Leticia Piana Santos

O DIREITO INTERNACIONAL DE PROTEÇÃO DE DADOS E AS RESPONSABILIDADES DOS TRIBUNAIS E ORGANIZAÇÕES INTERNACIONAIS

Dissertação com vista à obtenção do grau de
Mestre em Direito e Prática Jurídica Europeia
na especialidade Ciências Jurídico-Políticas

Orientadora: Dra. Ana Rita Amaral Campos Gil

Lisboa
2024

A liberdade é a possibilidade do isolamento. (...)
Se te é impossível viver só,
nasceste escravo.

Fernando Pessoa

AGRADECIMENTOS

A conclusão desta dissertação foi possível graças ao apoio incondicional de várias pessoas, às quais aproveito a oportunidade para expressar minha gratidão.

Em primeiro lugar, à minha família. Sem o esforço e o sacrifício dos meus pais, que ao longo de toda a vida renunciaram outras prioridades em prol da minha educação, eu não estaria aqui.

Ao meu irmão, João Pedro, que apesar de mais novo, me inspira diariamente a crescer.

Ao meu Rodrigo, pelo apoio constante na busca dos meus sonhos.

Às minhas amigas da faculdade, em especial Amanda, Brunas, Katrine, Leticia, Larissa e Matheus, por me acompanharem durante a árdua trajetória da graduação e do exercício da advocacia.

Por fim, mas não menos importante, rendo minhas considerações à minha orientadora, Dra. Ana Rita Gil, que me apresentou o Direito Internacional sob uma nova perspectiva e cujo conhecimento levarei para a vida.

MODO DE CITAR

As referências bibliográficas utilizadas ao longo desta dissertação são feitas com a indicação dos sobrenomes dos autores, o título da obra (livro, tese ou artigo acadêmico) e, quando disponível, a cidade, a editora e o ano de publicação, além dos *links* para consulta e a respectiva data de acesso.

No caso de documentos, consta o nome da organização responsável; para legislações, são indicados o nome do país e o número do ato normativo correspondente; e quanto às jurisprudências, são fornecidos o nome do Tribunal e o número da decisão. Todos acompanham o *link* para acesso e a data de consulta.

Nas notas de rodapé, *op. cit*. é utilizado para obras de um mesmo autor já citadas anteriormente, em casos de citações intercaladas; *ibid*. é empregado para referências a obras imediatamente anteriores; e, para um mesmo autor com diferentes obras, *op. cit.* é seguido pela especificação da nota de rodapé correspondente.

Adotamos o Acordo Ortográfico da Língua Portuguesa, aprovado pela Resolução da Assembleia da República n.º 35/2008, de 29 de julho. As citações e os nomes de documentos em língua estrangeira foram mantidos no idioma original, mas apresentados em itálico.

Todas as referências podem ser consultadas ao final do trabalho, onde estão organizadas em ordem alfabética.

LISTA DE ABREVIATURAS

ACNUR - Alto-Comissariado das Nações Unidas para os Refugiados

AEPD - Autoridade Europeia de Proteção de Dados

APEC - Cooperação Econômica Ásia-Pacífico

CADH - Convenção Americana sobre Direitos Humanos

CCF - Comissão para o Controle dos Arquivos da INTERPOL

CCPA - *California Consumer Privacy Act*

CDI - Comissão de Direito Internacional

CE - Comunidade Europeia

CECA - Comunidade Europeia do Carvão e do Aço

CEDH - Convenção Europeia dos Direitos Humanos

CEE - Comunidade Econômica Europeia

CICV - Comitê Internacional da Cruz Vermelha

CNIL - *Commission Nationale de l'Informatique et des Libertés*

CoE - Conselho da Europa

CPA - Corte Permanente de Arbitragem

DUDH - Declaração Universal dos Direitos Humanos

ECOSOC - Conselho Econômico e Social

EDPB - Comitê Europeu para a Proteção de Dados

EEE - Espaço Econômico Europeu

EPD - Encarregado de Proteção de Dados

EUA - Estados Unidos da América

EURATOM - Comunidade Europeia da Energia Atômica

IA - Inteligência Artificial

IASC - Comitê Permanente Interagências

IEP - Instituto Europeu de Patentes

ILOAT - Tribunal Administrativo da Organização Internacional do Trabalho

INTERPOL - Organização Internacional de Polícia Criminal

LGPD - Lei Geral de Proteção de Dados

OCDE - Organização para a Cooperação e Desenvolvimento Econômico

OIM - Organização Internacional para as Migrações

OIs - Organizações internacionais

OMS - Organização Mundial da Saúde

ONU - Organização das Nações Unidas

PIDCP - Pacto Internacional sobre Direitos Civis e Políticos

PNUD - Programa das Nações Unidas para o Desenvolvimento

RGPD - Regulamento Geral sobre a Proteção de Dados

SOFA - Acordo do *Status* das Forças

STF - Superior Tribunal Federal

TEDH - Tribunal Europeu dos Direitos Humanos

TIJ - Tribunal Internacional de Justiça

TJUE - Tribunal de Justiça da União Europeia

TPI - Tribunal Penal Internacional

UE - União Europeia

UNAT - Tribunal de Apelações das Nações Unidas

UNCTAD - Conferência das Nações Unidas sobre Comércio e Desenvolvimento

UNDT - Tribunal de Disputas das Nações Unidas

UNICEF - Fundo das Nações Unidas para a Infância

UNIDO - Organização das Nações Unidas para o Desenvolvimento Industrial

RESUMO

A presente dissertação explora a interseção entre o Direito Internacional de proteção de dados e a responsabilidade das organizações internacionais (OIs) e Tribunais internacionais no processamento de informações pessoais. A disseminação de novas tecnologias como inteligência artificial e *big data* está causando rápidos avanços na transformação digital e, como resultado, as OIs estão gradualmente adotando mais ferramentas digitais em suas operações e lidando com uma quantidade maior de dados. Nesse contexto, apesar do crescente número de leis de proteção de dados desenvolvidas pelos Estados, as OIs operam sob a proteção de suas imunidades e privilégios, muitas vezes eximindo-as da jurisdição das legislações domésticas. A situação levanta questões críticas sobre como as OIs podem ser responsabilizadas por violações da proteção de dados. Assim, o estudo investiga (i) a evolução do quadro legal internacional de proteção de dados, (ii) a relação entre as OIs e os regimes internacional e doméstico de proteção de dados, destacando o papel da autorregulamentação, (iii) como os Tribunais internacionais processam dados pessoais e suas respectivas políticas internas e (iv) os desafios que surgem para responsabilizar as OIs em casos de descumprimento da proteção de dados. Através da metodologia qualitativa, são analisados casos práticos envolvendo a Cruz Vermelha, o Fundo das Nações Unidas para a Infância e o Tribunal Penal Internacional. As falhas nos mecanismos existentes são destacadas e medidas, que variam desde o desenvolvimento de normas internas de responsabilidade até a expansão da jurisdição dos Tribunais administrativos das OIs, são propostas para melhorá-los. Esta discussão torna-se cada vez mais importante à medida que o processamento de dados se intensifica globalmente, deixando as organizações mais vulneráveis a ataques cibernéticos ou à utilização ou divulgação inadequada de dados, e questionando a eficácia da autorregulamentação.

Palavras-chave: proteção de dados; organizações internacionais; privilégios e imunidades; autorregulamentação; responsabilização.

ABSTRACT

The present dissertation explores the intersection between international data protection law, and the accountability of international organizations (IOs) and international courts in processing personal information. The spread of the new technologies such as artificial intelligence and big data are causing rapid advances in digital transformation, as result, IOs are gradually adopting more digital tools in their operations and are handling a greater amount of data. In this context, despite the increasing number of data protection laws developed by States, IOs operate under the protection of their immunities and privileges, often exempting them from the jurisdiction of domestic legislation. The situation raises critical questions of how IOs can be held accountable for data protection violations. Thus, the study investigates (i) the evolution of the international data protection framework, (ii) the relationship between IOs and international and domestic data protection regimes, highlighting the role of self-regulation, (iii) how international courts process personal data and their respective internal policies, and (iv) the challenges that arise when holding IOs accountable in cases of non-compliance with data protection. Through a qualitative methodology, practical cases involving the Red Cross, the United Nations Children's Fund, and the International Criminal Court are analyzed. The flaws in existing mechanisms are highlighted and measures, ranging from the development of internal accountability norms to the expansion of the jurisdiction of IOs' administrative courts are proposed to improve them. This discussion becomes increasingly important as data processing intensifies globally, leaving organizations more vulnerable to cyber-attacks or improper use or disclosure of data, and questioning the effectiveness of self-regulation.

Key words: data protection; international organizations; privileges and immunities; self-regulation; accountability.

ÍNDICE

INTRODUÇÃO

Na afirmação “o capitalismo de vigilância reivindica de maneira unilateral a experiência humana como matéria-prima gratuita para a tradução em dados comportamentais”[1], a autora Shoshana Zuboff reflete como as interações e comportamentos cotidianos dos indivíduos são coletados e transformados em dados que serão potencialmente explorados comercialmente, sem o devido consentimento. As informações coletadas são utilizadas para aprimorar serviços e criar produtos preditivos que buscam antecipar as ações dos indivíduos, alimentando um novo mercado focado em comportamentos futuros. Os capitalistas de vigilância se enriquecem com essas operações e têm cada vez mais cobiça por dados que representam “nossas vozes, personalidades e emoções”[2]. Em razão disso, o cuidado e a tutela das organizações que armazenam informações pessoais devem ser reforçados, a fim de mitigar os riscos decorrentes da exploração desenfreada de dados e preservar a dignidade humana num cenário simultâneo de digitalização e vigilância.

A transformação digital tem evoluído exponencialmente ao longo das últimas décadas. A terceira revolução industrial, conhecida como a revolução digital, foi marcada pela transição do analógico ao digital[3], causando um impacto profundo na maneira como nos comunicamos e como as empresas operam, a partir da disseminação da Internet e dos dispositivos móveis. Com o início do século XXI, a quarta revolução industrial trouxe inovações ainda mais radicais, como a inteligência artificial (IA), a robótica e a integração de sistemas digitais através da computação em nuvem e dispositivos inteligentes[4]. Atualmente, vemos a rápida adoção dessas tecnologias tanto no setor público quanto no privado, como uma forma de otimizar as atividades. No entanto, junto com os benefícios, surgem problemas na garantia de direitos fundamentais, nomeadamente a proteção de dados pessoais, que se tornou um elemento central na era digital.

---

[1] ZUBOFF, S. A Era do Capitalismo de Vigilância: a Luta por um Futuro Humano na Nova Fronteira do Poder. Nova York: Intrínseca, 2021. p. 22.
[2] *Ibid*., p. 23.
[3] XU, M. et al. The fourth industrial revolution: opportunities and challenges. International Journal of Financial Research, v. 9, n. 2. Toronto: Sciedu Press, 2018. p. 90-95. Disponível em: http://creo.sc-celje.si/pluginfile.php/2387/mod_resource/content/1/4.1.4_01_The%20fourth%20industrial%20revolution.pdf. Acesso em: 20 set. 2024.
[4] *Ibid*.

A ideia de informação pessoal é mais ampla do que o conceito clássico associado aos direitos de personalidade e inclui todos os aspectos que dizem respeito a um indivíduo, tanto em sua esfera familiar quanto social, sejam públicos ou privados, físicos ou psicológicos[5]. O direito à proteção de dados é essencial para garantir a dignidade dos indivíduos na gestão de suas informações e permitir que as pessoas tenham controle sobre suas vidas. As estruturas legais com tal objeto visam garantir um tratamento justo, transparente e responsável, de modo que as organizações sejam claras sobre como utilizam os dados e os titulares possam decidir quem tem acesso, como e por que eles são usados. Na relação entre organizações e indivíduos, a ideia é que exista confiança para que as pessoas se sintam seguras ao compartilhar suas informações. À medida em que as tecnologias avançam e são adotadas com mais frequência, os Estados passaram a aprimorar as leis de proteção de dados, pois as legislações existentes não cobriam adequadamente os novos riscos e desafios, especialmente devido ao envolvimento de terceiros com enorme capacidade de manipulação e desejo de obtenção das informações.

Igualmente, as organizações internacionais (doravante OIs) vêm acolhendo a transformação digital através da adoção de diferentes tecnologias e, a partir disso, vêm desenvolvendo regulamentos internos para o tratamento adequado dos dados pessoais. A autorregulamentação é necessária em virtude de que as referidas entidades (inclusive os Tribunais internacionais) são consideradas sujeitos de Direito Internacional e, por força de acordos internacionais, gozam de imunidades e privilégios e não se submetem às legislações domésticas criadas pelos Estados. Os benefícios foram criados para garantir que suas funções sejam executadas sem interferências dos governos e para que sejam independentes de interesses políticos. Dessa forma, as OIs formulam políticas internas baseadas em instrumentos legais internacionais e nacionais sobre proteção de dados, incluindo princípios gerais, direitos dos titulares dos dados pessoais, mecanismos internos de supervisão e medidas de responsabilização pelo uso ou divulgação inadequados.

Contudo, o que se tem observado são falhas nessas autorregulamentações, particularmente nas medidas de responsabilização às OIs que não cumprem suas políticas internas de proteção de dados. Ao violarem um direito fundamental de um indivíduo, a organização poderá utilizar dos seus privilégios de forma ilimitada e em

[5] CORDEIRO, A. B. M. Dados pessoais: conceito, extensão e limites. Revista de Direito Civil, a.3, n.2. Lisboa: CIDP, 2018. p. 297-321.

prejuízo ao direito de reparação do indivíduo afetado, que muitas vezes não poderá aceder a um Tribunal doméstico para buscar compensação judicial. A responsabilização das OIs é, portanto, complexa e enfrenta desafios únicos no contexto da proteção de dados. Numa perspectiva geral, o presente trabalho pretende expor como as OIs se encaixam no regime jurídico internacional de proteção de dados e quais são os desafios para a criação de mecanismos eficazes de responsabilização diante de suas imunidades e privilégios.

Para responder tal problemática, os capítulos estão estruturados da seguinte forma: o capítulo a seguir descreverá os principais instrumentos legais internacionais de proteção de dados, tanto no campo *soft law*, quanto no *hard law*, com ênfase para a Convenção 108+ do Conselho da Europa (CoE), por ser a única que criou obrigações vinculativas às partes signatárias e está aberta à ratificação das OIs, mesmo não havendo nenhuma que a ratificou; na sequência, fará observações pontuais sobre as leis domésticas que regulam o tema. No próximo capítulo, será feita uma análise sobre a interação das OIs com o regime jurídico de proteção de dados, especialmente tendo em conta os privilégios concedidos a essas organizações, justificando a sua não sujeição às leis nacionais e, ao mesmo tempo, demonstrando de que forma elas são mencionadas nos instrumentos legais internacionais e domésticos. Ademais, o capítulo explorará a autorregulamentação das OIs como uma tentativa de equilíbrio à ausência de regras legais vinculativas, fazendo observações específicas sobre as normas internas da Cruz Vermelha e do Fundo das Nações Unidas para a Infância (UNICEF).

No capítulo subsequente, os Tribunais internacionais (e seus regulamentos internos sobre proteção de dados) serão objeto de estudo, em particular o Tribunal Internacional de Justiça (TIJ), o Tribunal Penal Internacional (TPI) e o Tribunal de Justiça da União Europeia (TJUE). O último capítulo terá como objeto a responsabilização internacional das OIs e os desafios oriundos da falta de reconhecimento da proteção de dados como obrigação legal internacional. Ato contínuo, a responsabilização por Tribunais domésticos será analisada à luz da imunidade de jurisdição e da limitação de competência dos Tribunais administrativos das OIs, que usualmente se restringem às demandas trabalhistas com seus funcionários. Isso tudo ficará evidente ao analisar casos de violações da proteção de dados por três organizações: a Cruz Vermelha, a UNICEF e o TPI, fazendo referências às normas internas expostas nos capítulos anteriores. Por fim, serão oferecidas

possibilidades para aprimorar as medidas de responsabilização das OIs, que se submetem apenas às suas regulações internas e acabam por não adotar medidas sancionatórias.

O tema é relevante para a comunidade acadêmica, pois, apesar da abundância de trabalhos sobre a responsabilização das OIs, há uma escassez na pesquisa específica dessa temática em casos de violações da proteção de dados. Isso reforça a necessidade de discussão, mormente num cenário de avanço tecnológico e consequente aumento na quantidade de dados pessoais coletados, os quais são progressivamente mais vistos como ferramentas estratégicas e utilizados como armas contra os seus titulares. As OIs aproveitam as novas tecnologias e, simultaneamente, se expõem a maiores riscos, em especial as humanitárias que armazenam dados pessoais sensíveis – aqueles que revelam características genéticas, étnicas, religiosas, políticas etc. A falta de mecanismos eficazes de responsabilização (administrativa e judicial) por violações da proteção de dados cria um cenário de impunidade e permite que as OIs operem sem supervisão.

A metodologia adotada é sobretudo qualitativa[6], envolvendo a análise de instrumentos legais internacionais, como convenções, tratados, diretrizes, regulamentos, e leis domésticas. As políticas internas de OIs também serão criticamente examinadas e, depois, relacionadas com casos práticos de violação da proteção de dados por essas mesmas organizações. Ademais, o trabalho se apoiará na pesquisa bibliográfica, mediante a revisão da doutrina jurídica, artigos acadêmicos e teses, assim como em jurisprudências de Tribunais internacionais e domésticos e decisões proferidas pelos Tribunais administrativos das próprias OIs. Todo o material coletado possibilitará a conclusão sobre o equilíbrio entre imunidades e privilégios e a disponibilização de mecanismos alternativos de resolução de disputas, com foco no fortalecimento das medidas de responsabilização no contexto da proteção de dados.

Por fim, espera-se que o leitor reflita sobre a urgente necessidade de repensar as estruturas atuais de proteção de dados e de responsabilização das OIs, frente à crescente valorização e comercialização das informações pessoais – por atores muitas vezes mal-intencionados – e às ameaças à privacidade na nova era digital.

---

[6] Oliveira, A. F. S. de; MIALHE, J. L. A Possibilidade de Desenvolver Pesquisas no Campo Jurídico valendo-se da Metodologia de Abordagem Qualitativa, v. 2 n. 1. Revista de Pesquisa e Educação Jurídica. Brasília: Index Law Journals, 2016. p. 40-56. Disponível em: https://indexlaw.org/index.php/rpej/article/view/158. Acesso em: 21 set. 2024.

1. EVOLUÇÃO DO DIREITO INTERNACIONAL DE PROTEÇÃO DE DADOS

Este capítulo apresenta uma revisão acerca do desenvolvimento dos instrumentos regulatórios criados ao redor do globo a fim de proteger a privacidade e os interesses relacionados ao processamento dos dados pessoais. As principais regras – e que de certa forma são comuns a esses instrumentos regulatórios – derivam de um conjunto de princípios de "informação justa"[7], estipulando a maneira e os propósitos do processamento de dados; medidas para garantir a qualidade adequada dos dados; e medidas para garantir que o processamento seja transparente e acessível para o titular dos dados.

Numa perspectiva geral, esses instrumentos constituem um conjunto de normas jurídicas e de políticas públicas que, ao longo dos últimos cinquenta anos, se propagou pelo mundo e alcançou um elevado grau de importância normativa. Segundo dados da Conferência das Nações Unidas sobre Comércio e Desenvolvimento (UNCTAD), 137 dos 194 países (78%) já contam com uma lei de proteção de dados no seu ordenamento jurídico[8]. Essas iniciativas nacionais são inspiradas por um grande número de diretrizes e regulamentos internacionais.

Contudo, a análise precisa e pormenorizada de todas as normativas legais de proteção de dados ultrapassaria o escopo deste capítulo. O principal objetivo aqui é delinear – em ordem cronológica – os principais instrumentos internacionais e destacar alguns instrumentos domésticos de proteção de dados, de modo a contextualizar o quadro normativo em que se encontram as OIs, para depois expor mais detalhadamente como elas interagem com essas mesmas leis, regulamentos e diretrizes.

1.1. INSTRUMENTOS REGULATÓRIOS INTERNACIONAIS

[7] As Práticas Justas de Informação, publicadas pela OCDE em 1980, são um conjunto estabelecido de diretrizes para a privacidade do consumidor. Elas têm suas raízes em um relatório de 1973 do "Departamento de Saúde, Educação e Bem-Estar dos Estados Unidos" e foram elaboradas para facilitar a transferência transfronteiriça de informações de clientes como parte do comércio entre seus Estados-membros. U.S. DEPARTMENT OF HOMELAND SECURITY. Privacy Policy Guidance Memorandum. Washington: U.S. Department of Homeland Security, 2008. Disponível em: https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. Acesso em: 20 mar. 2024.

[8] UN TRADE AND DEVELOPMENT. Data Protection and Privacy Legislation Worldwide. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 20 mar. 2024.

Dentre os direitos fundamentais que servem de base para a formação das leis de proteção de dados, a título de exemplo o direito à dignidade e à liberdade de expressão[9], o direito à privacidade tem uma importância especial, tanto é que as legislações neste contexto frequentemente destacam a proteção desse direito como central em sua justificativa formal[10]. Isso também se reflete na jurisprudência desenvolvida em volta do artigo 17 do Pacto Internacional sobre Direitos Civis e Políticos (PIDCP) e do artigo 8 da Convenção Europeia dos Direitos Humanos (CEDH): ambas as disposições foram interpretadas de forma a exigir a implementação nacional dos princípios básicos das leis de proteção de dados com relação tanto ao setor público quanto ao privado[11].

O direito à vida privada é expressamente reconhecido nos dois principais instrumentos multilaterais de direitos humanos: a Declaração Universal dos Direitos Humanos (DUDH)[12] e o PIDCP[13], assim como nos principais instrumentos regionais: a CEDH[14] e a Convenção Americana sobre Direitos Humanos (CADH)[15]. A Carta Africana dos Direitos Humanos e dos Povos não qualifica o direito à privacidade como fundamental, mas isso não é padrão em todos os instrumentos de direitos humanos

---

[9] Os dois princípios refletem a importância de proteger o indivíduo em uma sociedade democrática: o direito à dignidade é a base para garantir que as informações pessoais de uma pessoa sejam tratadas de forma respeitosa, sem violar sua integridade moral ou sua privacidade, ao passo que a liberdade de expressão deve ser equilibrada com a proteção dos dados, pois embora seja essencial poder se expressar livremente, isso não pode ser feito à custa da privacidade alheia.

[10] Ver, por exemplo, a Lei Geral de Proteção de Dados n.º 13.709/2018 do Brasil, cujo objetivo é 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: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 mar. 2024.

[11] Merece destaque o caso Von Hannover v. Germany julgado pelo TEDH em 2004, que reconheceu a obrigação positiva dos Estados em estabelecer regras domésticas de proteção de dados, sob pena de infringir o artigo 8 da CEDH, inclusive se a violação for praticada por um ator privado. Para análise detalhada da jurisprudência, ver DE HERT, P.; GUTWIRTH, S. Data Protection in the Case Law of Strasbourg and Luxemburg. In: GUTWIRTH, S. et al. Reinventing Data Protection? 1. ed. Dordrecht: Springer, 2009. p. 3-45. Disponível em: https://doi.org/10.1007/978-1-4020-9498-9. Acesso em: 23 mar. 2024.

[12] UNICEF. Declaração Universal dos Direitos Humanos. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 22 mar. 2024.

[13] ONU. Pacto Internacional sobre Direitos Civis e Políticos. Disponível em: https://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf. Acesso em: 22 mar. 2024.

[14] TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM. Convenção Europeia dos Direitos Humanos. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf. Acesso em: 22 mar. 2024.

[15] COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. Convenção Americana sobre Direitos Humanos. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 22 mar. 2024.

existentes fora da esfera ocidental: é o exemplo da Declaração de Cairo sobre Direitos Humanos[16], que reconhece expressamente o direito à privacidade aos indivíduos.

Apesar da evidente demanda global por uma regulação unificada no âmbito da proteção de dados pessoais, ainda não existe uma convenção, tratado ou pacto internacional especificamente dedicado a esse tema. A Convenção do CoE para a Proteção das Pessoas Singulares no que diz respeito ao Tratamento Automatizado de Dados Pessoais (doravante "Convenção 108") é o instrumento que mais se aproxima dessa necessidade, eis que, mesmo sendo uma regulação europeia de caráter vinculativo, está aberta para ratificação por países fora da Europa e, por conseguinte, possibilita que nações de outros continentes se comprometam com as disposições da Convenção.

No campo de *soft law*, OIs independentes criaram vários instrumentos normativos sobre proteção de dados que se apresentam na forma de diretrizes, resoluções, políticas internas e códigos de conduta. Embora não sejam vinculativos, representam um grande peso político (quando pensamos na Organização das Nações Unidas – ONU) ou comercial (quando pensamos na Organização para a Cooperação e Desenvolvimento Econômico – OCDE). As Diretrizes sobre Proteção da Privacidade e Fluxos Transfronteiriços de Dados Pessoais, adotadas pela OCDE em 1981, são um dos instrumentos de *soft law* mais importantes para os Estados industrializados que participam do intercâmbio comercial e dependem de fluxos transfronteiriços de dados nas suas operações gerais[17].

Ainda vigente, o documento influenciou a elaboração de leis em diversas nações[18] e, não obstante careça de vinculação, estabeleceu princípios a nível internacional. De fato, as Diretrizes surgiram como resposta à dificuldade enfrentada por legisladores nacionais para formular regras que garantam a privacidade em ambas

---

[16] UNIVERSITY OF MINNESOTA – HUMAN RIGHTS LIBRARY. Cairo Declaration on Human Rights in Islam. Disponível em: http://hrlibrary.umn.edu/instree/cairodeclaration.html. Acesso em: 22 mar. 2024.
[17] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Paris: OECD, 2002. Disponível em: https://doi.org/10.1787/9789264196391-en. Acesso em: 20 mar. 2024.
[18] No Brasil, a LGPD adotou uma abordagem alinhada com as diretrizes da OCDE. Nesse sentido, ver o quadro comparativo em CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. Transferência Internacional de Dados: Orientações para a Indústria. Brasília: CNI, 2020. p. 66. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/46/fc/46fce346-06e8-4a05-b3e2-b8f6f15f0afd/id_240807_transferencia_internacional_de_dados_interativo.pdf. Acesso em: 25 mar. 2024. É o caso também da lei federal de privacidade da Austrália de 1988 que faz expressa referência às Diretrizes da OECD no preâmbulo, ver AUSTRÁLIA. Privacy Act 1988. Disponível em: https://www.legislation.gov.au/C2004A03712/2017-07-01/text. Acesso em: 25 mar. 2024.

as situações: quando os dados pessoais permanecem no país ou quando saem ou são transferidas para além das fronteiras nacionais. Assim, reconhecendo a possibilidade de confrontos transnacionais sobre fluxos transfronteiriços de dados como consequência de leis nacionais divergentes, a OCDE tentou harmonizar e buscar soluções em comum para os quadros nacionais dos países membros[19].

As Diretrizes da OCDE também serviram como base para o desenvolvimento do Quadro de Privacidade adotado pela Cooperação Econômica Ásia-Pacífico (APEC) em 2005. Esta normativa apresenta um conjunto de nove princípios de privacidade da informação, que foram adaptados e flexibilizados a partir dos princípios estabelecidos nas Diretrizes da OCDE[20]. A flexibilidade foi intencionalmente projetada para acomodar os diversos contextos culturais e legais dos vinte e dois Estados-membros da APEC[21], que podem voluntariamente implementar os princípios em suas economias nacionais.

Por sua vez, a Convenção 108 foi aprovada pelo Comitê de Ministros do CoE, adotada e aberta para ratificação em 28 de janeiro de 1981[22], cujo aniversário é agora comemorado anualmente como o Dia da Privacidade de Dados[23]. A convenção entrou em vigor formalmente em 1 de outubro de 1985. A sua versão original foi assinada e ratificada por todos os 47 membros do CoE. Ela também foi ratificada por nove países fora do CoE na África e América Latina: Argentina, Cabo Verde, Maurício, México,

---

[19] "(...) *there is a danger that disparities in national legislations could hamper the free flow of personal data across frontiers; these flows have greatly increased in recent years and are bound to grow further with the widespread introduction of new computer and communications technology. Restrictions on these flows could cause serious disruption in important sectors of the economy, such as banking and insurance*", declara o prefácio das Diretrizes da OECD.

[20] "*This Framework, which aims at promoting electronic commerce throughout the Asia Pacific region, is consistent with the core values of the OECD's 1980 Guidelines on the Protection of Privacy and Trans-Border Flows of Personal Data (OECD Guidelines), and reaffirms the value of privacy to individuals and to the information society*", dispõe o preâmbulo da APEC. APEC - Asia-Pacific Economic Cooperation. APEC Privacy Framework. Disponível em: https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf. Acesso em: 30 mar. 2024.

[21] Austrália, Brunei, Darussalam, Canadá, Indonésia, Japão, Malásia, Nova Zelândia, Filipinas, Cingapura, Coréia do Sul, Tailândia, Estados Unidos da América, China, Hong Kong, Taiwan, México, Papua Nova Guiné, Chile, Peru, Rússia e Vietnã.

[22] Sobre o contexto histórico da Convenção 108, ver COUNCIL OF EUROPE. "Background". Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: https://www.coe.int/en/web/data-protection/convention108/background#:~:text=In%201981%2C%20after%20four%20years,as%20Convention%20108%20%2D%20was%20concluded. Acesso em: 27 mar. 2024.

[23] GOVERNO DE PORTUGAL. "28 de janeiro, Dia Europeu da Proteção de Dados". Portal da Economia. Disponível em: https://www.sgeconomia.gov.pt/noticias/28-de-janeiro-dia-europeu-da-protecao-de-dados.aspx#:~:text=A%2028%20de%20janeiro%20comemora,a%20prote%C3%A7%C3%A3o%20dos%20dados%20pessoais. Acesso em: 27 mar. 2024.

Marrocos, Rússia, Senegal, Tunísia e Uruguai[24]. Na época, muitos países não possuíam regras abrangentes de proteção de dados para a coleta, armazenamento e uso de informações pessoais. Assim, o documento do CoE impulsionou uma maior harmonização nos padrões de proteção de dados e teve uma influência significativa na primeira geração de leis de proteção de dados, incluindo o primeiro *Data Protection Act* do Reino Unido em 1984[25].

A Convenção estabeleceu um Comitê Consultivo composto por representantes dos Estados signatários e complementado por observadores de outros Estados (membros ou não-membros[26]) e OIs, cuja função é interpretar as disposições e melhorar a implementação da Convenção, além de elaborar relatórios, diretrizes e princípios orientadores sobre tópicos como cláusulas contratuais que regem a proteção de dados durante a transferência de dados pessoais para terceiros não vinculados por um nível adequado de proteção[27]. Um protocolo adicional à Convenção foi adicionado em 2001, exigindo a nomeação de uma autoridade de proteção de dados e impondo certas restrições à exportação de dados para transferências a países não signatários da Convenção[28].

Em 2018, o CoE atualizou a Convenção 108, que passou a ser denominada Convenção 108+. A modernização foi necessária para enfrentar os avanços tecnológicos desde a sua adoção, numa época em que não existia Internet, *big data*,

---

[24] COUNCIL OF EUROPE. Conventions - Full List. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108. Acesso em: 30 mar. 2024.

[25] O Reino Unido promulgou seu primeiro *Data Protection Act* em 1984 e incorporou oito princípios de proteção de dados derivados da Convenção 108 do CoE, incluindo a obtenção e processamento justo e legal dos dados pessoais, que não poderiam ser mantidos por mais tempo que o necessário. PARLIAMENT OF THE UNITED KINGDOM. General Data Protection Regulation (GDPR) Briefing Paper. Disponível em: https://researchbriefings.files.parliament.uk/documents/LLN-2017-0065/LLN-2017-0065.pdf. Acesso em: 28 mar. 2024.

[26] É o caso do Brasil, Estado não membro e observador, que por intermédio da Autoridade Nacional de Proteção de Dados (ou ANPD) foi convidado a participar do Comitê Consultivo da Convenção 108 em 2021. ANPD. Semana da Proteção de Dados 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/semana-protecao-dados-2022. Acesso em: 30 mar. 2024.

[27] COUNCIL OF EUROPE. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). Disponível em: https://search.coe.int/cm?i=09000016804e0476. Acesso em: 30 mar. 2024.

[28] MINISTÉRIO PÚBLICO DE PORTUGAL. Protocolo Adicional à Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais, Relativo à Interceção de Comunicações, a Equipamentos de Interceptação e à Interceção de Tráfego de Comunicações (STCE n.º 185, E.T.S. n.º 108). Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/protocolo_adicional_convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal_aut_fluxos_transfront_dados.pdf. Acesso em: 01 abr. 2024.

geolocalização, redes sociais ou objetos conectados. Além do crescimento tecnológico, aumentaram o volume de dados processados, a escala das operações com dados, o valor econômico atribuído aos dados, a variedade de atores envolvidos, as ameaças aos dados, a disponibilidade geral dos dados no tempo e no espaço etc. A proteção dos indivíduos em 1981 não demandava tanta atenção e cautela como no mundo interconectado atual, onde os dados pessoais são cobiçados por governos, empresas e organizações no geral[29]. A modernização também expandiu a cobertura da Convenção para permitir que OIs também a ratificassem[30].

A importância desse instrumento legal se revela no fato de que, desde a sua criação em 1981 até os dias atuais, as normas do CoE se mantiveram centrais no desenvolvimento e implementação de padrões de proteção de dados a nível global. Primeiro, porque não existe outro documento internacional que compartilhe o mesmo *status* de legalmente vinculativo aos Estados signatários. Segundo, porque as disposições da Convenção são facilmente compreendidas quando comparadas com outros instrumentos legais da União Europeia (UE). Terceiro, dispõe sobre regras específicas sobre as competências e limites das autoridades fiscalizadoras. Por último, a Convenção tem uma base sólida nos direitos humanos, particularmente no direito à privacidade garantido no artigo 8 da CEDH[31].

Do CoE para a UE, o primeiro ato normativo especificamente sobre proteção de dados foi a Diretiva 95/46/CE[32], relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados – que depois veio a ser substituída em 2016 pelo Regulamento Geral sobre a Proteção de

[29] BENNETT, C. J. The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession. Waterloo: Centre for International Governance Innovation, 2020. p. 3–5. Disponível em: http://www.jstor.org/stable/resrep27512.8. Acesso em: 03 abr. 2024.

[30] COUNCIL OF EUROPE. Proposal for a COUNCIL DECISION authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0449&from=HU. Acesso em: 03 jun. 2024.

[31] Conforme exposto em DE HERT, P.; PAPAKONSTANTINOU, V. The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition. Computer Law & Security Review, v. 30, n. 6. Southampton: Elsevier, 2014. p. 633-642. Disponível em: https://doi.org/10.1016/j.clsr.2014.09.002. Acesso em: 30 maio 2024.

[32] UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:31995L0046. Acesso em: 02 abr. 2024.

Dados (RGPD[33]). A antiga Diretiva era vinculativa para os Estados-membros da UE, embora com ressalvas quanto à segurança pública, defesa e segurança do Estado[34]. Certos Estados não membros (Noruega, Islândia e Liechtenstein) que são partes do Acordo sobre o Espaço Econômico Europeu (Acordo EEE) de 1992 também estavam obrigados a implementar a Diretiva, com as mesmas ressalvas mencionadas anteriormente.

Além de alterar o cenário regulatório dos países membros da UE, a Diretiva também exerceu forte influência sobre países fora da União ao proibir a transferência de dados pessoais para países terceiros com nível "não adequado" de proteção[35]. Por consequência, muitas nações não europeias promulgaram leis de proteção de dados justamente para atender ao critério de adequação imposto pela UE. Ademais, a normativa estabelecia que a lei de proteção de dados de um Estado da UE pode se aplicar fora da UE na hipótese em que o controlador, mesmo não estando estabelecido no território da Comunidade, recorre a meios, automatizados ou não, situados nesse Estado-membro[36]. Isso tudo evidencia a presença e domínio da legislação da UE no resto do mundo.

Por sua vez, a ONU também se manifestou no plano da proteção de dados pessoais por meio da adoção das Diretrizes para a Regulação de Ficheiros Informatizados de Dados de Caráter Pessoal, pela resolução 45/95 da Assembleia Geral das Nações Unidas, de 14 de dezembro de 1990[37]. A primeira seção do documento trata dos princípios relativos às garantias mínimas que devem ser observadas pelas legislações nacionais, ao passo que a segunda seção cuida da aplicação das Diretrizes aos ficheiros de dados de caráter pessoal mantidos por OIs de caráter intergovernamental, dispondo que cada organização deve designar uma autoridade estatutariamente competente para supervisionar a observância das diretrizes[38]. O documento conta inclusive com uma cláusula humanitária, que permite uma exceção específica aos princípios quando um arquivo tem o objetivo de proteger

---

[33] JORNAL OFICIAL DA UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 30 mar. 2024.
[34] Artigo 3(2) da Diretiva 95/46/CE.
[35] Artigos 25 e 26 da Diretiva 95/46/CE.
[36] Artigo 4(1)(c) da Diretiva 95/46/CE.
[37] MINISTÉRIO PÚBLICO DE PORTUGAL. Diretrizes para a Proteção de Dados Pessoais no Ministério Público. Adotadas pela resolução 45/95 da Assembleia Geral das Nações Unidas, de 14 de dezembro de 1990. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/diretrizes-protecaodados.pdf. Acesso em: 30 mar. 2024.
[38] *Ibid*.

os direitos humanos e as liberdades fundamentais do indivíduo ou fornecer assistência humanitária. Em termos práticos, isso significa que, em certas circunstâncias, os requisitos padrão para o tratamento de dados podem ser suspensos se o objetivo for proteger os direitos humanos ou oferecer ajuda humanitária. Além disso, essa exceção deve ser prevista na legislação nacional para OIs intergovernamentais quando o acordo que estabelece a sede dessas organizações não impeça a aplicação da legislação interna; e para organizações não-governamentais internacionais quando estejam sujeitas à mesma legislação nacional[39].

Porém, a aplicabilidade ou influência das Diretrizes da ONU não alcançou a mesma força que outros instrumentos legais revisados acima: as Diretrizes da OCDE e a Convenção 108 – inclusive no âmbito das OIs humanitárias[40]. Em que pese seu peso político, as resoluções da Assembleia Geral das Nações Unidas não têm caráter vinculante aos Estados-membros da ONU. Além do que, analisando as três normativas, é possível inferir que a ONU regulou o tratamento dos dados pessoais somente nos ficheiros informatizados, ao passo que as regras da OCDE e do CoE são mais extensas, aptas a alcançar mais setores[41] e, em especial, estimulam a harmonização de legislações nacionais e autorregulamentações de empresas, companhias e organizações.

Com efeito, mais que incentivar a criação de leis nacionais e regulações internas, os instrumentos internacionais visam a harmonização das regras aplicáveis à proteção de dados, tanto para aprimorar o tratamento das informações pessoais, quanto para facilitar o fluxo desses dados no comércio internacional, salvaguardar a liberdade de expressão e incentivar a cooperação entre os governos[42]. Essas preocupações surgem porque muitas leis nacionais de proteção de dados –

---

[39] *Ibid*.

[40] BYGRAVE, L. A. International agreements to protect personal data. In: RULE, J. B. Global Privacy Protection: The First Generation. UK: Edward Elgar, 2008. Disponível em: https://doi.org/10.4337/9781848445123. Acesso em: 03 abr. 2024.

[41] A Convenção 108 foi expandida pelo CoE através de recomendações que são aplicáveis apenas a determinados setores. Para o setor policial, existe a Recomendação do Comitê de Ministros do Conselho da Europa n.º R(87)15 aos Estados-Membros sobre a regulamentação da utilização de dados pessoais no setor policial, 17.9.1987. Para o setor de telecomunicações, a Recomendação do Comitê de Ministros do Conselho da Europa n.º R(95)4 aos Estados-Membros sobre a proteção de dados pessoais na área de telecomunicações, 7.2.1995.

[42] KONG, L. Data Protection and Transborder Data Flow in the European and Global Context. European Journal of International Law, v. 21, n. 2. Oxford: Oxford University Press, 2010. p. 441–456. Disponível em: https://doi.org/10.1093/ejil/chq025. Acesso em: 04 abr. 2024.

principalmente europeias – costumavam operar com restrições de fluxo de dados para países com um nível de proteção de dados menor do que o país "exportador"[43].

Apesar de seus objetivos de harmonização, os instrumentos internacionais tendem a conceder aos países um grau significativo de flexibilidade no desenvolvimento de seus respectivos regimes de proteção de dados. Isso é especialmente o caso com os instrumentos de *soft law*[44], mas mesmo os instrumentos legalmente vinculativos permitem considerável flexibilidade nacional. É o caso da Convenção do CoE que não se destina a ser auto executável e permite derrogações em pontos significativos[45]. Outrossim, a Diretiva da UE tinha como objetivo facilitar uma aproximação em oposição à uniformidade completa das leis nacionais, o que dava uma considerável brecha de regulamentação aos Estados-membros da UE[46].

Por sua vez, o RGPD, implementado pela UE em maio de 2018, tentou fornecer um quadro mais harmonizado em todo o bloco econômico, com um conjunto mais consistente e único de regras para as empresas e organizações que operam em sua jurisdição. Ao contrário de uma Diretiva, que harmoniza e dá aos Estados alguma liberdade de escolher os meios para prosseguir os fins visados pela Diretiva, um Regulamento não precisa de ser transposto, já que integra automaticamente a ordem interna do Estado-membro e a legislação nacional deverá adequar-se ao mesmo. A intenção da UE era que, ao substituir um ato legislativo por outro, os Estados-membros não tivessem oportunidade de manobrar e introduzir as suas próprias vontades na lei doméstica[47].

Não obstante a relevância do Regulamento europeu na harmonização do processamento (coleta, armazenamento, utilização, transferência e exclusão) de dados pessoais – dentro e fora da Europa – não há uma legislação uniformizada em escala global[48]. Com exceção da Convenção do CoE, a comunidade internacional

---

[43] LYNSKEY, O. The foundations of EU data protection law. Oxford: Oxford University Press, 2015.
[44] BYGRAVE, L. A. Strasbourg Effect on EU Data Protection. Computer Law & Security Review, v. 40. Oslo, Norway: Elsevier Ltd., 2020. Disponível em: https://www.duo.uio.no/bitstream/handle/10852/92263/1/Strasbourg_effect_final.pdf. Acesso em: 05 abr. 2024.
[45] Ver artigo 11 da Convenção 108+.
[46] BYGRAVE, L. A., *op. cit*.
[47] MOEREL, L. GDPR Conundrums: The GDPR Applicability Regime, Part 1 - Controllers. Disponível em: https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/. Acesso em: 06 abr. 2024.
[48] O próprio artigo 10 do RGPD dá aos Estados-membros um certo nível de flexibilidade para adotar procedimentos próprios na legislação interna: "No que diz respeito ao tratamento de dados pessoais para cumprimento de uma obrigação jurídica, para o exercício de funções de interesse público ou o exercício da autoridade pública de que está investido o responsável pelo tratamento, os Estados-

carece de um instrumento legal vinculativo especificamente direcionado para o tratamento dos dados pessoais que seja ratificado pela maioria dos Estados (ou OIs) no mundo. Como resultado, a regulamentação sobre o tratamento de dados pessoais é deixada para as leis internas de cada país.

1.2. LEIS DOMÉSTICAS

No âmbito doméstico, importa destacar o papel crucial e influenciador dos países europeus na construção legal no campo da proteção de dados. A preocupação europeia é evidente quando percebemos que a maioria dos países, em algum momento da história, reconheceu os dados pessoais como um objeto jurídico a ser tutelado na mesma posição que outros direitos fundamentais[49]. De fato, a Europa abriga as leis de proteção de dados mais antigas[50], mais abrangentes e mais complexas, tanto a nível nacional quanto regional. Além disso, como mostrado no subcapítulo anterior, o continente europeu – por meio de suas instituições supranacionais – também é a base para as iniciativas internacionais mais ambiciosas e extensivas no campo.

Membros deverão poder manter ou aprovar disposições nacionais para especificar a aplicação das regras do presente regulamento."

[49] O direito à proteção de dados foi elevado ao nível de direito fundamental na CEDH, após o TEDH reconhecer que ele parcialmente se enquadrava no escopo protetor do artigo 7 da CEDH, que especifica: "1. Qualquer pessoa tem direito ao respeito da sua vida privada e familiar, do seu domicílio e da sua correspondência". Por seu turno, a Carta de Direitos Fundamentais da UE, no artigo 7, garante o direito à privacidade e o artigo 8 separa o direito à proteção dos dados pessoais do direito à privacidade e o define também como um direito fundamental.

[50] Em 1970, o Estado de Hesse na Alemanha Ocidental adotou a primeira lei do mundo especificamente sobre proteção de dados, denominada "Datenschutzgesetz" e, em 1977, adotou a primeira lei federal de proteção de dados ou "Bundesdatenschutzgesetz", devido ao caráter intervencionista do governo nazista na primeira metade do século XX. Por sua vez, a Suécia tem uma longa história de proteção de dados pessoais e foi o primeiro país a adotar uma legislação nacional com o dito objeto. A Lei de Dados de 1973 criou a Autoridade Sueca de Proteção de Dados, cuja função principal era conceder as licenças necessárias para o tratamento de dados pessoais. Seguindo a tradição alemã e sueca, a França introduziu no seu ordenamento jurídico a Lei nº 78-17 de 6 de janeiro de 1978, que foi promulgada na sequência do chamado escândalo denominado "SAFARI" em 1974, no jornal francês "Le Monde", fazendo referência ao plano da administração francesa de interligar ficheiros nominativos através de números de segurança social, surgindo assim a necessidade de regularização da utilização de dados pessoais. Ambos os cidadãos alemães e franceses, no final da década de 1970, rejeitaram a atitude intervencionista do Estado na sua vida privada e provocaram o legislador a assentar regras domésticas para o tratamento de informações de cunho pessoal. A tendência foi aceita por outros países europeus, que também incorporaram leis domésticas com o mesmo objetivo. Portanto, desde o século passado, países europeus mostraram preocupação com o tema e promulgaram leis de proteção de dados, antes mesmo de 1995, quando a EU promulgou a Diretiva n.º 95/46/CE – que culminou no atual RGPD. Para uma análise aprofundada das primeiras leis de proteção de dados, ver FLAHERTY, D. H. Protection Privacy in Surveillance Societies. Chapel Hill: University of North Carolina Press, 2014. p. 507.

Por isso, é certo dizer que a influência europeia – tanto por meio da Convenção 108 quanto da Diretiva/RGPD – está presente em muitas leis domésticas fora do continente[51]. Além disso, as decisões de adequação do Conselho da Europa também representam uma forte ferramenta de controle transfronteiriço, pois o efeito de uma decisão de adequação é que os dados pessoais fluam livremente dos 27 Estados-Membros da UE e dos três países membros do Acordo EEE para um país terceiro sem a necessidade de qualquer outra salvaguarda além daquelas estipuladas na legislação europeia[52].

Para transferência de dados pessoais para o outro lado do Atlântico, por exemplo, a relação entre a UE e os Estados Unidos da América (EUA) em relação à proteção de dados tem sido marcada por tensões entre a necessidade de facilitar o fluxo de dados transatlântico e a proteção da privacidade dos cidadãos da UE[53]. Mesmo sendo o país abrigador das maiores firmas de tecnologia do mundo, os EUA não possuem uma única lei federal que regule a proteção de dados de forma concentrada e abrangente, como acontece em outros Estados federados, tal como o Brasil com a Lei Geral de Proteção de Dados (LGPD) ou o Canadá com a Lei de Proteção de Informações Pessoais e Documentos Eletrônicos. Em vez disso, o Estado norte-americano conta com diversas legislações geralmente específicas para um determinado setor e vigente em determinado Estado.

O *California Consumer Privacy Act* (CCPA) é a legislação de privacidade mais ambiciosa e abrangente da história dos EUA, e foi o instrumento legal americano que mais se aproximou do RGPD, devido à ampla definição de dados pessoais apresentada, a ênfase na transparência e o estabelecimento de alguns direitos individuais. Contudo, existem diferenças substanciais entre os dois modelos,

---

[51] Nesse sentido, ver GREENLEAF, G. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law, v. 2, n. 2. Oxford: Oxford University Press, 2012.

[52] COMISSÃO EUROPEIA. Perguntas e respostas: Quadro de Proteção de Dados UE-EUA. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-data-transfer/adequacy-decisions/eu-us-data-privacy-framework_en. Acesso em: 14 abr. 2024.

[53] "*The United States, however, has yet to fully embrace the EU's data protection endeavor. The EU's omnibus approach to data protection is based on individual rights over data, detailed rules, a default prohibition on data processing, and a zealous adherence to the fair information practices (FIPs). In contrast, the patchwork approach of the United States is more permissive, indeterminate, and based upon people's vulnerabilities in their commercial relationship with companies*". HARTZOG W.; RICHARDS, N. Privacy's Constitutional Moment and the Limits of Data Protection. Boston College Law Review, v. 1, n. 5. Boston: Boston College Law Review, 2020. p. 1690. Disponível: https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4069&context=faculty_scholarship. Acesso em: 14 abr. 2024..

especialmente porque a lei americana não trata a privacidade como um direito humano fundamental da mesma forma que o regime europeu. É, na verdade, uma lei de privacidade transacional preocupada essencialmente em proteger os consumidores em suas interações com entidades comerciais[54]. Essas divergências entre as legislações demandou um monitoramento especial executado pela Comissão Europeia. A relação entre os EUA e a UE – após a invalidação do acordo de *Safe Harbour* pelo TJUE em duas oportunidades[55] – é atualmente regulada pelo Quadro de Privacidade dos Dados UE-EUA de 2023[56].

Em outros países americanos, no entanto, não houve o mesmo tipo de tensão com a UE, visto que a maioria já possui legislação doméstica inspirada no modelo europeu. Em 2024, os dados da UNCTAD[57] demonstram que os 137 países com leis de proteção de dados estão distribuídos geograficamente da seguinte forma: 33 países na África, 26 nas Américas, 34 na Ásia-Pacífico e 44 na Europa.

A análise pormenorizada das leis de proteção de dados de todos os países é inviável para esta tese, devido à complexidade e à variedade legislativa existente. O que se revela essencial é reconhecer a existência dessas leis, cujo número está crescendo gradativamente sob a influência do RGPD, da Convenção do CoE e dos instrumentos de *soft law*, principalmente da OCDE. Essas legislações regulam o tratamento e a transferência de dados pessoais tanto no âmbito doméstico quanto, em sua maioria, no internacional. Com essa compreensão, é possível avançar para a investigação de como as OIs interagem com esses instrumentos legais.

---

[54] Para mais detalhes sobre as semelhanças e diferenças entre a CCPA e o RGPD, ver CHANDER, A.; KAMINSKI M.E.; MCGEVERA, W. Catalyzing Privacy Law. Minnesota Law Review. Boulder, Colorado: University of Colorado Law School, 2021. Disponível em: https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2447&context=faculty-articles. Acesso em: 20 abr. 2024.

[55] DELOITTE. The Aftermath of Schrems II. Implications, insights, and expectations for the future. UK: Delloite, 2022. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-the-aftermath-of-schrems-ii.pdf. Acesso em: 22 abr. 2024.

[56] COUNCIL OF EUROPE. Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721. Acesso em: 22 abr. 2024.

[57] UN TRADE AND DEVELOPMENT, *op. cit*.

2. INTERSEÇÃO ENTRE AS OIs E O REGIME JURÍDICO DE PROTEÇÃO DE DADOS

Num mundo cada vez mais digital, as OIs vêm acolhendo tecnologias avançadas para desempenhar suas funções de forma mais célere, atual e eficaz. As OIs humanitárias[58], especialmente, estão abraçando diferentes ferramentas tecnológicas, como análise de dados, *big data*, *drones*, detecção remota, biometria, serviços de nuvem, aplicativos de mensagens, identidade digital, redes sociais, *blockchain*, IA e *machine learning*[59]. Por meio dessas tecnologias, as OIs coletam e tratam dados pessoais; portanto, se não adotarem medidas de controle ou forem objeto de violação, causarão prejuízos catastróficos (e muitas vezes irreversíveis) às pessoas afetadas[60].

A Organização Mundial da Saúde (OMS), por exemplo, coleta dados pessoais para monitorar surtos de doenças, pandemias e outras ameaças à saúde pública, e participa da cooperação internacional em saúde pública mediante a troca de dados com outras entidades (governos e OIs)[61]. No setor humanitário, o processamento de dados tem a mesma (ou maior) relevância, como acontece na utilização de biometria pelo Alto-Comissariado das Nações Unidas para os Refugiados (ACNUR) em campos refugiados, com o objetivo de identificar indivíduos e assegurar que os benefícios sejam recebidos pelas pessoas inequivocamente afetadas[62]. O uso inapropriado

---

[58] A classificação de uma OI em função do seu objeto compreende duas categorias: OI com fins gerais e OI de finalidade específica. A primeira se refere à organização "cujo objeto, definido no pacto constitutivo, abarca o conjunto das relações pacíficas entre os seus membros e a resolução dos conflitos internacionais"; a segunda categoria tem "um objeto circunscrito a algum ou alguns sectores particulares da cooperação internacional, na conformidade do respectivo pacto constitutivo". Tendo isso em mente, organizações de caráter humanitário são de finalidade específica, qual seja, fornecer assistência e proteção às pessoas afetadas por crises humanitárias, como conflitos armados, desastres naturais, fome e violações de direitos humanos. São exemplos a UNICEF e o ACNUR. CAMPOS, J. M. de; CAMPOS, J. L. M. de. Teoria Geral das Organizações Internacionais. In: CAMPOS, J. M. de; RIBEIRO, M. A. (coord.). Organizações Internacionais. Coimbra: Almedina, 2022. p. 51.

[59] Nesse sentido, ver INTERNATIONAL COMMITTEE OF THE RED CROSS. Handbook on Data Protection in Humanitarian Action - Second Edition. Disponível em: https://cash-hub.org/wp-content/uploads/sites/3/2017/08/4305.01_002-ebook-3.pdf. Acesso em: 6 maio 2024.

[60] Ver BANDEIRA, R. Talibã capturou dispositivos de biometria militar dos EUA, dizem veteranos. Disponível em: https://www.intercept.com.br/2021/08/18/taliba-dispositivos-biometria-militar-eua/. Acesso em: 6 maio 2024.

[61] WORLD HEALTH ORGANIZATION. Policy on use and sharing of data collected in Member States by the World Health Organization (WHO) outside the context of public health emergencies. Disponível em: https://cdn.who.int/media/docs/default-source/publishing-policies/data-policy/who-policy-on-use-and-sharing-of-data-collected-in-member-states-outside-phe_en.pdf?sfvrsn=713112d4_27. Acesso em: 03 jul. 2024.

[62] JANMYR, M. UNHCR and the Syrian refugee response: negotiating status and registration in Lebanon. The International Journal of Human Rights, v. 22, n. 3. Bergen: University of Bergen, 2018. p.

desse tipo de ferramenta tecnológica traz sérias preocupações de segurança, uma vez que dados vazados podem ser explorados por nações adversárias ou em conflito com o país de origem dos cidadãos afetados.

Por isso, a adoção de políticas internas visando a proteção de dados pessoais é essencial para assegurar que as OIs utilizem a tecnologia disponível de forma a respeitar os direitos fundamentais de privacidade e dignidade dos titulares dos dados; se não o fizerem, devem ser responsabilizadas pelo mau uso dos dados. Assim como os países têm progressivamente adotado leis de proteção de dados nas últimas décadas, as OIs têm desenvolvido regulamentações internas. Contudo, a criação de diversas normativas que regulam o processamento de dados pessoais – tanto pelos Estados, quanto pelas OIs que operam no território desses Estados – podem causar uma sobreposição de normas. Esse cruzamento entre as regulações (internas ou externas) poderia afetar as operações das OIs, tendo em vista que elas gozam de privilégios – como isenções fiscais, imunidade jurisdicional e inviolabilidade de arquivos – a fim proteger a sua imparcialidade e neutralidade, assegurando que elas possam atuar em múltiplos países sem se submeter a pressões políticas ou jurídicas que afetariam sua autonomia.

O regime dos privilégios é previsto no Direito Internacional para permitir o desempenho das atividades de um sujeito de forma independente. Os Estados gozam de imunidades por conta do princípio da soberania, segundo o qual todos os Estados são iguais e, dessa forma, um Estado não pode ser julgado nos Tribunais de outro[63]. Em contrapartida, a imunidade das OIs tem fundamento no princípio da necessidade funcional: considerando que elas operam nos territórios de Estados soberanos e estão expostas a potenciais interferências das autoridades nacionais, a criação de medidas de proteção é necessária para evitar a aplicação de leis locais que poderiam limitar ou comprometer a execução de seus mandatos[64].

393-419. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/13642987.2017.1371140. Acesso em: 03 jul. 2024.

[63] Isso foi reconhecido pelo TIJ em 2008 no caso Alemanha vs. Itália, dando provimento ao pedido da Alemanha para reconhecer a violação à sua imunidade jurisdicional pela Itália, que permitiu o ajuizamento de ações civis nos Tribunais italianos contra atos praticados pelo Terceiro Reich. INTERNATIONAL COURT OF JUSTICE. Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening). Disponível em: https://www.icj-cij.org/case/143. Acesso em: 10 set. 2024.

[64] NETO, J. C. Teoria geral das organizações internacionais. 2. ed. São Paulo: Saraiva, 2007.

O presente capítulo visa examinar a relação entre esses privilégios inerentes às OIs e a ordem legal existente (doméstica e internacional, inclusive os instrumentos de *soft law* mencionados no capítulo anterior).

2.1. NOÇÃO DE ORGANIZAÇÃO INTERNACIONAL

A importância das OIs é patente quando pensamos na globalização e na interdependência dos Estados. Os Estados (ou outros sujeitos legitimados) decidem criar uma OI[65] geralmente porque não conseguem solucionar um determinado problema ou vários problemas que esses sujeitos estão enfrentando individualmente e que, possivelmente, exigem a junção de forças para alcançar a necessária solução[66]. De fato, as OIs foram criadas para quase todas as matérias que demandam ou para as quais convêm a mútua colaboração internacional[67].

Uma definição precisa e padrão de OI não é possível, já que existem demasiadas formas institucionais de cooperação internacional, o que dificulta a conceituação jurídica de uma OI[68]. No entanto, para os objetivos deste capítulo, uma definição suficiente é a seguinte: "(...) uma associação de sujeitos de direito internacional (1) constituída com caráter de permanência (2) por um adequado ato jurídico internacional (3), com vista à realização de objetivos comuns aos seus membros (4) e prosseguidos através de órgãos próprios (5) habilitados a exprimir, na conformidade das regras pertinentes do pacto constitutivo (6) a vontade própria – juridicamente distinta da dos seus membros (7) – dessa especial pessoa jurídica (8)"[69].

As organizações com as referidas características são classificadas como intergovernamentais[70]. Talvez a mais notória é a ONU: composta por Estados-membros[71]; de cunho permanente[72]; criada por um tratado fundador, qual seja, a Carta

[65] Sobre o ato instituidor de uma OI, ver MARTINS, M. S. D´Oliveira; MARTINS, Afonso D´Oliveira. Direito das Organizações Internacionais. 2ª ed. Lisboa: Associação Acadêmica da Faculdade de Direito, 1996.
[66] WHITE, N. D. The Law of International Organisations. 3. ed. Manchester: Manchester University Press, 2017. p. 8.
[67] CAMPOS, *op. cit.*, p. 33.
[68] WHITE, *op. cit.*, p. 1.
[69] CAMPOS, *op. cit.*, p. 39.
[70] Ao contrário da organização não governamental, que não é criada ou governada por Estados.
[71] 193 Estados-membros.
[72] Desde a sua fundação em 1945, a ONU cresceu para incluir a vasta maioria dos Estados soberanos do mundo.

da ONU[73]; visa a segurança e paz internacional[74]; com seus próprios órgãos de governança e administração com competência para desempenhar as funções a que a OI foi criada[75]; de forma independente dos seus membros[76]; e com personalidade jurídica internacional amplamente reconhecida[77].

Outro exemplo é o Comitê Internacional da Cruz Vermelha (CICV), mas que diferente da ONU não foi estabelecida por um tratado fundador internacional de Estados e sim por uma associação privada chamada Sociedade de Utilidade Pública de Genebra. Destarte, é considerada uma OI *sui generis*: não é intergovernamental, pois não é formada por Estados, tampouco é ONG, pois tem capacidade de celebrar tratados internacionais[78]. Seu mandato foi internacionalmente reconhecido nas Convenções de Genebra de 1949 e nos protocolos subsequentes de 1977, além das próprias Resoluções da Conferência Internacional da Cruz Vermelha e do Movimento da Cruz Vermelha e do Crescente Vermelho[79]. Sua atuação é muitas vezes baseada em acordos bilaterais com Estados ou outros atores, em vez de uma estrutura multilateral tradicional[80].

O caso do CICV é, portanto, atípico. Em regra, os Estados concedem personalidade jurídica internacional e imunidades apenas a organizações intergovernamentais, que são criadas por tratados e geridas diretamente por Estados.

---

[73] ONU. Carta das Nações Unidas. Disponível em: https://unric.org/pt/wp-content/uploads/sites/9/2009/10/Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf. Acesso em: 15 maio 2024.

[74] Com base no artigo 1 da Carta da ONU, o princípio central dessa organização é a proibição do uso unilateral da força entre as nações. Embora enfrente dificuldades para executar plenamente seus objetivos, em virtude principalmente de interesses políticos e do veto dos membros permanentes no Conselho de Segurança, a ONU sempre exerceu um papel bastante relevante na comunidade internacional, pois fornece o único espaço global onde quase todos os países do mundo podem debater questões de paz e segurança em conjunto. Acerca da atuação da ONU, ver GIL, A. R. Um Livro de Casos de Direito das Nações Unidas – Guia de Estudo. In: GIL, A. R.; PATINHAS, M. C. (ed.). A ONU em ação: Conflitos Armados e Missões de Paz – Estudo de Casos. Lisboa: Lisbon Public Law Editions, 2024. Disponível em: https://lisbonpubliclaw.sharepoint.com/sites/Externos/Shared%20Documents/General/Editorial/EBook_ConflitosArmadosDireitoInternacional_V02.pdf. Acesso em: 10 set. 2024.

[75] Artigo 7 da Carta da ONU.

[76] Artigos 100 e 105 da Carta da ONU.

[77] INTERNATIONAL COURT OF JUSTICE. Reparation for Injuries Suffered in the Service of the United Nations. 1949. Disponível em: https://www.icj-cij.org/case/4. Acesso em: 20 maio 2024.

[78] CUNHA, M. N. F. da; VIEIRA, S. C. Cruz Vermelha: breve análise histórica de uma organização sui generis. Revista Curso Direito UNIFOR, v. 7, n. 2. Itaúna: UNIFOR, 2016. p. 39–54. Disponível em: https://revistas.uniformg.edu.br/cursodireitouniformg/article/view/419. Acesso em: 03 jul. 2024.

[79] COMITÊ INTERNACIONAL DA CRUZ VERMELHA. "Convenções de Genebra", Comitê Internacional da Cruz Vermelha. Disponível em: https://www.icrc.org/pt/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm. Acesso em: 20 maio 2024.

[80] DEBUF, E. Tools to do the job: The ICRC's legal status, privileges and immunities. International Review of the Red Cross, v. 97, n. 1-2. Genebra: ICRC, 2016. p. 319-344. Disponível em: https://international-review.icrc.org/sites/default/files/irc_97_1-2-13.pdf. Acesso em: 20 maio 2024.

Em contrapartida, embora seu mandato derive de tratados internacionais, o CICV não foi instituído por um tratado formal entre Estados, nem é controlado por eles, incluindo aqueles que assinaram os acordos que estabeleceram seu mandato. Ainda assim, devido à relevância de sua missão humanitária e ao papel central que desempenha no sistema jurídico das Convenções de Genebra, o CICV acabou sendo reconhecido e tratado, de fato, como uma OI convencional. Sua transformação, de uma entidade privada para uma OI, é demonstrada tanto pelo *status* de observador na ONU quanto pelo tratamento privilegiado que recebe dos Estados, comparável ao das organizações intergovernamentais[81].

Em suma, quando concebidas na sua forma tradicional, as OIs possuem as características padrão supramencionadas. Porém, há vezes em que outros tipos de organizações (não intergovernamentais) apresentam traços inerentes das OIs tradicionais – como um mandato sob o Direito Internacional, o reconhecimento da personalidade jurídica internacional e a concessão dos privilégios necessários para o exercício independente das suas funções – e passam a ser vistas da mesma forma.

2.2. PRIVILÉGIOS E IMUNIDADES DAS OIs

Antes da Segunda Guerra Mundial, as OIs não gozavam de privilégios e imunidades específicos, sendo aplicáveis apenas os mesmos benefícios diplomáticos atribuídos aos Estados e seus representantes[82]. A partir de 1940, porém, o cenário durante e pós-guerra deixou claro que essas prerrogativas não podiam ser simplesmente transpostas às OIs, que se diferenciam em natureza, objetivos e funcionamento quando comparadas com as entidades diplomáticas (por exemplo, as embaixadas). Um Estado goza desses benefícios para garantir sua soberania e igualdade, ao passo que uma OI para preservar sua independência e evitar interferência do Estado anfitrião[83].

---

[81] *Ibid*.

[82] Esses privilégios e imunidades diplomáticos foram codificados em três Convenções de Viena: sobre Relações Consulares, sobre Relações Diplomáticas e sobre a Representação dos Estados em suas Relações com Organizações Internacionais de Caráter Universal. Ver BUENO, E. P; FREIRE, M.; OLIVEIRA, PEREIRA, V. A. As origens históricas da diplomacia e a evolução do conceito de proteção diplomática dos nacionais. Anuario Mexicano de Derecho Internacional, v. 17. Cidade do México: Elsevier, 2017. p. 623-649. Disponível em: https://www.sciencedirect.com/science/article/pii/S1870465417300454. Acesso em: 11 maio 2024.

[83] BRABANDERE, E. Measures of Constraint and the Immunity of International Organisations. In: RUYS, T.; ANGELET, N.; FERRO, L. (Eds.). Part III - Immunity from Execution of States and

Assim, regras especificamente direcionadas às OIs foram criadas a partir de diferentes tipos de instrumentos legais: a previsão dos privilégios no regulamento interno das organizações, por exemplo o que dispõe o artigo 105 da Carta da ONU[84]; a Convenção sobre Privilégios e Imunidades das Nações Unidas de 1946[85] e a Convenção sobre Privilégios e Imunidades das Organizações Especializadas de 1947[86]; os acordos bilaterais entre as OIs e os Estados onde operam[87]; e a legislação nacional que também pode regular as facilidades conferidas às OIs[88].

Além desses instrumentos, os privilégios e imunidades das OIs também são garantidos através de outras Convenções não necessariamente com este estrito objeto. Os Estados partes nas Convenções de Genebra se comprometeram especificamente a respeitar a independência, imparcialidade e neutralidade do CICV como princípios fundamentais que regem sua ação[89]. No caso da ONU, em contrapartida, considera-se que mesmo os Estados não signatários da Convenção de 1946 deverão respeitar os benefícios concedidos às Nações Unidas, em virtude de uma declaração do seu Conselho Jurídico no sentido de que a Convenção é o instrumento regulador mundial das relações entre os Estados e a ONU[90].

Dentre as imunidades concedidas às OIs, a de jurisdição é considerada a mais relevante, pois significa ser inatingível por qualquer processo legal, exceto quando

---

International Organisations. The Cambridge Handbook of Immunities and International Law. Cambridge: Cambridge University Press, 2019. p. 327-349.

[84] 1. A Organização gozará, no território de cada um dos seus membros, dos privilégios e imunidades necessários à realização dos seus objetivos. 2. Os representantes dos membros das Nações Unidas e os funcionários da Organização gozarão, igualmente, dos privilégios e imunidades necessários ao exercício independente das suas funções relacionadas com a Organização. 3. A Assembleia Geral poderá fazer recomendações com o fim de determinar os pormenores da aplicação dos nº 1 e 2 deste Artº. ou poderá propor aos membros das Nações Unidas convenções nesse sentido.

[85] MINISTÉRIO PÚBLICO DE PORTUGAL. Convenção sobre os Privilégios e Imunidades das Nações Unidas. Disponível em: https://www.ministeriopublico.pt/instrumento/convencao-sobre-os-privilegios-e-imunidades-das-nacoes-unidas-9. Acesso em: 15 maio 2024.

[86] MINISTÉRIO PÚBLICO DE PORTUGAL. Convenção sobre os Privilégios e Imunidades das Organizações Especializadas das Nações Unidas. Disponível em: https://www.ministeriopublico.pt/instrumento/convencao-sobre-os-privilegios-e-imunidades-das-organizacoes-especializadas-das-nacoes-0. Acesso em: 15 maio 2024.

[87] A título de exemplo, o artigo III, seção 7, do acordo-sede de 1947 entre a ONU e os EUA. ONU. Agreement regarding the Headquarters of the United Nations. 1947. Disponível em: https://treaties.un.org/doc/Publication/UNTS/Volume%2011/volume-11-I-147-English.pdf. Acesso em: 15 maio 2024.

[88] Nos EUA, ver a lei federal 22 U.S. Code § 288a - Privileges, exemptions, and immunities of international organizations. 1945. Disponível em: https://www.law.cornell.edu/uscode/text/22/288a#:~:text=International%20organizations%2C%20their%20property%20and,for%20the%20purpose%20of%20any. Acesso em: 15 maio 2024.

[89] INTERNATIONAL COMMITTEE OF THE RED CROSS. Statutes of the International Red Cross and Red Crescent Movement. Disponível em: https://www.icrc.org/en/doc/assets/files/other/statutes-en-a5.pdf. Acesso em: 15 maio 2024.

[90] CAMPOS, *op. cit.*, p. 183.

haja renúncia da imunidade[91]. Esse tipo de imunidade impossibilita, portanto, que qualquer Tribunal nacional possa decidir nos casos envolvendo OIs, evitando o controle externo, a pressão exercida pelos Estados por meio dos seus órgãos judiciais ou administrativos e favorecimentos a um determinado Estado em detrimento de outro[92]. Isso tendo em conta que, para desempenharem devidamente suas funções, as OIs devem gozar de plena independência.

A imunidade de arquivo, por sua vez, significa que os documentos, estudos ou projetos de uma OI são invioláveis e, por conseguinte, não podem ser objeto de censura, buscas, requisições, confisco, expropriação ou qualquer outra forma de interferência pelas autoridades estatais. No caso da ONU, por exemplo, o Secretariado da organização defende que os seus arquivos estão sujeitos à Convenção de 1946 e não podem ser interferidos por meios judiciais, administrativos ou legislativos[93].

A inaplicabilidade das leis nacionais decorrente dessa barreira jurisdicional só poderá ocorrer se existir um privilégio específico estabelecido por tratado ou costume. No entanto, é possível inferir certa incompatibilidade entre a imunidade de jurisdição e as leis nacionais de proteção de dados. No exemplo acima, se uma lei nacional ou regulamento regional buscasse regulamentar o tratamento de dados nos arquivos pela ONU e suas respectivas agências, as disposições legais seriam incompatíveis com tal Convenção. Se há conflito normativo, pressupõe-se implicitamente uma hierarquia de normas, na qual as imunidades e privilégios ocupariam posição superior às leis domésticas[94].

A análise do subcapítulo a seguir visa compreender se essas leis domésticas estão de fato destinadas a serem aplicadas às OIs.

2.3. (IN)APLICABILIDADE DAS LEIS DOMÉSTICAS ÀS OIs

[91] Artigo II, seção 2 da Convenção sobre Privilégios e Imunidades das Nações Unidas.
[92] BRABANDERE, E., *op. cit.*, p. 329.
[93] UNITED NATIONS SECRETARIAT. Comments of the United Nations Secretariat on Behalf of the United Nations System Organizations on the 'Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies'. 2020. p. 14-15. Disponível em: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf. Acesso em: 17 maio 2023.
[94] *Ibid.*, p. 17.

Existem várias razões que justificam a não incidência das leis domésticas nas OIs, na medida em que os textos legais nacionais/regionais não foram projetados para esse tipo específico de sujeito de Direito Internacional Público. Por outro lado, alguns autores defendem que existe certa vinculação entre as OIs e as legislações domésticas onde operam. O presente subcapítulo pretende expor os dois entendimentos.

2.3.1. A incompatibilidade das leis domésticas com os atos das OIs

Por sua própria natureza, as OIs atuam internacionalmente e, em todos os países e regiões que operam, passam por uma variedade de leis de proteção de dados, cada uma regulando o assunto de forma distinta[95]. Para desempenharem suas funções de maneira eficaz, as OIs devem gerenciar o fluxo interno de dados de acordo com seus próprios regulamentos internos; caso contrário, uma lei doméstica poderia impedir a transferência de informações pessoais dentro do organograma de uma mesma OI, mesmo havendo normas internas uniformes[96]. Ou seja, o regulamento interno da OI deveria cobrir as necessidades de supervisão e resolução de disputas, para evitar o conflito entre as leis nacionais e o funcionamento interno de uma organização.

Além disso, se as OIs estivessem sujeitas a todas essas legislações diferentes, suas operações restariam prejudicadas, onerosas e mesmo impossíveis. As leis não serão uniformes e, portanto, podem entrar em conflito entre si. A ONU, inclusive, já se manifestou nesse sentido ao afirmar que a diversidade cultural, jurídica e política dos seus Estados-membros impossibilita a simples transposição para o sistema das Nações Unidas de uma lei doméstica específica em detrimento de outra[97].

O Manual sobre o *status* legal, privilégios e imunidades das Nações Unidas e do TIJ, elaborado pelo departamento legal do Secretariado da ONU em 1952[98], conta

---

[95] KUNER, C. Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, n. 187. Paris: OECD Publishing, 2011. Disponível em: https://www.oecd-ilibrary.org/docserver/5kg0s2fk315f-en.pdf?expires=1718302635&id=id&accname=guest&checksum=D1C103188793734108A87E9F5822CC24. Acesso em: 23 maio 2024.
[96] *Ibid*., p. 26.
[97] UNITED NATIONS SECRETARIAT, *op. cit*., p. 8.
[98] UNITED NATIONS SECRETARIAT. Handbook on the Legal Status, Privileges and Immunities of the United Nations. Disponível em: https://legal.un.org/ilc/documentation/english/st_leg_2.pdf. Acesso em: 24 jul. 2024.

com um compilado de leis e regulamentos dos Estados-membros sobre o assunto. Com relação ao EUA, importa destacar a opinião do Procurador-Geral do Estado de Nova York em 1946 quanto ao pedido da ONU de estabelecer sua sede no referido território. Na oportunidade, o jurista afirmou que os privilégios concedidos aos funcionários da ONU no âmbito do acordo-sede firmado com o Estado americano estariam acima das leis domésticas e, portanto, teriam pleno reconhecimento pelos Tribunais estadunidenses[99]. O documento também apresenta o relatório da Sexta Comissão sobre os privilégios e imunidades da ONU, no qual o Secretário Geral reiterou que quaisquer regulamentos aprovados pela organização estariam em posição superior a legislação local[100].

Nesse quesito, importa ressaltar que as OIs não estão no mesmo patamar que as corporações multinacionais, em que pese ambas operem num cenário internacional. As empresas sim estão sujeitas às leis domésticas e, de fato, podem escolher se exercem (ou não) suas atividades comerciais num determinado país ou região, a depender do seu modelo de negócio, expectativa de lucro naquele local e questões legais[101]. As OIs, por sua vez, foram criadas como pessoas de Direito Internacional para atingir um objetivo específico e, ao contrário das companhias multinacionais privadas, muitas vezes não terão a mesma liberdade de escolha com relação ao local de suas operações, pois deverão atuar conforme o mandato para que foram criadas e não conforme sua conveniência comercial ou política[102].

Ainda, as legislações dos países costumam criar uma autoridade nacional independente para o controle do tratamento de dados pessoais[103], com poderes de autorização, investigação e correção. O poder de fiscalização concedido pelas leis domésticas às autoridades de proteção de dados também poderia interferir na atuação independente das OIs. Isso ocorreria na situação hipotética em que a ONU, ao

---

[99] *Ibid*., p. 317.
[100] *Ibid*., p. 526.
[101] DALLARI, D. de A. Empresas Multinacionais e Soberania do Estado. Revista da Faculdade de Direito, Universidade de São Paulo, *[S. l.]*, v. 76. São Paulo: USP, 1981. p. 107–121. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/66917. Acesso em: 20 maio 2024.; DUARTE, F. de A. Multinational companies as subjects of international law: are we missing the point? In: DUARTE, M. L.; LANCEIRO, R. T. (Coord.). Ordem jurídica global do século XXI: sujeitos e actores no palco internacional. 1ª ed. Lisboa: AAFDL Editora, 2020. p. 561-594.
[102] SEITENFUS, Ricardo Antônio Silva. Manual das organizações internacionais. 4. ed. Porto Alegre, RS: Livraria do Advogado, 2005. 384p.; DELGADO, M. M. International organizations as subjects of international law. In: DUARTE, M. L.; LANCEIRO, R. T. (Coord.). Ordem jurídica global do século XXI: sujeitos e actores no palco internacional. 1ª ed. Lisboa: AAFDL Editora, 2020. p. 259-278.
[103] No Brasil, por exemplo, a Autoridade Nacional de Proteção de dados foi criada para fiscalizar o cumprimento da LGPD.

conduzir uma missão de paz e armazenar dados sensíveis sobre os movimentos de tropas, a situação dos civis e possíveis violações de direitos humanos, não poderia transferi-los aos seus parceiros internacionais para coordenar esforços de paz e segurança, por falta de permissão da entidade competente local.

2.3.2. A relação entre as leis domésticas e as OIs

Por trás do conceito de imunidade, deve existir algo do qual alguém é imune e, no caso das OIs, não há outra opção a não ser a legislação doméstica[104]. À luz dessa ideia, há argumentos em favor da aplicabilidade das leis domésticas dos respectivos países onde uma OI está operando.

Algumas situações específicas justificam essa teoria, como aconteceria na hipótese em que uma organização requer uma licença específica (ambiental ou para promover um evento, por exemplo) que só pode ser concedida por uma autoridade local e, portanto, será submetida à legislação nacional/regional para lograr suas operações no território[105]. Há situações também em que as OIs optam por não estabelecer suas próprias normas, por razões de necessidade e conveniência, restando, nessas circunstâncias, a única alternativa de recorrer à legislação local para solucionar ou remediar os acontecimentos[106].

Um acordo firmado entre o Estado anfitrião e a OI, ao fixar os privilégios das organizações, podem criar exceções às imunidades de jurisdição e execução. O acordo entre o CICV e a Suíça demonstra que uma lei doméstica poderá ser aplicada aos funcionários da OI que se envolvem em acidentes de trânsito – cujos danos configurem responsabilidade civil – ou em infrações nas estradas federais[107]. O documento também elenca outras situações nas quais a OI não terá imunidade, como em litígios decorrentes de prestação de serviços entre funcionários e a organização ou de apreensão judicial de salários, vencimentos e outros emolumentos devidos pelo

---

[104] KLABBERS, J. An introduction to international organizations law. 3. ed. Cambridge: Cambridge University Press, 2015. p. 136.
[105] *Ibid*., p. 136.
[106] SEYERSTED, F. Common Law of International Organizations. Leiden: Brill, 2008. p. 458.
[107] Artigo 13 do Acordo entre o CICV e o Conselho Federal Suíço. INTERNATIONAL REVIEW OF THE RED CROSS. Agreement between the International Committee of the Red Cross and the Swiss Federal Council to determine the legal status of the Committee in Switzerland. Disponível em: https://international-review.icrc.org/articles/agreement-between-international-committee-red-cross-and-swiss-federal-council-determine. Acesso em: 04 jul. 2024.

CICV aos seus empregados[108]. Neste caso, apesar de não ser considerada uma organização intergovernamental *per se*, o Estado suíço reconhece a personalidade jurídica internacional do CICV e concede privilégios (e derrogações a esses privilégios) equivalentes aos de outras OIs tradicionais.

Ademais, as leis domésticas podem influenciar o enquadramento legal das imunidades e privilégios concedidos às OIs. Nos EUA, existe um decreto presidencial cujo objetivo é definir a personalidade legal das OIs e o alcance dos benefícios que podem gozar as organizações nas quais o Estado federal faça parte[109]. Outrossim, o Reino Unido conta com um ato legislativo específico definindo as facilidades concedidas às OIs (e seus agentes e representantes) das quais seja membro[110]. Outras leis domésticas, como acontece no Canadá, surgem para garantir privilégios e imunidades a reuniões organizadas pelos órgãos internos das OIs, situação na qual os representantes dessas organizações gozarão de benefícios enquanto se manifestam nos encontros realizados no Estado anfitrião[111].

Porém, é possível inferir que esses argumentos são insuficientes para assentar a vinculação entre as OIs e as leis domésticas e, na verdade, esse tipo de legislação funciona mais de forma específica ou residual, podendo apenas definir o escopo das imunidades e privilégios. De fato, um acordo-sede entre uma OI e o Estado anfitrião costuma estabelecer que a organização deve respeitar as leis e regulamentos do Estado anfitrião, sem prejuízo das imunidades e privilégios que gozam[112]. Isso nos leva a concluir que a OI está sujeita à lei doméstica nos limites das suas imunidades e privilégios – e não o contrário.

---

[108] Artigo 5(1) do Acordo entre o CICV e o Conselho Federal Suíço.

[109] NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. Executive Order 9698 **-** Designating public international organizations entitled to enjoy certain privileges, exemptions, and immunities. 1946. Disponível em: https://www.archives.gov/federal-register/codification/executive-order/09698.html#:~:text=With%20respect%20to%20the%20designation,privileges%2C%20exemptions%2C%20and%20immunities. Acesso em: 30 maio 2024.

[110] UK PUBLIC GENERAL ACTS. International Organisations Act 1968. Disponível em: https://www.legislation.gov.uk/ukpga/1968/48. Acesso em: 30 maio 2024.

[111] A Lei de Missões Estrangeiras e Organizações Internacionais do Canadá assegura aos representantes de um Estado estrangeiro que seja membro ou participe de uma OI os privilégios e imunidades estabelecidos na Convenção sobre Privilégios e Imunidades das Nações Unidas. Também confere imunidade aos representantes de um Estado estrangeiro que seja membro de uma OI com sede no Canadá nos mesmos termos da Convenção de Viena sobre Relações Diplomáticas. CANADÁ. Foreign Missions and International Organizations Act. Disponível em: https://laws.justice.gc.ca/eng/acts/f-29.4/page-1.html#h-235020. Acesso em: 30 maio 2024.

[112] Veja o artigo 24 do acordo entre o Fundo Global de Luta contra AIDS, Tuberculose e Malária e o Conselho Federal Suíço. THE GLOBAL FUND. Agreement between the Swiss Federal Council and the Global Fund to Fight AIDS, Tuberculosis and Malaria in view of determining the legal status of the Global Fund in Switzerland. Disponível em:

2.4. AS OIs NOS INSTRUMENTOS LEGAIS INTERNACIONAIS E DOMÉSTICOS

No capítulo 1, vimos que os instrumentos legais de proteção de dados surgiram a partir da década de 1970 e, desde então, evoluíram conforme a ascensão da tecnologia e o aumento na utilização de dados pessoais pelas empresas e organizações. A Convenção 108+ é atualmente o único instrumento internacional vinculante que pode ser aplicado tanto a Estados quanto a OIs. No entanto, até o momento, nenhuma OI a ratificou, o que significa, na prática, que as OIs não estão obrigadas a nenhuma normativa internacional específica de proteção de dados. Devido às suas imunidades e privilégios, tampouco se sujeitam às leis domésticas, a não ser em situações particulares ou em relações com outros sujeitos que, esses sim, estão cobertos pela proteção dessas legislações locais.

Na ausência de normas jurídicas vinculativas a nível global, este capítulo examina como as Diretrizes da OCDE e outros atos não vinculativos de organizações como a ONU e a Assembleia Mundial da Privacidade, ou atos vinculativos de organizações regionais, como a Convenção do CoE e o RGPD, se referem às OIs. Após, o mesmo exame será feito com relação às leis nacionais da Suíça, do Brasil e de Portugal.

2.4.1. Diretrizes da OCDE

As Diretrizes de 1980 da OCDE representaram um marco fundamental na proteção e na transferência transnacional de dados pessoais. Elas estabeleceram princípios centrais como a limitação da coleta de dados, a qualidade dos dados, a definição da finalidade, a limitação de utilização, a segurança dos dados e a responsabilização. O alcance das Diretrizes compreende os dados pessoais que podem representar uma ameaça à privacidade e à liberdade individual, seja no setor público ou privado. Os riscos podem surgir em razão de como esses dados são processados, de sua própria natureza ou do contexto em que são utilizados.

---

https://www.theglobalfund.org/media/8551/core_headquarters_agreement_en.pdf. Acesso em: 04 jul. 2024.

Embora tenham sido direcionadas principalmente aos Estados-membros da OCDE, essas Diretrizes têm relevância global, inclusive para OIs que processam grandes quantidades de dados pessoais, muitas vezes em operações transnacionais, e que também podem ser influenciadas por essas normativas. O memorando explicativo prévio ao lançamento das Diretrizes destacou os esforços que seriam feitos para que, além dos Estados-membros, os demais não membros e as OIs se atentassem às novas regras[113].

As normas internas da ONU, por exemplo, foram inspiradas nos princípios consagrados pela OCDE em 1980, especialmente quanto ao livre fluxo de dados entre países com nível de proteção semelhante. Décadas depois, as Diretrizes ainda são respeitadas (apesar da falta de vinculação) nos instrumentos de autorregulação, inclusive nas orientações publicadas pela Cruz Vermelha em 2015[114].

2.4.2. ONU

Por sua parte, o Conselho Económico e Social (ECOSOC), por intermédio da Comissão de Direitos Humanos, endossou em 1988 as suas conclusões acerca dos estudos quanto às Diretrizes para a Regulação de Ficheiros Informatizados de Dados de Caráter Pessoal da ONU. Havia um consenso emergente para elaborar normas nesta área, tanto para incentivar Estados-membros a adotarem leis domésticas, quanto para organizações e agências internacionais regularem o armazenamento e utilização dos seus arquivos contendo dados pessoais[115], de acordo com os princípios adotados pela Assembleia Geral da ONU. Na primeira seção, as Diretrizes da ONU orientam os Estados-membros a adotarem regulamentos com base, dentre outros, no princípio da legalidade e finalidade especificada, segundo os quais os dados pessoais não podem ser utilizados em desacordo com a Carta da ONU e devem ser colhidos para um objetivo e por um período previamente especificado.

---

[113] OCDE LIBRARY. Explanatory memoranda of the OECD Privacy Guidelines. 2023. Disponível em: https://www.oecd-ilibrary.org/docserver/ea4e9759-en.pdf?expires=1720105882&id=id&accname=guest&checksum=F11F2F4D8256ECB73B6E92A029FF4E30. Acesso em: 1 jun. 2024.

[114] INTERNATIONAL COMMITTEE OF THE RED CROSS, *op. cit.* (nota de rodapé 59).

[115] ECONOMIC AND SOCIAL COUNCIL. Guidelines for the regulation of computerized personal data files - Final report submitted by Mr. Louis Joinet. 1988. Disponível em: https://digitallibrary.un.org/record/43365?ln=fr&v=pdf. Acesso em: 1 jun. 2024.

Na seção subsequente, as Diretrizes afirmam que esses requisitos devem ser aplicados também aos ficheiros mantidos por OIs, que deve designar uma autoridade para supervisionar o cumprimento das normas. Por último, dispõe sobre a possibilidade de derrogações dos princípios por intermédio de uma cláusula humanitária, concedendo às OIs privilégios quando seus ficheiros tenham por objetivo a proteção de direitos humanos. Por exemplo, organizações como o ACNUR, que coletam dados pessoais de refugiados, poderiam compartilhar informações sobre origem, condições médicas e histórico familiar com outros Estados e ONGs envolvidas no processo de reassentamento e proteção. Isso acontece apesar de que, em contextos normais, a partilha de tais dados sensíveis estaria sujeita a regras restritas de consentimento e uso limitado.

2.4.3. Assembleia Mundial da Privacidade

Um outro instrumento juridicamente não vinculativo é a Resolução sobre proteção de dados e OIs adotada pela Assembleia Mundial da Privacidade[116] em 2003. O documento convoca organizações internacionais e supranacionais a adotarem regulamentos internos, para aplicação dos princípios (e mecanismos necessários) estabelecidos nos principais instrumentos legais de proteção de dados, incluindo o estabelecimento de autoridades de supervisão interna. Segundo as conclusões da Resolução, as OIs não lograrão alcançar bons níveis de proteção de dados somente com leis domésticas, sendo imprescindível a adoção de políticas e práticas internas de acordo com as convenções e diretrizes internacionais[117].

Portanto, é possível inferir que os instrumentos de *soft law* não estimulam as OIs a seguirem as leis domésticas dos Estados onde são criadas ou operam; de outra forma, solicitam que deem efeito aos princípios internacionais de proteção de dados através dos seus próprios regulamentos e mecanismos de supervisão interna.

---

[116] Anteriormente conhecida como Conferência Internacional de Comissários de Proteção de Dados e Privacidade, é um fórum líder que une autoridades de privacidade e proteção de dados de todo o mundo. Desde a sua criação em 1979, a Assembleia tem proporcionado uma plataforma para a cooperação internacional e o diálogo sobre a regulamentação da privacidade e tem desempenhado um papel fundamental na definição dos padrões globais de privacidade. Em 2024, já organizou 45 conferências e conta com 130 membros. GLOBAL PRIVACY ASSEMBLY. History of the Assembly. Disponível em: https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/. Acesso em: 11 set. 2024.

[117] GLOBAL PRIVACY ASSEMBLY. Resolution on Data Protection and International Organisations. 2003. Disponível em: https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-International-Organisations.pdf. Acesso 1 jun. 2024.

2.4.4. Convenção 108+

Devido ao seu caráter vinculativo, a Convenção 108+ se diferencia das normas de *soft law* por estabelecer (e não somente orientar) padrões mínimos obrigatórios de proteção de dados que devem ser atendidos pelos Estados que a ratificam e organizações que eventualmente o façam. Porém, seus efeitos sobre as OIs seriam semelhantes àqueles dos instrumentos de *soft law*, no sentido de que as organizações estão sujeitas apenas aos seus próprios regulamentos internos sobre proteção de dados, independentemente de onde operem no mundo.

A Convenção 108+ permite a adesão de Estados não membros do CoE e de OIs de todo o mundo definidas como de Direito Internacional Público, malgrado sejam de natureza intergovernamental ou *sui generis*. A possibilidade de adesão de OIs não fazia parte da Convenção 108 na sua versão inicial, que só passou a existir com as alterações trazidas pelo Protocolo de 2018[118]. Contudo, desde então, nenhuma OI acedeu a Convenção, que atualmente conta com 55 ratificações por Estados (todos os membros do CoE e 9 não membros[119]).

A OI que pretenda ratificar a Convenção 108+ – assim como os países terceiros – será submetida a uma avaliação do seu nível de proteção de dados pessoais, a ser realizada pelo Comitê Consultivo do CoE, que poderá fazer recomendações para que as disposições normativas da Convenção sejam aplicadas na prática da organização[120] e, por conseguinte, emitir parecer favorável quanto à candidatura. Ou seja, para que uma organização seja aceita pelo CoE, é primeiramente necessário que já tenha sua própria regulação interna com um nível suficiente de proteção, através do estabelecimento de autoridades de controle[121] e meios de defesa disponíveis ao titular dos dados em caso de incumprimento[122].

Inclusive para as OIs não signatárias, a Convenção 108+ apenas permite a transferência de dados pessoais se a organização receptora contar com o nível adequado de proteção, com base nas disposições da Convenção[123], deixando de

[118] COUNCIL OF EUROPE, *op. cit.* (nota de rodapé 30).
[119] COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 108. Disponível em: https://www.coe.int/en/web/data-protection/convention108/parties. Acesso em: 03 jun. 2024.
[120] Artigo 23(e) da Convenção 108+.
[121] Artigo 15 da Convenção 108+.
[122] Artigo 12 da Convenção 108+.
[123] Artigo 14(2) da Convenção 108+.

distinguir as OIs que operam no território de um Estado-membro ou de um país terceiro. O critério de análise dessa adequação leva em conta a legislação do Estado terceiro ou as normativas internas da OI[124], o que novamente indica que as organizações não se subordinarão às leis locais, mas sim às suas próprias regras e jurisdição.

Nesse sentido, importa notar a alteração da palavra "território" contida na versão inicial da Convenção 108 para "jurisdição" na versão modernizada 108+. A interpretação dada pelo departamento jurídico do CoE[125] é de que a palavra "jurisdição" não tem condão exclusivamente territorial, sendo, portanto, mais adequada às organizações que não possuem um território determinado, mas agem na sua própria jurisdição conforme o seu mandato. Isso significa que a noção de jurisdição na versão modernizada da Convenção 108[126] não corresponde à soberania legal sobre um território e sim com a eficácia das normas de proteção de dados aplicáveis num contexto específico[127]. Essa alteração se deu justamente porque, como referido anteriormente, a oportunidade de adesão das OIs na Convenção só foi permitida por meio do Protocolo ulterior.

O trabalho do Comitê Consultivo também envolve uma avaliação contínua do nível de proteção de dados oferecido pelas partes da Convenção. Em que pese não existam OIs partes, o Comitê já divulgou um documento contendo instruções sobre o exame prévio que determinará se as organizações candidatas atendem ou não às expectativas do CoE[128]. A orientação acerca da imunidade das OIs é de que cada caso deve ser analisado separada e cuidadosamente, tendo em conta a situação excepcional em que uma OI esteja sujeita a outras normas de proteção de dados além das suas próprias, ao mesmo tempo sujeita às regras dessa outra jurisdição. Se essa

[124] Artigo 14(3)(a) da Convenção 108+.
[125] COUNCIL OF EUROPE. Directorate of Legal Advice and Public International Law. Legal opinion. 2021. Disponível em: https://rm.coe.int/legal-opinion-dlapil02-2021-the-interpretation-of-the-notion-of-jurisd/1680a19c58. Acesso em: 03 jun. 2024.
[126] A escolha do termo "território" na versão inicial da Convenção foi embasada na interpretação jurisprudencial do TEDH sobre o artigo 1 da CEDH: "a competência jurisdicional de um Estado à luz do artigo 1 é primariamente territorial". Ver ECHR. Case of Al-Skeini and others v. The United Kingdom. (Application no. 55721/07). Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-105606%22]}. Acesso em: 04 jun. 2024.
[127] COUNCIL OF EUROPE, *op. cit.* (nota de rodapé 125). p. 11.
[128] COUNCIL OF EUROPE. Consultative Committee of the Convention 108+. Draft Evaluation & Follow-Up Questionnaire. 2021. Disponível em: https://rm.coe.int/t-pd-2018-20rev8-evaluation-questionaire-june-2021-2752-1166-9251-1/1680a29c9c. Acesso em: 5 jun. 2024.

jurisdição não é parte da Convenção 108+ e tampouco possui um nível adequado de proteção, isso poderá comprometer o acesso da OI à Convenção[129].

O documento traz considerações sobre a responsabilidade das OIs em caso de violações das regras de proteção de dados. Segundo o Comitê, há disposições da Convenção que podem não ser cabíveis às OIs (não sujeitas às leis domésticas e que gozem de imunidade de jurisdição), em particular aquelas que garantem a reparação judicial aos titulares dos dados em caso de violações de direitos[130]. A Convenção estabelece às partes a obrigação de estabelecer sanções judiciais e compensação àquele que teve seu direito violado[131]; de dar poder à autoridade supervisora para iniciar o procedimento judicial cabível[132]; e de garantir a possibilidade de recurso contra a decisão da autoridade supervisora[133].

As questões de reparação judicial no contexto das OIs merecem mais investigação e serão minuciadas no capítulo 4. Por ora, importa mencionar que, no âmbito da Convenção 108+, as OIs devem disponibilizar "meios alternativos razoáveis" (em especial o acesso a uma agência independente para resolver disputas) a fim de equilibrar a imunidade de jurisdição que desfrutam. Isso indica que, para atender a Convenção e ser aceita pelo CoE, uma OI precisa providenciar e manter seu próprio mecanismo de reparação eficaz.

2.4.5. RGPD

Nos termos do artigo 4(26) do RGPD, uma OI é considerada "uma organização e os organismos de direito internacional público por ela tutelados, ou outro organismo criado por um acordo celebrado entre dois ou mais países ou com base num acordo dessa natureza". Semelhante à Convenção supra analisada, o Regulamento europeu dá uma definição abrangente às OIs, contemplando todas aquelas que operam com base num acordo internacional, assim promovendo a maior proteção possível do direito fundamental à proteção dos dados pessoais, mesmo quando ocorram transferências para uma organização sobre a qual o Regulamento

[129] *Ibid*., p. 4.
[130] *Ibid*., p. 6.
[131] Artigo 12 e o artigo 9 da Convenção 108+.
[132] Artigo 15, §2º da Convenção 108+.
[133] Artigo 15, §9º da Convenção 108+.

não tem aplicação direta[134]. A principal ideia é que o nível de segurança proporcionado ao fluxo transfronteiriço de dados pessoais para fora da UE seja preservado e não enfraquecido, sem prejuízo das derrogações previstas na lei para situações específicas[135].

A transferência de dados para partes terceiras é regulada da mesma maneira, sejam países de fora da UE, sejam OIs. Assim, para que a transferência se concretize de forma legal, é necessário o cumprimento prévio dos requisitos estipulados no Capítulo V do Regulamento. O primeiro deles é a decisão de adequação da Comissão Europeia a definir que "o país terceiro, um território ou um ou mais setores específicos desse país terceiro, ou a organização internacional em causa, assegura um nível de proteção adequado"[136]. Na falta de uma decisão de adequação, o segundo requisito é a apresentação de garantias adequadas pela parte receptora que não está sujeita ao RGPD, desde que os titulares dos dados gozem de direitos oponíveis e de medidas reparatórias eficazes[137]. O terceiro requisito, na falta de uma decisão da Comissão Europeia e das garantias adequadas, diz respeito às derrogações para situações específicas em que a transferência de dados é tão necessária a ponto de prescindir da análise quanto ao nível adequado de proteção oferecido pela parte receptora[138].

Portanto, o texto do Regulamento menciona as OIs em várias disposições legais, em particular regulando a transferência de dados pessoais para essas entidades. No entanto, não esclarece ou pormenoriza se as suas regras têm a intenção de serem diretamente aplicadas às OIs, o que pode causar tensões com a Comissão Europeia. Na verdade, uma decisão de adequação específica às OIs nunca foi emitida[139], já que a requisição de uma decisão de adequação, nos termos do artigo 45 do RGPD, poderia ser interpretada como uma submissão voluntária às leis europeias e, como resultado, a renúncia dos seus privilégios e imunidades[140].

---

[134] Considerando 101 do RGPD.
[135] Artigo 49(1)(a)(d)(f) do RGPD.
[136] Artigo 45 do RGPD.
[137] Artigo 46 do RGPD.
[138] Artigo 49 do RGPD.
[139] Os países cujo ordenamento já foi reconhecido como adequado pela Comissão Europeia são Andorra, Argentina, Canadá (organizações comerciais), Ilhas Faroé, Guernsey, Israel, Ilha de Man, Japão, Jersey, Nova Zelândia, República da Coreia, Suíça, Reino Unido, Estados Unidos (organizações comerciais que participam do Estrutura de Privacidade de Dados UE-EUA) e Uruguai.
[140] WICKREMASINGHE, Chanaka. International Organizations or Institutions, Immunities before National Courts. Max Planck Encyclopedias of International Law. Oxford: Oxford University Press, 2009. Disponível em: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e502. Acesso em: 9 jun. 2024.

Não há diferenciação entre as regras aplicáveis aos países terceiros e às OIs, e isso reforça a tese de que a normativa europeia não tem intenção de ser imposta a nenhuma parte terceira. De fato, o Comitê Europeu para a Proteção de Dados (EDPB) já se manifestou nesse sentido[141], afirmando que as disposições do RGPD não deverão ser entendidas em detrimento das imunidades e privilégios concedidos às OIs ou às missões diplomáticas e postos consulares não pertencentes à UE, sem prejuízo das normas relativas à transferência de dados pessoais a essas organizações, cujo cumprimento deverá ser alcançado pelo responsável/processador quando este se enquadre no âmbito de aplicação territorial do RGPD.

O Comitê também fez considerações quanto ao escopo territorial do RGPD "em um local onde a lei do Estado-membro se aplica por força do direito internacional público", conforme previsto no artigo 3(3). A respeito disso, o processamento de dados pessoais realizado por embaixadas e consulados dos Estados-membros da UE é uma atividade que se enquadra no âmbito material do artigo 2 do RGPD e, por consequência, os postos consulares ou missões diplomáticas desempenhadas por essas entidades, mesmo situadas num terceiro país, estão vinculadas às normas europeias[142]. Isso facilmente nos leva a concluir que, se a UE impõe as suas leis locais nas missões executadas fora do bloco econômico por seus Estados-membros, a mesma lógica se aplica às missões de países terceiros dentro da UE, bem como às OIs, que aplicariam as suas próprias regulações internas e não as do Estado europeu anfitrião.

Nesse contexto, interessa expor a relação entre as OIs humanitárias e o RGPD, especificamente no que concerne ao princípio básico do consentimento para o processamento dos dados pessoais (artigo 7 e Considerando 32 do GDPR)[143]. Em situações ordinárias, o consentimento é livremente dado, específico, inequívoco e revogado a qualquer tempo[144]. Porém, em intervenções humanitárias, o consentimento não é livre quando o acesso de uma pessoa a serviços essenciais depende do processamento de seus dados. Neste caso, a organização deve

---

[141] EDPB. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). 2019. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en. Acesso em: 10 jun. 2024.

[142] *Ibid*.

[143] GAZI, T. Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. Journal of International Humanitarian Action, [s.l.], v. 5, n. 9, 2020. Disponível em: https://link.springer.com/article/10.1186/s41018-020-00078-0. Acesso em: 11 jun. 2024.

[144] CORDEIRO, A. B. M. Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020. p. 171-172.

comunicar os indivíduos sobre as razões que justificam a coleta e armazenamento dos dados pessoais e encontrar outra base legal para tanto, vez que o consentimento não terá significado se os titulares dos dados não têm escolha a não ser aceitar a assistência[145].

Inclusive, o Considerando 112 do Regulamento propõe que a transferência "para uma organização humanitária internacional, de dados pessoais de um titular que seja física ou legalmente incapaz de dar o seu consentimento, com vista ao desempenho de missões, ao abrigo das Convenções de Genebra ou para cumprir o direito internacional humanitário aplicável aos conflitos armados, poderão ser consideradas necessárias por uma razão importante de interesse público ou por ser do interesse vital do titular dos dados". Tal disposição adequa a transferência de dados pessoais às OIs humanitárias dentro das derrogações previstas no artigo 49, mas não implica qualquer obrigação à organização receptora, que executará o processamento conforme as suas próprias regras.

Sob outro prisma, a aplicabilidade do RGPD poderia ser justificada quando as atividades operacionais de uma OI se enquadrem no âmbito material e territorial dos artigos 2 e 3. Nessa perspectiva, três principais argumentos sustentam essa justificação: (i) o processamento de dados por OIs não está previsto dentre as atividades expressamente não reguladas pelo RGPD, elencadas no artigo 2(2)[146]; (ii) o alcance extraterritorial do artigo 3 abrange também as OIs estabelecidas na UE ou em países fora da UE quando as atividades estejam relacionadas com "a oferta de bens ou serviços a esses titulares de dados na União, independentemente da exigência de os titulares dos dados procederem a um pagamento" ou o "controle do seu comportamento, desde que esse comportamento tenha lugar na União"[147]; e (iii) as transferências ulteriores definidas no artigo 44 indicam que o RGPD pode ser aplicado a OIs, pois o fluxo dos dados pessoais que foram inicialmente transferidos para um destinatário fora da UE e são posteriormente transferidos para outro país terceiro ou OI deve permanecer com o mesmo nível de segurança do começo ao fim[148].

---

[145] INTERNATIONAL COMMITTEE OF THE RED CROSS, *op. cit.* (nota de rodapé 59).
[146] KUNER, C. International Organizations and the EU General Data Protection Regulation. Cambridge: University of Cambridge Faculty of Law, 2018. p. 15. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3050675#paper-citations-widget. Acesso em: 15 jun. 2024.
[147] *Ibid*., p. 15-16.
[148] *Ibid*., p. 12.

Todavia, os referidos argumentos não bastam para afirmar a incidência do Regulamento doméstico europeu às OIs[149]. Primeiro, porque a lista do artigo 2(2) não é taxativa, tampouco tem o condão de apresentar uma lista de sujeitos; na verdade, exemplifica algumas atividades atípicas que não justificam a incidência da proteção fornecida pelo Regulamento. Segundo, o âmbito territorial do artigo 3 atinge apenas as corporações que, mesmo estabelecidas fora da UE, estão dentro do escopo do RGPD por processarem os dados pessoais de titulares na União, ao contrário dos Estados soberanos – ou OIs que são mencionadas nos mesmos termos – a quem o Regulamento não se aplica. Terceiro, o artigo 44 cria uma obrigação somente à parte transferidora inicial que, sem dúvidas, está sujeita ao RGPD e deverá assegurar o adequado nível de proteção inclusive nas transferências ulteriores, mas não vincula os receptores (países terceiros ou OIs) dos dados pessoais.

Em suma, apesar das argumentações em sentido contrário, o RGPD não foi projetado para se aplicar às OIs. Essa conclusão se fundamenta no tratamento equivalente que o Regulamento europeu confere a países terceiros e OIs: para ambos, a transferência de dados só é permitida mediante garantias adequadas, inexistindo qualquer disposição legal vinculativa às organizações.

2.4.6. Leis domésticas

O presente subcapítulo objetiva expor como as OIs são referenciadas nas leis domésticas de três nações em específico. A Suíça foi selecionada por sua posição como sede de muitas OIs e por ter uma legislação particular que trata diretamente da exclusão dessas entidades de seu regime de proteção de dados. No caso do Brasil, a escolha se justifica pela LGPD, que faz menção direta às pessoas de direito público externo no seu âmbito de aplicação, mas que, apesar disso, não incide sobre as OIs como sujeitos de Direito Internacional, conforme já confirmado em precedentes jurisprudenciais do Superior Tribunal Federal (STF) – a instância máxima do poder judiciário brasileiro. Por último, Portugal foi incluído devido à sua lei nacional

[149] MARELLI, M. The law and practice of international organizations' interactions with personal data protection domestic regulation: At the crossroads between the international and domestic legal orders. Computer Law & Security Review. v. 50. Amsterdam: Elsevier, 2023. Disponível em: https://www.sciencedirect.com/science/article/pii/S0267364923000596#sec0010. Acesso em: 01 jun. 2024.

subsequente ao RGPD que, apesar de manter uma forte consonância com as regras comunitárias da UE, introduziu isenções explícitas às OIs.

2.4.6.1. Lei Federal de Proteção de Dados da Suíça

A Lei Federal n.º 235.1 reveste-se de grande importância, considerando que a Suíça tem desempenhado o papel de Estado anfitrião de OIs por mais de 150 anos. Atualmente, abriga 40 dessas organizações, consolidando sua posição de destaque como um centro global de diplomacia e cooperação internacional[150]. A análise das suas disposições legais importa para este trabalho por ser uma das poucas leis domésticas que expressamente retiram as OIs do seu escopo material.

Já na primeira versão da lei federal em 1992, o legislador excluiu do seu escopo os dados pessoais processados pelo CICV[151] e, como divulgado pelo Conselho Federal Suíço à época, as OIs não seriam vinculadas ao projeto de lei, pois enquanto sujeitos de Direito Internacional Público não se submetem às leis domésticas[152]. A partir da revisão da lei em 2020[153], a referência específica ao CICV foi retirada e substituída por todos os beneficiários institucionais de privilégios e imunidades nos termos do artigo 2 da Lei Federal de 2007 sobre os Privilégios e Imunidades e Facilidades concedidos pela Suíça como Estado Hospedeiro. Ou seja, todas as entidades que gozem de privilégios e imunidades[154], por força legal, não serão atingidas pela lei federal de proteção de dados.

---

[150] FEDERAL DEPARTMENT OF FOREIGN AFFAIRS. International organizations in Switzerland. 2022. Disponível em: https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-organizations/international-organizations-switzerland.html . Acesso em: 20 jun. 2024.

[151] Artigo 2(2)(e) da Lei Federal de Proteção de Dados da Suíça de 1992. SUÍÇA. Swiss Federal Act on Data Protection. 1992. Disponível em: https://www.uaipit.com/uploads/legislacion/files/0000004341_Personal%20Data.pdf. Acesso em: 20 jun. 2024.

[152] FEDLEX. Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988. p. 448. Disponível em: https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/fr. Acesso em: 20 jun. 2024.

[153] SUÍÇA. Federal Act on Data Protection 235.1. 2020. Disponível em: https://www.fedlex.admin.ch/eli/cc/2022/491/en. Acesso em: 20 jun. 2024.

[154] Segundo o artigo 2 da Lei Federal de 2007, os beneficiários poderão ser: organizações intergovernamentais; instituições internacionais; organizações internacionais quase governamentais; missões diplomáticas; postos consulares; missões permanentes ou outras representações junto de organizações intergovernamentais; missões especiais; conferências internacionais; secretariados ou outros órgãos estabelecidos ao abrigo de um tratado internacional; comissões independentes; Tribunais internacionais; Tribunais arbitrais; outros organismos internacionais. SWITZERLAND. Loi fédérale sur les privilèges, les immunités et les facilités, ainsi que sur les aides financières accordés par la Suisse en tant qu'État hôte. 2007. Disponível em: https://www.fedlex.admin.ch/eli/cc/2007/860/fr. Acesso em: 20 jun. 2024.

Novamente, o Conselho Federal se manifestou sobre a versão mais recente da lei federal, assentando que as regras do direito suíço não se aplicam aos Estados que processam dados através de suas representações diplomáticas ou consulares instaladas na Suíça, da mesma forma que a Suíça não está obrigada a seguir as leis estrangeiras em atividades desse tipo no exterior. A lógica é a mesma para as OIs que desempenham funções em vários Estados, sendo insensato e contra a sua independência funcional exigir o cumprimento da legislação nacional de cada um[155].

2.4.6.2. LGPD do Brasil

A Lei Federal n.º 13.709/2018 passou a regular um grau de tutela mais rigoroso e consistente às informações pessoais coletadas no âmbito de aplicação territorial. A legislação brasileira foi inegavelmente inspirada no Regulamento europeu, com as devidas ressalvas em especial no que respeita às transferências internacionais de dados e aos mecanismos de salvaguarda do mesmo nível de proteção aos dados que saem das fronteiras nacionais[156]. No Brasil, o procedimento não é tão detalhado quanto na UE, havendo uma previsão genérica acerca dos critérios de adequação a serem observados pela autoridade nacional.

O termo organismo internacional é mencionado somente nos dispositivos que tratam da transferência internacional de dados, definida como aquela "para país estrangeiro ou organismo internacional do qual o país seja membro"[157]. Igual ao RGPD, a LGPD confere tratamento equivalente a qualquer parte terceira, não fazendo distinção entre a transferência de dados para um país ou para uma OI, desde que proporcionem "grau de proteção de dados pessoais adequado".

Quanto ao âmbito de aplicação territorial da LGPD, poder-se-ia argumentar que as OIs, enquanto pessoas jurídicas de direito público externo[158], estariam

[155] FEDLEX. Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales. 2017. p. 6633. Disponível em: https://www.fedlex.admin.ch/eli/fga/2017/2057/fr. Acesso em: 20 jun. 2024.
[156] INSTITUTO DE TECNOLOGIA E SOECIEDADE DO RIO. Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira. Rio de Janeiro: ITS, 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf. Acesso em: 21 jun. 2024.
[157] Artigo 5º, inciso XV, da LGPD.
[158] Artigo 42 do Código Civil: São pessoas jurídicas de direito público externo os Estados estrangeiros e todas as pessoas que forem regidas pelo direito internacional público. BRASIL. Lei n.° 10.406, de 10 de janeiro de 20002. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 21 jun. 2024.

vinculadas se operassem o tratamento de dados em alguma das seguintes situações: (i) dentro do território nacional; (ii) com o objetivo de fornecer bens ou serviços; (iii) com o objetivo de tratar dados de indivíduos localizados no território nacional; ou (iv) se os dados pessoais objeto do tratamento tenham sido coletados no território nacional[159]. Contudo, tal visão não merece prosperar, visto que a LGPD menciona a possibilidade de transferências internacionais de dados para "países ou organismos internacionais", o que indica o reconhecimento da personalidade jurídica distinta dessas organizações, sobre as quais o Estado brasileiro não tem jurisdição.

Além disso, as imunidades e privilégios das OIs já foram objeto de decisão pelo STF. O Tribunal consolidou o entendimento de que os privilégios são permanentes, mesmo quando em conflito com o direito positivo nacional, sendo a imunidade absoluta inclusive em litígios de natureza trabalhista[160]. A votação dos Ministros do Tribunal não foi unânime: aqueles contra o reconhecimento da imunidade total argumentaram a criação de um “limbo jurídico” que impossibilitaria os funcionários contratados pela OI (neste caso, o Programa das Nações Unidas para o Desenvolvimento – PNUD) do exercício de seus direitos sociais; aqueles a favor, que constituíam a maioria, fundamentaram a decisão com base no artigo 5º, §2º, da Constituição Federal: “Os direitos e garantias expressos nesta Constituição não excluem outros decorrentes (...) dos tratados internacionais em que a República Federativa do Brasil seja parte”.

Portanto, a lei brasileira é outro exemplo que demonstra a não incidência das leis nacionais sobre proteção de dados às OIs.

2.4.6.3. Lei n.º 58/2019, de 8 de agosto de Portugal

A partir da entrada em vigor do RGPD em 25 de maio de 2018, os Estados-membros da UE puderam adaptar o Regulamento ao contexto nacional. Portugal fez isso através da Lei n.º 58/2019, de 8 de agosto[161], que adequou a legislação nacional

[159] Artigo 3 da LGPD.
[160] Ver STF. RE 578543/MT - MATO GROSSO. RECURSO EXTRAORDINÁRIO. 2013. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur265485/false. Acesso em: 21 jun. 2024; e STF RE 597.368/MT - MATO GROSSO. RECURSO EXTRAORDINÁRIO. 2013. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur271139/false. Acesso em: 21 jun. 2024.
[161] PORTUGAL. Lei n.º 58/2019, de 8 de agosto. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses

às normas comunitárias. Considerando a análise anterior sobre o RGPD e reconhecendo que a legislação portuguesa não pode se desviar das regras estabelecidas pela UE, devido à sua natureza hierarquicamente superior[162], este subcapítulo não pretende apresentar uma análise detalhada da lei nacional portuguesa.

O que merece destaque, entretanto, é o artigo 54 da Lei n.º 58/2019[163], que expressamente exime as organizações de Direito Internacional Público da responsabilidade pelos crimes previstos na Seção III da lei, nos seguintes termos: "As pessoas coletivas e entidades equiparadas, com exceção do Estado, de pessoas coletivas no exercício de prerrogativas de poder público e de organizações de direito internacional público, são responsáveis pelos crimes previstos na presente secção, nos termos do artigo 11.º do Código Penal". O dispositivo legal evidencia não somente a não incidência das leis domésticas sobre as OIs, como também a isenção dessas entidades de qualquer responsabilidade criminal relacionada à tutela das informações pessoais, no que couber a lei.

Diante disso, depreende-se que existe uma abordagem diferenciada para as OIs, as quais mantêm autonomia normativa e podem se beneficiar de mecanismos próprios de controle e regulação interna, sem comprometer sua eficiência operacional. Com isso em mente, o próximo capítulo abordará a autorregulamentação.

2.5. AUTORREGULAMENTAÇÃO

Em face de uma questão política ou social, a primeira resposta dos governos é regulamentar ou legislar. Porém, há situações em que essa regulamentação tradicional de "comando e controle"[164] não é a melhor saída, especialmente para organizações que precisam de certa liberdade para executar suas funções de maneira eficaz. A análise anterior da interação entre os instrumentos legais de proteção de

dados. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982. Acesso em: 21 jun. 2024.

[162] LEXIONÁRIO. Princípio do primado do Direito da União Europeia. Disponível em: https://diariodarepublica.pt/dr/lexionario/termo/principio-primado-direito-uniao-europeia. Acesso em: 22 jun. 2024.

[163] CORDEIRO, A. B. M. Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019. Lisboa: Almedina, 2021. p. 662-663.

[164] ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. OECD Report on Alternatives to Traditional Regulation. 2006. Disponível em: https://pt.slideshare.net/slideshow/alternative-to-traditional-regulation-oecd/26792583#4. Acesso em: 23 jun. 2024.

dados e OIs revela que não há uma obrigatoriedade direta às organizações quanto à adoção das normas, sejam internacionais, sejam domésticas. Assim, as organizações podem se inspirar nas diretrizes legais, nomeadamente as internacionais, para desenvolver suas próprias regulamentações internas.

A autorregulamentação surge a partir da criação voluntária de regras internas, códigos de conduta, diretrizes de melhores práticas e mecanismos de monitoramento interno que regulam ou guiam as ações, o comportamento e os padrões de uma organização[165]. No contexto internacional, a adoção de normas internas fornece flexibilidade e adaptabilidade às OIs que operam simultaneamente em distintos cenários culturais. As práticas criadas especificamente por e para uma organização podem ser ajustadas ao problema específico que se destinam a resolver e podem mudar rapidamente em resposta a circunstâncias mutáveis.

No entanto, a adoção de regulamentação própria pode trazer impactos negativos, em especial, à responsabilização da organização em caso de descumprimento das suas práticas internas. Na ausência de mecanismos rígidos ou de uma autoridade independente para assegurar o cumprimento do regulamento, uma OI estará impune na hipótese em que cause prejuízos a um indivíduo ou à coletividade[166]. Assim como acontece nos regimes domésticos, os agentes regulatórios independentes têm um papel fundamental no fortalecimento da responsabilidade e da prestação de contas pelos tomadores de regras em relação às políticas de proteção de dados[167].

Apesar disso, a autorregulamentação se mostra atualmente como a melhor alternativa (senão a única) para regular as atividades de tratamento de dados pessoais realizadas pelas OIs. Num contexto em que as leis domésticas, no geral, não vinculam as organizações sobre as quais o Estado não exerce jurisdição, tampouco há submissão a um instrumento internacional com caráter vinculante, concerne às OIs adotar suas próprias regras e mecanismos, inspirando-se nas leis, diretrizes e regulamentos existentes. É isto que tem se observado nos últimos anos: um crescente

---

[165] *Ibid.*

[166] OKEKE, E. C. The Tension between the Jurisdictional Immunity of International Organizations and Right of Access to Court. In: QUAYLE, P. The Role of International Administrative Law at International Organizations. Leiden: Brill, 2021. Disponível em: https://brill.com/display/book/9789004441033/BP000003.xml. Acesso em: 05 jul. 2024.

[167] MEDZINI, R. Credibility in enhanced self-regulation: The case of the European data protection regime. In: MARGETTS H. et.al. Policy & Internet, v. 13, n. 3. New Jersey: Wiley, 2021. p. 366-384. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.251. Acesso em: 01 jul. 2024.

número de OIs estabelecendo seus próprios esquemas regulatórios gerais de proteção de dados e privacidade[168], aplicando exclusivamente suas regras e excluindo os regimes domésticos.

Os próximos subcapítulos farão uma análise das regras internas de duas OIs: o CICV e a UNICEF. A Cruz Vermelha, embora não seja formalmente classificada como uma organização intergovernamental, goza de privilégios e imunidades que a colocam em uma posição equivalente a muitas OIs, além de ser amplamente reconhecida pelo desenvolvimento de regras internas sobre o tratamento de dados pessoais, o que proporciona vasto material para o estudo. Por outro lado, a análise da UNICEF permite investigar as regras internas gerais da ONU e as particularidades de uma das suas agências internas. Ademais, ambas as organizações estiveram envolvidas em casos emblemáticos de vazamento de dados, conforme será detalhado no capítulo 4, sendo pertinente conhecer suas regulamentações internas antes de abordar os casos práticos.

2.5.1. Regras internas do CICV

O regulamento interno do CICV reafirma a sua independência das leis domésticas, enunciando que o processamento de dados pessoais será regulado exclusivamente pelas suas próprias regras e monitorado de forma independente pelo Escritório de Proteção de Dados da organização[169]. As "Regras do CICV sobre a Proteção de Dados Pessoais" (adotadas em 2015 e atualizadas em 2019) são organizadas em seis categorias: princípios básicos, direitos do titular dos dados, compromissos do CICV, transferência de dados, implementação das regras e atualização das regras.

Em síntese, as regras dispõem sobre o tratamento lícito (sempre que possível com consentimento), transparente e específico dos dados pessoais, dispondo que os dados devem ser "adequados e relevantes para os fins para os quais são coletados e

[168] A INTERPOL em 2011, o CICV em 2015, o ACNUR em 2016, a OMS em 2017, a UE em 2018, a OCDE em 2019 e o PNUD em 2021.
[169]COMITÊ INTERNACIONAL DA CRUZ VERMELHA. Regras do CICV sobre a proteção de dados pessoais. Disponível em: https://www.icrc.org/pt/o-cicv-e-protecao-de-dados#:~:text=Normas%20do%20CICV%20sobre%20Prote%C3%A7%C3%A3o,interagimos%20e%20cujos%20dados%20tratamos. Acesso em: 7 maio 2024.

tratados"[170] e devem ter "o maior grau de precisão e atualização possível"[171], não podendo ser mantidos por mais tempo que o necessário[172]. O titular dos dados poderá reivindicar direitos com o Escritório de Proteção de Dados e, de forma subsidiária, com a Comissão de Proteção de Dados, situação na qual "se uma reclamação for considerada justificada, medidas apropriadas devem ser tomadas"[173]. Em caso de violação de dados, as pessoas afetadas serão notificadas pelo Responsável, em estreita coordenação com o Escritório de Proteção de Dados"[174].

A transferência de dados para entidades fora do CICV só será concretizada se atender a determinados requisitos, entre eles: a identificação de uma base legal (consentimento, interesse vital, interesse público, interesse legítimo, execução de um contrato ou cumprimento de uma obrigação legal); e a avaliação prévia dos riscos a ser realizada pela Comissão de Proteção de Dados. Quanto à implementação efetiva das regras, as alegações de não cumprimento "devem ser comunicadas imediatamente ao Responsável do CICV, que deve investigá-las sem demora injustificada. Se uma reclamação tiver mérito, as medidas apropriadas devem ser tomadas para mitigar qualquer risco de dano ao Titular dos Dados". Ainda, a violação que resulte em danos "deve ser encaminhada ao Departamento de Recursos Humanos na sede do CICV e às estruturas de campo pelo Escritório de Proteção de Dados do CICV. Os membros da equipe do CICV envolvidos em uma violação grave podem estar sujeitos a medidas disciplinares"[175].

Além disso, o CICV, em parceria com o *Brussels Privacy Hub*, publicou em 2017 a primeira edição do "Manual sobre Proteção de Dados nas Ações Humanitárias". Novamente, assentou o posicionamento de que as OIs constituem a sua própria jurisdição, devendo processar os dados pessoais conforme suas próprias regras e nos limites das suas imunidades e privilégios. Ademais, reiterou a sujeição das OIs ao monitoramento interno e implementação dos seus próprios sistemas de *compliance*[176]. O manual é amplamente reconhecido como uma das referências mais completas na área de proteção de dados no contexto humanitário, cujas orientações não são direcionadas exclusivamente ao CICV, mas sim a qualquer OI humanitária (e

[170] *Ibid*., p. 7.
[171] *Ibid*.
[172] *Ibid*., p. 8.
[173] *Ibid*, p. 15.
[174] *Ibid*, p. 19.
[175] *Ibid*., p. 27.
[176] INTERNATIONAL COMMITTEE OF THE RED CROSS, *op. cit.* (nota de rodapé 59). p. 35.

seus membros), autoridades de proteção de dados, empresas privadas e outras partes envolvidas em atividades desse tipo[177].

A Parte I do Manual inclui considerações gerais, princípios básicos, informações sobre bases legais para o processamento, transferência internacional de dados e avaliações de impacto de proteção. A Parte II, por sua vez, refere-se a situações e tecnologias específicas. O documento menciona por várias vezes o princípio da responsabilidade, segundo o qual os controladores de dados devem cumprir com os princípios do Manual e comprovar a adoção de medidas que assegurem a tal conformidade, através da, por exemplo, criação de uma autoridade independente de fiscalização, da implementação de treinamentos para os funcionários e da comunicação às autoridades competentes. Contudo, assim como nas Regras Internas do CICV, as medidas concretas de responsabilização da OI e dos seus agentes em caso de violações não são pormenorizadas.

Ainda, o regulamento interno do CICV inclui a "Política sobre o Processamento de Dados Biométricos pelo CICV", que dispõe sobre o procedimento a ser adotado em caso de vazamento de dados armazenados nas instalações do CICV em Genebra, consistindo basicamente na notificação aos demais departamentos da OI interessados na violação: a Delegação que inseriu os dados, a Delegação que cobre o território onde o titular do dado se encontra e o Escritório de Proteção de Dados do CICV. Por último, existe o Código de Conduta sobre proteção de dados, especificamente direcionado ao programa "Restabelecimento de Laços Familiares", contendo princípios básicos, direitos dos titulares e disposições sobre a transferência ou publicação de dados; em caso de violação do código de conduta, haverá notificação do indivíduo afetado[178].

2.5.2. Regras internas da UNICEF

A UNICEF é um organismo subsidiário das Nações Unidas, o que significa que sua atuação está diretamente ligada ao sistema da organização "mãe" e às normas gerais que regem o funcionamento de suas entidades. A ONU adotou os

[177] *Ibid*., p. 25.
[178] INTERNATIONAL COMMITTEE OF THE RED CROSS. Restoring Family Links code of conduct on data protection. Disponível em: https://www.icrc.org/en/document/rfl-code-conduct. Acesso 01 jul. 2024.

Princípios sobre Proteção e Privacidade de Dados Pessoais[179], que fornecem um *framework* para o tratamento de dados pessoais dentro de suas diversas suborganizações. Esses princípios buscam harmonizar as práticas relacionadas ao processamento de dados pessoais dentro do sistema da ONU e garantir que o tratamento seja responsável, transparente e que os direitos humanos e a privacidade dos indivíduos sejam protegidos.

Eles servem como uma base comum para a proteção de dados pessoais em toda a estrutura da ONU e, ao mesmo tempo, permitem aos organismos desenvolver suas próprias políticas e diretrizes operacionais mais detalhadas sobre o processamento de dados pessoais, desde que essas políticas estejam em conformidade com os princípios gerais da ONU e com o mandato específico de cada organização. A Política de Proteção de Dados da UNICEF foi implementada em 2020, sem prejuízo das imunidades e privilégios conferidos pelas Convenção da ONU de 1946[180]. Não há menção expressa acerca das leis domésticas dos países onde ocorram as operações, porém, o documento ressalta que a adoção da Política está alinhada com os direitos e proteções de longa data conferidos pela convenção internacional, podendo a UNICEF atuar de forma independente e livre de eventual jurisdição nacional.

As normas regulam o processamento durante todo o ciclo de vida do dado pessoal: desde a coleta até a exclusão/retenção. Os princípios que regem as atividades executadas pela UNICEF incluem: processamento legítimo e justo, finalidade específica, necessidade e proporcionalidade, precisão, segurança e retenção limitada. O titular tem direito a requerer acesso, correção, exclusão, objeção ou restrição dos dados. A Política ainda estipula que será estabelecida uma regulação especificamente sobre vazamento de dados pessoais, criando canais de denúncia, revisão ou investigação de incidentes, medidas técnicas de resposta e notificações aos titulares dos dados. Contudo, tal regulamento ainda não foi publicado pela UNICEF.

---

[179] Os princípios foram desenvolvidos e aprovados pelo UN PPG, criado em setembro de 2016 e co-presidido pelo *UN Global Pulse* e pelo OICT. O UN PPG tem a missão de promover o diálogo e a cooperação sobre questões de privacidade e proteção de dados dentro do sistema da ONU. UNITED NATIONS - CEB. Principles on Personal Data Protection and Privacy. Disponível em: https://unsceb.org/principles-personal-data-protection-and-privacy-listing. Acesso em: 04 ago. 2024.

[180] UNICEF. UNICEF Policy on Personal Data Protection. 2020. Disponível em: https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf. Acesso em: 02 jul 2024.

No que respeita à responsabilização dos seus membros, o Anexo 3 do documento determina as atribuições dos funcionários envolvidos no processamento dos dados pessoais e na tomada de decisão sobre a proteção adequada, cabendo ao Vice-Diretor Executivo da OI tomar as decisões em caso de descumprimento das regras internas, situação na qual o agente poderá ser responsabilizado por negligência grave, imprudência ou conduta deliberada.

3. OPERAÇÕES DE TRATAMENTO DE DADOS PELOS TRIBUNAIS INTERNACIONAIS

O capítulo anterior dedicou-se a análise da interação entre as OIs e os instrumentos legais internacionais e domésticos de proteção de dados, tendo em conta as imunidades e privilégios que essas organizações gozam. A interação entre leis domésticas e OIs é uma área rica para discussão, porque elas frequentemente realizam atividades administrativas, políticas e operacionais que se sobrepõem às jurisdições nacionais, criando potenciais pontos de conflito e necessidade de harmonização legal.

O presente capítulo, por sua vez, tem por objetivo investigar como é feito e regulado o processamento de dados pessoais pelos Tribunais internacionais que, embora também gozem de imunidades e privilégios, exercem funções judiciais e não apenas administrativas. Esses Tribunais podem ser órgãos judiciais de OIs (o Tribunal Europeu dos Direitos Humanos – TEDH do CoE, o TJUE da UE ou o TIJ da ONU) ou podem ser eles mesmos organizações autônomas, como o TPI, que possui personalidade jurídica própria e independência em relação a outras OIs[181]. A principal função desses Tribunais é resolver disputas e julgar casos (às vezes inclusive envolvendo OIs) com base no Direito Internacional. Dada a sua natureza judicial, a interação com as leis domésticas dos Estados onde operam ou onde as partes estão localizadas é menos provável do que com outras organizações.

Ainda assim, os Tribunais (domésticos e internacionais) também processam dados pessoais. No exercício das suas funções jurisdicionais, o recolhimento e tratamento têm como objetivo garantir "a comunicação dos atos processuais às partes no processo"[182] e "permitir a difusão de informação útil sobre os processos judiciais,

[181] Os Tribunais *ad hoc* para a ex-Iugoslávia e Ruanda foram criados pelo Conselho de Segurança da ONU e, dessa forma, operavam como órgãos subsidiários. Por outro lado, o TPI é uma OI independente, criada com base em um tratado internacional, qual seja, o Estatuto de Roma. Apesar dessa independência, o TPI ainda mantém laços firmes com o Conselho de Segurança da ONU, decorrentes dos poderes concedidos ao Conselho pelo Capítulo VII da Carta da ONU (ação em caso de ameaça à paz, ruptura da paz e ato de agressão). MISTRY, H.; VERDUZCO, D. R. The UN Security Council and the International Criminal Court. London: Chatham House, 2012. Disponível em: https://www.chathamhouse.org/sites/default/files/field/field_document/20120316UNSecurityCouncilICC.pdf. Acesso em: 12 set. 2024.

[182] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. A proteção de dados pessoais tratados pelo Tribunal de Justiça da União Europeia. Disponível em: https://curia.europa.eu/jcms/jcms/p1_2699101/. Acesso em: 15 jul. 2024.

pendentes ou findos, em conformidade com o princípio da publicidade da justiça"[183]. Em funções não jurisdicionais, a coleta de dados pessoais pode ser necessária para o exercício das atividades administrativas do Tribunal, como acontece na gestão de recursos humanos, gestão financeira e contábil e na prestação de serviços às partes, testemunhas e vítimas[184].

Dessa forma, os Tribunais podem manter em seus registros informações pessoais de solicitantes, testemunhas e outras partes relevantes. Se esses dados são armazenados de forma eletrônica, estarão sujeitos a violações, utilização e divulgação indevidas, ataques cibernéticos e erros humanos. Para afastar esses riscos, a instituição deve adotar uma política de privacidade e proteção dos dados pessoais, além de implementar medidas rigorosas de segurança, por exemplo criptografia, autenticação dupla e monitoramento ativo de cibersegurança[185]. Isso visando assegurar a privacidade dos indivíduos, sem prejuízo da transparência das informações do Tribunal.

3.1. NOÇÃO DE TRIBUNAL INTERNACIONAL

Os Tribunais internacionais são geralmente criados a partir de estatutos internacionais[186], tratados fundadores[187] ou resoluções de uma OI[188], a fim de auxiliar os Estados a resolverem disputas que não puderam ser solucionados por meios diplomáticos ou internos. Assim, oferecem uma alternativa à resolução de conflitos ou à condenação criminal através dos Tribunais domésticos, que frequentemente carecem da estrutura ou imparcialidade necessárias para lidar com certas questões.

---

[183] *Ibid*.
[184] CUSTERS, B. et al. *Quis custodiet ipsos custodes*? Data protection in the judiciary in EU and EEA Member States. International Data Privacy Law, v. 12, n. 2. Oxford: IDPL, 2022. p. 109. Disponível em: https://academic.oup.com/idpl/article/12/2/93/6511894. Acesso em: 24 jul. 2024.
[185] SETIAWAN, H. et al. Digitalization of Legal Transformation on Judicial Review in the Constitutional Court. Journal of Human Rights, Culture and Legal System, vol. 4, n. 2. Surakarta: Lembaga Contrarius Indonesia, 2024. p. 263-298. Disponível em: https://jhcls.org/index.php/JHCLS/article/view/263. Acesso em: 15 jul. 2024.
[186] O TPI foi criado pelo Estatuto de Roma em 2002. Neste ponto, notar que o Estatuto de Roma também é um tratado internacional.
[187] A Carta das Nações Unidas estabeleceu a TIJ como o principal órgão judicial da ONU.
[188] A criação dos Tribunais *ad hoc* da ex-Ioguslávia foi através das Resoluções 827/1993 e 955/1994, respectivamente, do Conselho de Segurança da ONU.

Além disso, esses Tribunais contribuem para a uniformização da interpretação dos instrumentos internacionais[189].

O início da adjudicação internacional moderna se deu em 1794, quando a Grã-Bretanha e os Estados Unidos assinaram o "Tratado de Jay", cujo objetivo foi estabelecer um Tribunal misto, composto por membros nomeados por ambos os países para resolver reclamações formuladas por seus cidadãos; em caso de desavença, um árbitro parcial decidia o caso[190]. Outro marco significativo foi o Tratado de Washington de 1871, também entre a Grã-Bretanha e os Estados Unidos, por meio do qual os países criaram um Tribunal arbitral capaz de proferir decisões fundamentadas na lei, deixando de lado questões eminentemente diplomáticas[191]. Finalmente, em 1899, foi estabelecido um marco permanente para a resolução de disputas internacionais: a Corte Permanente de Arbitragem (CPA)[192].

Na UE, o Tribunal de Justiça começou na década de 1950, a partir da criação de cortes individuais para supervisionar o cumprimento das leis por três comunidades europeias: a Comunidade Europeia do Carvão e do Aço (CECA), a Comunidade Econômica Europeia (CEE) e a Comunidade Europeia da Energia Atômica (EURATOM). Em 1957, com o Tratado de Roma, os Tribunais dessas três comunidades foram unificados em um único Tribunal, o TJUE, que passou a atender as necessidades legais de toda a Comunidade Europeia (CE)[193]. Com o tempo, o TJUE deixou de ser meramente um Tribunal internacional para se tornar o "Tribunal Constitucional da Europa", sendo responsável por garantir o equilíbrio entre a integração europeia, os direitos nacionais, os direitos dos cidadãos e os compromissos internacionais assumidos pelos governos europeus[194]. Embora tenha que lidar com as pressões dos governos nacionais, o principal objetivo do TJUE é encontrar soluções jurídicas que satisfaçam os juízes nacionais, os quais também enfrentam o desafio de equilibrar as exigências da integração europeia com as

[189] CESARE, R. The sword and the scales: the United States and international courts and Tribunals. Cambridge; New York: Cambridge University Press, 2009. p. 1.
[190] BLACKABY, N. et al. An Overview of International Arbitration. Oxford: Oxford University Press, 2009. p. 1-83.
[191] *Ibid*.
[192] *Ibid*.
[193] TAMM, D. The History of the Court of Justice of the European Union Since its Origin. In: COURT OF JUSTICE OF THE EUROPEAN UNION (ED.). The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law. Hague: T. M. C. Asser Press, 2013.
[194] MESQUITA, M. J. R. de. The Court of Justice of the European Union. In: VICENTE, D. M. (Ed.). Towards a Universal Justice? Putting International Courts and Jurisdictions into Perspective. Hague: Brill/Nijhoff, 2016. p. 451-467.

constituições nacionais, sem se deixar influenciar demasiadamente pelas políticas populistas dos governos[195].

Dessa forma, o papel das cortes internacionais na resolução de disputas é fornecer um fórum neutro, imparcial e despolitizado. Os meios diplomáticos comuns, muitas vezes, não logram solucionar disputas que contenham fatos impugnados pelas partes envolvidas ou questões jurídicas mais complexas, que devem ser analisadas e decididas por juristas internacionais comprometidos a não proferir decisões em favor ou em prejuízo de um Estado específico. As influências políticas também podem entravar a solução de um conflito entre nações, fazendo com que as partes busquem o mecanismo de decisão por terceiros oferecido pela Corte internacional[196]. Na seara criminal, os Tribunais internacionais julgam crimes de extrema gravidade que afetam a comunidade internacional como um todo[197], podendo ter caráter permanente (TPI) ou *ad hoc* (Nuremberg, ex-Iugoslávia e Ruanda)[198].

O enfoque deste capítulo, portanto, será direcionado a três Tribunais: o primeiro é o TIJ, criado pela ONU para resolver disputas entre Estados e emitir pareceres consultivos tendo por base os direitos e as obrigações decorrentes do Direito Internacional; o segundo é o TPI, apto a decidir e condenar indivíduos por crimes de genocídio, crimes contra a humanidade, crime de guerra e crime de agressão; e o terceiro é o TJUE, que emite decisões sobre a interpretação da legislação da UE para os Tribunais nacionais dos Estados-membros e ouve várias ações envolvendo países e instituições europeias. A escolha de analisar esses três Tribunais em específico se deve à importância e ao impacto distinto que cada um deles exerce no campo jurídico internacional e europeu.

3.2. PRIVILÉGIOS E IMUNIDADES DOS TRIBUNAIS INTERNACIONAIS

[195] ALTER, K. J. et al. Too Much Power for the Judges? In: HUBERT, Z.; DUR, A. (Ed.). Key Controversies in European Integration. 3ed. London: Bloomsbury Academic, 2022. p. 52-53.
[196] BROWN, C. Review Essay - The Proliferation of International Courts and Tribunals: finding your way through the maze. Melbourne: Melbourne Law School, 2014. Disponível em: https://law.unimelb.edu.au/__data/assets/pdf_file/0006/1680261/Brown.pdf. Acesso em: 16 jul. 2024.
[197] Sobre a jurisdição penal internacional, ler MACHADO, J. Direito Internacional - do paradigma clássico ao pós-11 de setembro. 4 ed. Coimbra: Coimbra Editora, 2006. p. 446.
[198] PALOMBO, T. M. Dos Tribunais "ad hoc" ao Tribunal Penal Internacional, o que mudou e o que não mudou? São Paulo: Universidade Presbiteriana Mackenzie, 2021. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/82d7e827-11b5-4abe-9c7f-ba1e406cd067/content. Acesso em: 16 jul. 2024.

Os privilégios e imunidades conferidos aos membros do TIJ emergiram a partir do Pacto da Liga das Nações. A ideia dos membros do Comitê Consultivo da Liga das Nações, ao se reunirem em 1920 na cidade de Haia para redigir o estatuto da Corte Permanente de Justiça Internacional (antecessora do TIJ), era conceder aos juízes as mesmas benesses dos agentes diplomáticos, com base nos termos das Convenções de Haia sobre Solução Pacífica de 1899 e 1907. Em particular, os juízes deveriam gozar de estatuto diplomático tanto nos Países Baixos como nos países onde pudessem viajar para exercerem as atividades da Corte, a fim de garantir aos juristas o desempenho de suas funções de maneira independente e sem interferências externas[199].

Da mesma forma, os Tribunais *ad hoc* para a ex-Iugoslávia e para a Ruanda demonstraram que a independência operacional era essencial para a eficácia de um Tribunal criminal internacional, de forma que os Estados não dificultem a entrada de pessoal ou restrinjam as suas atividades no seu território. Assim, para que o TPI atendesse às expectativas de sua criação, foram concedidos os privilégios e imunidades necessários para um funcionamento independente e eficaz[200]. Ao contrário dos Tribunais *ad hoc*, que estavam integrados no sistema das Nações Unidas e se beneficiam dos instrumentos legais da organização, o TPI é completamente independente da ONU e teve que desenvolver e estabelecer seus próprios benefícios correspondentes[201].

O fundamento jurídico das imunidades e privilégios dos membros do TIJ consta no artigo 105 da Carta da ONU e no artigo 19 do Estatuto da Corte[202], segundo o qual: “Os membros do Tribunal quando no exercício das suas funções gozarão dos privilégios e imunidades diplomáticas”. Além das Convenções da ONU de 1946 e de 1947, que tratam das facilidades concedidas às Nações Unidas e seus órgãos

---

[199] ANDERSON, D.; WORDSWORTH, S. In: ZIMMERMANN, Andreas; TAMS, Christian J.; OELLERS-FRAHM, Karin; TOMUSCHAT, Christian (Ed.). The Statute of the International Court of Justice: A Commentary. 3 ed. Oxford: Oxford University Press, 2019. p. 64-65.

[200] BERESFORD, S. The Privileges and Immunities of the International Criminal Court: Are They Sufficient for the Proper Functioning of the Court or Is There Still Room for Improvement? San Diego: San Diego International Law Journal, v. 6, n. 1, 2002. p. 85-86. Disponível em: https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1261&context=ilj. Acesso em: 20 jul. 2024.

[201] INTERNATIONAL CRIMINAL COURT. Understanding the International Criminal Court. Disponível em: https://www.icc-cpi.int/sites/default/files/Publications/understanding-the-icc.pdf. Acesso em: 20 jul. 2024.

[202] MINISTÉRIO PÚBLICO DE PORTUGAL. Estatuto do Tribunal Internacional de Justiça. Disponível em: https://www.ministeriopublico.pt/instrumento/estatuto-do-Tribunal-internacional-de-justica-0. Acesso em: 21 jul. 2024.

especializados, os membros do TIJ estão resguardados por força da Resolução 90(I) de 1946[203], por meio da qual a Assembleia Geral da ONU estabeleceu as imunidades e privilégios dos juízes, oficiais, escrivães, advogados, representantes, assessores, testemunhas, peritos e outros envolvidos; o alcance desses benefícios; e a implementação na prática.

Por seu turno, o Estatuto de Roma dispõe sobre os privilégios e imunidades que se mostrem necessários ao cumprimento das funções do TPI no território dos Estados partes. Assim, confere benefícios diplomáticos aos juízes, ao procurador, aos procuradores-adjuntos e ao secretário[204]; concede as facilidades previstas no acordo sobre os privilégios e imunidades do Tribunal ao secretário-adjunto, ao pessoal do Gabinete do Procurador e ao pessoal da Secretaria[205]; e os advogados, peritos e testemunhas "cuja presença seja requerida na sede do Tribunal beneficiarão do tratamento que se mostre necessário ao funcionamento adequado deste (...)"[206]. Ademais, os privilégios são detalhados no Acordo sobre os Privilégios e Imunidades do TPI[207] e nos acordos-sede firmados com o Estado anfitrião[208].

Nesse contexto, importa notar que os benefícios dos diplomatas e dos juízes internacionais são distintos, pois os primeiros atuam em nome de um Estado específico, ao passo que os segundos julgam casos de forma imparcial, podendo envolver seus próprios países ou países terceiros. Ao contrário dos diplomatas, que dispõem de missões e malas diplomáticas, os juízes não têm esses instrumentos à sua disposição[209]. Por isso, desfrutam de imunidades diplomáticas de maneira mais abrangente do que os próprios diplomatas[210].

---

[203] INTERNATIONAL COURT OF JUSTICE. Resolution 90(I) of the General Assembly of the United Nations, II December 1946. Disponível em: https://www.icj-cij.org/other-texts/resolution-90. Acesso em: 21 jul. 2024.
[204] Artigo 48 (2) do Estatuto de Roma. MINISTÉRIO PÚBLICO DE PORTUGAL. Estatuto de Roma do Tribunal Penal Internacional. Disponível em: https://www.ministeriopublico.pt/instrumento/estatuto-de-roma-do-Tribunal-penal-internacional-22. Acesso em: 21 jul. 2024.
[205] Artigo 48 (3) do Estatuto de Roma.
[206] Artigo 48 (4) do Estatuto de Roma.
[207] MINISTÉRIO PÚBLICO PORTUGAL. Acordo sobre os Privilégios e Imunidades do Tribunal Penal Internacional. Disponível em: https://www.ministeriopublico.pt/instrumento/acordo-sobre-os-privilegios-e-imunidades-do-Tribunal-penal-internacional-0. Acesso em: 21 jul. 2024.
[208] INTERNATIONAL CRIMINAL COURT. Headquarters Agreement between the International Criminal Court and the Host State. Disponível em: https://www.icc-cpi.int/sites/default/files/NR/rdonlyres/99A82721-ED93-4088-B84D-7B8ADA4DD062/280775/ICCBD040108ENG1.pdf. Acesso em: 21 jul. 2024.
[209] ANDERSON, D.; WORDSWORTH, S., *op. cit*., p. 67-69.
[210] LING, Y. A Comparative Study Of The Privileges And Immunities Of United Nations Member Representatives And Officials With The Traditional Privileges And Immunities Of Diplomatic Agents. Washington and Lee Law Review, v. 3, n. 1. Washington: Washington and Lee Law Review, 1976. Disponível em:

Além da imunidade de jurisdição, por meio da qual os juízes, procuradores, secretários, relatores e demais membros não serão submetidos a processos judiciais decorrentes de atos praticados durante o exercício das suas funções oficiais[211] (e, em alguns casos, inclusive após a cessação dessas funções[212]), os Tribunais também gozam de imunidades relativas às suas instalações, fundos, bens, arquivos e documentos[213]. Tais benefícios só serão removidos se forem renunciados nos termos legais previamente estipulados.

Os privilégios e imunidades são concedidos ao TIJ para atender aos interesses próprios da Corte e não para interesses particulares dos beneficiários. O Secretário do Tribunal, a partir da aprovação do Presidente, tem o direito e o dever de renunciar a imunidade nos casos em que entender que o benefício impedirá o curso da justiça, desde que tal renúncia não prejudique os interesses do Tribunal. As imunidades gozadas pelo Secretário, por sua vez, poderão ser objeto de análise e eventual renúncia pela Corte. Ainda, aos agentes, assessores, testemunhas, peritos e indivíduos desempenhando missões em nome do órgão judicial, a autoridade competente tem o mesmo direito e obrigação do Secretário, na medida que também pode declarar renúncia à imunidade quando o referido benefício esteja impedindo o (e sem prejuízo ao) curso da justiça[214].

No TPI, a maioria absoluta dos juízes pode renunciar os privilégios e imunidades conferidos a um juiz ou procurador; a presidência pode renunciar os benefícios do Secretário do Tribunal; o Procurador é competente para renunciar as regalias do gabinete do Procurador; e o Secretário os privilégios dos funcionários do seu gabinete[215]. Semelhante ao que ocorre no TIJ, as imunidades no TPI podem ser renunciadas desde que não comprometam o funcionamento adequado do Tribunal. Por exemplo, se um funcionário do TPI cometer uma infração de trânsito e tentar usar sua imunidade para evitar o pagamento da multa, essa imunidade poderá ser retirada. Isso é feito visando, além de não prejudicar as atividades do Tribunal, impedir que a imunidade seja usada para benefício pessoal do funcionário[216]

---

https://heinonline.org/HOL/LandingPage?handle=hein.journals/waslee33&div=10&id=&page=. Acesso em: 22 jul. 2024.

[211] Artigo 17 do acordo-sede entre o TPI e os Países Baixos.

[212] Artigo 3º do Estatuto do TJUE.

[213] Artigos 4°, 6° e 7° do Acordo sobre os Privilégios e Imunidades do Tribunal Penal Internacional.

[214] Resolução 90(I) da Assembleia Geral da ONU, de 02/12/1946.

[215] Capítulo IV do acordo-sede entre o TPI e os Países Baixos.

[216] REES, Y. M. Article 48(5). In: KLAMBERG, M.; ANGOTTI, A (Ed.). Commentary on the Law of the International Criminal Court: The Statute. 2ed. Brussels: Torkel Opsahl Academic EPublisher, 2023. p.

Ainda, os privilégios dos membros do TJUE são garantidos no seu Estatuto[217]. O texto legal estabelece que os juízes gozam de imunidade jurisdicional e não podem ser processados por ações realizadas no exercício de suas funções oficiais, nem mesmo após deixarem o cargo. A imunidade se estende a todas as suas declarações e escritos feitos e só pode ser retirada pelo Tribunal competente que está examinando o caso, ou seja, se a decisão envolver um membro do Tribunal Geral ou de um Tribunal especializado, o Tribunal Pleno deverá consultar o Tribunal específico antes de tomar a decisão. Caso a imunidade seja retirada e um processo criminal seja iniciado contra um juiz, ele "só pode ser julgado, em qualquer dos Estados-Membros, pela instância competente para julgar os magistrados pertencentes ao órgão jurisdicional nacional da mais elevada hierarquia"[218]. Além disso, os juízes, advogados-gerais, secretário e relatores adjuntos do Tribunal estão sujeitos a regras específicas estabelecidas no Protocolo sobre os Privilégios e Imunidades da UE[219], que complementam e não substituem as disposições sobre imunidade judiciária mencionadas anteriormente.

Destarte, os privilégios conferidos aos Tribunais internacionais são fundamentais para assegurar a sua independência e evitar que suas funções sejam influenciadas ou comprometidas por leis domésticas e só poderão ser renunciadas nas condições previamente estabelecidas.

3.3. INAPLICABILIDADE DAS LEIS DOMÉSTICAS

O capítulo anterior argumentou que as leis domésticas não são intencionadas às OIs, conforme conclusões advindas a partir da análise dos principais instrumentos legais internacionais e leis nacionais específicas. A mesma lógica se aplica aos Tribunais internacionais, especialmente porque eles são OIs independentes ou são órgãos judiciais de OIs independentes e, dessa forma, compartilham características que os diferenciam das entidades sujeitas às leis nacionais. Os Tribunais

1072. Disponível em: https://www.diva-portal.org/smash/get/diva2:1822990/FULLTEXT01.pdf. Acesso em: 22 jul. 2023.

[217] UNIÃO EUROPEIA. Versão consolidada do Tratado da União Europeia - Protocolo (n. 3) relativo ao Estatuto do Tribunal de Justiça da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12016M%2FPRO%2F03. Acesso em: 12 set. 2024.

[218] Artigo 3º do Estatuto do TJUE.

[219] Artigos 11 a 14 e 17. UNIÃO EUROPEIA. Versão consolidada do Tratado da União Europeia - Protocolo (n. 7) relativo aos Privilégios e Imunidades da UE. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12008E/PRO/07. Acesso em: 12 set. 2024.

internacionais são criados por tratados internacionais e têm o mandato de resolver disputas de acordo com o Direito Internacional, o que lhes confere uma independência similar à das OIs.

Ainda assim, a probabilidade de interação entre OIs e leis domésticas é maior do que entre Tribunais internacionais e leis domésticas, uma vez que as OIs frequentemente envolvem-se em atividades operacionais dentro dos territórios nacionais, ao passo que os Tribunais internacionais funcionam mais como órgãos de adjudicação remotos. Portanto, é mais fácil concluir que, de modo geral, as leis domésticas não têm a intenção de serem aplicadas às Cortes internacionais.

Nessa perspectiva, desde a troca de cartas entre o Presidente do TIJ e o Ministro das Relações Exteriores dos Países Baixos em 1946, que estabeleceu as imunidades e privilégios da Corte antecessora do TIJ, o entendimento é que os juízes, durante o exercício das suas funções, devem gozar de todos os privilégios e imunidades diplomáticas em todos os países por quais passarem[220]. Essas facilidades devem ser respeitadas e aplicadas no âmbito do Direito Internacional Público e efetivamente reconhecidas e implementadas pelas leis internas dos países que aderiram ao Estatuto, a fim de que os juristas não se submetam às jurisdições locais enquanto desempenham seus ofícios em outros países, nos limites das suas atribuições[221].

Por seu turno, o TPI está sujeito às leis domésticas nos limites das inconsistências eventualmente existentes com as suas próprias regras. O acordo-sede celebrado entre o TPI e os Países Baixos estipula claramente que as leis e regulamentos nacionais serão aplicados nas instalações do Tribunal[222]. No entanto, o TPI tem o poder de estabelecer suas próprias regras necessárias para o desempenho adequado de suas operações e, em caso de inconsistências com as leis domésticas, estas não serão impostas ao Tribunal[223]. Na sequência, o acordo estipula que tais divergências serão resolvidas mediante consulta, negociação ou outra forma de acordo e, falhando tais meios, através de um Tribunal arbitral; enquanto pender a resolução, as regras do TPI serão aplicadas em detrimento das leis e regulamentos locais[224].

---

[220] ANDERSON, D.; WORDSWORTH, S., *op. cit.* (nota de rodapé 209).
[221] *Ibid*.
[222] Artigo 8(2) do acordo-sede entre o TPI e os Países Baixos.
[223] Artigo 8(3) do acordo-sede entre o TPI e os Países Baixos.
[224] Artigo 55 do acordo-sede entre o TPI e os Países Baixos.

Assim, é possível inferir que os Tribunais internacionais gozam de uma independência significativa em relação à ordem jurídica doméstica dos Estados anfitriões, cujas legislações só serão aplicadas com a prévia renúncia dos privilégios e imunidades conforme estabelecido nas Convenções da ONU, no acordo-sede ou no seu Estatuto fundador.

3.3.1. A relação entre o TJUE e o RGPD

Tendo em vista que as regras internas dos Tribunais internacionais, especificamente TIJ e TPI, prevalecem sobre as leis e regulamentos locais, o mesmo princípio se aplica às leis domésticas de proteção de dados. Em outras palavras, uma lei nacional que regulamenta o processamento de dados num determinado país não será imposta aos Tribunais cuja função é julgar litígios entre Estados ou crimes humanitários internacionais.

Nesse contexto, interessa destacar o caso do TJUE. Certamente, há diferenças fundamentais entre o Tribunal da UE e os Tribunais internacionais supra analisados: enquanto o TJUE opera num contexto regional e suas decisões se aplicam somente aos Estados-membros da UE, o TPI e o TIJ têm um alcance mais global, refletindo uma jurisdição verdadeiramente internacional[225]. Ainda assim, sua função de assegurar a interpretação e aplicação uniforme do direito da UE e sua jurisdição sobre litígios que envolvem múltiplas jurisdições dentro do bloco europeu conferem-lhe também um caráter internacional[226]. O TJUE atua em um contexto supranacional, acima das legislações domésticas dos países membros, cujas decisões têm implicações que transcendem as fronteiras de qualquer Estado-membro individual[227]. Sendo, portanto, um Tribunal europeu supranacional, suas atividades não se enquadram no âmbito da legislação nacional, da mesma forma que as demais Cortes internacionais.

---

[225] A diferenciação entre Justiça Universal e Justiça Regional deriva de um critério geográfico ou espacial: enquanto a primeira envolve um conjunto amplo de sujeitos de Direito Internacional, a segunda apenas um grupo mais restrito de sujeitos de Direito Internacional, geralmente definido por um critério geográfico ou geopolítico. A respeito disso, ver MESQUITA, M. J .R. de. Justiça Internacional (Lições), Parte I – Introdução. Lisboa: AAFDL, 2010. p. 89.

[226] PROENÇA, C. Tutela Jurisdicional Efetiva no Direito da União Europeia. Coimbra: Faculdade de Direito e de Economia, 2014. p. 110. Disponível em: https://estudogeral.uc.pt/bitstream/10316/26659/1/Tutela%20jurisdicional%20efetiva%20no%20direito%20da%20Uni%C3%A3o%20Europeiaa.pdf. Acesso em: 02 ago. 2024.

[227] *Ibid*., p. 50.

Nesse sentido, o RGPD se aplica ao poder judiciário, mas com importantes limitações: o TJUE está sujeito ao Regulamento somente nas suas funções administrativas. Quando os dados são tratados por Tribunais ou autoridades judiciais que atuam no exercício das suas competências judiciais, esses limites se justificam "a fim de assegurar a independência do poder judicial no exercício da sua função jurisdicional, nomeadamente a tomada de decisões"[228].

A supervisão interna quanto ao tratamento realizado por uma autoridade ou organismo público é responsabilidade do Encarregado de Proteção de Dados (EPD), exceto nas situações em que os Tribunais atuem conforme suas funções jurisdicionais[229]. Isso não significa que as Cortes estão proibidas de designar um EPD; pelo contrário, existem órgãos judiciais que nomearam uma autoridade independente de fiscalização interna, que não supervisionará as atividades realizadas pelos Tribunais enquanto órgãos jurisdicionais e sim apenas atuará em questões administrativas: é o caso do TJUE que nomeou um EPD interno para o controle do tratamento de dados pessoais nas atividades extrajudiciais[230].

A supervisão externa, por sua vez, se dá por meio da criação de autoridades nacionais de proteção de dados, cuja competência expressamente exclui a supervisão do processamento das operações dos Tribunais "que atuem no exercício da função jurisdicional"[231]. Ou seja, mesmo havendo concordância dos Tribunais com a fiscalização, a autoridade de controle independente não está autorizada a fazê-lo, pelo menos quanto às atividades eminentemente jurisdicionais. No acórdão C-245/20[232], o TJUE interpretou a situação no sentido de que a disponibilização temporária de registros judiciais, contendo dados pessoais, a pedido de jornalistas, está dentre as funções jurisdicionais de um Tribunal doméstico (no caso, o Conselho de Estado dos Países Baixos em formação jurisdicional) e, por conseguinte, fora da competência da autoridade de controle estabelecida no RGPD.

Outrossim, o Regulamento (UE) 2018/1725 fornece orientações sobre a competência da Autoridade Europeia de Proteção de Dados (AEPD), que não abrange

---

[228] Considerando 20 do RGPD.
[229] Artigo 37(1)(a) do RGPD.
[230] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Delegado para a proteção de dados. Disponível em: https://curia.europa.eu/jcms/jcms/p1_641404/pt/. Acesso em: 01 ago. 2024.
[231] Artigo 55(3) do RGPD.
[232] JORNAL OFICIAL DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Primeira Secção) de 24 de março de 2022. Processo C-245/20. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62020CA0245. Acesso em: 14 ago. 2024.

o monitoramento do tratamento de dados do TJUE “no exercício das suas funções jurisdicionais”[233]. Dessa forma, sendo o TJUE uma instituição da UE, a AEPD poderia supervisionar apenas as atividades não jurisdicionais, da mesma forma que o Delegado criado pelo TJUE para fiscalizar as atividades extrajudiciais da instituição. Quando o TJUE atua na sua capacidade judicial, o Tribunal estabeleceu, através de duas decisões em outubro de 2019, um mecanismo de supervisão interna, qual seja, a análise de reclamações por uma comissão interna[234]. Ademais, ao dispor sobre o tratamento de categorias especiais de dados pessoais, a norma europeia cria uma exceção à proibição de processamento de dados sensíveis, de forma a permitir ao TJUE o processamento desse tipo de informação no exercício da função jurisdicional[235].

Logo, as regras do RGPD e o controle interno e externo exercido, respectivamente, pelo EPD e pela ANPD só terão efeito sobre os atos administrativos praticados pelo TJUE. Por isso, é necessário ter em conta a diferença entre o processamento de dados no âmbito das tarefas jurisdicionais e não jurisdicionais. Para distingui-las, é possível identificar onde estão sendo tratados os dados pessoais: (i) aqueles em processos judiciais estão no âmbito das funções jurisdicionais; e (ii) aqueles que não constam em processos judiciais estão nas funções não jurisdicionais. Somente na segunda opção, o RGPD se aplica ao TJUE, situação que poderia ser considerada uma forma de autorregulamentação, na medida em que as normas da mesma OI (UE) seriam aplicadas a um de seus órgãos (TJUE), como será discutido a seguir.

3.4. AUTORREGULAMENTAÇÃO

Não sendo submetidos às leis domésticas ou às competências das autoridades nacionais de proteção de dados, os Tribunais internacionais devem se

[233] Considerando 74 e artigo 57(1)(a) do Regulamento (UE) 2018/1725.
[234] JORNAL OFICIAL DA UNIÃO EUROPEIA. Decisão do Tribunal de Justiça, de 1 de outubro de 2019, que institui um mecanismo interno de fiscalização em matéria de tratamento de dados pessoais efetuado no quadro das funções jurisdicionais do Tribunal de Justiça. 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:C2019/383/02. Acesso em: 03 ago. 2024; JORNAL OFICIAL DA UNIÃO EUROPEIA. Decisão do Tribunal Geral, de 16 de outubro de 2019, que institui um mecanismo interno de fiscalização em matéria de tratamento de dados pessoais efetuado no quadro das funções jurisdicionais do Tribunal Geral. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:C2019/383/03. Acesso em: 03 ago. 2024.
[235] Artigo 10(2)(f) do Regulamento (UE) 2018/1725.

autorregular para assegurar a proteção dos dados pessoais manejados durante os processos judiciais. O presente subcapítulo explora as diretrizes e práticas internas do TIJ, do TPI e do TJUE.

3.4.1. Regras internas do TIJ

Com exceção da política de privacidade do seu website[236], o TIJ não possui um regulamento interno (contendo diretrizes, regras ou recomendações) específico para a proteção de dados pessoais. Para compensar essa falta, na condição de principal órgão jurisdicional da ONU, o TIJ poderia se apoiar nas regras gerais dos Princípios da ONU sobre Proteção e Privacidade de Dados Pessoais[237], mencionados anteriormente. Apesar de serem princípios aplicáveis no âmbito das funções jurisdicionais e administrativas, o TIJ não os adotou formalmente, tampouco é explicitamente mencionado dentre as organizações da ONU que seguem tais diretrizes[238]. Isso é uma preocupação mencionada pelo Secretário-Geral na Estratégia de Dados para 2020-2022[239], documento no qual ele reconhece a implementação parcial desses princípios como um desafio e destaca a necessidade urgente de atualização e harmonização das políticas de dados entre as diversas organizações da ONU.

Destarte, na ausência de uma regulamentação interna específica e da adoção formal dos Princípios da ONU sobre proteção de dados pessoais, o TIJ se encontra num campo regulamentar praticamente vazio. A situação representa não somente um desafio, como também um risco aos indivíduos que têm seus dados pessoais (ou Estados com dados sobre segurança nacional) tratados pela Corte, eis que o órgão não está adequadamente equipado, em termos de regulamentação, para enfrentar as ameaças contemporâneas à segurança dos dados.

---

[236] INTERNATIONAL COURT OF JUSTICE. Privacy Policy. Disponível em: https://www.icj-cij.org/public/privacy_policy.html. Acesso em: 04 ago. 2024.
[237] UNITED NATIONS – CEB, *op. cit.* (nota de rodapé 179).
[238] UN PRIVACY POLICY GROUP. List of member organizations that prepared and endorsed the Personal Data Protection and Privacy Principles. Disponível em: https://unsceb.org/sites/default/files/2020-10/UNPPGMembersList_Revised.pdf. Acesso em: 04 ago. 2024.
[239] UNITED NATIONS. Data Strategy of the Secretary-General for Action by Everyone, Everywhere. Disponível em: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf. Acesso em: 04 ago. 2024.

3.4.2. Regras internas do TPI

Tendo em vista que o TPI lida com um volume muito maior de dados sensíveis de indivíduos, há uma concentração significativa de informações sobre pessoas em situações vulneráveis, como vítimas e testemunhas de crimes graves, o que demanda a existência de dispositivos regulamentares mais rigorosos e específicos para proteger e garantir a segurança dos envolvidos.

A Diretiva Presidencial de 8 de março de 2005, intitulada Política de Segurança da Informação[240], estabelece os princípios fundamentais para a proteção das informações dentro do TPI. Essencialmente, exige que todos os usuários de informações produzidas, transmitidas e armazenadas pelo Tribunal cumpram rigorosamente as disposições e restrições de segurança impostas. Complementando a diretiva, a Política de Proteção da Informação do TPI foi promulgada pela Instrução Administrativa ICC/AI/2007/001 de 19 de junho de 2007[241], a qual estabelece níveis de proteção e critérios de classificação (“não classificado”, “confidencial”, “secreto” e “restrito”) dos dados coletados e armazenados em qualquer meio ou forma, judicial ou não judicial. Também menciona que a violação da Instrução ou o comprometimento da informação poderão ser objeto de sanções disciplinares.

No entanto, a política de privacidade – definida pela ICC/AI/2007/001 – se tornou obsoleta devido às alterações no Regulamento do Registro em 4 de dezembro de 2013[242], que redefiniram os níveis de confidencialidade aplicáveis aos registros judiciais (“público”, “confidencial”, “sob sigilo” e “secreto”) e criaram inconsistências com as classificações antes estabelecidas pela Instrução de 2007. Por exemplo, o Regulamento não prevê uma classificação equivalente ao termo “restrito”, utilizado pela ICC/AI/2007/001 para informações internas do Tribunal. A incoerência impacta as atividades do Gabinete do Procurador, pois ao classificar um registro judicial como “restrito”, tal classificação só terá efeito dentro do âmbito da Instrução Administrativa, uma vez que, de acordo com o Regulamento, esse registro não será considerado

[240] INTERNATIONAL CRIMINAL COURT. Presidential Directive ICC/PRESD/G/2005/001. Disponível em: https://www.legal-tools.org/doc/3ae5ed/pdf. Acesso em: 05 ago. 2024.
[241] INTERNATIONAL CRIMINAL COURT. Administrative Instrutction ICC/AI/2007/001. DIsponível em: https://www.icc-cpi.int/sites/default/files/2022-05/ICC%20AI%202007%20001%20%28ENG%29%20-%20ICC%20INFORMATION%20PROTECTION%20POLICY.PDF. Acesso em: 05 ago. 2024.
[242] INTERNATIONAL CRIMINAL COURT. Regulations of the Registry. Disponível em: https://www.icc-cpi.int/sites/default/files/RegulationsRegistryEng.pdf. Acesso em: 05 ago. 2024.

"confidencial" e, portanto, será tratado como "público"[243]. No caso Procurador *vs*. Laurent Gbagbo e Charles Blé Goudé[244], a falta de marcação adequada de registros judiciais levou a riscos de divulgação irresponsável das declarações das testemunhas, o que levou o Tribunal a confirmar a confidencialidade das informações e orientar o Procurador a adotar medidas mais seguras e em conformidade com as instruções normativas aplicáveis[245].

Não obstante a orientação do Tribunal, nada foi feito para readequar as práticas do Gabinete do Procurador quanto à marcação dos registros judiciais[246], tampouco para ao menos harmonizar as regulações internas do TPI. De fato, existem normas sobre proteção de dados espalhadas em outros documentos regulatórios do Tribunal, mas não uma política interna única e concentrada. Segundo as Regras de Procedimento e Prova[247], o Secretário do Tribunal é responsável por manter um banco de dados com todas as informações detalhadas de cada caso apresentado ao Tribunal, cujo acesso será público e disponível nos idiomas oficiais. Porém, essas informações podem ser restritas se um juiz ordenar que certos documentos ou dados não sejam divulgados, especialmente para proteger dados pessoais sensíveis[248].

Ainda, conforme os Regulamentos do Registro[249], o Registro deve manter um banco de dados eletrônico seguro para armazenar e processar as informações fornecidas em solicitações feitas por vítimas, além de qualquer documentação ou informações adicionais enviadas por elas ou por seus representantes legais. O banco de dados também armazenará comunicações recebidas das vítimas ou relacionadas a elas, incluindo informações específicas disponibilizadas ao Registro por outros órgãos do Tribunal. Somente funcionários designados do Registro e, quando necessário, a Câmara e os participantes do processo podem acessar as informações

---

[243] LAUCCI, C. The Wider Policy Framework of Ethical Behaviour: Outspoken Observations from a True Friend of the International Criminal Court. In: BERGSMO, M.; DITTRICH, V. (Ed.). Integrity in International Justice. Brussels: Torkel Opsahl Academic EPublisher, 2020. p. 871. Disponível em: https://www.legal-tools.org/doc/rz9zv6/pdf. Acesso em: 05 ago. 2024.
[244] INTERNATIONAL CRIMINAL COURT. ICC-02/11-01/15. Disponível em: https://www.legal-tools.org/doc/4dc909/pdf/. Acesso em: 05 ago. 2024.
[245] *Ibid*.
[246] LAUCCI, C., *op. cit.*, p. 872.
[247] INTERNATIONAL CRIMINAL COURT. Rules of Procedure and Evidence. 2013. Disponível em: https://www.icc-cpi.int/sites/default/files/RulesProcedureEvidenceEng.pdf. Acesso em: 06 ago. 2024.
[248] Regra 15 de Procedimento e Prova.
[249] INTERNATIONAL CRIMINAL COURT, *op. cit*. (nota de rodapé 242).

contidas nesse banco[250]. Por sua vez, o Manual de Práticas da Câmara do TPI[251] criou um Protocolo sobre o Manuseio de Informações Confidenciais e proibiu a todos os envolvidos a divulgação a terceiros de qualquer documento ou informação confidencial, criando exceções às atividades investigativas realizadas por uma parte ou participante ou à divulgação para a preparação ou apresentação do seu caso. Por fim, o Código de Conduta para membros do Tribunal cita expressamente que as condutas que resultem em violações à Instrução Administrativa ICC/AI/2007/001 podem incorrer em medidas disciplinares em face dos responsáveis[252].

3.4.3. Regras internas do TJUE

O TJUE, ao lidar com o tratamento de dados pessoais em suas funções não jurisdicionais, como o registro de dados de funcionários ou gestão de processos internos, adota como base o RGPD[253]. Tais operações são monitoradas pelo Delegado para a Proteção de Dados (referido EPD no RGPD), que é responsável pela criação e manutenção de um registro central das atividades de tratamento, que inclui informações detalhadas sobre a finalidade do processamento, os responsáveis, os destinatários e a duração da retenção de dados[254]. Além disso, as pessoas cujos dados são tratados têm o direito de acessar, corrigir, apagar ou limitar o uso de seus dados, conforme previsto no Regulamento europeu. Porém, o TJUE pode restringir esses direitos em certas situações excepcionais, dentre elas, investigações internas, colaborações com outras instituições da União ou quando o Tribunal participa de processos judiciais.

O controle sobre o tratamento de dados pessoais no TJUE é realizado internamente pelo Delegado, que está disponível para responder a questões sobre como os dados são tratados nas atividades não jurisdicionais da instituição. As pessoas que desejam exercer seus direitos ou obter esclarecimentos podem entrar

---

[250] Regulamento 98 do Registro.
[251] INTERNATIONAL CRIMINAL COURT. Chambers Practice Manual. 2023. Disponível em: https://www.icc-cpi.int/sites/default/files/2023-07/230707-chambers-manual-eng.pdf. Acesso em: 07 ago. 2024.
[252] Seção 5.3(m) do Código de Conduta. INTERNATIONAL CRIMINAL COURT. Code of Conduct for Staff Members. 2012. Disponível em: https://www.icc-cpi.int/sites/default/files/Vademecum/OT1036136_ICC%20AI%202011%20002%20%28ENG%29%20-%20CODE%20OF%20CONDUCT%20OF%20STAFF%20MEMBERS.PDF. Acesso em: 07 ago. 2024.
[253] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, *op. cit.* (nota de rodapé 182).
[254] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Registo central das atividades de tratamento. Disponível em: https://curia.europa.eu/jcms/jcms/p1_3301336/pt/. Acesso em: 13 set. 2024.

em contato com ele, utilizando um formulário específico que facilita a comunicação sobre questões relacionadas ao tratamento de seus dados[255]. Já a fiscalização externa é feita pela AEPD, à qual qualquer pessoa pode recorrer caso acredite que o tratamento de seus dados não está em conformidade com o RGPD. No entanto, como mencionado anteriormente, essa autoridade não tem competência para supervisionar o tratamento de dados realizados no âmbito das funções jurisdicionais do TJUE, restringindo-se apenas às atividades administrativas da instituição.

Paralelamente, nas funções jurisdicionais, o Tribunal de Justiça segue suas próprias regras específicas para o tratamento de dados pessoais, conforme estipulado em seu Regulamento de Processo[256]. Se o órgão jurisdicional de reenvio emitiu decisões com anonimização de pedidos de decisão prejudicial ou omissão de dados pessoais, tanto de pessoas quanto de entidades envolvidas em litígios, o Tribunal deverá manter o mesmo sigilo[257]. Além disso, pode, de ofício ou a pedido das partes, adotar as medidas de anonimização, aplicando o mesmo procedimento em casos de recurso de decisões do Tribunal Geral[258]. Quando uma parte de um processo no Tribunal de Justiça desejar que seus dados pessoais não sejam divulgados em publicações judiciais, ela pode solicitar anonimato junto ao Tribunal. Contudo, esse pedido deve ser feito o quanto antes, pois, uma vez que o processo tenha sido publicado no Jornal Oficial da UE, pode ser mais difícil assegurar a anonimização eficaz devido às exigências tecnológicas e de informação[259]. Assim, a confidencialidade só será garantida se o pedido for apresentado de forma tempestiva.

Os pedidos referentes ao tratamento de dados pessoais nas publicações judiciais do Tribunal de Justiça, como a Coletânea de Jurisprudência, são geridos pela Secretaria. O Secretário tem até dois meses para responder a esses pedidos, e a ausência de resposta nesse período equivale a uma rejeição tácita. Em caso de indeferimento, a parte pode recorrer ao Comitê do TJUE, responsável pela supervisão do cumprimento das regras de proteção de dados. O Comitê, por sua vez, tem um

---

[255] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA, *op. cit.* (nota de rodapé 230).
[256] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Versão consolidada do Regulamento de Processo do Tribunal de Justiça de 25 de setembro de 2012. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-08/rdp-cour-pt.pdf. Acesso em: 13 set. 2024.
[257] Artigo 95 do Regulamento de Processo do Tribunal de Justiça.
[258] Artigo 195(3) do Regulamento de Processo do Tribunal de Justiça.
[259] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. A proteção de dados pessoais no âmbito das publicações relativas aos processos judiciais no Tribunal de Justiça. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-11/tra-doc-pt-div-c-0000-2015-201508723-05_00.pdf. Acesso em: 13 set. 2024.

prazo de quatro meses para decidir sobre o recurso, e a ausência de resposta dentro desse prazo confirma a decisão original do Secretário. Importa ressaltar que o Comitê só pode julgar decisões referentes ao tratamento de dados pelas quais o Secretário é diretamente responsável, sem poder interferir em decisões judiciais do Tribunal[260].

Por seu turno, o Regulamento de Processo do Tribunal Geral[261] também estabelece regras próprias sobre a proteção de dados pessoais nas instâncias judiciais. Durante o processo, o Tribunal pode omitir, por iniciativa própria ou a pedido de uma das partes, os nomes e outros dados pessoais de indivíduos envolvidos no processo, sejam eles partes ou terceiros, nos documentos acessíveis ao público[262]. Da mesma forma, é permitida a omissão de dados que não sejam pessoais, mas que possam ter uma justificativa legítima para não serem divulgados, assegurando a confidencialidade quando necessária[263]. Ademais, quando informações confidenciais são apresentadas ao Tribunal durante uma diligência de instrução, elas não poderão ser comunicadas à outra parte. Caso o Tribunal conclua que essas informações são essenciais para a decisão, uma ponderação entre a confidencialidade e o direito à proteção jurisdicional será feita, podendo o Tribunal impor compromissos específicos ou solicitar versões não confidenciais dos documentos[264]. Na situação em que uma parte pretende basear seus argumentos em informações confidenciais que, se divulgadas, poderiam prejudicar a segurança da UE ou suas relações internacionais, a parte deve apresentar essas informações separadamente[265]. Ainda, da mesma forma que o Tribunal de Justiça, o Tribunal Geral deve respeitar a anonimização ou omissão de dados decididos por um Tribunal de reenvio no âmbito de um processo prejudicial, mantendo a confidencialidade nos documentos acessíveis ao público[266].

As regras do Regulamento de Processo do Tribunal Geral foram explicadas e especificadas nas Disposições Práticas de Execução, que veio para conciliar o "princípio da publicidade e da informação do público com a proteção de dados

---

[260] *Ibid*.
[261] TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Regulamento de Processo do Tribunal Geral de 4 de março de 2015. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-08/version_consolidee_rp_pt.pdf. Acesso em: 13 set. 2024.
[262] Artigo 66 do Regulamento de Processo do Tribunal Geral.
[263] Artigo 66-A do Regulamento de Processo do Tribunal Geral.
[264] Artigo 103 do Regulamento de Processo do Tribunal Geral.
[265] Artigo 105 do Regulamento de Processo do Tribunal Geral.
[266] Artigo 201 do Regulamento de Processo do Tribunal Geral.

pessoais e com a proteção de alguns outros dados mencionados nos processos que lhe são submetidos"[267].

3.5. PRIVACIDADE VS. TRANSPARÊNCIA

A implementação de um *software* especializado e sistemas de informação permite aos órgãos judiciais melhorar a eficiência da gestão de dados nos processos de revisão judicial e expandir o acesso público aos documentos. Os registros públicos guardados por um Tribunal (doméstico e internacional) contam com os chamados dados de reputação[268] e tem caráter extremamente valioso, pois revelam situações delicadas sobre, a título de exemplo, quem cometeu crimes, ganhou ou perdeu uma ação judicial, se divorciou ou decretou falência. Por isso, tais registros são analisados por particulares e instituições públicas e privadas para, dentre outras, averiguar a capacidade de crédito de um solicitante de empréstimo, os antecedentes criminais de um candidato a emprego e a idoneidade de um futuro inquilino. Mais, os pesquisadores de dados judiciais acedem aos registros dos Tribunais para conduzir estudos acadêmicos, formular políticas públicas, analisar a eficiência do sistema judiciário e identificar tendências e padrões.

A transparência nos Tribunais presume que, em regra, os dados de reputação são públicos e, portanto, podem ser acessados por qualquer interessado. Ocorre que isso entra em conflito com a autodeterminação informativa, aquela que dá poder aos indivíduos para controlar as suas próprias informações, desde o momento até a forma de compartilhamento dos dados pessoais[269]. Por isso, há um dilema entre a privacidade e a transparência, dois princípios que, embora fundamentais, frequentemente se encontram em tensão: a privacidade é essencial para a proteção dos dados pessoais e a integridade dos indivíduos envolvidos nos processos judiciais; e a transparência, indispensável para a responsabilidade e a legitimidade das

---

[267] UNIÃO EUROPEIA. Disposições Práticas de Execução do Regulamento de Processo do Tribunal Geral. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024Q02097. Acesso em: 13 set. 2024.

[268] LOPUCKI, L. M. Court-System Transparency. Iowa Law Review, v. 94. Los Angeles: UCLA School of Law, 2007. p. 516. Disponível em: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=2117&context=facultypub. Acesso em: 10 ago. 2024.

[269] RUARO, R. L. Privacidade e Autodeterminação Informativa Obstáculos ao Estado de Vigilância? Revista Eletrônica da UFPI, v. 2, n. 1. Teresina: UFPI, 2015. Disponível em: https://revistas.ufpi.br/index.php/raj/article/download/4505/2647. Acesso em: 14 ago. 2024.

decisões judiciais, assegura que os Tribunais operem sob um adequado escrutínio público.

Na tentativa de balancear ambos os princípios, num cenário em que há a divulgação eletrônica dos registros judiciais, os Tribunais vêm adotando restrições em favor da privacidade. Em regra, se os arquivos judiciais estão disponíveis no Tribunal, assim estarão ao público. Contudo, nos casos envolvendo menores de idade, violência doméstica, previdência social e processos criminais, as autoridades judiciárias podem optar por omitir (inclusive permanentemente) os dados mais sensíveis antes da divulgação[270]. No cenário doméstico dos EUA, as Cortes federais removem quatro tipos de dados pessoais antes da divulgação das decisões, quais sejam: (i) número da segurança social, exceto os últimos quatro dígitos; (ii) números das contas bancárias, exceto os últimos quatro dígitos; (iii) datas de nascimento, exceto o ano; e (iv) nomes dos menores de idade, exceto as iniciais[271].

No cenário internacional, os Tribunais lidam quase sempre com casos que envolvem informações não só pessoais, como também sensíveis[272]. O TIJ lida exclusivamente com disputas entre Estados, o que reduz a necessidade de proteger dados sensíveis, mas não elimina completamente essa preocupação. No julgado Nicarágua *vs*. Colômbia[273], relativo a uma disputa em relação às violações da soberania das zonas marítimas da Nicarágua, o TIJ decidiu disponibilizar ao público as cópias das peças e documentos escritos pelas partes[274], com exceção de determinados anexos que foram mantidos em sigilo por razões de segurança do Estado, atendendo ao pedido da Colômbia de que os dados contidos nesses anexos eram classificados como sigilosos na sua legislação nacional.

---

[270] LOPUCKI, L. M., *op. cit.*, p. 517.

[271] US COURTS. Federal Rules of Civil Procedure. 2023. Disponível em: https://www.uscourts.gov/sites/default/files/civil_federal_rules_pamphlet_dec_1_2023.pdf. Acesso em: 07 ago. 2024.

[272] Segundo o art. 5º, incisos I e II, da LGPD do Brasil, um dado pessoal identifica uma pessoa natural, ao passo que um dado sensível está relacionado com a "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

[273] INTERNATIONAL COURT OF JUSTICE. Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua V. Colombia). 2022. Disponível em: https://jusmundi.com/en/document/pdf/decision/en-alleged-violations-of-sovereign-rights-and-maritime-spaces-in-the-caribbean-sea-nicaragua-v-colombia-judgment-thursday-21st-april-2022. Acesso em: 06 ago. 2024.

[274] Artigo 53 das regras da TIJ.

No caso do TPI, o Estatuto de Roma estabelece diretrizes para a proteção de vítimas e testemunhas, prevendo que o Tribunal deve tomar medidas apropriadas para proteger a segurança, a dignidade e a privacidade, considerando fatores como idade, sexo e condições de saúde, especialmente em casos de violência sexual ou contra crianças[275]. As audiências podem ser realizadas a portas fechadas ou por meios eletrônicos[276] e as vítimas podem expressar suas preocupações durante o processo, desde que não haja prejuízo aos direitos do arguido[277]. O Tribunal ainda pode permitir que as provas sejam resumidas, ao invés de apresentadas na íntegra[278]. Ademais, os Estados podem solicitar proteção para seus funcionários e para suas informações confidenciais[279].

Um exemplo notável em que o TPI implementou medidas rigorosas para proteger a identidade das vítimas e testemunhas é o caso Procurador *vs.* Thomas Lubanga Dyilo, cuja acusação era o recrutamento de crianças para atuarem como soldados na República Federativa do Congo. O Tribunal permitiu a participação anônima na audiência inicial, sob o fundamento de que a segurança em algumas áreas do Congo estava comprometida e isso dificultava a proteção das vítimas e testemunhas nessas regiões[280]. A defesa se opôs ao anonimato, argumentando que o acusado tinha o direito de saber quem estava trazendo as acusações contra ele e buscando compensação[281]. Para resolver o embate, a Corte decidiu que o anonimato seria concedido, mas com limites à participação das partes anônimas no processo, que só poderiam acessar documentos e compareceram presencialmente nas audiências públicas. As vítimas que concordaram com a divulgação das suas identidades teriam maior participação nos atos processuais. Dessa forma, o Tribunal não considera o anonimato uma prática ideal ou preferível, mas tampouco descarta completamente sua adoção em situações específicas.

---

[275] Artigo 68(1) do Estatuto de Roma.
[276] Artigo 68(2) do Estatuto de Roma.
[277] Artigo 68(3) do Estatuto de Roma.
[278] Artigo 68(5) do Estatuto de Roma.
[279] Artigo 68(3) do Estatuto de Roma.
[280] INTERNATIONAL CRIMINAL COURT. Situation in the Democratic Republic of the Congo in the Case of the Prosecutor v. Thomas Lubanga Dyilo. Decision on the Arrangements for Participation of Victims a/0001/06, a/0002/06 and a/0003/06 at the Confirmation Hearing. Disponível em: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2006_03267.PDF . Acesso em: 08 ago. 2024.
[281] INTERNATIONAL CRIMINAL COURT. Situation in the Democratic Republic of the Congo in the Case of the Prosecutor v. Thomas Lubanga Dyilo. Defence Observations Relative to the Proceedings and Manner of Participation of Victims a/0001/06 to a/0003/06. Disponível em: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2006_03069.PDF. Acesso em: 08 ago. 2024.

Além do anonimato, a remoção de informações pessoais antes da divulgação dos registros judiciais também é defendida como uma medida para proteger a privacidade das partes num processo. Todavia, a prática pode comprometer a transparência de um determinado Tribunal, na medida em que impõe limites às pesquisas analíticas e estatísticas realizadas com base nos padrões e resultados das decisões judiciais. Os registros sem identificação dificultam a validação dos dados, impedem a vinculação de registros judiciais a outros bancos de dados e impossibilitam a correspondência de identidades nos próprios dados do Tribunal. Além disso, a abertura das Cortes ao público e à imprensa – isso especificamente em contextos domésticos – reduz a eficácia da remoção dos dados pessoais, já que tais informações serão provavelmente reveladas durante as audiências públicas[282].

Portanto, a privacidade não deve ser mantida em detrimento da transparência: há de existir um equilíbrio entre os dois princípios. Os dados de processos judiciais são cruciais para entender os resultados do sistema judiciário, assim que os registros devem ser públicos para promover a justiça. Ao mesmo tempo, a disponibilização ética e inteligente desses dados, com omissões ou remoções para proteger a privacidade, pode igualar o acesso à informação pública.

[282] LOPUCKI, L. M., *op. cit.*, p. 518-521.

4. RESPONSABILIZAÇÃO DAS ORGANIZAÇÕES E TRIBUNAIS INTERNACIONAIS POR VIOLAÇÕES À PROTEÇÃO DE DADOS PESSOAIS

A questão da responsabilização por violações à proteção de dados pessoais apresenta desafios jurídicos únicos no contexto do Direito Internacional. Como resultado da inexistência de um instrumento legal internacional vinculativo às OIs, bem como, da aplicação limitada das leis domésticas devido às imunidades e privilégios, as organizações permanecem à mercê de regulações internas, sem sujeição à jurisdição das normas externas estabelecidas pela comunidade internacional ou pelos governos nacionais. Nesse contexto, quando ocorre uma violação da proteção de dados pessoais pelas OIs, as vítimas deveriam ter assegurado o direito a algum tipo de compensação ou reparação adequada. No entanto, há obstáculos significativos nessas situações, especialmente quando essas entidades invocam suas imunidades para evitar a responsabilização ou carecem de mecanismos internos para resolução de disputas.

O presente capítulo pretende explorar a responsabilidade internacional e o alcance do direito à proteção de dados no contexto do Direito Internacional, abordando os desafios específicos diante das imunidades e privilégios que as OIs possuem. Em seguida, o capítulo fará uma análise de casos práticos em que ocorreram violações da proteção de dados por parte de organizações, examinando se houve responsabilização ou, pelo menos, aprimoramento da segurança cibernética. Por fim, serão propostas medidas para fortalecer os mecanismos de responsabilização das OIs, incluindo uma análise da noção de *accountability*, da viabilidade de criar órgãos de supervisão independentes e das alternativas para garantir a reparação na seara administrativa.

4.1. NOÇÃO DE RESPONSABILIDADE INTERNACIONAL

O conceito de responsabilidade internacional se relaciona com a personalidade jurídica das OIs[283]. No passado, acreditava-se que apenas os Estados eram dotados de personalidade jurídica internacional, mas com o surgimento e a expansão das OIs, essas entidades também passaram a ser caracterizadas da

[283] Sobre os pressupostos da responsabilidade internacional, ver BAPTISTA, E. C. Direito Internacional Público: Sujeitos e Responsabilidade. Coimbra: Almedina, 2004. p. 478-479.

mesma forma, o que significa que elas têm a capacidade de fazer reivindicações internacionais e são responsáveis por seus atos ilícitos. O TIJ confirmou esse entendimento na sua opinião consultiva em 1949 sobre Reparações por Danos Sofridos no Serviço das Nações Unidas[284], estabelecendo que organizações como a ONU podem reivindicar e proteger seus direitos internacionalmente.

A responsabilidade internacional decorre da violação de uma obrigação legal internacional – seja por ação, seja por omissão – por Estados ou OIs a eles atribuída[285]. O desenvolvimento e a codificação das normas neste contexto são atribuídos principalmente à Comissão de Direito Internacional (CDI)[286] criada pela Assembleia Geral da ONU. Os Artigos sobre a Responsabilidade das OIs[287], elaboradas pela CDI, estabelecem que qualquer violação de uma obrigação internacional pode resultar em responsabilidade, exigindo reparação completa às vítimas e servindo como um desincentivo para condutas impróprias. Para que a responsabilidade seja atribuída, além da violação de uma obrigação internacional, a conduta não pode ser justificável por circunstâncias que excluam a ilicitude, tampouco será baseada em conceitos subjetivos como dano ou culpa, mas sim em uma violação clara de normas do Direito Internacional. Ou seja, é objetiva e independe do nexo causal entre o ato ilícito e o dano causado[288].

Para compreender isso, é essencial diferenciar dois conceitos-chave: atribuição de conduta e atribuição de responsabilidade. A atribuição de conduta refere-se ao fato de que, como Estados e OIs não podem agir por conta própria, suas ações ou omissões são realizadas por outros atores (como órgãos ou agentes) e, então, atribuídas ao Estado ou à OI em questão. Quando um Estado ou uma OI comete uma violação legal por meio de seus órgãos, isso gera responsabilidade internacional. Essa

---

[284] INTERNATIONAL COURT OF JUSTICE. Advisory opinion on the Reparation for Injuries Suffered in the Service of the United Nations. Disponível em: https://www.icj-cij.org/case/4. Acesso em: 20 ago. 2024.

[285] MOHAY, Á. et al. The Articles on the Responsibility of International Organisations – Still Up in the Air after More Than a Decade? Pécs Journal of International and European Law, 2023/I-II. Pécs: University of Pécs, 2023. pp. 17. Disponível em: https://www.researchgate.net/publication/376254094_The_Articles_on_the_Responsibility_of_International_Organisations_-_Still_Up_in_the_Air_after_More_Than_a_Decade. Acesso em: 20 ago. 2024.

[286] LEGAL UN. International Law Comission. Disponível em: https://legal.un.org/ilc/. Acesso em: 20 ago. 2024.

[287] LEGAL UN. Draft articles on the responsibility of international organizations. 2011. Disponível em: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf. Acesso em: 20 ago. 2024.

[288] SAMARA, C. International Responsibility of International Organizations (The Draft Articles of the International Law Commission). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3480061. Acesso em: 21 ago. 2024.

responsabilidade é direta, pois a conduta realizada pelos agentes é imputada ao Estado ou à OI que eles representam[289]. Por outro lado, a atribuição de responsabilidade vai além da conduta e contempla não somente atos ou omissões próprios da OI, como também condutas ilícitas de outros Estados ou OIs, nas quais tenha exercido influência ou controle, por meio de ações como auxílio, assistência, direção ou coerção[290].

Num cenário em que as OIs utilizam tecnologias para aprimoramento de suas funções, pode-se pensar sobre a aplicabilidade dessas normas nas situações em que as decisões e ações são tomadas por sistemas autônomos habilitados por IA, sem intervenção humana direta. Nesse cenário, os Artigos reconhecem que as OIs podem atuar não apenas por meio de seres humanos, mas também por meio de outros "agentes", cujo termo foi definido de forma ampla pelo TIJ e, no contexto dos Artigos da CDI, refere-se a qualquer pessoa, entidade ou coisa que esteja encarregada de realizar ou ajudar a realizar as funções de uma organização. A definição ampla de "agente" pode ser estendida para incluir equipamentos de IA e permitir a atribuição de suas ações diretamente à OI, o que implica que as organizações não poderiam evitar a responsabilidade por erros ou violações de direitos fundamentais simplesmente por que as ações foram cometidas por máquinas ou sistemas autônomos[291].

Assim, não haveria óbice legal para que as OIs sejam responsabilizadas por violações cometidas por suas ferramentas de IA, mesmo sem intervenção humana. Sem embargo, surgem outros desafios nesse contexto, em particular a falta de amplo reconhecimento do direito à proteção de dados como uma obrigação legal internacional, os privilégios e imunidades concedidos às OIs e os limites dos mecanismos alternativos de resolução de disputas.

4.1.1. Desafios da proteção de dados como obrigação legal internacional

Sendo a responsabilidade internacional decorrente do descumprimento de uma obrigação legal internacional, podemos pensar se essa lógica se aplica da mesma forma em casos de violação das normas de proteção de dados.

---

[289] *Ibid*.
[290] *Ibid*.
[291] PACHOLSKA, M. Many Hands in The Black Box: Artificial Intelligence and the Responsibility of International Organizations. Hague: T.M.C. Asser Institute, 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4501072. Acesso em: 12 set. 2024.

No caso dos Estados, as regras do Direito Internacional consuetudinário sobre responsabilidade podem se aplicar às atividades cibernéticas. Isso fica evidente nas declarações de diversos Estados[292] após a criação do mandato do Grupo de Peritos Governamentais sobre o Comportamento Responsável dos Estados no Ciberespaço no contexto da segurança internacional, conforme a resolução 73/266A da Assembleia Geral da ONU[293]. O entendimento geral é que, quando um Estado é alvo de uma atividade cibernética que constitui um ato internacionalmente ilícito, ele pode invocar a responsabilidade jurídica internacional do Estado responsável, inclusive se o ato for realizado por órgãos do Estado, por pessoas ou entidades com autoridade para exercer funções governamentais em nome do Estado, ou por agentes que atuem sob instruções, direção ou controle do Estado; ou ainda, quando o Estado reconhece e adota o ato como seu. Além disso, os Estados podem ser internacionalmente responsáveis por auxiliar ou assistir atividades cibernéticas ilícitas conduzidas por outro Estado.

No entanto, a situação é diferente para as OIs. Apesar de adotarem políticas de proteção de dados, o fizeram como uma prática recomendada ou em resposta a demandas de mercado ou reputacionais e não por reconhecerem uma obrigação legal internacional[294]. Por exemplo, o CICV não se considera obrigado pelas normas legais internas em relação à proteção de dados, tratando-as como voluntárias e não

---

[292] AUSTRIA. Cyber activities and international law: Austrian position paper. Disponível em: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf. Acesso em: 21 ago. 2024; NEW ZEALAND. The application of international law to state activity in cyberspace. Wellington: Department of the Prime Minister and Cabinet, 2020. Disponível em: https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf. Acesso em: 21 ago. 2024; UNITED KINGDOM. The application of international law to states' conduct in cyberspace: UK statement. London: Her Majesty's Government, 2021. Disponível em: https://assets.publishing.service.gov.uk/media/60b775388fa8f54899011dec/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf. Acesso em: 21 ago. 2024; CANADA. The application of international law in cyberspace. Ottawa: Global Affairs Canada, 2022. Disponível em: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a6. Acesso em: 21 ago. 2024.

[293] UNITED NATIONS GENERAL ASSEMBLY. Resolution 73/266 adopted by the General Assembly on 22 December 2018. Advancing responsible State behaviour in cyberspace in the context of international security. Disponível em: https://documents.un.org/doc/undoc/gen/n18/465/01/pdf/n1846501.pdf. Acesso em: 21 ago. 2024.

[294] LUBIN, A. Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study. In: BUCHAN, R.; LUBIN, A. The Rights to Privacy and Data Protection in Times of Armed Conflict. Tallinn: CCDCOE, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4115810. Acesso em: 21 ago. 2024.

vinculativas, refletindo apenas "melhores práticas reconhecidas". Essa postura levanta questões sobre até que ponto a proteção de dados pode ser considerada um direito humano refletido no Direito Internacional consuetudinário e se as obrigações derivadas desse direito poderiam se estender a atores não estatais, como as OIs. Conquanto seja possível que, com o tempo, a proteção de dados se torne uma obrigação de caráter consuetudinário, aplicar esse direito às OIs ainda é difícil, especialmente considerando que as organizações raramente são partes formais de tratados de direitos humanos, tampouco o são de convenções internacionais sobre proteção de dados.

Um outro exemplo ilustrativo é o da Organização Internacional para as Migrações (OIM), que em 2020 resumiu e simplificou suas políticas de responsabilidade por meio de um novo quadro de Responsabilidade para com as Populações Atingidas[295]. Mesmo sendo baseado em princípios como “não discriminação”, "não causar danos" e "tolerância zero para abuso sexual e exploração", em nenhum momento o documento afirma que a OIM respeitará instrumentos legais internacionais específicos. Inclusive com relação à proteção de dados, as normas internas de responsabilização expressamente mencionam as boas práticas estabelecidas nos Princípios de Proteção de Dados da OIM e da ONU[296].

Destarte, apesar da sua crescente relevância, a proteção de dados ainda não é reconhecida como uma obrigação legal internacional pelas OIs, o que dificulta a responsabilização em casos de violações, mormente num contexto em que as normas aplicáveis são mais voluntárias do que vinculativas.

4.1.2. Desafios diante da imunidade jurisdicional das OIs

Os privilégios das OIs, com particular relevância a imunidade de jurisdição, frequentemente entram em tensão com o direito de acesso à justiça, garantido por instrumentos internacionais de direitos humanos como a DUDH e o PIDCP. A rejeição do litígio impossibilita a reparação judicial em favor dos indivíduos que sofreram danos causados por essas organizações.

---

[295] INTERNATIONAL ORGANIZATION FOR MIGRATION. IOM framework for addressing accountability to affected populations. Disponível em: https://publications.iom.int/system/files/pdf/iom-aap-framework.pdf. Acesso em: 21 ago. 2024.

[296] INTERNATIONAL ORGANIZATION FOR MIGRATION. Data protection. Disponível em: https://www.iom.int/data-protection. Acesso em: 21 ago. 2024.

Nesse cenário, é possível questionar se a imunidade jurisdicional das OIs deve ser condicionada à disponibilidade de mecanismos alternativos para resolução de disputas. Alguns instrumentos legais, como a Convenção sobre Privilégios e Imunidades das Nações Unidas e a Convenção sobre Privilégios e Imunidades das Agências Especializadas da ONU, exigem que as organizações ofereçam uma forma alternativa ou apropriada para resolver disputas de natureza contratual ou privada. De acordo com um relatório do Secretário-Geral da ONU[297], a prática da organização é incluir uma cláusula padrão em seus contratos comerciais, que estabelece a arbitragem como método de resolução de disputas não solucionadas por negociação direta, preservando ao mesmo tempo seus privilégios e imunidades. A ideia é que as imunidades e privilégios não prejudiquem o compromisso da organização com a arbitragem: a ONU concorda em aceitar a decisão arbitral como a adjudicação final, mas mantém sua proteção contra processos judiciais, a menos que haja uma renúncia expressa da imunidade.

O relatório também descreve como a ONU lida com outros tipos de disputas privadas. Para reclamações de lesões pessoais ou danos a propriedade ocorridos dentro do distrito da sede em Nova Iorque, a organização tem regulamentos especiais para limitar o valor das compensações; em outros locais, as disputas são resolvidas por negociação amigável ou arbitragem. Enquanto isso, os acidentes envolvendo veículos operados pela ONU são cobertos por um seguro comercial global. Para reivindicações de compensação relacionadas a operações de manutenção da paz, a ONU celebra Acordo do *Status* das Forças (SOFA) com os países anfitriões, que preveem a criação de uma comissão de reclamações permanente. Além disso, a ONU disponibiliza mecanismos internos de resolução de disputas para funcionários que apresentam reclamações relacionadas a suas condições de emprego.

O TIJ abordou a questão no caso Georges *vs*. Nações Unidas[298], no qual a Corte de Apelações dos EUA questionou se o cumprimento pela ONU da sua obrigação prevista na Seção 29 da sua Convenção sobre Privilégios e Imunidades é uma condição para gozar dos privilégios, ou seja, se a falha em prover mecanismos alternativos afeta sua imunidade jurisdicional. O Tribunal decidiu que não e aplicou o

[297] UNITED NATIONS. Report of the 5th Committee. Disponível em: https://digitallibrary.un.org/record/202035?ln=fr&v=pdf. Acesso em: 16 set. 2024.
[298] UNITED STATES COURT OF APPEALS. Georges v. United Nations. Disponível em: https://cases.justia.com/federal/appellate-courts/ca2/15-455/15-455-2016-08-18.pdf?ts=1471554006. Acesso em: 16 set. 2024.

princípio de que a menção explícita de uma exceção, como a renúncia expressa à imunidade, implica a exclusão de outras condições, como a falha em fornecer mecanismos de resolução. Portanto, a ausência de um mecanismo alternativo de resolução de disputas não afeta a imunidade da ONU, pois tal condição não está expressamente prevista nas seções da Convenção.

Ainda que existam meios alternativos de resolução de disputas, um Tribunal pode rejeitar a imunidade de jurisdição. Isso acontece se a OI demandada oferece um mecanismo interno que não seja independente ou imparcial[299]. Na maioria dos casos, a imunidade foi assegurada pelos Tribunais em litígios trabalhistas contra OIs que instalaram seus próprios Tribunais administrativos para resolução desse tipo específico de caso[300]. A ONU, por exemplo, estabeleceu o seu Tribunal Administrativo em 1950 por meio da Resolução 351 A (IV) da Assembleia Geral[301], cuja jurisdição abrange disputas trabalhistas entre as Nações Unidas e o seu pessoal. Em 2009, o sistema interno jurisdicional da ONU foi reformado e passou a ter duas instâncias: a primeira no Tribunal de Disputas (UNDT) e a segunda no Tribunal de Apelações das Nações Unidas (UNAT)[302]. É interessante notar que outras OIs, como a Organização Internacional de Aviação Civil e a Organização Marítima Internacional, acolheram a jurisdição dos Tribunais internos da ONU para resolver disputas trabalhistas com seus funcionários[303].

Entretanto, o mesmo mecanismo interno para resolução de disputas não está disponível na ONU para os conflitos relativos à proteção de dados pessoais e, apesar disso, a organização ainda defende sua imunidade de jurisdição nesses casos. Os dados digitais da ONU são considerados "bens e ativos" e, como tal, estão protegidos por imunidade contra qualquer forma de interferência, incluindo a judicial. Nesse sentido, o Conselheiro Jurídico da ONU destacou que a imunidade legal também inclui a inviolabilidade absoluta dos arquivos e documentos da ONU, independentemente

---

[299] OKEKE, E. C., *op. cit.* (nota de rodapé 166).
[300] REINISCH, A. The Immunity of International Organizations and the Jurisdiction of their Administrative Tribunals. Oxford: Oxford University Press, 2008. Disponível em: https://deicl.univie.ac.at/fileadmin/user_upload/i_deicl/VR/VR_Personal/Reinisch/Publikationen/TheImmunityIOs_2008.pdf. Acesso em: 12 set. 2024.
[301] UNITED NATIONS. Resolution 351 A (iv) of 24 November 1949 - Establishment of a United Nations Administrative Tribunal. Disponível em: https://digitallibrary.un.org/record/666782?v=pdf. Acesso em: 13 set. 2024.
[302] UNITED NATIONS GENERAL ASSEMBLY. Resolution A/RES/63/253 - Administration of justice at the United Nations. Disponível em: https://documents.un.org/doc/undoc/gen/n08/485/97/pdf/n0848597.pdf. Acesso em: 15 set. 2024.
[303] OKEKE, E. C., *op. cit.* (nota de rodapé 166).

de onde ou como são armazenados, seja em servidores físicos, seja em serviços de nuvem[304].

A Organização Internacional de Polícia Criminal (INTERPOL), por sua vez, é um exemplo que lida de maneira mais eficaz as reivindicações não contratuais relacionadas às suas operações no contexto da proteção de dados pessoais. À medida que a tecnologia avançava e a INTERPOL se tornava mais eficiente, surgiram pressões para que a organização oferecesse mecanismos de reparação para indivíduos afetados por suas ações. Em resposta a essa necessidade e também em reação à tentativa da autoridade francesa de proteção de dados (*Commission Nationale de l'Informatique et des Libertés* - CNIL) de exercer jurisdição sobre os arquivos da INTERPOL, a organização estabeleceu a Comissão para o Controle dos Arquivos da INTERPOL (CCF). A França argumentava que os indivíduos deveriam ter acesso aos dados que lhes dizem respeito, conforme previsto pela sua legislação de proteção de dados de 1978, que dava à CNIL o poder de controlar arquivos computadorizados no país. A INTERPOL contrapôs, afirmando que a lei francesa não poderia ser aplicada às informações policiais processadas por seu secretariado geral, pois os dados enviados pelos países membros não pertenciam à INTERPOL, que atuava apenas como depositária[305]. Para reconciliar esses objetivos conflitantes, ambas as partes concordaram em criar a CCF, uma comissão destinada a garantir que os direitos individuais fossem protegidos enquanto se preservava o funcionamento eficaz da cooperação policial internacional[306].

Em 1993, um Tribunal doméstico francês (*Tribunal de Grande Instance de Lyon*) julgou o caso Balkir *vs*. INTERPOL, no qual o reclamante, um refugiado e opositor do regime turco, buscava anular um mandado de prisão internacional registrado nos arquivos da organização. A INTERPOL argumentou que o Tribunal francês não tinha competência para julgar o caso, alegando que não é uma ONG sujeita à lei francesa de associações, mas sim uma entidade com personalidade

---

[304] UNITED NATIONS. Letter to the Chair of the EDPB with attached Comments of the United Nations to Guidelines 2/2020. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf. Acesso em: 02 set. 2024.

[305] MARTHA, R. S. J. Challenging Acts of INTERPOL in Domestic Courts. In: REINISCH, A (Ed.) Challenging Acts of International Organizations Before National Courts. Oxford: Oxford University Press, 2010. p. 231-234.

[306] INTERPOL. Commission for the Control of INTERPOL's Files (CCF). Disponível em: https://www.interpol.int/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF. Acesso em: 16 set. 2024.

jurídica internacional, reconhecida pela França e por outros países. O Tribunal concordou com a INTERPOL, afirmando que, por não ter sido criada por leis nacionais e possuir personalidade jurídica supranacional, a OI não está sujeita às leis e Tribunais nacionais. Assim, a decisão reafirmou que, devido à sua natureza intergovernamental e ao acordo de sede entre a França e a INTERPOL, os Tribunais nacionais não têm jurisdição sobre as atividades da INTERPOL, que possui um sistema interno de controle de informações policiais que está além da aplicação das leis domésticas[307].

Em suma, o direito de acesso aos Tribunais judiciais é constantemente limitado pela imunidade jurisdicional das OIs, especialmente se as organizações dispõem de um meio alternativo de resolução de disputas. As demandas contra OIs podem ser submetidas a Tribunais administrativos internos, mas que têm uma jurisdição restrita às questões trabalhistas.

4.1.3. Desafios diante da jurisdição limitada dos Tribunais administrativos

Os Tribunais administrativos internacionais são criados para resolver disputas entre funcionários e as OIs que os empregam. A necessidade de criação de um sistema interno de justiça decorre justamente da proteção conferida às organizações contra a jurisdição dos Tribunais nacionais. Desse modo, os Tribunais administrativos garantem que os funcionários dessas OIs tenham um fórum onde possam recorrer em caso de disputas trabalhistas, como questões salariais, condições de trabalho, promoções e rescisões[308]. As fontes do Direito Administrativo Internacional, que regem os Tribunais administrativos, incluem os estatutos das próprias OIs, contratos de trabalho, decisões dos órgãos legislativos da organização (como as resoluções da Assembleia Geral da ONU) e regulamentos internos[309]. Em termos de jurisdição, os Tribunais são limitados a disputas trabalhistas entre as organizações e seu pessoal[310].

---

[307] MARTHA, R. S. J. International Financial Institutions and Claims of Private Parties - Immunity Obliges. In: CISSÉ, H. et al. International Financial Institutions and Global Legal Governance. Washington: World Bank, 2012. Disponível em: https://www.iilj.org/wp-content/uploads/2016/08/Kingsbury-et-al_International-Financial-Institutions-and-Global-Legal-Governance.pdf. Acesso em: 14 set. 2024.
[308] AMERANSINGHE, C. F. International Administrative Tribunals. In: ROMANO, C. et al. The Oxford Handbook of International Adjudication. Oxford: Oxford University Press, 2013.
[309] *Ibid*.
[310] *Ibid*.

Os remédios reparatórios disponíveis geralmente incluem a anulação de decisões administrativas[311] e compensações financeiras[312].

O Tribunal Administrativo da Organização Internacional do Trabalho (ILOAT)[313], embora não tenha sido criado especificamente para julgar casos de violação de proteção de dados, tem sido um fórum aberto a esses tipos de disputas quando o descumprimento ocorre na relação laboral. O ILOAT, cuja jurisdição foi aceita por mais de 50 OIs[314], com destaque para o CICV, a UNESCO, a Organização das Nações Unidas para o Desenvolvimento Industrial (UNIDO), a INTERPOL, a OIM e o TPI, é um exemplo de Tribunal administrativo que já aceitou casos envolvendo a gestão inadequada de dados pessoais de funcionários. Apesar de sua jurisdição estar formalmente limitada a disputas trabalhistas, essas OIs podem ser submetidas a litígios administrativos que envolvem o tratamento inadequado de informações pessoais, se tal questão afeta os direitos dos funcionários no contexto da relação de trabalho.

Um exemplo relevante é o Julgamento nº 3338 da 118ª Sessão do ILOAT[315], envolvendo um funcionário do Instituto Europeu de Patentes (IEP). O reclamante contestou a decisão unilateral do IEP de encaminhar suas informações pessoais ao Ministério das Relações Exteriores dos Países Baixos sem seu consentimento, em relação à sua condição de residente permanente após a perda de sua nacionalidade holandesa. O Tribunal reconheceu que houve uma violação dos requisitos de proteção de dados, pois as informações pessoais do funcionário foram compartilhadas sem o prévio consentimento do titular. Mesmo tendo sido fixada uma compensação ínfima de 100 euros, a decisão revela que as OIs têm obrigações perante seus funcionários e o tratamento dos respectivos dados pessoais e, em caso de descumprimento das

311 COUNCIL OF EUROPE. Statute of the Administrative Tribunal. Disponível em: https://www.coe.int/en/web/Tribunal/statute. Acesso em: 17 set. 2024.
312 INTERNATIONAL LABOUR ORGANIZATION. Statute of the Administrative Tribunal of the International Labour Organization. Disponível em: https://www.ilo.org/resource/statute-administrative-Tribunal-international-labour-organization. Acesso em: 17 set. 2024.
313 INTERNATIONAL LABOUR ORGANIZATION. ILO Administrative Tribunal. Disponível em: https://www.ilo.org/ilo-administrative-Tribunal#news. Acesso em: 17 set. 2024.
314 INTERNATIONAL LABOUR ORGANIZATION. Organizations recognizing the jurisdiction. Disponível em: https://www.ilo.org/ilo-administrative-Tribunal/organizations-recognizing-jurisdiction. Acesso em: 17 set. 2024.
315 INTERNATIONAL LABOUR ORGANIZATION ADMINISTRATIVE TRIBUNAL. 118th Session - Judgment No. 3338. 2014. Disponível em: https://webapps.ilo.org/dyn/triblex/triblexmain.fullText?p_lang=en&p_judgment_no=3338&p_language_code=EN. Acesso em: 17 set. 2024.

práticas gerais da organização, poderão ser responsabilizadas na seara administrativa.

Outro caso é o Julgamento nº 2944 decidido na 109ª Sessão do ILOAT[316], envolvendo a UNESCO. A reclamante, funcionária da organização desde 1979, apresentou uma queixa alegando, entre outros pontos, que a UNESCO havia divulgado intencionalmente dados pessoais sobre ela e sua família a terceiros, incluindo autoridades do seu país de origem e outros funcionários da organização. A funcionária requereu uma compensação de 300.000 euros por conta dos danos causados pela divulgação não autorizada de suas informações pessoais. No entanto, o Tribunal concluiu que não havia evidências suficientes para demonstrar que tais divulgações ocorreram de forma indevida. Em que pese a decisão tenha sido desfavorável à reclamante, o julgado ilustra a disposição do ILOAT em analisar alegações de violação de dados pessoais, ainda que dentro da sua competência limitada a disputas trabalhistas.

Destarte, infere-se que os Tribunais administrativos têm competência restrita às demandas trabalhistas, assim que violações da proteção de dados pelas OIs – que aceitarem a jurisdição – só poderão ser julgadas (e eventualmente punidas) se ocorrerem no âmbito da relação laboral entre a organização e o funcionário, o que deixa lacunas na proteção jurídica fora do contexto empregatício.

4.2. CASOS PRÁTICOS DE VAZAMENTO DE DADOS POR OIs

Tendo em conta os desafios enfrentados para a responsabilização das OIs, interessa compreender no campo prático o tipo de violação da proteção de dados pessoais e as providências tomadas pelas organizações para lidar com os danos resultantes. O objetivo é averiguar se a autorregulamentação implementada foi suficiente para mitigar os impactos ou se houve algum tipo de responsabilização. Para tanto, serão analisados três casos específicos em que a proteção de dados de OIs foi comprometida por ataques cibernéticos ou pela divulgação inadequada de informações.

[316] INTERNATIONAL LABOUR ORGANIZATION ADMINISTRATIVE TRIBUNAL. 109th Session Judgment No. 2944. 2010. Disponível em: https://webapps.ilo.org/dyn/triblex/triblexmain.fullText?p_lang=en&p_judgment_no=2944&p_language_code=EN. Acesso em: 17 set. 2024.

4.2.1. Caso Cruz Vermelha

Em janeiro de 2022, o CICV foi alvo de um ataque cibernético devastador que expôs dados pessoais de mais de 515 mil pessoas ao redor do mundo. Entre as informações comprometidas estavam detalhes confidenciais de indivíduos em situação de vulnerabilidade, incluindo aqueles separados de suas famílias por conflitos, migração e desastres naturais, além de pessoas desaparecidas e detidas. Após o ataque, o Diretor-Geral do CICV, Robert Mardini, manifestou publicamente seu pesar pela falha em proteger adequadamente essas informações, ressaltando a gravidade do ocorrido[317]. O ataque, que teve início em novembro de 2021, explorou a vulnerabilidade dos indivíduos registrados no sistema interno de comunicação utilizado pela Cruz Vermelha, permitindo que os invasores tivessem acesso irrestrito a informações sensíveis.

Apesar da gravidade do incidente, ele não foi um caso isolado. Em janeiro de 2024, a Cruz Vermelha Italiana também foi alvo de outro ataque cibernético, no qual dados pessoais de mais de 16.500 pessoas foram roubados. As informações pertenciam a indivíduos de diferentes países que buscavam reunir-se com familiares ou estavam envolvidos em casos de rastreamento dentro do serviço de localização do CICV intitulado “Restabelecimento de Laços Familiares”. Parte dos dados, que incluíam nomes, localizações e detalhes familiares, foi divulgada online, agravando ainda mais a vulnerabilidade das pessoas contempladas pelo programa[318]. Ambos os incidentes evidenciam que a Cruz Vermelha tem se tornado um alvo frequente de cibercriminosos, principalmente devido ao manejo de dados sensíveis de indivíduos em situações de extrema vulnerabilidade, muitas vezes em conflitos armados.

Analisando os acontecimentos à luz das normas internas do CICV, fica claro que houve uma falha em garantir a segurança dos dados pessoais. De acordo com as diretrizes da organização, é imperativo que os dados sejam protegidos com um nível de segurança adequado, levando em conta “a natureza dos dados e os riscos para os

[317] INTERNATIONAL COMMITTEE OF THE RED CROSS. ICRC cyber-attack: Sharing our analysis. Disponível em: https://www.icrc.org/en/document/icrc-cyber-attack-analysis. Acesso em: 04 set. 2024.
[318] SVENSKA RÖDA KORSET. Cyberattack on the Italian Red Cross on January 18. Disponível em: https://www.rodakorset.se/en/who-we-are/pressrum/roda-korset-berattar/cyberattack-on-italian-red-cross/. Acesso em: 04 set. 2024.

titulares e para o mandato do CICV" [319]. A proteção deve abranger desde a segurança física até a cibernética, com medidas específicas para evitar acessos não autorizados. No entanto, os ataques de 2022 e 2024 mostraram que a proteção adotada pela organização é insuficiente e que o cumprimento das suas normas internas é parcial, particularmente no que respeita à segurança cibernética.

Em resposta ao primeiro ataque, o CICV disse que tomou medidas para mitigar os danos, tendo por base o que dispõe as suas regras internas. O Escritório de Proteção de Dados foi informado[320] e uma extensa operação foi lançada para notificar todas as pessoas cujas informações foram comprometidas. O processo, complexo e demorado, envolveu desde comunicações por telefone até visitas presenciais a comunidades isoladas, para garantir que todos os afetados fossem devidamente informados. Além disso, os servidores comprometidos foram imediatamente retirados do ar e, segundo as informações do CICV, relançados apenas após passarem por rigorosos testes de segurança[321]. Também houve uma intensificação da cooperação com parceiros para enfatizar a necessidade de proteger as organizações humanitárias tanto no ambiente digital quanto no físico[322].

Apesar das medidas adotadas para mitigar os danos, a repetição do ataque cibernético em 2024 levanta dúvidas quanto ao aprimoramento dos sistemas de segurança. Mesmo havendo violação das regras internas do CICV, não há informação de que houve responsabilização administrativa (muito menos judicial) em face da organização.

4.2.2. Caso UNICEF

Em agosto de 2019, a UNICEF passou por um incidente de vazamento de dados pessoais dos usuários de sua plataforma online, chamada "Agora", utilizada por funcionários, parceiros e apoiadores para treinamento sobre direitos das crianças e

[319] Artigo 21 das Regras do CICV (nota de rodapé 169).
[320] Artigo 20 das Regras do CICV (nota de rodapé 169).
[321] INTERNATIONAL COMMITTEE OF THE RED CROSS. Cyber attack on ICRC: What we know. Disponível em: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know. Acesso em: 05 set. 2024.
[322] INTERNATIONAL COMMITTEE OF THE RED CROSS. Safeguarding Humanitarian Data. Disponível em: https://rcrcconference.org/app/uploads/2022/05/16_CoD22-Safeguarding-Humanitarian-Data-Background-document-FINAL-EN.pdf. Acesso em: 05 set. 2024.

ações humanitárias[323]. Por um erro humano[324], um e-mail foi enviado a cerca de 20 mil pessoas contendo nomes, endereços de e-mail, informações profissionais e de gênero, incluindo dados como local de trabalho, tipo de contrato e nomes de supervisores de 8.254 usuários matriculados em cursos de imunização[325]. O incidente ressaltou a necessidade de treinamento do pessoal encarregado do tratamento de dados pessoais, ou que simplesmente tenha acesso a eles[326].

Recentemente, um novo incidente veio à tona, quando em abril de 2024 um invasor cibernético, identificado pelo codinome "888", alegou ter acessado dados sensíveis da UNICEF, comprometendo informações de onze países. O ataque resultou no vazamento de arquivos confidenciais e dados pessoais como nomes, endereços, números de contato e coordenadas geográficas[327]. Novamente, a situação acentua a fragilidade das organizações humanitárias perante invasões cibernéticas e a necessidade urgente de aprimoramento e investimento nos sistemas de segurança, especialmente quando considerado ao lado de outros vazamentos recentes dentro do sistema da ONU, como o da UNDP também em 2024[328].

Ao interpretar as ocorrências com base na normativa interna da UNICEF e da ONU, infere-se que, como parte do Grupo de Política de Privacidade da ONU, a UNICEF deve seguir os Princípios sobre Proteção e Privacidade de Dados Pessoais, que exigem a implementação de medidas adequadas para garantir a segurança dos dados contra acesso não autorizado, perda ou danos[329]. A política interna da UNICEF,

---

[323] CHADWICK, V. UNICEF data leak reveals personal info of 8,000 online learners. Disponível em: https://www.devex.com/news/unicef-data-leak-reveals-personal-info-of-8-000-online-learners-95558. Acesso em: 04 set. 2024.
[324] SCROXTON, A. UN agency Unicef praised for response to accidental data leak. Disponível em: https://www.computerweekly.com/news/252470581/UN-agency-Unicef-praised-for-response-to-accidental-data-leak. Acesso em: 04 set. 2024.
[325] VELTEC NETWORKS. UNICEF's Accidental Data Leak Highlights Importance of Employee Security Training. Disponível em: https://www.veltecnetworks.com/unicefs-data-leak/. Acesso em: 04 set. 2024.
[326] Segundo o Relatório Global sobre Custos por Violações de Dados de 2024 da *International Business Machines Corporation* (IBM), as falhas de TI ou erros humanos causaram quase metade de todas as violações: os ataques cometidos por invasores externos ou criminosos internos representam 55% de todas as violações; 23% correspondem a falhas de TI e 22% a erros humanos. INTERNATIONAL BUSINESS MACHINES CORPORATION. Cost of a Data Breach Report 2024. Disponível em: https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf. Acesso em: 19 set. 2024.
[327] BREACHLOCK. UNICEF Hit by Threat Actor 888 Affecting 11 Countries. Disponível em: https://www.breachlock.com/resources/advisories/unicef-hit-by-threat-actor-888-affecting-11-countries/. Acesso em: 05 set. 2024.
[328] UNITED NATIONS DEVELOPMENT PROGRAMME. UNDP Investigates Cyber-Security Incident. Disponível em: https://www.undp.org/speeches/undp-investigates-cyber-security-incident. Acesso em: 19 set. 2024.
[329] UNITED NATIONS – CEB, *op. cit.* (nota de rodapé 179).

em vigor desde 2020, também determina que a organização deve oferecer treinamentos e conscientizar seu pessoal para garantir a implementação eficaz dessas diretrizes[330]. Dado que ambos os incidentes ocorreram sob a vigência dessas normativas, é claro que houve descumprimento das regras internas, especialmente no que diz respeito à prevenção de vazamentos e à proteção contra ataques cibernéticos.

Após o primeiro incidente em 2019, a UNICEF adotou algumas medidas para mitigar os riscos, como a desativação da funcionalidade de envio de anexos pela plataforma "Agora" e a solicitação para que os destinatários excluíssem o e-mail contendo os dados pessoais. Um pedido de desculpas foi emitido e a organização afirmou que uma revisão interna seria realizada para evitar a repetição do erro. Contudo, nenhuma comunicação clara sobre a notificação de autoridades competentes foi feita e a UNICEF inclusive reafirmou a sua posição de que, como entidade da ONU, não está sujeita ao RGPD[331]. Já em relação ao segundo vazamento em 2024, até o momento não houve uma manifestação pública sobre medidas de segurança aprimoradas ou sobre ações para prevenir novos ataques[332].

Esse conjunto de incidentes revela a insuficiência da autorregulação da ONU em garantir a tomada de medidas concretas e eventual responsabilização em casos de violações de dados pessoais.

4.2.3. Caso TPI

Em setembro de 2023, o TPI divulgou que seus sistemas haviam sido alvo de um ataque cibernético, comprometendo a segurança de uma das mais importantes instituições jurídicas internacionais, responsável por julgar crimes de guerra e crimes contra a humanidade. O TPI lida com dados altamente sensíveis, incluindo provas de processos criminais e informações confidenciais de testemunhas protegidas, porém, o Tribunal não especificou publicamente quais áreas de seus sistemas foram

[330] UNICEF, *op. cit.* (nota de rodapé 180).
[331] CHADWICK, V., *op. cit.* (nota de rodapé 323).
[332] CROFT, D. UNICEF data allegedly leaked on BreachForums. Disponível em: https://www.cyberdaily.au/security/10489-unicef-data-allegedly-leaked-on-breachforums?ref=doingfedtime.com. Acesso em: 05 set. 2024.

acessadas[333]. Uma das principais especulações em torno desse incidente sugere um possível envolvimento da Rússia. A despeito da falta de confirmação oficial, o momento do ataque coincide com o mandado de prisão expedido em março de 2023 em desfavor de Vladimir Putin pelos crimes de guerra cometidos na Geórgia e na Ucrânia. O referido rumor também foi intensificado após um incidente anterior em 2022, quando um agente militar russo foi interceptado tentando se infiltrar no TPI[334].

O próprio Procurador do TPI, Karim Khan, em agosto de 2023[335], havia alertado sobre a crescente ameaça de ataques cibernéticos e o impacto que esses poderiam ter na administração da justiça internacional. Ele destacou que crimes cibernéticos, como ataques de *hackers*, podem se enquadrar na jurisdição do Tribunal, caso interfiram na administração da justiça, e ressaltou que ações como desinformação, destruição de dados, alteração ou vazamento de informações confidenciais podem constituir crimes, uma vez que estão aptos a obstruir investigações e processos em andamento. Tais práticas não apenas comprometem a segurança das informações, mas também minam a capacidade do Tribunal de cumprir seu mandato de promover justiça internacional, sendo, portanto, passíveis de investigação e eventual responsabilização penal.

A normativa interna do TPI busca essencialmente categorizar e proteger os dados conforme o nível de risco associado. Ocorre que as políticas de privacidade não tratam especificamente dos procedimentos a serem adotados em caso de ataques cibernéticos, mas sim apenas determinam que a segurança da informação deve ser garantida por meio de uma abordagem coordenada e baseada em uma avaliação contínua dos riscos. As medidas de proteção adotadas devem ser de natureza técnica, processual e física, sempre proporcionais ao risco identificado. A política enfatiza que a gestão de riscos de segurança deve estar integrada à cultura organizacional do Tribunal, permeando todas as práticas e planos da instituição[336]. Também há disposições sobre a divulgação de informações a terceiros, estabelecendo que qualquer liberação de dados que afete a privacidade dos

---

[333] STERLING, T.; BERG, S. van den. War crimes Tribunal ICC says it has been hacked. Disponível em: https://www.reuters.com/world/international-criminal-court-reports-cybersecurity-incident-2023-09-19/. Acesso em: 06 set. 2024.

[334] *Ibid.*

[335] KAHN, K. A. Technology Will Not Exceed Our Humanity. Disponível em: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/. Acesso em: 06 set. 2024.

[336] INTERNATIONAL CRIMINAL COURT, *op. cit.* (nota de rodapé 240).

funcionários deve ser aprovada pelo chefe da respectiva unidade organizacional, além do chefe da seção de recursos humanos[337].

Diante do ataque, o TPI alegou que agiu rapidamente para mitigar seus efeitos, contando com o apoio das autoridades holandesas (sede da Corte) e de especialistas externos em segurança cibernética. Na oportunidade, foi realizada uma análise forense do incidente para identificar suas causas e impactos, bem como para implementar medidas preventivas. Os primeiros indícios apontam para um ataque altamente sofisticado com o objetivo de espionagem, uma ação que pode ser interpretada como uma tentativa de minar o mandato da Corte. Caso evidências confirmem que dados específicos foram comprometidos, o TPI se comprometeu a notificar diretamente os indivíduos, organizações ou Estados afetados[338]. Na tentativa de aprimorar sua segurança digital, o TPI também criou o Fundo Especial para Segurança, uma iniciativa liderada pelo Registrador do Tribunal, que busca recursos para implementar melhorias urgentes em suas defesas cibernéticas e físicas[339].

Apesar dessas ações, o ataque ao TPI expôs uma violação clara de suas normativas internas, que exigem a proteção eficaz dos dados sob sua custódia. Ainda que tenha adotado medidas para fortalecer sua cibersegurança, o Tribunal não forneceu detalhes sobre o tipo de informação comprometida ou sobre a identidade dos responsáveis pelo ataque, o que levanta questões sobre a eficácia das respostas do TPI e sua capacidade de garantir a segurança dos dados segundo seu regramento interno. Adicionalmente, até o momento, não houve confirmação sobre a notificação dos possíveis afetados pela violação de seus dados pessoais, tampouco sobre a possibilidade de compensações pelos danos sofridos.

4.3. FORTALECIMENTO DOS MECANISMOS DE RESPONSABILIZAÇÃO

Os privilégios e imunidades, longe de serem meros benefícios, asseguram às OIs uma operação independente num cenário internacional multilateral e sujeito à

[337] INTERNATIONAL CRIMINAL COURT, *op. cit.* (nota de rodapé 241).
[338] INTERNATIONAL CRIMINAL COURT. Measures taken following the unprecedented cyber-attack on the ICC. Disponível em: https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc. Acesso em: 06 set. 2024.
[339] GOV UK. UK donation to the International Criminal Court's Special Fund for Security will help to protect the Court from future cyber-attacks. Disponível em: https://www.gov.uk/government/news/uk-donation-to-the-international-criminal-courts-special-fund-for-security-will-help-to-protect-the-court-from-future-cyber-attacks. Acesso em: 06 set. 2024.

interferência direta de Estados soberanos e suas legislações. Por isso e em particular quando existem mecanismos alternativos de resolução de disputas, comumente utilizados para demandas trabalhistas, os privilégios não deveriam ser relativizados, pois nessas situações existe um foro (idealmente) imparcial e neutro apto a pôr fim à controvérsia e, ao mesmo tempo, deixar intacta a imunidade jurisdicional de uma organização. Todavia, o problema surge quando OIs praticam ilícitos que não podem ser objeto de análise por meios alternativos, principalmente por limites de competência dos seus Tribunais administrativos, como acontece com a violação da proteção de dados.

Nesses casos, havendo descumprimento das normativas internas ou das políticas de proteção de dados por parte das OIs, os mecanismos de responsabilização devem, sem dúvidas, ser aprimorados. O cenário atual caracteriza-se pela impunidade, em que as OIs têm o controle quase absoluto sobre as medidas a serem tomadas, muitas vezes sem qualquer supervisão independente. Por serem sujeitos de Direito Internacional e estarem obrigadas a respeitar o direito à privacidade, a questão que permanece é se a violação desse direito deveria implicar a renúncia à sua imunidade. Caso contrário, dada a ausência de responsabilização judicial, são imperativos o desenvolvimento de um quadro de proteção de dados com medidas de *accountability* mais concretas e robustas, a criação de mecanismos independentes de supervisão e a implementação de um sistema eficaz de reparação administrativa.

4.3.1. Aprimoramento do *accountability* nas regras internas

Inobstante tenham avançado significativamente ao adotarem políticas internas e boas práticas no tratamento dos dados pessoais, as normas das OIs precisam ir além e incorporar uma abordagem mais robusta em termos de responsabilização. Para que a proteção de dados seja realmente eficaz, deve haver um maior comprometimento com os mecanismos de *accountability*.

As medidas de *accountability* estão relacionadas com a gestão responsável de dados pessoais, desde a coleta, o compartilhamento, o armazenamento e até o

processamento dos dados, de acordo com as exigências legais e contratuais[340]. A organização é responsável por esses dados desde o momento da coleta até a sua destruição, inclusive nas transferências para terceiros, sendo passíveis de sanções em caso de negligência. O processo de responsabilização pode ser dividido em cinco etapas: (i) prevenção: adoção de medidas preventivas de segurança, como controle de acesso e uso; (ii) detecção: identificação de violações às políticas de segurança; (iii) coleta de evidências: registro de informações relevantes sobre o histórico do sistema e as atividades realizadas; (iv) julgamento: determina quem foi o responsável pela violação; e (v) punição: aplicação de sanções adequadas[341]. Tal noção de *accountability* seria extremamente vantajosa se aplicada nas regras internas das OIs, que frequentemente fazem menções vagas sobre segurança cibernética e se reduzem a notificação das pessoas afetadas.

Em abril de 2023, o Comitê Permanente Interagências (IASC)[342] publicou suas orientações sobre a gestão pelas OIs dos dados pessoais nas ações humanitárias[343]. O documento fornece exemplos relevantes de como os princípios de segurança, transparência e responsabilidade podem ser aplicados na prática[344] e, a partir disso, inspirou outras OIs a revisarem suas políticas internas sobre o assunto – o ACNUR foi uma delas. De acordo com a sua Política Geral sobre Proteção de Dados Pessoais e Privacidade[345], o titular pode apresentar queixas quanto ao processamento dos seus dados pessoais pela organização e, se não satisfeito com a resposta, pode solicitar revisão por meio do Comitê de Proteção de Dados, cuja função é avaliar a solicitação

---

[340] FEIGENBAUM, J. et al. Systematizing,"Accountability" in Computer Science. New Haven: University of Yale, 2012. Disponível em: https://www.cs.yale.edu/publications/techreports/tr1452.pdf. Acesso em: 19 set. 2024.

[341] *Ibid*.

[342] Derivado da Resolução 46/182 de 1991 da Assembleia Geral da ONU, cuja principal finalidade é coordenar esforços entre OIs humanitárias e fornecer uma resposta internacional coerente e oportuna a emergências humanitárias. UNITED NATIONS. Resolution A/RES/46/182. Disponível em: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F46%2F182&Language=E&DeviceType=Desktop&LangRequested=False. Acesso em: 19 set. 2024.

[343] INTER-AGENCY STANDING COMMITTEE. Operational Guidance – Data Responsibility in Humanitarian Action. Disponível em: https://interagencystandingcommittee.org/sites/default/files/migrated/2023-04/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action%2C%202023.pdf. Acesso em: 19 set. 2024.

[344] INTER-AGENCY STANDING COMMITTEE. Examples of Data Responsibility in Practice in Practice. Disponível em: https://docs.google.com/document/d/1f5zOBLaL8mlitmOZBiLTnsVQCqyh5XnqJXt_WHooDXs/edit. Acesso em: 19 set. 2024.

[345] UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES. General Policy on Personal Data Protection and Privacy. Disponível em: https://www.refworld.org/policy/strategy/unhcr/2022/en/124207. Acesso em: 19 set. 2024.

e fazer recomendações ao Alto Comissário, o qual toma a decisão final sobre a concessão ou rejeição do pedido de reparação. As medidas corretivas podem incluir desde a entrega de informações ao titular sobre o processamento de seus dados, retificação ou exclusão de dados incorretos, até a suspensão do tratamento de dados. Apesar dessas possibilidades, a política do ACNUR expressamente rejeita eventual concessão de compensações financeiras, além de reafirmar sua posição frente às leis domésticas, devido aos privilégios conferidos pela Convenção da ONU de 1946.

Em conclusão, é evidente que ainda há espaço para melhorias significativas no que diz respeito à responsabilização interna das OIs, levando em conta não apenas as medidas preventivas de segurança, como também processos claros para a detecção e a punição de violações.

4.3.2. Criação de mecanismos independentes de supervisão interna

A Comissão CCF criada pela INTERPOL é um exemplo positivo de mecanismo independente de supervisão interna, cujo formato poderia ser replicado em outras OIs. A CCF é dividida em duas Câmaras, compostas por advogados especialistas em Direito Internacional Criminal, em direitos humanos e proteção de dados, além de peritos em proteção e processamento eletrônico de dados. Apesar de fazer parte do organograma da INTERPOL, é considerada independente e imparcial, desempenhando três funções principais: supervisão**,** assessoria e tratamento de solicitações. A Comissão oferece um meio alternativo para que pessoas cujos dados estão nos arquivos da INTERPOL possam buscar reparação (ainda que não financeira)[346]. Existem várias decisões proferidas pela CCF expressamente reconhecendo que o armazenamento de dados pessoais pela INTERPOL não atendia às regras internas da organização.

Um exemplo notório é o caso do advogado brasileiro Rodrigo Tacla Duran, acusado pelo Ministério Público Federal por estar envolvido no recebimento de propinas pela Odebrecht em troca de contratos públicos com a Petrobras. Seus dados estavam nos arquivos da INTERPOL em razão da difusão vermelha de captura

[346] INTERPOL. Frequently Asked Questions. Disponível em: https://www.interpol.int/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF/Frequently-Asked-Questions. Acesso em: 19 set. 2024.

internacional para fins de extradição ao Brasil. Na reclamação apresentada[347], o advogado alegou que o seu direito ao devido processo seria violado caso retornasse ao país, eis que ele denunciou irregularidades no sistema judiciário brasileiro diante da Comissão Parlamentar de Inquérito relacionada à Operação Lava Jato e isso gerou represálias e conflitos com o juiz responsável pelo seu caso, o que comprometeu ainda mais a imparcialidade do sistema. A CCF, ao analisar o caso, considerou que as garantias processuais presentes na legislação brasileira não foram atendidas suficientemente para rebater essas alegações e determinou que os dados relativos ao advogado fossem removidos dos arquivos da INTERPOL, por não estarem em conformidade com as normas aplicáveis ao tratamento de dados pessoais pela organização, especificamente os direitos a um juiz imparcial e ao devido processo legal consagrados na DUDH[348].

Dessa forma, a CCF exemplifica como um mecanismo interno de supervisão pode, de fato, tomar decisões desfavoráveis à própria organização, caso as alegações do requerente sejam pertinentes. A criação de estruturas semelhantes em outras OIs seria uma medida adequada para transmitir mais transparência nas operações e mais justiça aos titulares que desejam impugnar o tratamento dos seus dados pessoais.

4.3.2. Implementação de sistemas eficazes de reparação administrativa

O alargamento das competências dos Tribunais administrativos das OIs é a solução mais adequada para enfrentar a falta da responsabilização judicial das organizações por violações da proteção de dados. Isso significaria que, além da competência para julgar conflitos entre a organização e os seus funcionários, o Tribunal administrativo teria jurisdição sobre causas trazidas por particulares (fora da relação laboral) que tiveram seu direito à proteção de dados violado pela organização em questão.

A jurisdição dos Tribunais administrativos é geralmente vista como um complemento aos privilégios das OIs, ou seja, ainda que gozem de imunidade

[347] CCF - INTERPOL. CCF/106/R.808.16-18/c.3858.18. Disponível em: https://www.conjur.com.br/wp-content/uploads/2023/09/conduta-sergio-moro-tacla-duran-violou1.pdf. Acesso em: 19 set. 2024.
[348] Artigo 34(1) das Regras sobre Processamento de Dados. INTERPOL. INTERPOL's Rules on the Processing of Data. Disponível em: https://www.interpol.int/content/download/5694/file/26%20E%20RulesProcessingData_RPD_2023.pdf. Acesso em: 20 set. 2024.

jurisdicional, as organizações devem fornecer um recurso equivalente ao judicial para compensar tal proteção. Esse vínculo é cada vez mais reconhecido como uma exigência legal, decorrente de obrigações internacionais e de direitos humanos que envolvem o acesso à justiça[349]. Porém, a principal razão para a criação dos Tribunais é proporcionar aos funcionários das OIs um fórum de reivindicação de seus direitos relacionados ao emprego e, dessa forma, assegurar que tenham uma via efetiva para buscar reparação em caso de descumprimentos legais.

Nesse contexto, vale ressaltar o caso do Tribunal administrativo do CoE. Segundo o regulamento interno da referida OI[350], qualquer titular de dados pode apresentar uma queixa junto ao Comissário de Proteção de Dados, o qual comunicará suas conclusões ao Secretário-Geral. Este, por sua vez, poderá conceder compensação em determinados casos. Essa decisão poderá ser apelada no Tribunal Administrativo do CoE, porém, a normativa deixa claro que a jurisdição é limitada às impugnações dos "funcionários, ex-funcionários, requerentes dos seus direitos e candidatos num recrutamento". Caso a impugnação seja formulada por uma pessoa que não se encaixe nessas categorias (um particular), deverá ser buscado um acordo amigável. Não havendo sucesso na composição em três meses, a disputa será resolvida por meio de arbitragem final e vinculativa para ambas as partes – e não mediante decisão de um Tribunal[351].

Somente em casos atípicos, os Tribunais administrativos estenderam sua jurisdição para julgar casos trazidos por partes privadas sem vínculo trabalhista com a OI. O Tribunal administrativo da ONU fez isso em 1971 e permitiu o processamento de uma demanda proposta por um particular[352], sob o fundamento de que o contrato celebrado entre o requerente e a ONU claramente previa o estabelecimento de mecanismos apropriados para ouvir e decidir disputas. Portanto, se o Tribunal não tivesse competência para julgar o caso, o reclamante não teria acesso a nenhum tipo

---

[349] REINISCH, A. The Immunity of International Organizations and the jurisdiction of their Administrative Tribunals. New York: Global Administrative Law Series, 2007. Disponível em: https://iilj.org/wp-content/uploads/2016/08/Reinisch-The-Immunity-of-International-Organizations-and-the-Jurisdiction-of-Their-Administrative-Tribunals-2007-2.pdf. Acesso em: 20 set. 2024.

[350] COUNCIL OF EUROPE. Resolution CM/Res(2022)14 on establishing the Council of Europe Regulations on the Protection of Personal Data. Disponível em: https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680a6e929%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}. Acesso em: 20 set. 2024.

[351] Artigo 18 do Regulamento sobre Proteção de Dados Pessoais do CoE.

[352] UNITED NATIONS. Juridical Yearbook. Disponível em: https://legal.un.org/unjuridicalyearbook/pdfs/english/by_volume/1971/chpV.pdf. Acesso em: 20 set. 2024.

de procedimento recursal para defender seus direitos. O tema foi debatido durante a 74ª Sessão da CDI em 2023[353], que tratou do acesso à justiça para partes privadas em litígios com OIs. Devido à imunidade dessas organizações, a Comissão poderá concentrar-se em aspectos relevantes do regime de privilégios e imunidades, incluindo a necessidade de estabelecer mecanismos adequados para a resolução de disputas.

Não obstante, até o momento, a jurisdição administrativa existente se restringe à resolução de disputas entre a OI e o seu pessoal, deixando em aberto a proteção de direitos de particulares que não possuem vínculo empregatício com essas organizações. Por isso, ampliar as competências dos Tribunais administrativos das OIs seria um importante passo para alcançar o equilíbrio entre imunidade jurisdicional e responsabilização, em particular com relação à proteção de dados.

[353] INTERNATIONAL LAW COMISSION. Seventy-fourth session (first part). Disponível em: https://legal.un.org/ilc/documentation/english/summary_records/a_cn4_sr3617.pdf. Acesso em: 20 set. 2024.

CONCLUSÕES

O lugar ocupado pelas organizações internacionais no regime jurídico de proteção de dados é diretamente influenciado pelos seus privilégios e imunidades, que são concedidos pelos Estados onde as OIs operam a fim de evitar interferências externas e parcialização das suas atividades. De fato, não se pode esperar que uma organização, cujo mandato exige a atuação em vários territórios com culturas e leis distintas, se submeta à jurisdição local de cada um, já que isso comprometeria sobremaneira a independência das suas operações. Além disso, a falta de um instrumento legal internacional de proteção de dados vinculativo às OIs contribui para um cenário regulatório externo oco, deixando as organizações exclusivamente à mercê de suas regulações internas. Diante desse cenário, a problemática discutida neste trabalho foi a falta de responsabilização das OIs por violação da proteção de dados.

Num primeiro momento, verificamos que o Direito Internacional de proteção de dados foi criado por OIs independentes preocupadas com o fluxo transfronteiriço de informações pessoais e se apresenta na forma de instrumentos legais sem ou com força vinculante. No *soft law*, as Diretrizes da OCDE de 1980 marcaram um ponto de inflexão ao orientar diversas nações e organizações a harmonizarem normas sobre o assunto. Já no campo *hard law*, a Convenção 108+ do CoE desponta como o único instrumento internacional vinculativo aberto à ratificação pelas OIs e, apesar de representar um importante avanço para a construção de uma arquitetura regulatória global, não conta com nenhuma organização signatária. Ademais, o RGPD logrou estabelecer um padrão nas transferências internacionais e influenciou legislações em todo o mundo, mesmo com jurisdição limitada aos membros da UE. Ainda, o estudo demonstrou que o crescimento de leis domésticas não bastou para cobrir as lacunas na responsabilização das OIs, eis que seus privilégios frequentemente obstam a sujeição às normas nacionais.

A imunidade das OIs encontra respaldo no princípio da necessidade funcional, que garante sua operação livre de interferências dos Estados em cujos territórios atuam. Tal como os Estados soberanos se beneficiam de imunidades sob o princípio da igualdade entre nações, as OIs dependem dessas garantias para exercerem seus mandatos sem ingerência externa. A partir da análise dos instrumentos legais internacionais de *soft law* e *hard law*, assim como da análise das leis nacionais

específicas da Suíça, do Brasil e de Portugal, foi possível inferir que as normas domésticas não estão intencionadas às OIs, que, por outro lado, adotam regulamentos internos baseados em princípios gerais de proteção de dados consagrados no Direito Internacional e doméstico, como fizeram o CICV e a UNICEF. Contudo, essa autorregulamentação muitas vezes falha ao instituir mecanismos sancionatórios com pouco ou nenhum efeito, pois geralmente se resumem à comunicação da violação da proteção de dados aos cargos superiores da organização e à notificação das pessoas afetadas.

Os Tribunais internacionais, por sua vez, compartilham a mesma natureza das OIs e, portanto, também gozam de privilégios previstos no respectivo Estatuto e que foram concedidos pelo Estado sede. Assim, igualmente, têm a faculdade de criar regras próprias sobre a proteção de dados, como fizeram o TIJ, o TPI e o TJUE. Primeiro, concluímos que o TIJ carece de uma política interna própria e opera somente com base nos Princípios da ONU sobre Proteção de Dados, mas que, por si só, não atendem às necessidades específicas do órgão judicial. Segundo, as regras internas do TPI são esparsas e desuniformes, potencialmente criando inconsistências nos procedimentos internos de categorização das informações contidas nos processos judiciais e deixando de prever medidas para evitar ou controlar ataques cibernéticos nos seus sistemas. Por último, o TJUE conta com regras mais claras e organizadas sobre proteção de dados: no exercício das funções não jurisdicionais o Tribunal deverá observar o RGPD no que couber; por outro lado, as funções jurisdicionais não são submetidas à legislação doméstica e são supervisionadas internamente por uma comissão de proteção de dados.

Tendo esse cenário em mente, passamos a examinar a responsabilidade internacional das OIs – aquela que decorre do descumprimento de uma obrigação internacional legal atribuída à organização. A intepretação dada aos Artigos da CDI sobre a Responsabilidade Internacional das OIs é que a definição de “agentes” é ampla e pode incluir aqueles que operam sem intervenção humana, como os sistemas de IA, o que significa que mesmo havendo uma falha cibernética, a OI poderia ser responsabilizada por ter relação direta com o agente responsável pelo ato ilícito. Porém, no contexto específico da proteção de dados surgem desafios que ultrapassam tal interpretação. Primeiro, a falta de reconhecimento da proteção de dados como uma obrigação jurídica vinculativa, sendo tratada pelas OIs como uma mera prática recomendada. Em segundo lugar, a imunidade jurisdicional

inegavelmente entra em conflito com o princípio fundamental de acesso aos Tribunais judiciais, em especial se as organizações envolvidas no litígio oferecem um mecanismo alternativo de resolução de disputas, como acontece com a instalação (ou aceitação de jurisdição) de um Tribunal administrativo. Disso surge o terceiro desafio: a jurisdição dos Tribunais administrativos se restringe às disputas trabalhistas entre uma OI e seu pessoal, logo que as violações da proteção de dados cometidas pela OI só serão julgadas se ocorrerem dentro da relação laboral. Diante dessas dificuldades, passamos a analisar se a autorregulamentação estaria suprindo a falta da responsabilidade administrativa/judicial das OIs. Porém, os três casos de ataques cibernéticos sofridos pelo CICV, pela UNICEF e pelo TPI evidenciaram as falhas nas regras internas, porque as ocorrências se repetiram e não foram divulgadas medidas de responsabilização em face das organizações.

Nesse contexto, finalmente podemos nos indagar como garantir, ou pelo menos aprimorar, a reparação aos afetados pela violação da proteção de dados por OIs. A resposta é melhorar os mecanismos existentes de responsabilização, começando pelo comprometimento com o processo completo de *accountability*, desde a prevenção até a punição. A criação de comissões realmente independentes e neutras também é uma medida que pode cooperar com a reparação, na medida em que os membros imparciais podem tomar decisões contra a própria organização quando suas regras internas são descumpridas. Por fim, na falta de reparação judicial, defendemos a reparação administrativa mediante a expansão da competência dos Tribunais administrativos, que passariam a julgar causas trazidas por particulares (fora da relação laboral) que tiveram seu direito à proteção de dados violado pela organização em questão.

Todos os argumentos e fundamentos expostos levam à conclusão de que, na ausência de mecanismos jurídicos eficazes de responsabilização e reparação, a proteção de dados nas OIs está em risco. Portanto, o tema deve continuar aberto à urgente discussão. O poder que as organizações exercem sobre os dados pessoais nos remete ao fenômeno do capitalismo de vigilância e, inegavelmente, deve ser melhor regulado, em especial porque a proteção de dados emerge não só como uma questão legal, mas como um imperativo ético da era digital.

REFERÊNCIAS

22 U.S. Code § 288a - Privileges, exemptions, and immunities of international organizations. 1945. Disponível em: https://www.law.cornell.edu/uscode/text/22/288a#:~:text=International%20organizations%2C%20their%20property%20and,for%20the%20purpose%20of%20any. Acesso em: 15 maio 2024.

ALTER, K. J. et al. Too Much Power for the Judges? In: HUBERT, Z.; DUR, A. (Ed.). Key Controversies in European Integration. 3ed. London: Bloomsbury Academic, 2022.

AMERANSINGHE, C. F. International Administrative Tribunals. In: ROMANO, C. et al. The Oxford Handbook of International Adjudication. Oxford: Oxford University Press, 2013.

ANDERSON, D.; WORDSWORTH, S. In: ZIMMERMANN, Andreas; TAMS, Christian J.; OELLERS-FRAHM, Karin; TOMUSCHAT, Christian (Ed.). The Statute of the International Court of Justice: A Commentary. 3 ed. Oxford: Oxford University Press, 2019.

APEC - Asia-Pacific Economic Cooperation. APEC Privacy Framework. Disponível em: https://www.apec.org/docs/default-source/Publications/2005/12/APEC-Privacy-Framework/05_ecsg_privacyframewk.pdf. Acesso em: 30 mar. 2024.

AUSTRALIA. Privacy Act 1988. Disponível em: https://www.legislation.gov.au/C2004A03712/2017-07-01/text. Acesso em: 25 mar. 2024.

AUSTRIA. Cyber activities and international law: Austrian position paper. Disponível em: https://docs-library.unoda.org/Open-Ended_Working_Group_on_Information_and_Communication_Technologies_-_(2021)/Austrian_Position_Paper_-_Cyber_Activities_and_International_Law_(Final_23.04.2024).pdf. Acesso em: 21 ago. 2024.

AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS. Semana da Proteção de Dados 2022. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/semana-da-protecao-de-dados-2022/semana-protecao-dados-2022. Acesso em: 30 mar. 2024.

BANDEIRA, R. Talibã capturou dispositivos de biometria militar dos EUA, dizem veteranos. Disponível em: https://www.intercept.com.br/2021/08/18/taliba-dispositivos-biometria-militar-eua/. Acesso em: 6 maio 2024.

BENNETT, C. J. The Council of Europe's Modernized Convention on Personal Data Protection: Why Canada Should Consider Accession. Waterloo: Centre for International Governance Innovation, 2020. p. 3-5. Disponível em: http://www.jstor.org/stable/resrep27512.8. Acesso em: 03 abr. 2024.

BAPTISTA, E. C. Direito Internacional Público: Sujeitos e Responsabilidade. Coimbra: Almedina, 2004.

BERESFORD, S. The Privileges and Immunities of the International Criminal Court: Are They Sufficient for the Proper Functioning of the Court or Is There Still Room for Improvement? San Diego: San Diego International Law Journal, v. 6, n. 1, 2002. Disponível em: https://digital.sandiego.edu/cgi/viewcontent.cgi?article=1261&context=ilj. Acesso em: 20 jul. 2024.

BLACKABY, N. et al. An Overview of International Arbitration. Oxford: Oxford University Press, 2009.

BRABANDERE, E. Measures of Constraint and the Immunity of International Organisations. In: RUYS, T.; ANGELET, N.; FERRO, L. (Eds.). Part III - Immunity from Execution of States and International Organisations. The Cambridge Handbook of Immunities and International Law. Cambridge: Cambridge University Press, 2019. p. 327-349.

BRASIL. Lei n.° 10.406, de 10 de janeiro de 20002. Institui o Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 21 jun. 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: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 23 mar. 2024.

BREACHLOCK. UNICEF Hit by Threat Actor 888 Affecting 11 Countries. Disponível em: https://www.breachlock.com/resources/advisories/unicef-hit-by-threat-actor-888-affecting-11-countries/. Acesso em: 05 set. 2024.

BROWN, C. Review Essay - The Proliferation of International Courts and Tribunals: finding your way through the maze. Melbourne: Melbourne Law School, 2014. Disponível em: https://law.unimelb.edu.au/__data/assets/pdf_file/0006/1680261/Brown.pdf. Acesso em: 16 jul. 2024.

BUENO, E. P; FREIRE, M.; OLIVEIRA, PEREIRA, V. A. As origens históricas da diplomacia e a evolução do conceito de proteção diplomática dos nacionais. Anuario Mexicano de Derecho Internacional, v. 17. Cidade do Mexico: Elsevier, 2017. p. 623-649. Disponível em: https://www.sciencedirect.com/science/article/pii/S1870465417300454. Acesso em: 11 maio 2024.

BYGRAVE, L. A. International agreements to protect personal data. In: RULE, J. B. Global Privacy Protection: The First Generation. Cheltenham, UK: Edward Elgar, 2008. Disponível em: https://doi.org/10.4337/9781848445123. Acesso em: 03 abr. 2024.

BYGRAVE, L. A. Strasbourg Effect on EU Data Protection. Computer Law & Security Review, v. 40. Oslo: Elsevier Ltd., 2020. Disponível em: https://www.duo.uio.no/bitstream/handle/10852/92263/1/Strasbourg_effect_final.pdf. Acesso em: 05 abr. 2024.

CAMPOS, J. M. de; CAMPOS, J. L. M. de. Teoria Geral das Organizações Internacionais. In: CAMPOS, J. M. de; RIBEIRO, M. A. (coord.). Organizações Internacionais. Coimbra: Almedina, 2022. p. 51.

CANADA. Foreign Missions and International Organizations Act. Disponível em: https://laws.justice.gc.ca/eng/acts/f-29.4/page-1.html#h-235020. Acesso em: 30 maio 2024.

CANADA. The application of international law in cyberspace. Ottawa: Global Affairs Canada, 2022. Disponível em: https://www.international.gc.ca/world-monde/issues_development-enjeux_developpement/peace_security-paix_securite/cyberspace_law-cyberespace_droit.aspx?lang=eng#a6. Acesso em: 21 ago. 2024.

CCF - INTERPOL. CCF/106/R.808.16-18/c.3858.18. Disponível em: https://www.conjur.com.br/wp-content/uploads/2023/09/conduta-sergio-moro-tacla-duran-violou1.pdf. Acesso em: 19 set. 2024.

CESARE, R. The sword and the scales: the United States and international courts and Tribunals. Cambridge; New York: Cambridge University Press, 2009.

CHADWICK, V. UNICEF data leak reveals personal info of 8,000 online learners. Disponível em: https://www.devex.com/news/unicef-data-leak-reveals-personal-info-of-8-000-online-learners-95558. Acesso em: 04 set. 2024.

CHANDER, A.; KAMINSKI M.E.; MCGEVERA, W. Catalyzing Privacy Law. Minnesota Law Review. Boulder, Colorado: University of Colorado Law School, 2021. Disponível em: https://scholar.law.colorado.edu/cgi/viewcontent.cgi?article=2447&context=faculty-articles. Acesso em: 20 abr. 2024.

COMISSÃO EUROPEIA. Perguntas e respostas: Quadro de Proteção de Dados UE-EUA. Disponível em: https://ec.europa.eu/info/law/law-topic/data-protection/international-data-transfer/adequacy-decisions/eu-us-data-privacy-framework_en. Acesso em: 14 abr. 2024.

COMISSÃO INTERAMERICANA DE DIREITOS HUMANOS. Convenção Americana sobre Direitos Humanos. Disponível em: https://www.cidh.oas.org/basicos/portugues/c.convencao_americana.htm. Acesso em: 22 mar. 2024.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. "Convenções de Genebra", Comitê Internacional da Cruz Vermelha. Disponível em: https://www.icrc.org/pt/doc/war-and-law/treaties-customary-law/geneva-conventions/overview-geneva-conventions.htm. Acesso em: 20 maio 2024.

COMITÊ INTERNACIONAL DA CRUZ VERMELHA. Regras do CICV sobre a proteção de dados pessoais. Disponível em: https://www.icrc.org/pt/o-cicv-e-protecao-de-dados#:~:text=Normas%20do%20CICV%20sobre%20Prote%C3%A7%C3%A3o,interagimos%20e%20cujos%20dados%20tratamos. Acesso em: 7 maio 2024.

CONFEDERAÇÃO NACIONAL DA INDÚSTRIA. Transferência Internacional de Dados: Orientações para a Indústria. 2020. p. 66. Disponível em: https://static.portaldaindustria.com.br/media/filer_public/46/fc/46fce346-06e8-4a05-b3e2-b8f6f15f0afd/id_240807_transferencia_internacional_de_dados_interativo.pdf. Acesso em: 25 mar. 2024.

CORDEIRO, A. B. M. Comentário ao Regulamento Geral de Proteção de Dados e à Lei n.º 58/2019. Lisboa: Almedina, 2021.

CORDEIRO, A. B. M. Dados pessoais: conceito, extensão e limites. Revista de Direito Civil, a.3, n.2. Lisboa: CIDP, 2018. p. 297-321.

CORDEIRO, A. B. M. Direito da Proteção de Dados: à luz do RGPD e da Lei n.º 58/2019. Coimbra: Almedina, 2020.

COUNCIL OF EUROPE. "Background". Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data. Disponível em: https://www.coe.int/en/web/data-protection/convention108/background#:~:text=In%201981%2C%20after%20four%20years,as%20Convention%20108%20%2D%20was%20concluded. Acesso em: 27 mar. 2024.

COUNCIL OF EUROPE. Chart of signatures and ratifications of Treaty 108. Disponível em: https://www.coe.int/en/web/data-protection/convention108/parties. Acesso em: 03 jun. 2024.

COUNCIL OF EUROPE. Consultative Committee of the Convention 108+. Draft Evaluation & Follow-Up Questionnaire. 2021. Disponível em: https://rm.coe.int/t-pd-2018-20rev8-evaluation-questionaire-june-2021-2752-1166-9251-1/1680a29c9c. Acesso em: 5 jun. 2024.

COUNCIL OF EUROPE. Consultative Committee of the Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (T-PD). Disponível em: https://search.coe.int/cm?i=09000016804e0476. Acesso em: 30 mar. 2024.

COUNCIL OF EUROPE. Conventions - Full List. Disponível em: https://www.coe.int/en/web/conventions/full-list?module=signatures-by-treaty&treatynum=108. Acesso em: 30 mar. 2024.

COUNCIL OF EUROPE. Data Protection: European Commission adopts new adequacy decision for safe and trusted EU-US data flows. Disponível em: https://ec.europa.eu/commission/presscorner/detail/en/ip_23_3721. Acesso em: 22 abr. 2024.

COUNCIL OF EUROPE. Directorate of Legal Advice and Public International Law. Legal opinion. 2021. Disponível em: https://rm.coe.int/legal-opinion-dlapil02-2021-the-interpretation-of-the-notion-of-jurisd/1680a19c58. Acesso em: 03 jun. 2024.

COUNCIL OF EUROPE. Proposal for a COUNCIL DECISION authorising Member States to sign, in the interest of the European Union, the Protocol amending the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (ETS No. 108). Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:52018PC0449&from=HU. Acesso em: 03 jun. 2024.

COUNCIL OF EUROPE. Resolution CM/Res(2022)14 on establishing the Council of Europe Regulations on the Protection of Personal Data. Disponível em: https://search.coe.int/cm#{%22CoEIdentifier%22:[%220900001680a6e929%22],%22sort%22:[%22CoEValidationDate%20Descending%22]}. Acesso em: 20 set. 2024.

COUNCIL OF EUROPE. Statute of the Administrative Tribunal. Disponível em: https://www.coe.int/en/web/Tribunal/statute. Acesso em: 17 set. 2024.

CROFT, D. UNICEF data allegedly leaked on BreachForums. Disponível em: https://www.cyberdaily.au/security/10489-unicef-data-allegedly-leaked-on-breachforums?ref=doingfedtime.com. Acesso em: 05 set. 2024.

CUNHA, M. N. F. da; VIEIRA, S. C. Cruz Vermelha: breve análise histórica de uma organização sui generis. Revista Curso Direito UNIFOR, v. 7, n. 2. Itaúna: UNIFOR, 2016. p. 39–54. Disponível em: https://revistas.uniformg.edu.br/cursodireitouniformg/article/view/419. Acesso em: 03 jul. 2024.

CUSTERS, B. et al. Quis custodiet ipsos custodes? Data protection in the judiciary in EU and EEA Member States. International Data Privacy Law, v. 12, n. 2. Oxford: IDPL, 2022. Disponível em: https://academic.oup.com/idpl/article/12/2/93/6511894. Acesso em: 24 jul. 2024.

DALLARI, D. de A. Empresas Multinacionais e Soberania do Estado. Revista da Faculdade de Direito da Universidade de São Paulo, v. 76. São Paulo: USP, 1981. p. 107-121. Disponível em: https://www.revistas.usp.br/rfdusp/article/view/66917. Acesso em: 20 maio 2024.

DUARTE, F. de A. Multinational companies as subjects of international law: are we missing the point? In: DUARTE, M. L.; LANCEIRO, R. T. (Coord.). Ordem jurídica global do século XXI: sujeitos e actores no palco internacional. 1ª ed. Lisboa: AAFDL Editora, 2020. p. 561-594.

DE HERT, P.; GUTWIRTH, S. Data Protection in the Case Law of Strasbourg and Luxemburg. In: GUTWIRTH, S. et al. Reinventing Data Protection? 1. ed. Dordrecht: Springer, 2009. p. 3-45. Disponível em: https://doi.org/10.1007/978-1-4020-9498-9. Acesso em: 23 mar. 2024.

DE HERT, P.; PAPAKONSTANTINOU, V. The Council of Europe Data Protection Convention reform: Analysis of the new text and critical comment on its global ambition. Computer Law & Security Review, v. 30, n. 6. Southampton: Elsevier, 2014. p. 633-642. Disponível em: https://doi.org/10.1016/j.clsr.2014.09.002. Acesso em: 30 maio 2024.

DEBUF, E. Tools to do the job: The ICRC's legal status, privileges and immunities. International Review of the Red Cross, v. 97, n. 1-2. Genebra: ICRC, 2016. p. 319-344. Disponível em: https://international-review.icrc.org/sites/default/files/irc_97_1-2-13.pdf. Acesso em: 20 maio 2024.

DELOITTE. The Aftermath of Schrems II. Implications, insights, and expectations for the future. UK: Delloite, 2022. Disponível em: https://www2.deloitte.com/content/dam/Deloitte/nl/Documents/risk/deloitte-nl-risk-the-aftermath-of-schrems-ii.pdf. Acesso em: 22 abr. 2024.

ECHR. Case of Al-Skeini and others v. The United Kingdom. (Application no. 55721/07). Disponível em: https://hudoc.echr.coe.int/eng#{%22itemid%22:[%22001-105606%22]}. Acesso em: 04 jun. 2024.

ECONOMIC AND SOCIAL COUNCIL. Guidelines for the regulation of computerized personal data files - Final report submitted by Mr. Louis Joinet. 1988. Disponível em: https://digitallibrary.un.org/record/43365?ln=fr&v=pdf. Acesso em: 1 jun. 2024.

EDPB. Guidelines 3/2018 on the territorial scope of the GDPR (Article 3). 2019. Disponível em: https://www.edpb.europa.eu/our-work-tools/our-documents/guidelines/guidelines-32018-territorial-scope-gdpr-article-3-version_en. Acesso em: 10 jun. 2024.

FEDERAL DEPARTMENT OF FOREIGN AFFAIRS. International organizations in Switzerland. 2022. Disponível em: https://www.eda.admin.ch/eda/en/fdfa/foreign-policy/international-organizations/international-organizations-switzerland.html . Acesso em: 20 jun. 2024.

FEDLEX. Message concernant la loi fédérale sur la protection des données (LPD) du 23 mars 1988. p. 448. Disponível em: https://www.fedlex.admin.ch/eli/fga/1988/2_413_421_353/fr. Acesso em: 20 jun. 2024.

FEDLEX. Message concernant la loi fédérale sur la révision totale de la loi fédérale sur la protection des données et sur la modification d'autres lois fédérales. 2017. p. 6633. Disponível em: https://www.fedlex.admin.ch/eli/fga/2017/2057/fr. Acesso em: 20 jun. 2024.

FEIGENBAUM, J. et al. Systematizing,"Accountability" in Computer Science. New Haven: University of Yale, 2012. Disponível em: https://www.cs.yale.edu/publications/techreports/tr1452.pdf. Acesso em: 19 set. 2024.

FLAHERTY, D. H. Protection Privacy in Surveillance Societies. Chapel Hill: University of North Carolina Press, 2014.

GAZI, T. Data to the rescue: how humanitarian aid NGOs should collect information based on the GDPR. Journal of International Humanitarian Action, v. 5, n. 9. 2020. Disponível em: https://link.springer.com/article/10.1186/s41018-020-00078-0. Acesso em: 11 jun. 2024.

GIL, A. R. Um Livro de Casos de Direito das Nações Unidas – Guia de Estudo. In: GIL, A. R.; PATINHAS, M. C. (ed.). A ONU em ação: Conflitos Armados e Missões de Paz – Estudo de Casos. Lisboa: Lisbon Public Law Editions, 2024. Disponível em: https://lisbonpubliclaw.sharepoint.com/sites/Externos/Shared%20Documents/General/Editorial/EBook_ConflitosArmadosDireitoInternacional_V02.pdf. Acesso em: 10 set. 2024.

GLOBAL PRIVACY ASSEMBLY. History of the Assembly. Disponível em: https://globalprivacyassembly.org/the-assembly-and-executive-committee/history-of-the-assembly/. Acesso em: 11 set. 2024.

GLOBAL PRIVACY ASSEMBLY. Resolution on Data Protection and International Organisations. 2003. Disponível em: https://globalprivacyassembly.org/wp-content/uploads/2015/02/Resolution-on-Data-Protection-and-International-Organisations.pdf. Acesso 1 jun. 2024.

GOV UK. UK donation to the International Criminal Court's Special Fund for Security will help to protect the Court from future cyber-attacks. Disponível em: https://www.gov.uk/government/news/uk-donation-to-the-international-criminal-courts-special-fund-for-security-will-help-to-protect-the-court-from-future-cyber-attacks. Acesso em: 06 set. 2024.

GOVERNO DE PORTUGAL. "28 de janeiro, Dia Europeu da Proteção de Dados". Portal da Economia. Disponível em: https://www.sgeconomia.gov.pt/noticias/28-de-janeiro-dia-europeu-da-protecao-de-dados.aspx#:~:text=A%2028%20de%20janeiro%20comemora,a%20prote%C3%A7%C3%A3o%20dos%20dados%20pessoais. Acesso em: 27 mar. 2024.

GREENLEAF, G. The influence of European data privacy standards outside Europe: implications for globalization of Convention 108. International Data Privacy Law, v. 2, n. 2. Oxford: Oxford University Press, 2012.

HARTZOG W.; RICHARDS, N. Privacy's Constitutional Moment and the Limits of Data Protection. Boston College Law Review, v. 1, n. 5. Boston: Boston College Law Review, 2020. Disponível: https://scholarship.law.bu.edu/cgi/viewcontent.cgi?article=4069&context=faculty_scholarship. Acesso em: 14 abr. 2024.

INSTITUTO DE TECNOLOGIA E SOCIEDADE DO RIO. Transferência de dados entre Europa e Brasil: Análise da Adequação da Legislação Brasileira. Rio de Janeiro: ITS, 2019. Disponível em: https://itsrio.org/wp-content/uploads/2019/12/Relatorio_UK_Azul_INTERACTIVE_Justificado.pdf. Acesso em: 21 jun. 2024.

INTER-AGENCY STANDING COMMITTEE. Examples of Data Responsibility in Practice in Practice. Disponível em: https://docs.google.com/document/d/1f5zOBLaL8mlitmOZBiLTnsVQCqyh5XnqJXt_WHooDXs/edit. Acesso em: 19 set. 2024.

INTER-AGENCY STANDING COMMITTEE. Operational Guidance – Data Responsibility in Humanitarian Action. Disponível em: https://interagencystandingcommittee.org/sites/default/files/migrated/2023-04/IASC%20Operational%20Guidance%20on%20Data%20Responsibility%20in%20Humanitarian%20Action%2C%202023.pdf. Acesso em: 19 set. 2024.

INTERNATIONAL BUSINESS MACHINES CORPORATION. Cost of a Data Breach Report 2024. Disponível em: https://table.media/wp-content/uploads/2024/07/30132828/Cost-of-a-Data-Breach-Report-2024.pdf. Acesso em: 19 set. 2024.

INTERNATIONAL COMMITTEE OF THE RED CROSS. Cyber attack on ICRC: What we know. Disponível em: https://www.icrc.org/en/document/cyber-attack-icrc-what-we-know. Acesso em: 05 set. 2024.

INTERNATIONAL COMMITTEE OF THE RED CROSS. Handbook on Data Protection in Humanitarian Action - Second Edition. Disponível em: https://cash-hub.org/wp-content/uploads/sites/3/2017/08/4305.01_002-ebook-3.pdf. Acesso em: 6 maio 2024.

INTERNATIONAL COMMITTEE OF THE RED CROSS. ICRC cyber-attack: Sharing our analysis. Disponível em: https://www.icrc.org/en/document/icrc-cyber-attack-analysis. Acesso em: 04 set. 2024.

INTERNATIONAL COMMITTEE OF THE RED CROSS. Restoring Family Links code of conduct on data protection. Disponível em: https://www.icrc.org/en/document/rfl-code-conduct. Acesso 01 jul. 2024.

INTERNATIONAL COMMITTEE OF THE RED CROSS. Safeguarding Humanitarian Data. Disponível em: https://rcrcconference.org/app/uploads/2022/05/16_CoD22-Safeguarding-Humanitarian-Data-Background-document-FINAL-EN.pdf. Acesso em: 05 set. 2024.

INTERNATIONAL COMMITTEE OF THE RED CROSS. Statutes of the International Red Cross and Red Crescent Movement. Disponível em: https://www.icrc.org/en/doc/assets/files/other/statutes-en-a5.pdf. Acesso em: 15 maio 2024.

INTERNATIONAL COURT OF JUSTICE. Advisory opinion on the Reparation for Injuries Suffered in the Service of the United Nations. Disponível em: https://www.icj-cij.org/case/4. Acesso em: 20 ago. 2024.

INTERNATIONAL COURT OF JUSTICE. Alleged Violations of Sovereign Rights and Maritime Spaces in the Caribbean Sea (Nicaragua V. Colombia). 2022. Disponível em: https://jusmundi.com/en/document/pdf/decision/en-alleged-violations-of-sovereign-

rights-and-maritime-spaces-in-the-caribbean-sea-nicaragua-v-colombia-judgment-thursday-21st-april-2022. Acesso em: 06 ago. 2024.

INTERNATIONAL COURT OF JUSTICE. Jurisdictional Immunities of the State (Germany v. Italy: Greece intervening). Disponível em: https://www.icj-cij.org/case/143. Acesso em: 10 set. 2024.

INTERNATIONAL COURT OF JUSTICE. Privacy Policy. Disponível em: https://www.icj-cij.org/public/privacy_policy.html. Acesso em: 04 ago. 2024.

INTERNATIONAL COURT OF JUSTICE. Reparation for Injuries Suffered in the Service of the United Nations. 1949. Disponível em: https://www.icj-cij.org/case/4. Acesso em: 20 maio 2024.

INTERNATIONAL COURT OF JUSTICE. Resolution 90(I) of the General Assembly of the United Nations, II December 1946. Disponível em: https://www.icj-cij.org/other-texts/resolution-90. Acesso em: 21 jul. 2024.

INTERNATIONAL CRIMINAL COURT. Administrative Instrutction ICC/AI/2007/001. DIsponível em: https://www.icc-cpi.int/sites/default/files/2022-05/ICC%20AI%202007%20001%20%28ENG%29%20-%20ICC%20INFORMATION%20PROTECTION%20POLICY.PDF. Acesso em: 05 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Chambers Practice Manual. 2023. Disponível em: https://www.icc-cpi.int/sites/default/files/2023-07/230707-chambers-manual-eng.pdf. Acesso em: 07 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Code of Conduct for Staff Members. 2012. Disponível em: https://www.icc-cpi.int/sites/default/files/Vademecum/OT1036136_ICC%20AI%202011%20002%20%28ENG%29%20-%20CODE%20OF%20CONDUCT%20OF%20STAFF%20MEMBERS.PDF. Acesso em: 07 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Headquarters Agreement between the International Criminal Court and the Host State. Disponível em: https://www.icc-cpi.int/sites/default/files/NR/rdonlyres/99A82721-ED93-4088-B84D-7B8ADA4DD062/280775/ICCBD040108ENG1.pdf. Acesso em: 21 jul. 2024.

INTERNATIONAL CRIMINAL COURT. ICC-02/11-01/15. Disponível em: https://www.legal-tools.org/doc/4dc909/pdf/. Acesso em: 05 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Measures taken following the unprecedented cyber-attack on the ICC. Disponível em: https://www.icc-cpi.int/news/measures-taken-following-unprecedented-cyber-attack-icc. Acesso em: 06 set. 2024.

INTERNATIONAL CRIMINAL COURT. Presidential Directive ICC/PRESD/G/2005/001. Disponível em: https://www.legal-tools.org/doc/3ae5ed/pdf. Acesso em: 05 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Regulations of the Registry. Disponível em: https://www.icc-cpi.int/sites/default/files/RegulationsRegistryEng.pdf. Acesso em: 05 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Rules of Procedure and Evidence. 2013. Disponível em: https://www.icc-cpi.int/sites/default/files/RulesProcedureEvidenceEng.pdf. Acesso em: 06 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Situation in the Democratic Republic of the Congo in the Case of the Prosecutor v. Thomas Lubanga Dyilo. Decision on the Arrangements for Participation of Victims a/0001/06, a/0002/06 and a/0003/06 at the Confirmation Hearing. Disponível em: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2006_03267.PDF. Acesso em: 08 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Situation in the Democratic Republic of the Congo in the Case of the Prosecutor v. Thomas Lubanga Dyilo. Defence Observations Relative to the Proceedings and Manner of Participation of Victims a/0001/06 to a/0003/06. Disponível em: https://www.icc-cpi.int/sites/default/files/CourtRecords/CR2006_03069.PDF. Acesso em: 08 ago. 2024.

INTERNATIONAL CRIMINAL COURT. Understanding the International Criminal Court. Disponível em: https://www.icc-cpi.int/sites/default/files/Publications/understanding-the-icc.pdf. Acesso em: 20 jul. 2024.

INTERNATIONAL LABOUR ORGANIZATION ADMINISTRATIVE TRIBUNAL. 109th Session Judgment No. 2944. 2010. Disponível em: https://webapps.ilo.org/dyn/triblex/triblexmain.fullText?p_lang=en&p_judgment_no=2944&p_language_code=EN. Acesso em: 17 set. 2024.

INTERNATIONAL LABOUR ORGANIZATION ADMINISTRATIVE TRIBUNAL. 118th Session -Judgment No. 3338. 2014. Disponível em: https://webapps.ilo.org/dyn/triblex/triblexmain.fullText?p_lang=en&p_judgment_no=3338&p_language_code=EN. Acesso em: 17 set. 2024.

INTERNATIONAL LABOUR ORGANIZATION. ILO Administrative Tribunal. Disponível em: https://www.ilo.org/ilo-administrative-Tribunal#news. Acesso em: 17 set. 2024.

INTERNATIONAL LABOUR ORGANIZATION. Organizations recognizing the jurisdiction. Disponível em: https://www.ilo.org/ilo-administrative-Tribunal/organizations-recognizing-jurisdiction. Acesso em: 17 set. 2024.

INTERNATIONAL LABOUR ORGANIZATION. Statute of the Administrative Tribunal of the International Labour Organization. Disponível em: https://www.ilo.org/resource/statute-administrative-Tribunal-international-labour-organization. Acesso em: 17 set. 2024.

INTERNATIONAL LAW COMISSION. Seventy-fourth session (first part). Disponível em: https://legal.un.org/ilc/documentation/english/summary_records/a_cn4_sr3617.pdf. Acesso em: 20 set. 2024.

INTERNATIONAL ORGANIZATION FOR MIGRATION. Data protection. Disponível em: https://www.iom.int/data-protection. Acesso em: 21 ago. 2024.

INTERNATIONAL ORGANIZATION FOR MIGRATION. IOM framework for addressing accountability to affected populations. Disponível em: https://publications.iom.int/system/files/pdf/iom-aap-framework.pdf. Acesso em: 21 ago. 2024.

INTERNATIONAL REVIEW OF THE RED CROSS. Agreement between the International Committee of the Red Cross and the Swiss Federal Council to determine the legal status of the Committee in Switzerland. Disponível em: https://international-review.icrc.org/articles/agreement-between-international-committee-red-cross-and-swiss-federal-council-determine. Acesso em: 04 jul. 2024.

INTERPOL. Commission for the Control of INTERPOL's Files (CCF). Disponível em: https://www.interpol.int/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF. Acesso em: 16 set. 2024.

INTERPOL. Frequently Asked Questions. Disponível em: https://www.interpol.int/Who-we-are/Commission-for-the-Control-of-INTERPOL-s-Files-CCF/Frequently-Asked-Questions. Acesso em: 19 set. 2024.

INTERPOL. INTERPOL's Rules on the Processing of Data. Disponível em: https://www.interpol.int/content/download/5694/file/26%20E%20RulesProcessingData_RPD_2023.pdf. Acesso em: 20 set. 2024.

JANMYR, M. UNHCR and the Syrian refugee response: negotiating status and registration in Lebanon. The International Journal of Human Rights, v. 22, n. 3. Bergen: University of Bergen, 2018. p. 393-419. Disponível em: https://www.tandfonline.com/doi/pdf/10.1080/13642987.2017.1371140. Acesso em: 03 jul. 2024.

JORNAL OFICIAL DA UNIÃO EUROPEIA. Acórdão do Tribunal de Justiça (Primeira Secção) de 24 de março de 2022. Processo C-245/20. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:62020CA0245. Acesso em: 14 ago. 2024.

JORNAL OFICIAL DA UNIÃO EUROPEIA. Decisão do Tribunal de Justiça, de 1 de outubro de 2019, que institui um mecanismo interno de fiscalização em matéria de tratamento de dados pessoais efetuado no quadro das funções jurisdicionais do Tribunal de Justiça. 2019. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:C2019/383/02. Acesso em: 03 ago. 2024.

JORNAL OFICIAL DA UNIÃO EUROPEIA. Decisão do Tribunal Geral, de 16 de outubro de 2019, que institui um mecanismo interno de fiscalização em matéria de

tratamento de dados pessoais efetuado no quadro das funções jurisdicionais do Tribunal Geral. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:C2019/383/03. Acesso em: 03 ago. 2024.

JORNAL OFICIAL DA UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 30 mar. 2024.

KAHN, K. A. Technology Will Not Exceed Our Humanity. Disponível em: https://digitalfrontlines.io/2023/08/20/technology-will-not-exceed-our-humanity/. Acesso em: 06 set. 2024.

KLABBERS, J. An introduction to international organizations law. 3. ed. Cambridge: Cambridge University Press, 2015. p. 136.

KONG, L. Data Protection and Transborder Data Flow in the European and Global Context. European Journal of International Law, v. 21, n. 2. Oxford: Oxford University Press, 2010. p. 441–456. Disponível em: https://doi.org/10.1093/ejil/chq025. Acesso em: 04 abr. 2024.

KUNER, C. International Organizations and the EU General Data Protection Regulation. Cambridge: University of Cambridge Faculty of Law, 2018. p. 15. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3050675#paper-citations-widget. Acesso em: 15 jun. 2024.

KUNER, C. Regulation of Transborder Data Flows under Data Protection and Privacy Law: Past, Present and Future. OECD Digital Economy Papers, n. 187. Paris: OECD Publishing, 2011. Disponível em: https://www.oecd-ilibrary.org/docserver/5kg0s2fk315f-en.pdf?expires=1718302635&id=id&accname=guest&checksum=D1C103188793734108A87E9F5822CC24. Acesso em: 23 maio 2024.

LAUCCI, C. The Wider Policy Framework of Ethical Behaviour: Outspoken Observations from a True Friend of the International Criminal Court. In: BERGSMO, M.; DITTRICH, V. (Ed.). Integrity in International Justice. Brussels: Torkel Opsahl Academic EPublisher, 2020. p. 871. Disponível em: https://www.legal-tools.org/doc/rz9zv6/pdf. Acesso em: 05 ago. 2024.

LEGAL UN. Draft articles on the responsibility of international organizations. 2011. Disponível em: https://legal.un.org/ilc/texts/instruments/english/draft_articles/9_11_2011.pdf. Acesso em: 20 ago. 2024.

LEGAL UN. International Law Comission. Disponível em: https://legal.un.org/ilc/. Acesso em: 20 ago. 2024.

LEXIONÁRIO. Princípio do primado do Direito da União Europeia. Disponível em: https://diariodarepublica.pt/dr/lexionario/termo/principio-primado-direito-uniao-europeia. Acesso em: 22 jun. 2024.

LING, Y. A Comparative Study Of The Privileges And Immunities Of United Nations Member Representatives And Officials With The Traditional Privileges And Immunities Of Diplomatic Agents. Washington and Lee Law Review, v. 3, n. 1. Washington: Washington and Lee Law Review, 1976. Disponível em: https://heinonline.org/HOL/LandingPage?handle=hein.journals/waslee33&div=10&id=&page=. Acesso em: 22 jul. 2024.

LOPUCKI, L. M. Court-System Transparency. Iowa Law Review, v. 94. Los Angeles: UCLA School of Law, 2007. p. 516. Disponível em: https://scholarship.law.ufl.edu/cgi/viewcontent.cgi?article=2117&context=facultypub. Acesso em: 10 ago. 2024.

LUBIN, A. Data Protection as an International Legal Obligation for International Organizations: The ICRC as a Case Study. In: BUCHAN, R.; LUBIN, A. The Rights to Privacy and Data Protection in Times of Armed Conflict. Tallinn: CCDCOE, 2022. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4115810. Acesso em: 21 ago. 2024.

LYNSKEY, O. The foundations of EU data protection law. Oxford: Oxford University Press, 2015.

MACHADO, J. Direito Internacional - do paradigma clássico ao pós-11 de setembro. 4 ed. Coimbra: Coimbra Editora, 2006.

MARTHA, R. S. J. Challenging Acts of INTERPOL in Domestic Courts. In: REINISCH, A (Ed.) Challenging Acts of International Organizations Before National Courts. Oxford: Oxford University Press, 2010.

MARTHA, R. S. J. International Financial Institutions and Claims of Private Parties - Immunity Obliges. In: CISSÉ, H. et al. International Financial Institutions and Global Legal Governance. Washington: World Bank, 2012. Disponível em: https://www.iilj.org/wp-content/uploads/2016/08/Kingsbury-et-al_International-Financial-Institutions-and-Global-Legal-Governance.pdf. Acesso em: 14 set. 2024.

MARTINS, M. S. D´Oliveira; MARTINS, Afonso D´Oliveira. Direito das Organizações Internacionais. 2ª ed. Lisboa: Associação Acadêmica da Faculdade de Direito, 1996.

MEDZINI, R. Credibility in enhanced self-regulation: The case of the European data protection regime. In: MARGETTS H. et.al. Policy & Internet, v. 13, n. 3. New Jersey: Wiley, 2021. p. 366-384. Disponível em: https://onlinelibrary.wiley.com/doi/full/10.1002/poi3.251. Acesso em: 01 jul. 2024.

MESQUITA, M. J .R. de. Justiça Internacional (Lições), Parte I – Introdução. Lisboa: AAFDL, 2010.

MESQUITA, M. J. R. de. The Court of Justice of the European Union. In: Vicente, D. M. (Ed.). Towards a Universal Justice? Putting International Courts and Jurisdictions into Perspective. Hague: Brill/Nijhoff, 2016. p. 451-467.

MINISTÉRIO PÚBLICO PORTUGAL. Acordo sobre os Privilégios e Imunidades do Tribunal Penal Internacional. Disponível em: https://www.ministeriopublico.pt/instrumento/acordo-sobre-os-privilegios-e-imunidades-do-Tribunal-penal-internacional-0. Acesso em: 21 jul. 2024.

MINISTÉRIO PÚBLICO DE PORTUGAL. Convenção sobre os Privilégios e Imunidades das Nações Unidas. Disponível em: https://www.ministeriopublico.pt/instrumento/convencao-sobre-os-privilegios-e-imunidades-das-nacoes-unidas-9. Acesso em: 15 maio 2024.

MINISTÉRIO PÚBLICO DE PORTUGAL. Convenção sobre os Privilégios e Imunidades das Organizações Especializadas das Nações Unidas. Disponível em: https://www.ministeriopublico.pt/instrumento/convencao-sobre-os-privilegios-e-imunidades-das-organizacoes-especializadas-das-nacoes-0. Acesso em: 15 maio 2024.

MINISTÉRIO PÚBLICO DE PORTUGAL. Diretrizes para a Proteção de Dados Pessoais no Ministério Público. Adotadas pela resolução 45/95 da Assembleia Geral das Nações Unidas, de 14 de dezembro de 1990. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/diretrizes-protecaodados.pdf. Acesso em: 30 mar. 2024.

MINISTÉRIO PÚBLICO DE PORTUGAL. Estatuto de Roma do Tribunal Penal Internacional. Disponível em: https://www.ministeriopublico.pt/instrumento/estatuto-de-roma-do-Tribunal-penal-internacional-22. Acesso em: 21 jul. 2024.

MINISTÉRIO PÚBLICO DE PORTUGAL. Estatuto do Tribunal Internacional de Justiça. Disponível em: https://www.ministeriopublico.pt/instrumento/estatuto-do-Tribunal-internacional-de-justica-0. Acesso em: 21 jul. 2024.

MINISTÉRIO PÚBLICO DE PORTUGAL. Protocolo Adicional à Convenção para a Proteção das Pessoas no que diz respeito ao Tratamento Automatizado de Dados Pessoais, Relativo à Interceção de Comunicações, a Equipamentos de Interceptação e à Interceção de Tráfego de Comunicações (STCE n.º 185, E.T.S. n.º 108). Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/documentos/instrumentos/protocolo_adicional_convencao_protecao_pessoas_tratamento_automatizado_dados_caracter_pessoal_aut_fluxos_transfront_dados.pdf. Acesso em: 01 abr. 2024.

MISTRY, H.; VERDUZCO, D. R. The UN Security Council and the International Criminal Court. London: Chatham House, 2012. Disponível em: https://www.chathamhouse.org/sites/default/files/field/field_document/20120316UNSecurityCouncilICC.pdf. Acesso em: 12 set. 2024.

MOEREL, L. GDPR Conundrums: The GDPR Applicability Regime, Part 1 - Controllers. Disponível em: https://iapp.org/news/a/gdpr-conundrums-the-gdpr-applicability-regime-part-1-controllers/. Acesso em: 06 abr. 2024.

MOHAY, Á. et al. The Articles on the Responsibility of International Organisations – Still Up in the Air after More Than a Decade? Pécs Journal of International and European Law, 2023/I-II. Pécs: University of Pécs, 2023. pp. 17. Disponível em: https://www.researchgate.net/publication/376254094_The_Articles_on_the_Responsibility_of_International_Organisations_-_Still_Up_in_the_Air_after_More_Than_a_Decade. Acesso em: 20 ago. 2024.

NATIONAL ARCHIVES AND RECORDS ADMINISTRATION. Executive Order 9698 - Designating public international organizations entitled to enjoy certain privileges, exemptions, and immunities. 1946. Disponível em: https://www.archives.gov/federal-register/codification/executive-order/09698.html#:~:text=With%20respect%20to%20the%20designation,privileges%2C%20exemptions%2C%20and%20immunities. Acesso em: 30 maio 2024.

NETO, J. C. Teoria geral das organizações internacionais. 2. ed. São Paulo: Saraiva, 2007.

NEW ZEALAND. The application of international law to state activity in cyberspace. Wellington: Department of the Prime Minister and Cabinet, 2020. Disponível em: https://www.dpmc.govt.nz/sites/default/files/2020-12/The%20Application%20of%20International%20Law%20to%20State%20Activity%20in%20Cyberspace.pdf. Acesso em: 21 ago. 2024.

OCDE LIBRARY. Explanatory memoranda of the OECD Privacy Guidelines. 2023. Disponível em: https://www.oecd-ilibrary.org/docserver/ea4e9759-en.pdf?expires=1720105882&id=id&accname=guest&checksum=F11F2F4D8256ECB73B6E92A029FF4E30. Acesso em: 1 jun. 2024.

OKEKE, E. C. The Tension between the Jurisdictional Immunity of International Organizations and Right of Access to Court. In: QUAYLE, P. The Role of International Administrative Law at International Organizations. Leiden: Brill, 2021. Disponível em: https://brill.com/display/book/9789004441033/BP000003.xml. Acesso em: 05 jul. 2024.

Oliveira, A. F. S. de; MIALHE, J. L. A Possibilidade de Desenvolver Pesquisas no Campo Jurídico valendo-se da Metodologia de Abordagem Qualitativa. Revista de Pesquisa e Educação Jurídica, v. 2 n. 1. Brasília: Index Law Journals, 2016. p. 40-56. Disponível em: https://indexlaw.org/index.php/rpej/article/view/158. Acesso em: 21 set. 2024.

ONU. Agreement regarding the Headquarters of the United Nations. 1947. Disponível em: https://treaties.un.org/doc/Publication/UNTS/Volume%2011/volume-11-I-147-English.pdf. Acesso em: 15 maio 2024.

ONU. Carta das Nações Unidas. Disponível em: https://unric.org/pt/wp-content/uploads/sites/9/2009/10/Carta-das-Na%C3%A7%C3%B5es-Unidas.pdf. Acesso em: 15 maio 2024.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data. Disponível em: https://doi.org/10.1787/9789264196391-en. Acesso em: 20 mar. 2024.

ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT. OECD REPORT ON ALTERNATIVES TO TRADITIONAL REGULATION. 2006. Disponível em: https://pt.slideshare.net/slideshow/alternative-to-traditional-regulation-oecd/26792583#4. Acesso em: 23 jun. 2024.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Pacto Internacional sobre Direitos Civis e Políticos. Disponível em: https://www.cne.pt/sites/default/files/dl/2_pacto_direitos_civis_politicos.pdf. Acesso em: 22 mar. 2024.

PACHOLSKA, M. Many Hands in The Black Box: Artificial Intelligence and the Responsibility of International Organizations. Hague: T.M.C. Asser Institute, 2023. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4501072. Acesso em: 12 set. 2024.

PALOMBO, T. M. Dos Tribunais “ad hoc” ao Tribunal Penal Internacional, o que mudou e o que não mudou? São Paulo: Universidade Presbiteriana Mackenzie, 2021. Disponível em: https://adelpha-api.mackenzie.br/server/api/core/bitstreams/82d7e827-11b5-4abe-9c7f-ba1e406cd067/content. Acesso em: 16 jul. 2024.

PARLIAMENT OF THE UNITED KINGDOM. General Data Protection Regulation (GDPR) Briefing Paper. Disponível em: https://researchbriefings.files.parliament.uk/documents/LLN-2017-0065/LLN-2017-0065.pdf. Acesso em: 28 mar. 2024.

PORTUGAL. Lei n.º 58/2019, de 8 de agosto. Assegura a execução, na ordem jurídica nacional, do Regulamento (UE) 2016/679 do Parlamento e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://diariodarepublica.pt/dr/detalhe/lei/58-2019-123815982. Acesso em: 21 jun. 2024.

PROENÇA, C. Tutela Jurisdicional Efetiva no Direito da União Europeia. Coimbra: Faculdade de Direito e de Economia, 2014. p. 110. Disponível em: https://estudogeral.uc.pt/bitstream/10316/26659/1/Tutela%20jurisdicional%20efetiva%20no%20direito%20da%20Uni%C3%A3o%20Europeiaa.pdf. Acesso em: 02 ago. 2024.

REES, Y. M. Article 48(5). In: KLAMBERG, M.; ANGOTTI, A (Ed.). Commentary on the Law of the International Criminal Court: The Statute. 2ed. Brussels: Torkel Opsahl

Academic EPublisher, 2023. p. 1072. Disponível em: https://www.diva-portal.org/smash/get/diva2:1822990/FULLTEXT01.pdf. Acesso em: 22 jul. 2023.

REINISCH, A. The Immunity of International Organizations and the Jurisdiction of their Administrative Tribunals. Oxford: Oxford University Press, 2008. Disponível em: https://deicl.univie.ac.at/fileadmin/user_upload/i_deicl/VR/VR_Personal/Reinisch/Publikationen/TheImmunityIOs_2008.pdf. Acesso em: 12 set. 2024.

REINISCH, A. The Immunity of International Organizations and the jurisdiction of their Administrative Tribunals. New York: Global Administrative Law Series, 2007. Disponível em: https://iilj.org/wp-content/uploads/2016/08/Reinisch-The-Immunity-of-International-Organizations-and-the-Jurisdiction-of-Their-Administrative-Tribunals-2007-2.pdf. Acesso em: 20 set. 2024.

RUARO, R. L. Privacidade e Autodeterminação Informativa Obstáculos ao Estado de Vigilância? Revista Eletrônica da UFPI, v. 2, n. 1. Teresina: UFPI, 2015. Disponível em: https://revistas.ufpi.br/index.php/raj/article/download/4505/2647. Acesso em: 14 ago. 2024.

SAMARA, C. International Responsibility of International Organizations (The Draft Articles of the International Law Commission). Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3480061. Acesso em: 21 ago. 2024.

SCROXTON, A. UN agency Unicef praised for response to accidental data leak. Disponível em: https://www.computerweekly.com/news/252470581/UN-agency-Unicef-praised-for-response-to-accidental-data-leak. Acesso em: 04 set. 2024.

SEITENFUS, Ricardo Antônio Silva. Manual das organizações internacionais. 4. ed. Porto Alegre, RS: Livraria do Advogado, 2005; DELGADO, M. M. International organizations as subjects of international law. In: DUARTE, M. L.; LANCEIRO, R. T. (Coord.). Ordem jurídica global do século XXI: sujeitos e actores no palco internacional. 1ª ed. Lisboa: AAFDL Editora, 2020. p. 259-278.

SETIAWAN, H. et al. Digitalization of Legal Transformation on Judicial Review in the Constitutional Court. Journal of Human Rights, Culture and Legal System, vol. 4, n. 2. Surakarta: Lembaga Contrarius Indonesia, 2024. Disponível em: https://jhcls.org/index.php/JHCLS/article/view/263. Acesso em: 15 jul. 2024.

SEYERSTED, F. Common Law of International Organizations. Leiden: Brill, 2008.

STERLING, T.; BERG, S. van den. War crimes Tribunal ICC says it has been hacked. Disponível em: https://www.reuters.com/world/international-criminal-court-reports-cybersecurity-incident-2023-09-19/. Acesso em: 06 set. 2024.

SUPREMO TRIBUNAL FEDERAL. RE 578543/MT - MATO GROSSO. RECURSO EXTRAORDINÁRIO. 2013. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur265485/false. Acesso em: 21 jun. 2024.

SUPREMO TRIBUNAL FEDERAL. RE 597.368/MT - MATO GROSSO. RECURSO EXTRAORDINÁRIO. 2013. Disponível em: https://jurisprudencia.stf.jus.br/pages/search/sjur271139/false. Acesso em: 21 jun. 2024.

SVENSKA RÖDA KORSET. Cyberattack on the Italian Red Cross on January 18. Disponível em: https://www.rodakorset.se/en/who-we-are/pressrum/roda-korset-berattar/cyberattack-on-italian-red-cross/. Acesso em: 04 set. 2024.

SWITZERLAND. Federal Act on Data Protection 235.1. 2020. Disponível em: https://www.fedlex.admin.ch/eli/cc/2022/491/en. Acesso em: 20 jun. 2024.

SWITZERLAND. Loi fédérale sur les privilèges, les immunités et les facilités, ainsi que sur les aides financières accordés par la Suisse en tant qu'État hôte. 2007. Disponível em: https://www.fedlex.admin.ch/eli/cc/2007/860/fr. Acesso em: 20 jun. 2024.

SWITZERLAND. Swiss Federal Act on Data Protection. 1992. Disponível em: https://www.uaipit.com/uploads/legislacion/files/0000004341_Personal%20Data.pdf. Acesso em: 20 jun. 2024.

TAMM, D. The History of the Court of Justice of the European Union Since its Origin. In: COURT OF JUSTICE OF THE EUROPEAN UNION (ED.). The Court of Justice and the Construction of Europe: Analyses and Perspectives on Sixty Years of Case-law. Hague: T. M. C. Asser Press, 2013.

THE GLOBAL FUND. Agreement between the Swiss Federal Council and the Global Fund to Fight AIDS, Tuberculosis and Malaria in view of determining the legal status of the Global Fund in Switzerland. Disponível em: https://www.theglobalfund.org/media/8551/core_headquarters_agreement_en.pdf. Acesso em: 04 jul. 2024.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. A proteção de dados pessoais tratados pelo Tribunal de Justiça da União Europeia. Disponível em: https://curia.europa.eu/jcms/jcms/p1_2699101/. Acesso em: 15 jul. 2024.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. A proteção de dados pessoais no âmbito das publicações relativas aos processos judiciais no Tribunal de Justiça. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2015-11/tra-doc-pt-div-c-0000-2015-201508723-05_00.pdf. Acesso em: 13 set. 2024.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Delegado para a proteção de dados. Disponível em: https://curia.europa.eu/jcms/jcms/p1_641404/pt/. Acesso em: 01 ago. 2024.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Registo central das atividades de tratamento. Disponível em: https://curia.europa.eu/jcms/jcms/p1_3301336/pt/. Acesso em: 13 set. 2024.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Regulamento de Processo do Tribunal Geral de 4 de março de 2015. Disponível em:

https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-08/version_consolidee_rp_pt.pdf. Acesso em: 13 set. 2024.

TRIBUNAL DE JUSTIÇA DA UNIÃO EUROPEIA. Versão consolidada do Regulamento de Processo do Tribunal de Justiça de 25 de setembro de 2012. Disponível em: https://curia.europa.eu/jcms/upload/docs/application/pdf/2024-08/rdp-cour-pt.pdf. Acesso em: 13 set. 2024.

TRIBUNAL EUROPEU DOS DIREITOS DO HOMEM. Convenção Europeia dos Direitos Humanos. Disponível em: https://gddc.ministeriopublico.pt/sites/default/files/convention_por.pdf. Acesso em: 22 mar. 2024.

U.S. DEPARTMENT OF HOMELAND SECURITY. Privacy Policy Guidance Memorandum. Washington: U.S. Department of Homeland Security, 2008. Disponível em: https://www.dhs.gov/xlibrary/assets/privacy/privacy_policyguide_2008-01.pdf. Acesso em: 20 mar. 2024.

UK PUBLIC GENERAL ACTS. International Organisations Act 1968. Disponível em: https://www.legislation.gov.uk/ukpga/1968/48. Acesso em: 30 maio 2024.

UN PRIVACY POLICY GROUP. List of member organizations that prepared and endorsed the Personal Data Protection and Privacy Principles. Disponível em: https://unsceb.org/sites/default/files/2020-10/UNPPGMembersList_Revised.pdf. Acesso em: 04 ago. 2024.

UN TRADE AND DEVELOPMENT. Data Protection and Privacy Legislation Worldwide. Disponível em: https://unctad.org/page/data-protection-and-privacy-legislation-worldwide. Acesso em: 20 mar. 2024.

UNIÃO EUROPEIA. Diretiva 95/46/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:31995L0046. Acesso em: 02 abr. 2024.

UNIÃO EUROPEIA. Disposições Práticas de Execução do Regulamento de Processo do Tribunal Geral. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:32024Q02097. Acesso em: 13 set. 2024.

UNIÃO EUROPEIA. Versão consolidada do Tratado da União Europeia - Protocolo (n. 3) relativo ao Estatuto do Tribunal de Justiça da União Europeia. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A12016M%2FPRO%2F03. Acesso em: 12 set. 2024.

UNIÃO EUROPEIA. Versão consolidada do Tratado da União Europeia - Protocolo (n. 7) relativo aos Privilégios e Imunidades da UE. https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX:12008E/PRO/07. Acesso em: 12 set. 2024.

UNICEF. Declaração Universal dos Direitos Humanos. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 22 mar. 2024.

UNICEF. UNICEF Policy on Personal Data Protection. 2020. Disponível em: https://www.unicef.org/supply/media/5356/file/Policy-on-personal-data-protection-July2020.pdf.pdf. Acesso em: 02 jul 2024.

UNITED KINGDOM. The application of international law to states' conduct in cyberspace: UK statement. Disponível em: https://assets.publishing.service.gov.uk/media/60b775388fa8f54899011dec/application-of-international-law-to-states-conduct-in-cyberspace-uk-statement.pdf. Acesso em: 21 ago. 2024.

UNITED NATIONS - CEB. Principles on Personal Data Protection and Privacy. Disponível em: https://unsceb.org/principles-personal-data-protection-and-privacy-listing. Acesso em: 04 ago. 2024.

UNITED NATIONS DEVELOPMENT PROGRAMME. UNDP Investigates Cyber-Security Incident. Disponível em: https://www.undp.org/speeches/undp-investigates-cyber-security-incident. Acesso em: 19 set. 2024.

UNITED NATIONS GENERAL ASSEMBLY. Resolution 73/266 adopted by the General Assembly on 22 December 2018. Advancing responsible State behaviour in cyberspace in the context of international security. Disponível em: https://documents.un.org/doc/undoc/gen/n18/465/01/pdf/n1846501.pdf. Acesso em: 21 ago. 2024.

UNITED NATIONS GENERAL ASSEMBLY. Resolution A/RES/63/253 - Administration of justice at the United Nations. Disponível em: https://documents.un.org/doc/undoc/gen/n08/485/97/pdf/n0848597.pdf. Acesso em: 15 set. 2024.

UNITED NATIONS HIGH COMMISSIONER FOR REFUGEES. General Policy on Personal Data Protection and Privacy. Disponível em: https://www.refworld.org/policy/strategy/unhcr/2022/en/124207. Acesso em: 19 set. 2024.

UNITED NATIONS SECRETARIAT. Comments of the United Nations Secretariat on Behalf of the United Nations System Organizations on the 'Guidelines 2/2020 on Articles 46 (2) (a) and 46 (3) (b) of Regulation 2016/679 for Transfers of Personal Data between EEA and non-EEA Public Authorities and Bodies'. 2020. Disponível em: https://edpb.europa.eu/sites/default/files/webform/public_consultation_reply/2020.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf. Acesso em: 17 maio 2023.

UNITED NATIONS SECRETARIAT. Handbook on the Legal Status, Privileges and Immunities of the United Nations. Disponível em: https://legal.un.org/ilc/documentation/english/st_leg_2.pdf. Acesso em: 24 jul. 2024.

UNITED NATIONS. Data Strategy of the Secretary-General for Action by Everyone, Everywhere. Disponível em: https://www.un.org/en/content/datastrategy/images/pdf/UN_SG_Data-Strategy.pdf. Acesso em: 04 ago. 2024.

UNITED NATIONS. Juridical Yearbook. Disponível em: https://legal.un.org/unjuridicalyearbook/pdfs/english/by_volume/1971/chpV.pdf. Acesso em: 20 set. 2024.

UNITED NATIONS. Letter to the Chair of the EDPB with attached Comments of the United Nations to Guidelines 2/2020. Disponível em: https://www.edpb.europa.eu/sites/default/files/webform/public_consultation_reply/20200.05.14_letter_to_edpb_chair_with_un_comments_on_guidelines_2-2020.pdf. Acesso em: 02 set. 2024.

UNITED NATIONS. Report of the 5th Committee. Disponível em: https://digitallibrary.un.org/record/202035?ln=fr&v=pdf. Acesso em: 16 set. 2024.

UNITED NATIONS. Resolution 351 A (iv) of 24 November 1949 - Establishment of a United Nations Administrative Tribunal. Disponível em: https://digitallibrary.un.org/record/666782?v=pdf. Acesso em: 13 set. 2024.

UNITED NATIONS. Resolution A/RES/46/182. Disponível em: https://undocs.org/Home/Mobile?FinalSymbol=A%2FRES%2F46%2F182&Language=E&DeviceType=Desktop&LangRequested=False. Acesso em: 19 set. 2024.

UNITED STATES COURT OF APPEALS. Georges v. United Nations. Disponível em: https://cases.justia.com/federal/appellate-courts/ca2/15-455/15-455-2016-08-18.pdf?ts=1471554006. Acesso em: 16 set. 2024.

UNIVERSITY OF MINNESOTA – HUMAN RIGHTS LIBRARY. Cairo Declaration on Human Rights in Islam. Disponível em: http://hrlibrary.umn.edu/instree/cairodeclaration.html. Acesso em: 22 mar. 2024.

US COURTS. Federal Rules of Civil Procedure. 2023. Disponível em: https://www.uscourts.gov/sites/default/files/civil_federal_rules_pamphlet_dec_1_2023.pdf. Acesso em: 07 ago. 2024.

VELTEC NETWORKS. UNICEF's Accidental Data Leak Highlights Importance of Employee Security Training. Disponível em: https://www.veltecnetworks.com/unicefs-data-leak/. Acesso em: 04 set. 2024.

WHITE, N. D. The Law of International Organisations. 3. ed. Manchester: Manchester University Press, 2017.

WICKREMASINGHE, Chanaka. International Organizations or Institutions, Immunities before National Courts. Max Planck Encyclopedias of International Law. Oxford: Oxford University Press, 2009. Disponível em: https://opil.ouplaw.com/display/10.1093/law:epil/9780199231690/law-9780199231690-e502. Acesso em: 9 jun. 2024.

WORLD HEALTH ORGANIZATION. Policy on use and sharing of data collected in Member States by the World Health Organization (WHO) outside the context of public health emergencies. Disponível em: https://cdn.who.int/media/docs/default-source/publishing-policies/data-policy/who-policy-on-use-and-sharing-of-data-collected-in-member-states-outside-phe_en.pdf?sfvrsn=713112d4_27. Acesso em: 03 jul. 2024.

XU, M. et al. The fourth industrial revolution: opportunities and challenges. International Journal of Financial Research, v. 9, n. 2. Toronto: Sciedu Press, 2018. p. 90-95. Disponível em: http://creo.sc-celje.si/pluginfile.php/2387/mod_resource/content/1/4.1.4_01_The%20fourth%20industrial%20revolution.pdf. Acesso em: 20 set. 2024.

ZUBOFF, S. A Era do Capitalismo de Vigilância: a Luta por um Futuro Humano na Nova Fronteira do Poder. Nova York: Intrínseca, 2021. p. 22.