 09 nov. 2024.

reforçando a relevância de uma postura preventiva para mitigar os danos potenciais[223].

Luhmann também discute as dificuldades relacionadas à atribuição de responsabilidades no contexto da gestão de riscos, evidenciando que a complexidade social e a interdependência das decisões tornam desafiador rastrear as causas diretas dos danos. Ele observa que a tentativa de controlar racionalmente os riscos é limitada, pois consequências não-desejadas frequentemente surgem e precisam ser consideradas. Essa realidade exige uma abordagem baseada no princípio da precaução, na qual as decisões são tomadas com o devido reconhecimento das incertezas e dos possíveis impactos futuros, mesmo que não haja certeza sobre a ocorrência de danos[224].

Ao cabo, Luhmann dispõe que a prevenção não pode ser vista como um esforço de eliminação total dos riscos, mas sim como uma gestão informada e consciente, que considera a multiplicidade de fatores que influenciam os resultados. O autor defende que, em uma sociedade onde a racionalidade nunca é completamente suficiente para garantir segurança, a precaução se torna um imperativo necessário, ainda que as decisões continuem envolvendo riscos inevitáveis e incalculáveis[225].

Neste mesmo sentido, para Gabriel Wedy, este princípio se aplica em situações em que há evidências científicas claras e robustas que indicam a probabilidade de ocorrência de um determinado risco. Assim, atua-se de forma preventiva em face de eventos cuja materialização é quase certa ou altamente provável, buscando minimizar seus impactos negativos[226].

Por outro lado, o princípio da precaução se destina a contextos de incerteza científica, ou seja, quando os riscos não são plenamente conhecidos ou prováveis, mas ainda assim há indícios suficientes para justificar a adoção de medidas cautelosas. Ele se concentra em evitar danos graves ou irreversíveis, mesmo que

---

223 DAVID, Marília Luz. Sobre os conceitos de risco em Luhmann e Giddens. **Em tese**, Florianópolis, v. 8, n. 1, p. 30-47, jan./jul. 2011. Disponível em: https://periodicos.ufsc.br/index.php/emtese/article/view/1806-5023.2011v8n1p30. Acesso em: 09 nov. 2024.

224 *Ibid*.

225 *Ibid*.

226 WEDY, Gabriel. Princípios diferentes: Precaução no Direito Ambiental não quer dizer o mesmo que prevenção. *In*: CONSULTOR jurídico. [*S. l.*], 30 maio 2014. Disponível em: https://www.conjur.com.br/2014-mai-30/gabriel-wedy-precaucao-direito-ambiental-nao-prevencao. Acesso em: 09 nov. 2024.

não haja certeza científica sobre a sua ocorrência. Esse princípio é amplamente adotado no direito ambiental, justamente por lidar com situações em que os danos ao meio ambiente, em muitos casos, podem ser irreversíveis ou de difícil reparação, exigindo uma postura mais cuidadosa e protetiva em face da incerteza[227]. Nesse sentido, Wedy ensina:

> A prevenção tem por finalidade a adoção de ações ou de inações para evitar eventos previsíveis; já o princípio da precaução visa a gerir riscos em princípio não prováveis por completo. O princípio da prevenção visa a inibir o dano potencial sempre indesejável, e o princípio da precaução visa a impedir o risco de perigo abstrato. Quando se aborda o princípio da prevenção, deve-se passar da avaliação de risco de perigo – utilizada na análise do princípio da precaução – para a avaliação de concreto e forte risco de dano[228].

Destarte, tendo em vista a crescente complexidade dos riscos contemporâneos, marcada por avanços tecnológicos e a globalização, demanda uma abordagem jurídica que contemple a prevenção e a precaução como princípios fundamentais. Nesse contexto, Ulrich Beck ensina que vivemos em uma “sociedade de risco” permeada por ameaças invisíveis e de alta complexidade, que exigem políticas preventivas mesmo diante da incerteza quanto à extensão ou aos efeitos dessas ameaças. Complementando essa visão, Niklas Luhmann destaca a relevância da comunicação e do conhecimento especializado para a gestão dos riscos, enfatizando que as decisões a esse respeito transcendem a esfera técnica, repercutindo diretamente na esfera social, influenciando a percepção pública e a confiança nas instituições.

Em que pese no campo da cibersegurança, especialmente no tema da presente monografia, a aviação civil, os princípios da prevenção e da precaução são imprescindíveis. Como sustentam Sales Sarlet e Linden Ruaro, o risco, por definição, é o resultado de escolhas conscientes, e, no ambiente digital, uma atuação preventiva é importante para proteger dados sensíveis e a dignidade da pessoa humana. Ao passo que, como tratado por Gabriel Wedy, o princípio da prevenção visa evitar a ocorrência de danos previsíveis, impondo medidas para mitigar riscos já conhecidos, enquanto o princípio da precaução lida com a incerteza,

---

227 WEDY, Gabriel. Princípios diferentes: Precaução no Direito Ambiental não quer dizer o mesmo que prevenção. *In*: CONSULTOR jurídico. [*S. l.*], 30 maio 2014. Disponível em: https://www.conjur.com.br/2014-mai-30/gabriel-wedy-precaucao-direito-ambiental-nao-prevencao. Acesso em: 09 nov. 2024.

228 *Ibid*.

requerendo ações diante de ameaças ainda não totalmente comprovadas, mas que podem gerar danos irreversíveis.

A relevância desses princípios para a aviação civil, um setor estratégico e de alta sensibilidade, não pode ser subestimada. Assim como no direito ambiental, onde se busca evitar catástrofes irreversíveis, é necessário que a aviação adote uma postura cautelosa frente às ameaças cibernéticas. Ainda que não se conheça toda a extensão desses riscos, as consequências de um ataque podem ser devastadoras para a segurança dos passageiros e a continuidade das operações aéreas. Nesse sentido, a proteção da dignidade da pessoa humana e dos dados sensíveis no ambiente digital exige a integração dos princípios da prevenção e da precaução na estrutura jurídica, como defendem Sarlet e Ruaro.

Por fim, a discussão se encaminha para a análise da responsabilidade do Estado frente à estrutura regulatória existente e a necessidade de promover a educação digital como forma de prevenir ataques cibernéticos no setor de aviação civil, tema que será aprofundado no próximo capítulo.

5.3 Da responsabilidade do Estado frente à estrutura regulatória e a estimulação em educação digital e prevenção de ataques cibernéticos na Aviação Civil Brasileira

Evilázio Teixeira analisa a perspectiva de Platão sobre a educação enquanto responsabilidade fundamental do Estado. Teixeira argumenta que, segundo Platão, a educação pública deve ser administrada pelo Estado e direcionada ao bem da sociedade como um todo, não apenas ao desenvolvimento individual dos cidadãos. Para Platão, a tarefa de educar não cabe unicamente aos indivíduos ou às famílias, mas ao Estado, que, em sua concepção, desempenha um papel central na formação moral e social do indivíduo. A educação é vista, assim, como um elemento vital para que o cidadão não apenas participe da vida pública, mas também contribua para a justiça e harmonia social, pilares essenciais de uma sociedade ideal[229].

Ao passo que, a abordagem de Platão coloca a educação e o Estado em uma interdependência, onde um sustenta o outro para que ambos prosperem. O filósofo destaca que a educação pública e a participação cidadã são de suma importância

[229] COSTA, César Augusto Soares da. A educação enquanto responsabilidade do Estado. **Educação**, Porto Alegre, v. 32, n. 2, p. 236-237, maio/ago. 2009. Disponível em: https://revistaseletronicas.pucrs.br/faced/article/view/5526/4021. Acesso em: 09 nov. 2024.

para o desenvolvimento moral, e só se atinge a perfeição do Estado quando os cidadãos, orientados por um sistema educacional ético, alcançam também sua própria perfeição. Não obstante, Teixeira reforça que, para Platão, a justiça se manifesta na organização justa da sociedade, onde cada pessoa ocupa seu lugar de maneira harmoniosa, promovendo, dessa forma, a felicidade coletiva. Dessa forma, a reflexão sobre o papel do Estado na educação transcende as esferas individualistas e passa a ser um compromisso moral, estabelecendo-se como um alicerce para a construção de uma sociedade justa e virtuosa[230].

Além disso, cumpre mencionar que a Constituição Federal de 1988 consagra a educação como um direito fundamental e dever do Estado, reconhecendo-a como pilar para o desenvolvimento social e instrumento essencial para a promoção da cidadania e igualdade[231].

Dessa forma, a Constituição Federal atribui ao Estado o dever inalienável de assegurar o acesso universal e de qualidade à educação, reconhecendo-a como direito de todos. Fundamentada nos princípios constitucionais da dignidade da pessoa humana, da igualdade e da justiça social, a educação figura como um dos pilares para a formação da cidadania e para a promoção do desenvolvimento social. Compreendida a responsabilidade do Estado na garantia da educação, faz-se necessário abordar a questão da cibersegurança, um tema ainda pouco conhecido e discutido no Brasil, especialmente em âmbito educacional e social.

Conforme pesquisa da Kaspersky, aponta para um desconhecimento alarmante por parte dos brasileiros sobre a LGPD o Brasil ocupa a liderança entre os países pesquisados em relação à falta de conhecimento sobre esses direitos, com 20% dos brasileiros admitindo desconhecê-los, seguido por Chile (16%), Argentina

---

230 COSTA, César Augusto Soares da. A educação enquanto responsabilidade do Estado. **Educação**, Porto Alegre, v. 32, n. 2, p. 236-237, maio/ago. 2009. Disponível em: https://revistaseletronicas.pucrs.br/faced/article/view/5526/4021. Acesso em: 09 nov. 2024.

231 "Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho. Art. 206. O ensino será ministrado com base nos seguintes princípios: I – igualdade de condições para o acesso e permanência na escola; [...] Art. 208. O dever do Estado com a Educação será efetivado mediante a garantia de: [...] III - atendimento educacional especializado aos portadores de deficiência, preferencialmente na rede regular de ensino; [...] IV - atendimento em creche e pré-escola às crianças de 0 a 6 anos de idade. [...] Art. 213. Os recursos públicos serão destinados às escolas, podendo ser dirigidos a escolas comunitárias, confessionais ou filantrópicas, definidas em lei, que: I – comprovem finalidade não lucrativa e apliquem seus excedentes financeiros em educação". BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 nov. 2024.

(15%) e Colômbia (10%). Para o especialista Roberto Rebouças, gerente-executivo da Kaspersky no Brasil, esse desconhecimento é agravado pelo fato de que muitos brasileiros (40%) não sabem sequer como os dados são coletados na internet, o que torna a conscientização sobre a privacidade um passo fundamental para a proteção de dados[232].

Ainda segundo a pesquisa, assim como para a ANAC, a negligência dos funcionários configura-se como a principal vulnerabilidade das redes corporativas, seja pela falta de atualização de programas, contas comprometidas ou cliques em *links* maliciosos, o que pode resultar em vazamentos de dados sensíveis e penalidades para as empresas, incluindo multas e até proibições de tratamento de dados. Rebouças ressalta que a educação em cibersegurança nas empresas é essencial, uma vez que o erro humano é frequentemente o elo mais fraco na cadeia de proteção e pode impactar diretamente na integridade das informações corporativas e na segurança digital da organização[233].

Ainda nesta seara, o representante da empresa de segurança cibernética Trellix, Rafael Gonçalves, também entende que o maior desafio enfrentado pelas empresas atualmente é o elevado volume de eventos de segurança e a escassez de mão de obra qualificada, especialmente na área de cibersegurança. Ele mencionou um estudo da PUC Campinas que revelou um déficit de 500 mil pessoas capacitadas em tecnologia no Brasil, das quais 140 mil seriam necessárias no campo da cibersegurança. Segundo Gonçalves, é necessário integrar diferentes sistemas tecnológicos, independentemente da plataforma ou do fabricante, e criar uma agência que possa coordenar e padronizar ações de cibersegurança, tanto no setor público quanto no privado, dispondo a falta de priorização e padronização nas empresas[234].

Dentre estes motivos, houve uma audiência pública sobre os riscos internacionais à segurança digital, promovida pela Subcomissão Permanente de Defesa Cibernética, destacou-se que o Fórum Econômico Mundial (WEF) que

---

232 PESQUISA da Kaspersky revela que 20% dos brasileiros não têm conhecimento sobre a LGPD. *In*: KASPERSKY. [*S. l.*], 14 nov. 2024. Disponível em: https://www.kaspersky.com.br/about/press-releases/pesquisa-da-kaspersky-revela-que-20-dos-brasileiros-nao-tem-conhecimento-sobre-a-lgpd. Acesso em: 09 nov. 2024.

233 *Ibid*.

234 CIBERSEGURANÇA deve ter agência estatal com parceria privada, conclui debate. *In*: SENADO notícias. Brasília, DF, 11 jul. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/07/11/ciberseguranca-deve-ter-agencia-estatal-com-parceria-privada-conclui-debate. Acesso em: 09 nov. 2024.

considera a segurança cibernética um dos dez principais riscos globais, tanto para o setor público quanto para o privado. Para eles, desde a pandemia do Covid-19, os ataques cibernéticos dobraram globalmente e se tornaram cada vez mais sofisticados. Segundo notícias do Senado Federal, em 2020, o custo médio de uma violação de dados para uma instituição governamental foi de aproximadamente US$ 4,441 milhões (cerca de R$ 24 milhões). Segundo eles, embora o Brasil possua um alto nível de digitalização, ainda precisa amadurecer no que se refere à segurança cibernética[235].

Ao passo que a Subcomissão, vinculada à Comissão de Relações Exteriores e Defesa Nacional (CRE), foi criada por iniciativa do senador Esperidião Amin com o objetivo de acompanhar a política pública relacionada à defesa cibernética e propor soluções. O senador destacou que o Brasil está atrasado nesse tema e que é essencial que o Executivo adote medidas para prevenir e combater os riscos de ataques, que podem afetar setores como bancos, sistema financeiro, logística, hidrelétricas e energia. Ele também defende a criação de uma agência governamental e o compartilhamento de experiências internacionais, ressaltando os prejuízos econômicos globais, que giram em torno de 14%, com impacto significativo também em áreas como saúde, educação e infraestrutura[236].

O senador Sérgio Moro também reforçou a importância da criação de uma agência nacional de cibersegurança no Brasil, sublinhando que o desafio reside na estruturação e financiamento desse órgão. Ao passo que, o senador Marcos Pontes, defendeu a formação de um conselho de segurança cibernética composto por representantes dos setores reguladores, da sociedade civil, do Exército e do setor privado[237].

Ao passo que, o senador Jorge Seif sugeriu a terceirização das atividades de cibersegurança para empresas privadas, argumentando que estas estão mais avançadas tecnologicamente que as agências governamentais e poderiam proteger melhor as plataformas digitais do governo brasileiro[238].

---

235 CIBERSEGURANÇA deve ter agência estatal com parceria privada, conclui debate. *In*: SENADO notícias. Brasília, DF, 11 jul. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/07/11/ciberseguranca-deve-ter-agencia-estatal-com-parceria-privada-conclui-debate. Acesso em: 09 nov. 2024.

236 *Ibid*.

237 *Ibid*.

238 *Ibid*.

Ainda na seara divulgada pelo Senado Federal, mencionam que nos Estados Unidos, Patricia Soller, líder do Colaborativo Conjunto de CiberDefesa, compartilhou a experiência do governo norte-americano, enfatizando a importância das legislações sobre cibersegurança e a atuação da Agência Americana de Cibersegurança e Infraestrutura (Cisa), que coordena o trabalho de defesa cibernética em colaboração com o FBI[239], empresas privadas e parceiros internacionais, incluindo o Brasil. Ela destacou que a colaboração internacional é importantíssima para entender riscos específicos em setores críticos, como o setor de água e o nuclear[240].

Por fim, Paulo Manzato, representante da Cloudfare, também defendeu a abordagem colaborativa entre o setor público e privado, ressaltando que o compartilhamento de informações sobre ameaças cibernéticas é vital para antecipar e neutralizar ataques. Ele enfatizou a necessidade de cooperação, educação e capacitação para uma defesa eficaz[241].

É responsabilidade do Estado promover uma educação que atenda às necessidades atuais, incluindo a conscientização sobre cibersegurança. Pesquisa da Kaspersky mostra que 20% dos brasileiros desconhecem a LGPD e temas de proteção de dados, expondo o risco real de violações digitais. Não obstante, como demonstrado ao longo da presente monografia, a ANAC, também aponta vulnerabilidades na segurança cibernética da aviação, reforçando a importância de uma educação que aborde essas questões. Investir na formação digital é, portanto, essencial para a proteção coletiva, ponto que será melhor desenvolvido nas considerações finais.

---

239 O FBI (Federal Bureau of Investigation) é a polícia federal dos Estados Unidos. Sua sede fica em Washington, DC, e sua função é investigar e aplicar a lei federal no país. FBI. *In*: MANUAL de Comunicação da SECOM – Senado Federal. Brasília, DF, [2024?]. Disponível em: https://www12.senado.leg.br/manualdecomunicacao/estilos/fbi. Acesso em: 17 out. 2024.

240 CIBERSEGURANÇA deve ter agência estatal com parceria privada, conclui debate. *In*: SENADO notícias. Brasília, DF, 11 jul. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/07/11/cibersegurança-deve-ter-agencia-estatal-com-parceria-privada-conclui-debate. Acesso em: 09 nov. 2024.

241 *Ibid*.

6 CONSIDERAÇÕES FINAIS

À medida que a trajetória histórica da aviação ganhou destaque a partir da Primeira Guerra Mundial, o setor aéreo consolidou-se como um dos principais motores do desenvolvimento econômico global, sendo atualmente uma das alavancas essenciais da economia brasileira. Conforme apontado por Silva e Santos, o transporte aéreo é um dos elementos mais dinâmicos para o turismo e para a economia mundial, oferecendo uma conectividade global que impulsiona o crescimento do setor turístico no Brasil, facilitando o deslocamento de turistas e promovendo o desenvolvimento de novos destinos. Contudo, com esse crescimento exponencial, surgem novos desafios, como a necessidade de proteger os dados pessoais dos passageiros e garantir a segurança cibernética das infraestruturas aeroportuárias e das companhias aéreas.

Dessa forma, ao longo desta monografia, foram discutidos os primórdios e a evoluções do direito aeronáutico, a interseção entre cibersegurança, aviação e o direito, os riscos decorrentes do uso de infraestruturas tecnológicas, os principais incidentes cibernéticos que assolam o setor aéreo nos últimos anos bem como as leis que regem o tema no Brasil, incluindo a Lei Federal nº 7.565/1986 (Código Brasileiro de Aeronáutica), a Lei Federal nº 11.182/2005 (Cria a Agência Nacional de Aviação Civil – ANAC, e dá outras providências), a Lei Federal nº 12.965/2014 (Marco Civil da Internet), a Lei Federal nº 13.709/2018 (Lei Geral de Proteção de Dados Pessoais (LGPD)), Decreto nº 11.856/2023 (Institui a Política Nacional de Cibersegurança e o Comitê Nacional de Cibersegurança), o Decreto nº 11.491/2023 (Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001).

Também foi discutida que a competência para processar e julgar as ações que norteiam a cibersegurança na aviação pertence à Justiça Federal quando a União ou suas autarquias, como a ANAC, estão diretamente envolvidas, conforme o art. 109, inciso I, da Constituição Federal, mesmo que a União, no sentido mais amplo, não tenha interesse direto no caso. Por outro lado, a Justiça Estadual poderá ser competente em situações que envolvem exclusivamente concessionárias privadas de aeroportos, desde que não haja participação ou interesse direto da ANAC ou da União. No entanto, como visto no capítulo 5.1, essa competência da Justiça Estadual não é automática; deve-se analisar a natureza específica do litígio e

verificar se realmente não há necessidade de envolver a União ou a ANAC para garantir a correta jurisdição.

Ao passo que, foi abordada a importância da precaução e da prevenção em matéria de cibersegurança, conceitos que, segundo Niklas Luhmann, são essenciais diante da complexidade das decisões humanas e dos riscos por elas gerados. Luhmann destaca que a sociedade moderna precisa aceitar que, apesar de todos os esforços, é impossível eliminar completamente os riscos, reforçando a necessidade de uma gestão consciente e informada. Ulrich Beck complementa essa análise ao afirmar que as ameaças contemporâneas são invisíveis e exigem conhecimento especializado, aumentando a dependência dos indivíduos em relação aos produtores de conhecimento. Nesse contexto, cabe ao Estado a responsabilidade de enfrentar essas ameaças por meio de uma estrutura regulatória robusta e de promover educação digital e políticas públicas mais eficazes, especialmente no que concerne a prevenção de ataques cibernéticos na Aviação Civil Brasileira.

E assim, após um estudo das normas brasileiras aplicáveis à cibersegurança na aviação civil, é possível concluir que o Brasil, ao contrário do que muitos autores e doutrinas afirmam, não carece de regulamentação estatal nesse campo. O que se observa, em verdade, é uma vasta rede de legislações que, embora abordem a cibersegurança de maneira indireta, são eficazes e podem, sem dúvida, ser aplicadas ao setor de aviação civil. Contudo, cumpre salientar que a lacuna existente no problema de pesquisa não está na ausência de leis propriamente dita, mas sim na falha de aplicação eficiente das normas vigentes pelos agentes e operadores do Direito. A criação e implementação de novas leis não resolverá o problema se as já existentes não forem devidamente aplicadas e interpretadas conforme a realidade e as especificidades do setor.

Assim, ao longo deste trabalho, observaram-se três vertentes que fundamentam a conclusão. A primeira vertente nada mais é do que o que foi abordado no capítulo 3.2, ou seja, trata das relações contratuais entre empresas aéreas e aeroportuárias e empresas de tecnologia e segurança cibernéticas. Tendo em vista que as companhias aéreas e os aeroportos frequentemente contratam empresas de tecnologia para fornecer serviços de segurança cibernética e armazenamento de dados, como o ataque à SITA, uma das maiores fornecedoras de TI para o setor aéreo que comprometeu informações de passageiros de companhias aéreas em todo o mundo, inclusive dos clientes da Latam e em seguida,

o Apagão Cibernético de 2024, ocorrido pela empresa CrowdStrike, causado por uma atualização de conteúdo para computadores com o sistema operacional *Windows*, relacionada ao sensor *Falcon*, resultou na chamada "tela azul da morte", e desencadeou tal apagão no mundo inteiro.

Dessa forma, como analisado, a Lei Federal nº 7.565/1986 (Código Brasileiro de Aeronáutica), em seus artigos 1º, 21 e 49, impõe às companhias aéreas a responsabilidade de garantir a segurança das operações, incluindo, implicitamente, a segurança digital. Ao passo que, a negligência na proteção cibernética pode comprometer a regularidade e eficiência dos serviços, violando a própria essência do código.

Ademais, a Lei Federal nº 13.709/2018 (LGPD) estabelece, no art. 46, que agentes de tratamento, como as companhias aéreas, adotem medidas de segurança para proteger dados pessoais, destacando a relevância de práticas rigorosas de proteção da informação. Como analisado no capítulo 4.2, o descumprimento do referido artigo acarreta consequências, incluindo sanções administrativas aplicadas pela Autoridade Nacional de Proteção de Dados (ANPD), que por sua vez, podem variar de advertências a multas substanciais, além da publicização da infração e, em casos graves, a suspensão das atividades de tratamento de dados.

Além disso, a responsabilidade civil na LGPD, que é objetiva, pode gerar a obrigação de reparar danos causados aos titulares de dados, mesmo sem a necessidade de comprovação de culpa, bastando a demonstração do dano e do nexo causal. Ainda cumpre dispor que essa responsabilidade se alinha aos dispositivos do Código Civil Brasileiro, nos artigos 186 e 927, que tratam da reparação de danos, e aos princípios de proteção do consumidor estabelecidos no Código de Defesa do Consumidor, nos artigos 14 e 20, que estabelecem a responsabilidade objetiva por falhas na prestação de serviços.

Porquanto, ainda que não se tenha acesso direto aos contratos, a legislação brasileira oferece dispositivos claros e eficientes para responsabilização das empresas que prestam serviços ao setor da aviação em casos de falha na proteção dos dados e dos sistemas.

Neste sentido, entende-se que a LGPD e as normas correlatas fortalecem a estrutura jurídica para proteger os dados pessoais e garantir a segurança cibernética no setor aéreo. Ademais, essas normas complementam o arcabouço legislativo já analisado e reforçam a necessidade de uma aplicação mais eficaz das leis

existentes, demonstrando que o Brasil dispõe de mecanismos legais suficientes para enfrentar os desafios da cibersegurança na aviação civil.

A segunda vertente destaca as violações internas, nas quais funcionários das próprias empresas aéreas ou aeroportos podem cometer atos ilícitos, valendo-se de seu acesso e conhecimento técnico. Essa vertente foi abordada no capítulo 3.1, quando a própria ANAC menciona que qualquer indivíduo ou entidade com uma motivação específica pode ser um potencial agente de uma ciberameaça. Entre os exemplos citados estão: terroristas, ativistas, criminosos, curiosos, vândalos, funcionários internos da organização (como empregados em geral e superusuários de TI), organizações criminosas, organizações terroristas, empresas concorrentes, empresas terceirizadas (como equipes de segurança física, limpeza ou TI), organizações ativistas, nações/estados hostis, e grupos financiados por Estados.

Além disso, conforme salientado pela ANAC, uma ameaça pode até ser desencadeada por alguém sem uma motivação explícita, como em casos de negligência ou falta de conscientização sobre práticas de segurança, por exemplo, deixar um sistema logado ou conectar dispositivos não autorizados, como um *USB* pessoal.

A ANAC ainda aponta que as motivações para tais ataques são amplas, variando desde ganho financeiro até espionagem industrial, destruição, ativismo, ou mesmo questões geopolíticas. Contudo, conforme o entendimento das autoras Ana Maria Lumi Kamimura Murata e Paula Ritzmann Torres no capítulo 4.3, esses atos ilícitos podem ser enquadrados em diferentes esferas do direito brasileiro, como o Código Penal, que prevê sanções para crimes como estelionato (art. 171), crimes contra a honra (arts. 138 a 140) e crimes contra o patrimônio (arts. 155 a 183), além das disposições específicas sobre crimes cibernéticos previstas na Lei nº 12.737/2012 (Lei Carolina Dieckmann).

Além disso, como analisado no capítulo 4.1, a Lei Federal nº 11.182/2005, que criou a Agência Nacional de Aviação Civil, confere à referida autarquia a competência para regular e fiscalizar as práticas de segurança no setor aéreo, abrangendo a implementação de protocolos de compliance e a prevenção de ataques internos. No mesmo sentido, a LGPD, em seu art. 50, prevê a obrigatoriedade de programas de governança em privacidade, contemplando o desenvolvimento de treinamentos e a adoção de medidas preventivas para mitigar riscos cibernéticos decorrentes de ações humanas. Ademais, essas disposições

encontram complemento normativo no Marco Civil da Internet, Lei Federal nº 12.965/2014, estudada no capítulo 4.2, que, em seu art. 13, determina que os provedores de serviços devem adotar medidas de segurança capazes de prevenir a violação de dados e sistemas, exigência que também se aplica às empresas aéreas que operam redes digitais no âmbito de suas atividades.

Além disso, se faz necessário mencionar que, embora o foco tenha sido direcionado às consequências cibernéticas mais amplas, vale complementar que as repercussões podem também alcançar o âmbito trabalhista, onde as violações cometidas por funcionários podem ensejar sanções previstas na Consolidação das Leis do Trabalho (CLT). Nesse sentido, o art. 482 da CLT prevê a possibilidade de demissão por justa causa para empregados que cometem atos de improbidade ou causam danos ao empregador. Portanto, novamente, entende-se que não há necessidade de novas leis/regulamentos específicos, visto que o ordenamento jurídico brasileiro já possui normas adequadas para tratar dessas questões, bastando que sejam aplicadas de forma eficaz.

A terceira e última vertente aborda os riscos enfrentados pelos passageiros que se conectam a redes públicas, seja nos aeroportos ou a bordo das aeronaves, uma questão amplamente reconhecida pelos doutrinadores como “conveniência”. No capítulo 3, o perigo dessas conexões é estudado a partir de um relatório da Coronet, que aponta que milhões de viajantes estão vulneráveis a ataques cibernéticos, já que muitas dessas redes carecem de criptografia adequada, expondo dispositivos a riscos como roubo de informações sensíveis e instalação de *softwares* maliciosos. Segundo Dror Liwer, diretor de segurança e cofundador da Coronet, a prioridade que os usuários dão à conveniência em detrimento da segurança é um fator extremamente crítico e que facilita essas ameaças.

Não obstante, como analisado no capítulo 4.2, o Decreto nº 11.856/2023 determina a importância de desenvolver campanhas de conscientização sobre segurança digital, especialmente em ambientes de grande fluxo de pessoas, como aeroportos e a partir disso, entende-se que o problema se conecta diretamente com o que foi abordado no capítulo 5.3, onde uma pesquisa da Kaspersky revelou um desconhecimento preocupante sobre cibersegurança por parte dos brasileiros, especialmente no tocante à LGPD. O estudo mostrou que 20% dos brasileiros desconhecem seus direitos de privacidade de dados, e 40% não sabem como suas informações são coletadas na *internet*. Roberto Rebouças, da Kaspersky, entende

que essa falta de conscientização agrava a vulnerabilidade digital e menciona sobre a importância de uma educação em cibersegurança. Portanto, a negligência em priorizar a segurança digital, tanto por parte de usuários quanto de funcionários, acaba se tornando o elo mais fraco na proteção de dados, o que é ainda mais preocupante em ambientes como aeroportos, onde a conectividade é de fato importante, especialmente nos tempos atuais; contudo, muitas vezes, insegura.

À vista dessas três vertentes, conclui-se que o problema de pesquisa buscava responder até que ponto as normas e estruturas regulatórias brasileiras, incluindo o direito aeronáutico e o direito digital, são eficazes para mitigar e enfrentar as ameaças cibernéticas que impactam a aviação civil e as infraestruturas aeroportuárias no Brasil. Ademais, indagava-se como o Estado poderia atuar na criação e implementação de políticas mais eficazes de prevenção cibernética no setor aéreo brasileiro.

Conclui-se, portanto, que o Brasil possui uma rede normativa abrangente e capaz de mitigar as questões de cibersegurança na aviação civil, abrangendo legislações como o Código Brasileiro de Aeronáutica (Lei Federal nº 7.565/1986), a Lei Geral de Proteção de Dados (Lei Federal nº 13.709/2018), o Marco Civil da Internet (Lei Federal nº 12.965/2014) e os regulamentos específicos da ANAC, além dos decretos expostos. A ausência de regulamentações específicas para cibersegurança na aviação, por si só, não configura um problema, como interpretada por diversos autores trazidos à baila, uma vez que as normas já existentes no Brasil (Código Civil, o Código de Defesa do Consumidor, a Lei Geral de Proteção de Dados, o Marco Civil da Internet, o Código Penal e a Consolidação Leis do Trabalho), se devidamente aplicadas, são suficientes para cobrir os principais aspectos da proteção de dados e da segurança cibernética na aviação e quiçá em quaisquer outras áreas afetadas.

O que se evidencia como imprescindível é uma aplicação mais eficaz das leis existentes. O princípio da efetividade jurídica, aliado à interpretação sistemática e finalística das normas, impõe ao poder público a obrigação de garantir que as regulamentações sejam operacionalizadas com maior rigor e eficiência.

Todavia, como alternativa subsidiária à aplicação mais rigorosa das normas já existentes, defende-se que o poder público deva investir massivamente em educação digital, visando prevenir incidentes cibernéticos e promover uma cultura de segurança cibernética tanto abrangente quanto específica (aviação) no Brasil. Com

base no princípio da prevenção e da precaução, se mostrou imprescindível em antecipar riscos e adotar medidas que minimizem a ocorrência de danos relacionados à cibersegurança. Nesse sentido, entende-se que a conscientização desde cedo sobre os riscos do uso de redes públicas e a importância da proteção de dados pessoais tornam-se fundamentais, especialmente em um setor sensível como o da aviação civil.

A inclusão de disciplinas voltadas à segurança digital no currículo escolar, com conteúdo que ensinem boas práticas de proteção de dados e o uso responsável da internet, seria um avanço necessário para a construção de uma sociedade mais segura digitalmente. Essas iniciativas educacionais devem ser acompanhadas de campanhas de conscientização nacional promovidas pelo governo, utilizando meios de comunicação, como por exemplo as plataformas digitais oficiais e redes sociais, *Instagram*, *Facebook*, *X*, *TikTok etc*, para atingir diferentes faixas etárias e perfis socioeconômicos. Entende-se que essas campanhas, idealmente desenvolvidas em parceria com empresas de tecnologia da informação, poderiam informar a população sobre os riscos cibernéticos e a importância da proteção de dados, especialmente em ambientes públicos, como aeroportos e aeronaves.

Além da educação básica, o investimento em infraestrutura digital é igualmente importante. Assim, para integrar o ensino digital de forma eficaz, é necessário garantir que todas as escolas, tanto urbanas quanto rurais, disponham de equipamentos adequados e acesso à *internet* de qualidade. Essa igualdade de acesso é completamente necessária para proporcionar a todos os estudantes as mesmas oportunidades de aprendizado sobre tecnologia, riscos no meio digital, práticas de segurança cibernética, e conhecimento sobre como e onde buscar seus direitos quando vítimas de ataques cibernéticos.

Paralelamente, é imprescindível que as empresas privadas de aviação desenvolvam conteúdos específicos sobre incidentes cibernéticos que afetam o setor, demonstrando preocupação ativa e transparência quanto às medidas de proteção e prevenção adotadas. Essas ações não apenas aumentam a confiança dos passageiros, mas também refletem o compromisso das companhias em colaborar para solucionar problemas caso ocorram, como exemplificado pelo incidente envolvendo o programa Latam Pass em 2021.

Ademais, conforme analisado no capítulo 3.1, a ANAC relatou diversos incidentes cibernéticos que marcaram o setor entre 2015 e 2020, incluindo o ataque

aos sistemas da LOT em 2015, que paralisou a emissão de planos de voo no *hub* de Varsóvia; a falha de sistemas no aeroporto de Orly devido a *software* desatualizado; e o ataque de *malware* ao Aeroporto Internacional de Kiev Boryspil, rastreado até a Rússia. Outros eventos preocupantes incluem o incidente com drones reportado pela British Airways próximo ao aeroporto de Heathrow em 2017, o vazamento de mais de 860 mil passaportes e cartões de crédito da Cathay Pacific em 2018, e o *ransomware* que afetou o aeroporto de Bristol no mesmo ano, deixando o serviço de informações de voo inoperante por dois dias. O ataque à SITA em 2021, que expôs dados de passageiros brasileiros, é mais uma evidência da seriedade dessas ameaças.

Portanto, sinalizar sobre a importância da segurança cibernética nos *gates* e áreas de embarque dos aeroportos seria uma medida relevante para conscientizar e prevenir tais ataques, uma vez que as redes *Wi-Fi* dos aeroportos são públicas e, consequentemente, mais vulneráveis. Nas aeronaves, onde o *Wi-Fi* gratuito, ainda que com limitações, ou a conexão paga são oferecidos, as empresas devem estar cientes dos riscos inerentes às violações cibernéticas. Ao demonstrar essas preocupações aos passageiros e investir em práticas de segurança mais robustas, as companhias aéreas terão a oportunidade de redobrar os cuidados com os equipamentos internos, minimizando as chances de exploração de vulnerabilidades.

É importante reiterar, conforme abordado no capítulo 3, que as ameaças cibernéticas são recorrentes e sérias. O Diretor de Estratégia e Gerenciamento de Segurança da Agência Europeia de Segurança da Aviação (EASA) revelou que aeroportos ao redor do mundo enfrentam cerca de 1.000 ciberataques por mês. E, portanto, entende-se que as companhias aéreas têm um papel fundamental não apenas em proteger seus sistemas, mas também em conscientizar os passageiros sobre os riscos de redes públicas, especialmente nos aeroportos e a bordo das aeronaves.

Ao cabo, além das iniciativas já discutidas, é indispensável o contínuo aprofundamento acadêmico no tema da cibersegurança para os estudantes e operadores do Direito Aeronáutico. Conforme mencionado no capítulo 2.2, Poletti destaca a importância de critérios como conveniência, interesse e oportunidade na inclusão de disciplinas específicas sobre Direito Aeronáutico. Seguindo essa linha, seria igualmente relevante inserir conteúdos sobre cibersegurança na aviação, dado o crescente impacto da tecnologia no setor. Fomentar o interesse em estudos

especializados, como programas de pós-graduação e mestrados que abordem a interseção entre Direito Aeronáutico e cibersegurança, é necessário. Afinal, a cibersegurança é um campo moderno, dinâmico e em constante transformação, e a evolução tecnológica impõe aos profissionais do Direito a necessidade de estarem em contínua atualização para compreender as nuances das mudanças e suas repercussões jurídicas no cenário atual.

REFERÊNCIAS

AFSHAR, Vala. Cybercrime threatens business growth. Take these steps to mitigate your risk. *In*: ZDNET. [*S. l.*], 21 abr. 2022. Disponível em: https://www.zdnet.com/article/cybercrime-can-be-the-biggest-threat-to-business-growth/. Acesso em: 08 nov. 2024.

ALECRIM, Emerson; HIGA, Paulo. O que é GPS? *In*: TECNOBLOG. [*S. l.*], [2023]. Disponível em: https://tecnoblog.net/responde/o-que-e-gps/. Acesso em: 16 out. 2024.

ALECRIM, Emerson; HIGA, Paulo. O que é USB? *In*: TECNOBLOG. [*S. l.*], [2023]. Disponível em: https://tecnoblog.net/responde/o-que-e-usb/. Acesso em: 16 out. 2024.

ALVARENGA, Ricardo. **Direito aeronáutico**: dos contratos e garantias sobre aeronaves. Belo Horizonte: Del Rey, 1992.

ANAC investe em segurança cibernética na aviação civil. *In*: AGÊNCIA nacional de aviação civil. Brasília, DF, 21 dez. 2023. Disponível em: https://www.gov.br/anac/pt-br/noticias/2023/anac-investe-em-seguranca-cibernetica-na-aviacao-civil. Acesso em: 08 nov. 2024.

ANAC. **Manual de Conscientização de Segurança Cibernética da Aviação Civil**. Brasília: Agência Nacional de Aviação Civil, [2023]. Disponível em: https://www.anac.gov.br/manual-conscientizacao. Acesso em: 08 nov. 2024.

APAGÃO cibernético afeta setor aéreo e voos são cancelados. *In*: CNN Brasil. São Paulo, 27 jul. 2024. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/apagao-cibernetico-afeta-setor-aereo-e-voos-sao-cancelados/. Acesso em: 08 nov. 2024.

ATAERO - Adicional de Tarifas Aeronáuticas. *In*: DEPARTAMENTO de controle do espaço aéreo – DECEA. Brasília, DF, [2024?]. Disponível em: https://www.decea.mil.br/index.cfm?i=utilidades&p=glossario&single=2172. Acesso em: 09 nov. 2024.

AZAMBUJA, Antonio João Gonçalves de; NETO, João Souza. Modelo de maturidade de segurança cibernética para os órgãos da Administração Pública Federal. **Revista do serviço público**, Brasília, DF, v. 71, n. 3, p. 660-712, 2020. Disponível em: https://revista.enap.gov.br/index.php/RSP/article/view/3210. Acesso em: 08 nov. 2024.

BAARS, Hans; HINTZBERGEN, Kees; HINTZBERGEN, Jule; SMULDERS, André. **Fundamentos de segurança da informação**: com base na ISO 27001 e na ISO 27002. São Paulo: Brasport, 2018. *E-book*.

BECK, Ulrich. **Sociedade de risco**: rumo a uma Outra Modernidade. 2. ed. São Paulo: Editora 34, 2011.

BOBBIO, Norberto. **Teoria geral do direito**. 3. ed. São Paulo: Martins Fontes, 2010.

BOTELHO, José Ricardo. Segurança operacional na aviação nasce da cooperação. *In*: AEROFLAP. [*S. l.*], 22 abr. 2022. Disponível em: https://www.aeroflap.com.br/seguranca-operacional-na-aviacao-nasce-da-cooperacao/. Acesso em: 08 nov. 2024.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 09 nov. 2024.

BRASIL. Agência Nacional de Aviação Civil. **Manual de conscientização em segurança cibernética na aviação civil**. Brasília, DF: Agência Nacional de Aviação Civil, [2024?]. Disponível em: https://www.gov.br/anac/pt-br/assuntos/regulados/aeroportos-e-aerodromos/avsec/arquivos/Manual_de_conscientizacao_sobre_Ciberseguranca.pdf. Acesso em: 08 nov. 2024.

BRASIL. Agência Nacional de Telecomunicações. **Segurança Cibernética**. Brasília, DF: Agência Nacional de Telecomunicações, [2024?]. Disponível em: https://www.gov.br/anatel/pt-br/assuntos/seguranca-cibernetica/politicas-publicas#:~:text=Seguran%C3%A7a%20Cibern%C3%A9tica%20%C3%A9%20definida%20como,a%20autenticidade%20dos%20dados%20armazenados%2C. Acesso em: 08 nov. 2024.

BRASIL. Congresso Nacional Câmara dos Deputados. **Projeto de Lei nº 3.357, de 2015.** Autoria: Deputado Vicentinho Junior. Brasília, DF: Câmara dos Deputados, [2015]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2024070. Acesso em: 09 nov. 2024.

BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei nº 84, de 1999**. Dispõe sobre os crimes cometidos na área de informática, suas penalidades e dá outras providências. Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal e a Lei nº 9.296, de 24 de julho de 1996, e dá outras providências. Autoria: Deputado Luiz Piauhylino. Brasília, DF: Câmara dos Deputados, [1999]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=15028. Acesso em: 09 nov. 2024.

BRASIL. Congresso Nacional. Câmara dos Deputados. **Projeto de Lei nº 5.441, de 2020.** Define os crimes cibernéticos e dá outras providências. Autoria: Deputado David Soares. Brasília, DF: Câmara dos Deputados, [2020]. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2266423. Acesso em: 09 nov. 2024.

BRASIL. **Decreto nº 11.491, de 12 de abril de 2023**. Promulga a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm#:~:text=DECRETO%20N%C2%BA%2011.491%2C%20DE%2012,23%20de%20novembro%20de%202001. Acesso em: 09 nov. 2024.

BRASIL. **Decreto nº 11.856, de 26 de dezembro de 2023**. Institui a Política Nacional de Cibersegurança – PNCiber e dá outras providências. Brasília, DF: Presidência da República, 2023. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2023/decreto/D11856.htm. Acesso em: 09 nov. 2024.

BRASIL. **Decreto-lei nº 2.848, de 7 de dezembro de 1940**. Código Penal. Rio de Janeiro, DF: Presidência da República. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 09 nov. 2024.

BRASIL. **Lei nº 10.695, de 1º de julho de 2003**. Altera e acresce parágrafo ao art. 184 e dá nova redação ao art. 186 do Decreto-Lei no 2.848, de 7 de dezembro de 1940 – Código Penal, alterado pelas Leis nos 6.895, de 17 de dezembro de 1980, e 8.635, de 16 de março de 1993, revoga o art. 185 do Decreto-Lei no 2.848, de 1940, e acrescenta dispositivos ao Decreto-Lei no 3.689, de 3 de outubro de 1941 – Código de Processo Penal. Brasília, DF: Presidência da República, 2003. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2003/l10.695.htm. Acesso em: 09 nov. 2024.

BRASIL. **Lei nº 11.182, de 27 de setembro de 2005.** Cria a Agência Nacional de Aviação Civil – ANAC, e dá outras providências. Brasília, DF: Presidência da República, 2005. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2004-2006/2005/Lei/L11182.htm. Acesso em: 08 nov. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 08 nov. 2024.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 08 nov. 2024.

BRASIL. **Lei nº 7.565, de 19 de dezembro de 1986**. Dispõe sobre o Código Brasileiro de Aeronáutica. Brasília, DF: Presidência da República, 1986. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7565compilado.htm. Acesso em: 08 nov. 2024.

BRASIL. **Lei nº 7.565, de 19 de dezembro de 1986.** Dispõe sobre o Código Brasileiro de Aeronáutica. Brasília, DF: Presidência da República, 1986. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l7565compilado.htm. Acesso em: 08 nov. 2024.

BRASIL. **Lei nº 8.069, de 13 de julho de 1990**. Dispõe sobre o Estatuto da Criança e do Adolescente e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8069.htm. Acesso em: 09 nov. 2024.

BRASIL. **Lei nº 8.078, de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Presidência da República, 1990. Disponível em: https://www.procon.df.gov.br/wp-content/uploads/2019/08/Codigo-do-consumidor-FINAL.pdf. Acesso em: 08 nov. 2024.

BRASIL. **Lei nº 8.987, de 13 de fevereiro de 1995.** Dispõe sobre o regime de concessão e permissão da prestação de serviços públicos previsto no art. 175 da Constituição Federal, e dá outras providências. Brasília, DF: Presidência da República 1995. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8987cons.htm. Acesso em: 09 nov. 2024.

BRASIL. **Lei nº 9.277, de 10 de maio de 1996**. Autoriza a União a delegar aos municípios, estados da Federação e ao Distrito Federal a administração e exploração de rodovias e portos federais. Brasília, DF: Presidência da República, 1996. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9277.htm. Acesso em: 09 nov. 2024.

BRASIL. Tribunal Regional Federal. **Agravo de instrumento 081128254.2022.4.05.0000**. Civil e processo civil. Administrativo. Ação possessória. Contrato de arrendamento [...]. 7ª Turma. Relatora: Des. Germana de Oliveira Moraes, 31 de janeiro de 2023. Disponível em: https://pje.trf5.jus.br/pjeconsulta/ConsultaPublica/DetalheProcessoConsultaPublica/documentoSemLoginHTML.seam?idProcessoDocumento=02772ed042ea5ab75e27c3d0298e2ccc#. Acesso em: 11 nov. 2024.

CEDEÑO, Karina. Veja os 10 aeroportos com maior risco de ataque de hackers nos EUA. *In*: PANROTAS. [*S. l.*], 23 jul. 2018. Disponível em: https://www.panrotas.com.br/viagens-corporativas/seguranca/2018/07/veja-os-10-aeroportos-com-maior-risco-de-ataque-de-hackers-nos-eua_157329.html. Acesso em: 08 nov. 2024.

CIBERSEGURANÇA deve ter agência estatal com parceria privada, conclui debate. *In*: SENADO notícias. Brasília, DF, 11 jul. 2024. Disponível em: https://www12.senado.leg.br/noticias/materias/2024/07/11/cibersegurança-deve-ter-agencia-estatal-com-parceria-privada-conclui-debate. Acesso em: 09 nov. 2024.

COMITÊ GESTOR DA INTERNET NO BRASIL. **TIC Domicílios 2022:** pesquisa do uso da Internet no Brasil. São Paulo: Comitê Gestor da Internet, 2022. Disponível em: https://cetic.br/media/docs/publicacoes/2/20230825143348/resumo_executivo_tic_domicilios_2022.pdf. Acesso em: 08 nov. 2024.

CONVENÇÃO de Budapeste é promulgada no Brasil. *In*: MINISTÉRIO da Justiça e Segurança Pública. Brasília, DF, 17 abril 2023. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/convencao-de-budapeste-e-promulgada-no-brasil. Acesso em: 09 nov. 2024.

COSTA, César Augusto Soares da. A educação enquanto responsabilidade do Estado. **Educação**, Porto Alegre, v. 32, n. 2, p. 236-237, maio/ago. 2009. Disponível em: https://revistaseletronicas.pucrs.br/faced/article/view/5526/4021. Acesso em: 09 nov. 2024.

COVID-19. *In*: GOV.BR. Brasília, DF, [2024?]. Disponível em: https://www.gov.br/saude/pt-br/assuntos/covid-19. Acesso em: 08 nov. 2024.

CYBER security oversight. *In*: CIVIL aviation authoroty. London, c2024. Disponível em: https://www.caa.co.uk/commercial-industry/cyber-security/cyber-security-oversight/. Acesso em: 08 nov. 2024.

DAVID, Marília Luz. Sobre os conceitos de risco em Luhmann e Giddens. **Em tese**, Florianópolis, v. 8, n. 1, p. 30-47, jan./jul. 2011. Disponível em: https://periodicos.ufsc.br/index.php/emtese/article/view/1806-5023.2011v8n1p30. Acesso em: 09 nov. 2024.

DIA DO nascimento de Alberto Santos-Dumont. *In*: LABORATÓRIO químico-farmacêutico da aeronáutica. Brasília, DF, [2024?]. Disponível em: https://www2.fab.mil.br/laqfa/index.php/2014-12-11-17-51-57. Acesso em: 08 nov. 2024.

DIFERENÇA entre hacker e cracker. *In*: HUGE networks. [*S. l.*], [2024?]. Disponível em: https://www.huge-networks.com/blog/ciberseguranca/diferenca-hacker-e-cracker. Acesso em: 08 nov. 2024.

DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. 3. ed. São Paulo: Revista dos Tribunais, 2021.

DONOHUE, Brian. Wi-Fi a bordo é seguro? *In*: KASPERSKY. [*S. l.*], 06 dez. 2013. Disponível em: https://www.kaspersky.com.br/blog/wi-fi-a-bordo-e-seguro/1787/. Acesso em: 08 nov. 2024.

EMPRESA afirma que vazamento expôs CPF de 220 milhões de brasileiros. *In*: CONJUR. [*S. l.*], 20 jan. 2021. Disponível em: https://www.conjur.com.br/2021-jan-20/empresa-afirma-vazamento-expos-cpf-220-milhoes/. Acesso em: 03 nov. 2024.

FBI. *In*: MANUAL de Comunicação da SECOM – Senado Federal. Brasília, DF, [2024?]. Disponível em: https://www12.senado.leg.br/manualdecomunicacao/estilos/fbi. Acesso em: 17 out. 2024.

FURTADO, Teresa. O que é wireless. *In*: TECHTUDO. [*S. l.*], 28 dez. 2011. Disponível em: https://www.techtudo.com.br/noticias/2011/12/o-que-e-wireless.ghtml. Acesso em: 08 nov. 2024.

GARRET, Filipe. O que é malware? Veja significado, tipos e saiba remover. *In*: TECHTUDO. [*S. l.*], 27 mar. 2024. Disponível em: https://www.techtudo.com.br/listas/2021/03/o-que-e-malware-veja-significado-tipos-e-saiba-remover.ghtml. Acesso em: 08 nov. 2024.

GUSMÃO, Roberto José Faria de. História da aviação. *In*: LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (org.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018.

HAAS, Guilherme. O que é o Windows? *In*: CANALTECH. [*S. l.*], 17 fev. 2024. Disponível em: https://canaltech.com.br/windows/o-que-e-o-windows/. Acesso em: 08 nov. 2024.

HUREL, Louise Marie. Cibersegurança no Brasil: uma análise da estratégia nacional. **Instituto Igarapé**, Rio de Janeiro, p. 1-35, abr. 2021. Disponível em: https://igarape.org.br/wp-content/uploads/2021/04/AE-54_Seguranca-cibernetica-no-Brasil.pdf. Acesso em: 08 nov. 2024.

LAURANCE, Felipe. Clientes do Latam Pass têm dados vazados após ataque de hacker. *In*: CNN Brasil. São Paulo, 25 ago. 2022. Disponível em: https://www.cnnbrasil.com.br/economia/macroeconomia/clientes-do-latam-pass-tem-dados-vazados-apos-ataque-de-hacker/. Acesso em: 08 nov. 2024.

LEITE E SILVA, Juliano Veloso. Direito aeronáutico: linhas gerais. *In:* LAENDER, Alessandro Azzi; MOURA, Sérgio Luís; LEITE E SILVA, Juliano Veloso (org.). **Direito aeronáutico**. Belo Horizonte: D'Plácido, 2018.

LOUISE Marie Hurel. *In*: CENTRO brasileiro de relações internacionais. Rio de janeiro, [2024?]. Disponível em: https://www.cebri.org/br/especialista/1180/louise-marie-hurel. Acesso em: 08 nov. 2024.

MAIA, Karolline Barbosa; COSTA, Cezar Henrique Ferreira. Crimes cibernéticos. **Revista Ibero-Americana de Humanidades, Ciências e Educação**, São Paulo, v. 9, n. 10, p. 109-126, out. 2023. Disponível em: https://periodicorease.pro.br/rease/article/view/11580/5222. Acesso em: 08 nov. 2024.

MISTÉRIO do sumiço do voo MH370 da Malaysia Airlines completa 10 anos sem solução. *In*: CNN BRASIL. São Paulo, 08 mar. 2024. Disponível em: https://www.cnnbrasil.com.br/internacional/misterio-do-sumico-do-voo-mh370-da-malaysia-airlines-completa-10-anos-sem-solucao-veja-o-que-se-sabe/. Acesso em: 08 nov. 2024.

MURATA, A. M. L. K.; TORRES, M. P. R. A convenção de Budapeste sobre os crimes cibernéticos foi promulgada, e agora? **Boletim IBCCRIM**, [*S. l.*], v. 31, n. 368, p. 13-16, jul. 2023. Disponível em: https://publicacoes.ibccrim.org.br/index.php/boletim_1993/article/view/575/108. Acesso em: 09 nov. 2024.

O QUE É a CrowdStrike. *In*: CROWDSTRIKE. [*S. l.*], c2024. Disponível em: https://www.crowdstrike.com.br/produtos/faq/. Acesso em: 08 nov. 2024.

O QUE É a Política Nacional de Cibersegurança: marco no combate aos crimes virtuais. *In*: SECRETARIA de Comunicação da Presidência da República. Brasília, DF, 29 dez. 2023. Disponível em: https://www.gov.br/secom/pt-br/fatos/brasil-contra-fake/noticias/2023/12/o-que-e-a-politica-nacional-de-ciberseguranca-marco-no-combate-aos-crimes-virtuais. Acesso em: 09 nov. 2024.

O QUE É criptografia de dados? Definição e explicação. *In*: KASPERSKY. [*S. l.*], c2024. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/encryption. Acesso em: 08 nov. 2024.

O QUE É um botnet? *In*: AKAMAI. [*S. l.*], c2024. Disponível em: https://www.akamai.com/pt/glossary/what-is-a-botnet. Acesso em: 08 nov. 2024.

O QUE É um firewall? *In*: MICROSOFT. [*S. l.*], c2024. Disponível em: https://support.microsoft.com/pt-br/office/o-que-%C3%A9-um-firewall-6870c88d-69b6-4db4-9cb1-0e4afa7a8603. Acesso em: 08 nov. 2024.

O QUE É um hacker black hat? *In*: KASPERSKY. [*S. l.*], c2024. Disponível em: https://www.kaspersky.com.br/resource-center/threats/black-hat-hacker. Acesso em: 08 nov. 2024.

PAUPÉRIO, Artur Machado. **Introdução ao estudo do direito**. Rio de Janeiro: Forense, 1988.

PEDUZZI, Pedro. Apagão cibernético afetou voos da Azul e aplicativo do Bradesco: problema já foi corrigido, diz empresa de segurança cibernética. *In*: AGÊNCIA Brasil. Brasília, DF, 19 jul. 2024. Disponível em: https://agenciabrasil.ebc.com.br. Acesso em: 08 nov. 2024.

PESQUISA da Kaspersky revela que 20% dos brasileiros não têm conhecimento sobre a LGPD. *In*: KASPERSKY. [*S. l.*], 14 nov. 2024. Disponível em: https://www.kaspersky.com.br/about/press-releases/pesquisa-da-kaspersky-revela-que-20-dos-brasileiros-nao-tem-conhecimento-sobre-a-lgpd. Acesso em: 09 nov. 2024.

PINTO, Victor Carvalho. **O marco regulatório da aviação civil:** elementos para a reforma do Código Brasileiro de Aeronáutica. Brasília, DF: Senado Federal, 2008. Disponível em: https://www12.senado.leg.br/publicacoes/estudos-legislativos/tipos-de-estudos/textos-para-discussao/td-42-o-marco-regulatorio-da-aviacao-civil-elementos-para-a-reforma-do-codigo-brasileiro-de-aeronautica/view. Acesso em: 08 nov. 2024.

POLETTI, Ronaldo. A questão da autonomia do direito aeronáutico. **Revista de Informação Legislativa**, v. 31, n. 123, p. 103-112, jul./set. 1994. Disponível em: https://www2.senado.leg.br/bdsf/bitstream/handle/id/176260/000491490.pdf?sequence=1&isAllowed=y. Acesso em: 08 nov. 2024.

QUE É ransomware? Entenda como funciona e como remover o malware. *In*: TECHTUDO. [*S. l.*], 27 mar. 2021. Disponível em: https://www.techtudo.com.br/guia/2023/05/o-que-e-ransomware-entenda-como-funciona-e-como-remover-o-malware-edsoftwares.ghtml. Acesso em: 08 nov. 2024.

REAL brasileiro para dólar americano. *In*: WISE. [*S. l.*], c2024. Disponível em: https://wise.com/br/currency-converter/brl-to-usd-rate. Acesso em: 08 nov. 2024.

REDE cabeada: o que é. *In*: COMPASS soluções em tecnologia. Joinville, 09 nov. 2021. Disponível em: https://compass.srv.br/rede-cabeada-o-que-e/. Acesso em: 08 nov. 2024.

SAMPAIO, Nelson de Souza. Fontes do Direito – II. *In*: ENCICLOPÉDIA Saraiva do Direito. São Paulo: Saraiva, falta ano. v. 38.

SARLET, Gabrielle Bezerra Sales; RUARO, Regina Linden. A proteção de dados sensíveis no sistema normativo brasileiro sob o enfoque da lei geral de proteção de dados (LGPD) – l. 13.709/2018. **Revista direitos fundamentais & democracia**, [*S. l.*], v. 26, n. 2, p. 81-106, maio/ago. 2021. Disponível em: https://revistaeletronicardfd.unibrasil.com.br/index.php/rdfd/article/view/2172/694. Acesso em: 08 nov. 2024.

SARMENTO, Eduardo Sócrates Castanheira. Direito processual aeronáutico. **Revista brasileira de direito aeroespacial**, [*s. l.*], n. 80, 2000. Disponível em: https://sbda.org.br/wp-content/uploads/2018/10/1697.htm. Acesso em: 08 nov. 2024.

SILVA, Odair Vieira da; SANTOS, Rosiane Cristina dos. Trajetória histórica da aviação mundial. **Revista Científica Eletrônica de Turismo**, Garça, v. 6, n. 1, jun. 2009. Disponível em: https://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/WydybjUDpYtjIL4_2013-5-23-10-51-57.pdf. Acesso em: 08 nov. 2024.

SOBRE a CrowdStrike. *In*: CROWDSTRIKE. [*S. l.*], c2024. Disponível em: https://www.crowdstrike.com.br/sobre-crowdstrike/. Acesso em: 08 nov. 2024.

TECNOLOGIA da Informação e Comunicação (TIC): o que são e para que servem? *In*: ALGAR telecom. [*S. l.*], 24 ago. 2022. Disponível em: https://blog.algartelecom.com.br/significado-de-tics-entenda-de-uma-vez-por-todas/. Acesso em: 08 nov. 2024.

TUSCO, Claudio. LATAM emite nota sobre o vazamento de dados de seus clientes em ataque hacker. *In*: PONTOS pra voar. [*S. l.*], 13 mar. 2021. Disponível em: https://pontospravoar.com/latam-emite-nota-sobre-vazamento-de-dados-de-seus-clientes-em-ataque-hacker/. Acesso em: 08 nov. 2024.

WEDY, Gabriel. Princípios diferentes: Precaução no Direito Ambiental não quer dizer o mesmo que prevenção. *In*: CONSULTOR jurídico. [*S. l.*], 30 maio 2014. Disponível em: https://www.conjur.com.br/2014-mai-30/gabriel-wedy-precaucao-direito-ambiental-nao-prevencao. Acesso em: 09 nov. 2024.

WHAT is DDOS Attack? *In*: FORTINET. [*S. l.*], c2024. Disponível em: https://www.fortinet.com/resources/cyberglossary/ddos-attack. Acesso em: 08 nov. 2024.

X (TWITTER). *In*: TECNOBLOG. [*S. l.*], c2005-2024. Disponível em: https://tecnoblog.net/sobre/twitter/. Acesso em: 08 nov. 2024.