Nesta edição: Eugénie Coche, Ans Kolk, Kate Robertson, Rafael A. F. Zanatta, Gabriela Vergili, Pedro Saliba, Rubens Harry Born

POLITICS

Uma publicação do Instituto Nupef Ano 13 | nº39 | out 2024

O nexo entre o ambiental e o digital

+ Quando a digitalização encontra a regulação além das fronteiras: um esclarecimento com percepções acionáveis

+ Um tratado global para combater o cibercrime - sem combater o spyware mercenário

+ Informações e governança democrática em assuntos ambientais

Nupef

POLITICS

[https://politics.org.br]

Nupef nic.br cgi.br

POLITICS
Uma publicação do Nupef [nupef.org.br] jul. 2025

A tiragem das nossas edições é pequena. Se você quiser receber gratuitamente a edição impressa, envie um e-mail para politics@nupef.org.br com seu nome, endereço completo - incluindo o CEP - e a sua área de atuação.

Todas as edições da POLI**TICS** estão disponíveis em politics.org.br

A POLI**TICS** procura aderir à terminologia e abreviaturas do Sistema Internacional de Unidades (SI), adotado pelo Instituto Nacional de Metrologia do Brasil (Inmetro). Assim, todos os textos são revisados para assegurar, na medida do possível e sem prejuizo ao conteúdo, aderência ao SI. Para mais informação: http://www.inmetro.gov.br/consumidor/unidLegaisMed.asp

ano xiii

39

ISSN: 1984-8803

[editorial]

Esta edição da poliTICs trata das relações contrastantes entre a soberania dos estados e a universalização de uma Internet única, e analisa as influências e impactos da digitalização no enfrentamento dos desafios ambientais. A edição é particularmente rica nas extensas bibliografias apresentadas nos textos.

A partir de uma análise comparada da atual legislação europeia referente a sistemas e tecnologias digitais, Eugénie Coche e Ans Kolk sintetizam os objetivos, aplicações e relação entre as cinco principais regulações europeias. O texto é uma excelente referência para as ações regulatórias a nível internacional no contexto das incompatibilidades entre as soberanias geopolíticas e a universalização de uma Internet única.

Rafael Zanatta, Gabriela Vergili e Pedro Saliba, do Data Privacy Brasil, analisam as quatro dimensões do nexo entre os temas ambientais e o contexto digital: a relação entre ampliação do acesso à informação digital e políticas ambientais bem formuladas; a dimensão do consumo de recursos energéticos na produção tecnológica; a relação entre clima e recursos hídricos nos datacentros e infraestruturas digitais; e o caráter difuso dos bens protegidos (tanto meio ambiente quanto dados pessoais).

Kate Robertson, pesquisadora sênior do Citizen Lab da Universidade de Toronto, faz uma detalhada resenha dos desafios do enfrentamento dos crimes cibernéticos no contexto transfronteiras, e analisa as deficiências e riscos do tratado de crime cibernético, cuja versão final está para ser votada ainda este ano na Assembleia Geral da ONU.

Rubens Harry Born, engenheiro civil, membro do IDEC com décadas de experiência e expertise nos temas de defesa ambiental, defende que "avançar a governança democrática ambiental, notadamente na eficaz aplicação dos direitos de acesso à informação, à participação e à justiça, deve ser compreendida como uma tarefa necessária e urgente, por um lado, e por outro, facilitada pelo acervo normativo da legislação de meio ambiente e por uma sociedade cada vez mais usuária de meios digitais de produção de conhecimentos e de relações sociais. Enfim, de construção de sociedade digital com responsabilidade ambiental."

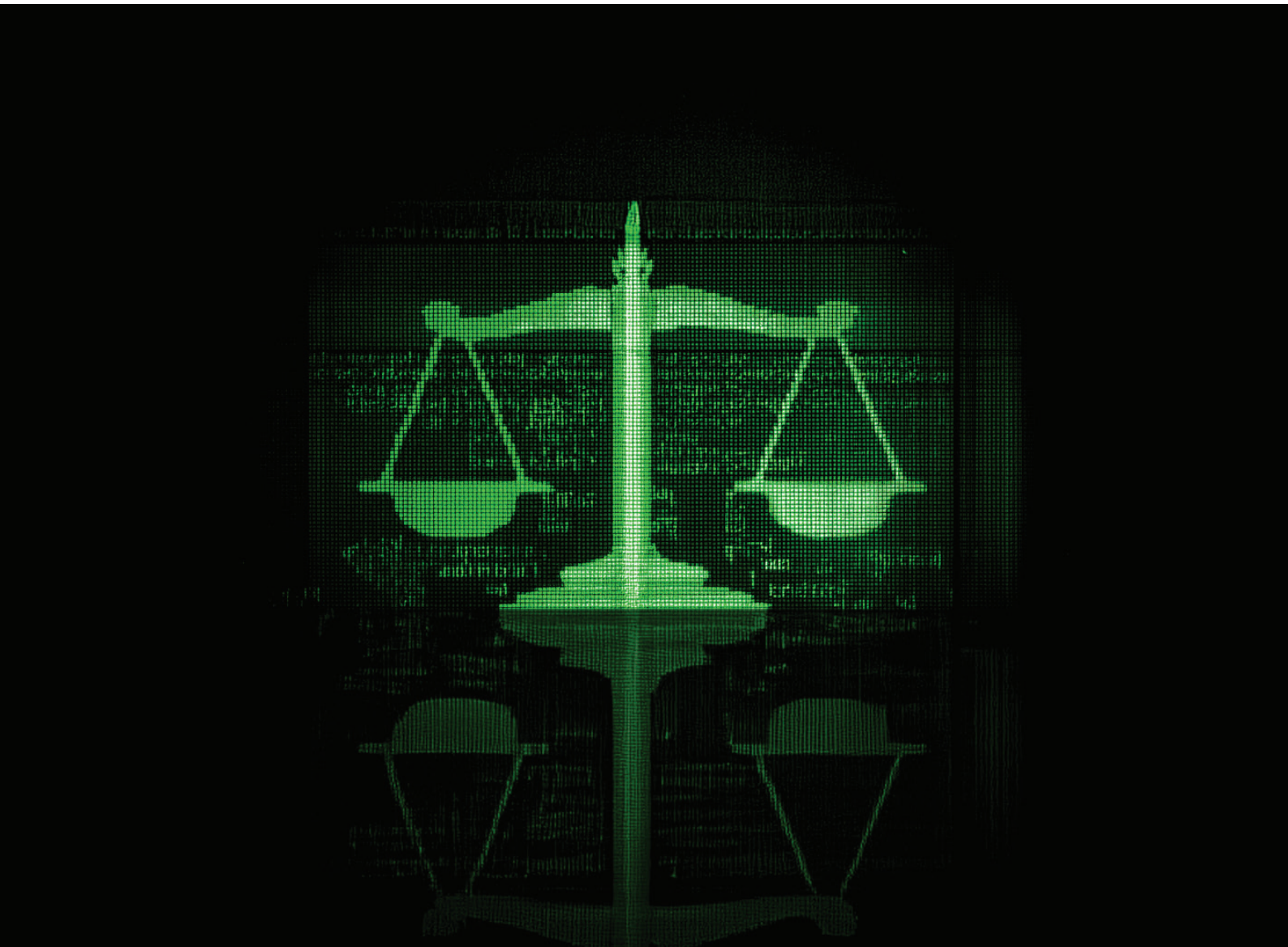
Boa leitura!

[índice]

ISSN: 1984-8803

Quando a digitalização encontra a regulação além das fronteiras:

um esclarecimento com percepções acionáveis



Tradução do original reproduzida com autorização das autoras
Coche, E., & Kolk, A. 2024. When Digitalization Meets Regulation across Borders: An Explainer with Actionable Insights. AIB Insights. https://doi.org/10.46697/001c.122505.

Eugénie Coche, Ans Kolk

Uma enxurrada de regulamentos tem surgido em todo o mundo para governar o uso, a transferência e armazenamento de dados, afetando empresas digitais e tradicionais, de todos os tamanhos. Para orientar os negócios profissionais e educadores, este artigo fornece percepções sobre os principais componentes da legislação sobre tecnologia digital e o que eles significam para diferentes tipos de empresas. Tomamos a União Europeia como ponto de partida, dada a sua definição de regras proeminente e extraterritorial, mas também refletimos sobre outras regulações digitais transfronteiras (futuras). Nossa análise de detalhes relevantes revela a necessidade que os profissionais estejam preparados e com visão de futuro, considerando as especificidades das empresas, princípios éticos convergentes internacionalmente e gerações (futuras) com consciência digital.

Introdução

Nos últimos anos, tem-se assistido a um aumento exponencial das leis que regulam o uso, o armazenamento e a transferência de dados, afetando as empresas multinacionais (EMNs/MNEs*) de formas distintas (Coche, Kolk, & Ocelík, 2024). Apesar das convergências regulatórias em países e regiões, variações – decorrentes de diferentes tradições e motivos – permanecem. Enquanto a União Europeia (UE/EU) é frequentemente caracterizada pelo seu forte enfoque nos direitos humanos, os Estados Unidos pela inovação digital e a China pela segurança nacional (Bradford, 2023), todas as jurisdições compartilham uma crescente necessidade de "soberania tecnológica" (Comissão Europeia, 2020: 3).

Assim, os estudiosos dos negócios internacionais (NIs/IBs) estão cada vez mais conscientes de que "o contexto nacional ainda im-

* Ao longo da tradução procuramos reproduzir algumas siglas relevantes em português e inglês na primeira citação das mesmas. Uma pequena tabela ao final serve de referência para todas as usadas no texto.

porta na era digital" (Meyer, Li, Brouthers, & Jean, 2023: 578). Para orientar profissionais e educadores empresariais, este artigo oferece percepções sobre os principais componentes das leis digitais e o que elas significam para diferentes tipos de EMNs. Tomamos a UE como ponto de partida, dada a sua importância definição de regras sobre esses tópicos, com o Regulamento Geral de Proteção de Dados de 2018 (RGPD/GDPR) como o primeiro caso bem conhecido sobre o assunto.

O RGPD foi introduzido para fortalecer os direitos de proteção de dados pessoais europeus. Ampliou a definição de "dados pessoais"; concedeu novos direitos aos indivíduos; impôs novas obrigações para as empresas; e ganhou relevância global através de regras extraterritoriais associadas a multas (por exemplo, Multa de € 1,2 bilhão da Meta). Ao regular empresas sediadas tanto na UE quanto fora dela, o RGPD desempenhou um papel fundamental na digitalização das EMNs. Mais recentemente, a estratégia digital da UE avançou para regular outros aspectos da digitalização (Comissão Europeia, 2020), principalmente através de cinco atos principais que complementam o RGPD (resumidos na Tabela 1). Com base numa análise jurídica e usando a empresa Alphabet como exemplo ilustrativo (devido ao seu poder de mercado e versatilidade), descobrimos as implicações distintas desses atos e identificamos três principais percepções relevantes para os NIs e as MNEs.

LEI DE SERVIÇOS DIGITAIS (LSD/DSA)

A LSD foi criada para tornar o ambiente online mais seguro, nomeadamente para combater melhor o conteúdo ilegal, conscientizar os usuários sobre práticas de publicidade, combater a desinformação e esclarecer regras de responsabilidade. Impõe obrigações de devida diligência para todos os "intermediários online", incluindo fornecedores de serviços de infraestrutura e de hospedagem, plataformas online e mercados. Essas obrigações têm como alvo o conteúdo hospedado (por exemplo, postagens em mídias sociais) e variam desde a proibição de "padrões encobertos" (que por exemplo dificultam a alteração de configurações "por padrão" por parte dos usuários) a permitir que os usuários notifiquem e descartem conteúdo ilegal.

É importante ressaltar que a lei reconhece heterogeneidade das empresas, tendo em conta o tamanho, o impacto e modelo de negócio. Micro e pequenas empresas (ou seja, menos de 50 funcionários e faturamento anual ou balanço patrimonial não excedendo €10 milhões) estão isentas de inúmeras obrigações (por exemplo, fornecer relatórios anuais de transparência) e provedores de serviços de hospedagem (por exemplo, serviços em nuvem) enfrentam menos regras do que plataformas (por exemplo, redes sociais) por serem principalmente obrigados a ter mecanismos de "notificação e ação" em vigor. Entre as plataformas, os mercados online enfrentam desafios adicionais obrigações (por exemplo, também coletar informações sobre seus comerciantes); enquanto "plataformas e motores de busca online de grande dimensão" (PMBGs/VLOPs) -- operados como tal pela Comissão Europeia com base no número de usuários ativos (ou seja, mais de 45 milhões) -- estão sujeitos ao regime mais rigoroso.

Como PMBG, a Alphabet tem obrigações para com o YouTube, incluindo a necessidade de conduzir avaliações anuais de "riscos sistêmicos" para combater riscos pré-definidos (por exemplo, processos eleitorais ilegítimos) e aplicar medidas de mitigação adequadas (por exemplo, adaptação de algoritmos).

Como PMBG, a Alphabet tem obrigações para com o YouTube, incluindo a necessidade de conduzir avaliações anuais de "riscos sistêmicos" para combater riscos pré-definidos (por exemplo, processos eleitorais ilegítimos) e aplicar medidas de mitigação adequadas (por exemplo, adaptação de algoritmos).

Tabela 1. Resumo de Atos e implicações para a Alphabet

	Objetivos	Aplicação extraterritorial	Obrigações para as firmas			Implicações concretas para a Alphabet	
			Modelo de negócios		Tamanho	Obrigações legais	Ações práticas
LSD/ DSA	Trata de conteúdo ilegal online	Aplica-se qual seja o local ou o estabelecimento da firma [Art.2(1)]	Aplicável só a intermediários online	Menos obrigações para PSIs. Entre plataformas, mais obrigações para mercados	Menos obrigações para PMEs/ SMEs. Mais obrigações para PMBGs/ VLOPs	Youtube (PMBGs/ VLOPs): - mais transparência com os usuários - ferramentas de moderação de conteúdo - avaliações anuais de risco sistêmico	Youtube bloqueou anúncios dirigidos a menores e criou um novo centro de transparência
LMD/ DMA	Competição justa	Ibidem [Art.1(2)]	Aplica-se só a "gatekeepers" que oferecem serviços centrais de plataformas	Obrigações variam pelo tipo de plataformas (aplicativos de lojas, motores de busca)	Limite estabelecido cobre apenas firmas muito grandes	Google Search não pode priorizar seus serviços de lojas Google em relação a competidoras	A Google introduziu "unidades agregadoras" e "chips de refinamento" em seus serviços de busca (facilitando comparação de resultados pelos usuários)
LD/DA	Aperfeiçoa acesso a IdC/ IoT e a dados do setor públco	Ibidem [Art.1(3)]	Obrigações distintas para fabricantes de IdC/IoT ou provedores de serviços de processamento de dados (incluindo serviços de nuvem e de borda)	Portais não deveriam receber dados; PMEs/ SMEs não deveriam compartilhar dados.	Dados do smartwatch do Google devem, por padrão, ser facilmente acessíveis a seus usuários e, sob pedido, a concorrentes não-Google do mercado	A Google introduziu suas "APIs caseiras" para permitir compartilhamento de dados entre dispositivos caseiros intelingentes.	
LGD/ DGA	Aprimora confiabilidade no compartilhamento de dados	Ibidem [Art.11(3) jo. 19(3)]	Obrigações distintas para altruismo de dados e firmas de intermediação de dados	N/A	Notificar a autoridade competetne da UE sobre futuro serviço de intermediação de dados e criar uma entidade legal separada	n/a (até o momento a Alphabet não oferece estes serviços)	
LIA/ AIA	Garantir a confiabilidade e a imparcialidade dos sistemas de IA	Ibidem [Art.2(1)}	- Diferentes obrigações para provedores de IA, implantadores, importadores e distribuidores - Certos modelos de negócios baseados em IA (por exemplo, sistemas de pontuação social; modelos de IA de propósito geral) são proibidos ou regulamentados de maneiras específicas	Tratamento favorecido para pequenas e médias empresas	O Gemini tem que alertar seus usuários que estão interagindo com um sistema de IA e toda informação técnica sobre seu modelo de IA tem que ser mantida atualizada	O Google aderiu à Coalizão para Proveniência e Autenticidade de Conteúdo para promover a transparência no conteúdo gerado por IA	

LEI DE MERCADOS DIGITAIS (LMD/DMA)

Complementando a LSD, a LMD aborda principalmente desequilíbrios de mercado para garantir que o mercado digital seja o mais contestável e aberto possível. Para entender sua razão de ser, uma mera referência ao caso do Google Shopping (Persh, 2021), que começou em 2010, mas ainda é debatido, é suficiente: o mecanismo de busca destacava seus próprios serviços no topo dos resultados, relegando concorrentes, mas a UE só poderia intervir depois de os danos terem ocorrido. A LMD procura ajudar a UE a prevenir comportamentos anticompetitivos. Portanto, ela impõe obrigações e restrições aos "gatekeepers" – plataformas dominantes capazes de distorcer os mercados digitais a seu favor. Seis empresas – todas estrangeiras, incluindo a Alphabet – atingiram o limiar cumulativo da lei quando esta foi adotada, sendo importantes na UE em volume de negócios anual (pelo menos € 7,5 bilhões) e atuando como portas de entrada para os negócios (ou seja, 45 milhões de usuários ativos mensais na UE e dez mil usuários ativos empresariais anuais na UE nos três últimos exercícios financeiros). As empresas designadas como tal devem abster-se proativamente de se envolverem em práticas desleais. Isso inclui a proibição de combinar dados pessoais dos usuários em plataformas distintas, de dar preferência a seus próprios serviços ou de "prender" usuários.

O Google Android, por exemplo, não tem mais permissão para forçar seus usuários a escolher o Google Chrome como mecanismo de busca padrão ou Google Play como loja de aplicativos. Da mesma forma, a LMD introduz obrigações para permitir que os usuários acessem e compartilhem dados, intimamente interligados com a estratégia de dados explicada abaixo.

LEI DE DADOS (LD/DA)

A estratégia de dados da UE – uma parte da sua estratégia digital – visa otimizar o valor dos dados em todos os setores econômicos. Complementa iniciativas anteriores de liberalização de dados, como o direito de portabilidade de dados do RGPD (ou seja, para que os indivíduos acessem dados sobre eles) e leis setoriais específicas que exigem que empresas compartilhem dados com terceiros (por exemplo, "open banking"). Entre as novidades, a LD apresenta obrigações de compartilhamento de dados relacionados à Internet das Coisas (IdC/IoT) – ou seja, provenientes de dispositivos conectados. Estabelece regras de partilha de dados entre empresas, entre estas e consumidores, e entre empresas e governos, tendo em conta a heterogeneidade das empresas (por exemplo, os "gatekeepers" não devem receber dados; as micro e pequenas empresas não devem partilhá-los). Uma obrigação fundamental para os fabricantes de IdC é projetar e fabricar seus produtos conectados de tal forma que os usuários e terceiros possam "por padrão" (ou seja, sem intervenção do usuário) aceder aos dados gerados gratuitamente.

Portanto, a Alphabet precisa garantir que os dados de seu "smartwatch" Google possam ser facilmente acessados por serviços não-Google (p.ex., manutenção). A lei obriga ainda as empresas a compartilhar dados de forma "justa, razoável e não discriminatória", com restrições aos custos de compensação (por exemplo, claramente com base em custos das empresas para coletar, produzir e disponibilizar os dados solicitados) e à utilização desses dados para o desenvolvimento de produtos competitivos. Por exemplo, os destinatários dos dados não podem usar os dados do "smartwatch" do Google para criar um "smartwatch" próprio.

LEI DE GOVERNANÇA DE DADOS (LGD/DGA)

Complementando a LD, a LGD visa tornar os dados mais acessíveis e promover a inovação baseada em dados. Diferente da LD, que diz respeito a situações de partilha obrigatória de dados, a LGD busca estabelecer confiança para práticas voluntárias de compartilhamento de dados. Inclui regras para encorajar o crescimento de dois tipos de serviços: organizações de "altruísmo de dados" e "intermediários de dados". A primeira categoria permite que indivíduos e empresas compartilhem seus dados para fins altruístas, como o combate à poluição. Essas organizações podem ser registradas como confiáveis se não tiverem fins lucrativos e atenderem a certos requisitos do "livro de regras" da UE (por exemplo, os dados devem ser armazenados com segurança).

Em contraste, os serviços de intermediação de dados são de empresas com fins lucrativos que devem atuar como terceiros neutros em transações de compartilhamento de dados (por exemplo, mercados de dados como o Dawex francês). Devido aos poderes de mercado significativos de negócios baseados em plataformas, a LGD exige que essas empresas (potencialmente Alphabet, caso desenvolva tais serviços) notifiquem as autoridades competentes da UE. Elas também precisam cumprir obrigações como o uso justo de dados (por exemplo, os dados não podem ser usado para outros fins que não o descarte de dados), desagregação de serviços de dados (em uma entidade legal separada) e preços justos e não discriminatórios.

LEI DE INTELIGÊNCIA ARTIFICIAL (LIA/AIA)

A LIA regulamenta o uso de sistemas de IA, que se referem a qualquer sistema baseado em máquinas que permita às empresas gerar "resultados como previsões, conteúdo, recomendações, ou decisões que podem influenciar ambientes físicos ou virtuais". Para tornar esses sistemas confiáveis, a lei impõe obrigações e restrições a todos os agentes da cadeia de valor da IA: provedores de IA (ou seja, desenvolvedores de sistemas), implantadores (ou seja, usuários de sistemas), importadores e distribuidores.

Crucialmente, como parte da abordagem baseada em risco da UE, todos os atores devem examinar a finalidade do sistema de IA e, por sua vez, avaliar seus riscos, que podem ser: inaceitáveis; altos; limitados; ou mínimos. A primeira categoria envolve uma lista exaustiva de práticas de IA (por exemplo, sistemas de pontuação social) que são proibidas. A segunda diz respeito aos sistemas de IA que envolvem grandes riscos sociais, como sistemas automatizados de contratação ou de pontuação de crédito, que a lei permite caso todas as suas obrigações de longo alcance sejam cumpridas. Isso inclui a necessidade dos fornecedores de IA realizarem "avaliações de conformidade" pré-comercialização (seguindo requisitos técnicos, legais e éticos) antes de colocarem os seus serviços no mercado da UE, e os implementadores de IA realizarem "avaliações de impacto sobre direitos fundamentais" (incluindo a identificação de riscos específicos e medidas de supervisão humana). A terceira categoria é vista como menos arriscada (por exemplo, chatbots, geradores de deepfake, modelos de IA de uso geral (IAUG/GPAI)) para os quais a lei exige principalmente transparência para com os usuários e fornecedores de sistemas a jusante, com obrigações adicionais para os modelos IAUG que apresentam "riscos sistêmicos (ou seja, ter capacidade de alto impacto, ter a capacidade computacional dos modelos de treinamento em consideração). Finalmente, a LIA sujeita sistemas de IA de risco mínimo, como filtros de spam ou videogames habilitados para IA, a códigos de conduta voluntários.

Portanto, caso o serviço Gemini da Alphabet (entendido como o "concorrente" do ChatGPT)

seja classificado como um modelo de IAUG de risco sistêmico, suas obrigações incluem a necessidade de avaliar e mitigar tais riscos, realizar avaliações de modelos e implementar medidas adequadas de cibersegurança.

RUMO A PERCEPÇÕES ACIONÁVEIS

As cinco leis acima discutidas têm relevância direta para as empresas da UE e para as EMNs sediadas em outros países não pertencentes à UE, como o exemplo da Alphabet bem ilustra. Crucialmente, essas regulamentações abrangem uma série de questões relacionadas a dados que correspondem a processos em todo o mundo. Curiosamente, embora a UE não tenha grandes empresas de tecnologia "nacionais", a sua definição de regras estende-se para além da região. Esta extraterritorialidade também se aplica a algumas regulamentações da UE em outros domínios como a sustentabilidade (ver exemplos na Tabela 2).

Enquanto o chamado "efeito Bruxelas" (Bradford, 2019), em que a UE influencia as mudanças regulatórias e corporativas fora de suas fronteiras através de seus primeiros movimentos regulatórios, pode ser visto como negativo (oneroso) ou positivo (governança baseada em valores), postulamos que as restrições à digitalização são simplesmente uma realidade a ser enfrentada – com mais por vir, também em outros países (cf. Tabela 2). Além disso, com a "geração Z" e "geração Alfa" como estudantes e (futuros) funcionários, a conscientização digital está se tornando generalizada. Para estarem preparados, os profissionais e educadores empresariais podem usar três percepções de nossa análise jurídica.

Em primeiro lugar, o efeito Bruxelas, que já era evidente com o RGPD (Bradford, 2019; Coche, Kolk, & Ocelík, 2024), provavelmente se estenderá às leis discutidos em nosso artigo, mais notavelmente a LIA (Siegmann & Anderljung, 2022). Isso é importante, uma vez que estas leis são "regulamentos" (não "diretivas"), tornam-se imediatamente leis nacionais dos Estados-Membros, tendo assim uma aplicação imediata em toda a UE.

Assim, para as empresas com atividades na UE, isto proporciona clareza e pode facilitar o seu crescimento, não apenas dentro, mas também fora da UE. Isto também significa que as EMNs sediadas no estrangeiro poderão ser beneficiadas se tiverem uma visão de futuro e implementarem imediatamente as regras emergentes da UE, estando assim preparadas caso outros países adotem em futuro (próximo) regulações similares (Tabela 2). Isso poderia criar uma vantagem competitiva em relação aos parceiros comerciais (globais) ou evitar uma desvantagem, especialmente quando os consumidores estão cada vez mais conscientes de seus direitos de privacidade de dados. Portanto, deixar o mercado da UE – como o "X" sugeriu em relação à LSD – pode não ser a resposta mais adequada tendo em vista as tendências regulatórias futuras mundialmente.

Em segundo lugar, uma vez que estas leis afetam todas as EMNs e não apenas empresas exclusivamente digitais (cf. Stallkamp, 2021), recomendamos a todos profissionais que façam da governança de dados uma prioridade, considerando as especificidades de suas empresas. Isso pode envolver o projeto de "front-end" (por exemplo, mais transparência para os usuários) e mudanças no sistema de "back-end" (por exemplo, tecnologias de compartilhamento de dados); bem como reconfigurações de modelos de negócios e/ou cadeias de valor (por exemplo, contratantes de IA responsáveis).

No entanto, conforme ilustrado pela mudança no modelo de negócios "pague ou aceite" da Meta (ou seja, os usuários pagam ou consentem com a publicidade comportamental) – controverso sob o RGPD (EDPB, 2024), a LMD e a LSD – as empresas devem abordar

essas leis de forma holística (ou seja, considerando todas as dimensões relevantes). Em vista da LIA, isso também significa para as EMNs a adoção de uma abordagem baseada no risco em relação a todas suas atividades digitais e, portanto, avaliá-las à luz de direitos humanos e princípios éticos convergentes internacionalmente (por exemplo, "justiça"; "confiabilidade"; OCDE, 2024). Além de ajudar as EMNs a economizar custos de (futuros) litígios e reputação, isso também pode ajudar a atender os interesses dos acionistas "conscientes da privacidade" (SEC, 2023: proposta 15).

Terceiro, para favorecer esse comportamento empresarial orientado pela ética, recomendamos que os educadores empresariais façam com que os seus alunos (ou seja, futuros profissionais, também usuários de serviços digitais) sejam totalmente conscientes das implicações dos direitos humanos em relação à gestão de dados e às tecnologias baseadas em IA. No mínimo, isso requer deixar de lado a ideia de que as empresas tem a "posse" dos dados dos clientes, que é legalmente inválido, mas ainda sugerido na literatura de NIs (cf., Madan, Savani e Katsikeas, 2022). Na verdade, os dados de natureza não competitiva, aliados ao seu potencial de valor infinito (por exemplo, big data) e aos envolvimentos com direitos humanos (por exemplo, privacidade de dados), torna-os um objeto de propriedade ambígua (cf. Geiregat, 2022). Isso explica o surgimento de novos modelos de governança, bem como as crescentes obrigações de compartilhamento de dados das EMNs (Coche, Kolk, & Dekker, 2024: 19).

CONCLUSÕES

Este artigo tomou a UE como exemplo para mostrar como os NIs são afetados pela regulamentação. Discutimos cinco leis que moldam a digitalização das EMNs não só dentro, mas também fora da UE, e usamos o caso da Alphabet para ilustrar como essas leis complementam-se e influenciam as atividades de uma empresa de tecnologia estrangeira de grande porte (cf. Tabela 1). Nossa a exposição do panorama regulatório digital da UE, com atenção às especificidades de cada lei, afasta-se dos traços gerais frequentemente adotados em estudos dos NIs.

O efeito Bruxelas influente e potencial dessas leis contrasta com as suposições de que é bastante excepcional para as nações "coordenarem seus quadros jurídicos a nível internacional, por exemplo, através da OMC/WTO ou da UE" (Meyer et al., 2023: 582). Da mesma forma, quando se tem apenas uma visão panorâmica destas leis, os gestores de MNEs ou educadores dos NIs podem associá-las a (novo) "tecnonacionalismo" (Luo & Van Assche, 2023) ou a medidas geopolíticas. No entanto, as leis da UE incorporam principalmente uma ambição de garantir que as tecnologias – independentemente dos países de origem das empresas – estão totalmente alinhadas com os valores europeus (Irion, Burri, Kolk e Milan, 2021).

Enquanto o pacote regulatório resultante pode afetar particularmente empresas sediadas no exterior, isso se deve ao seu poder de mercado e peculiaridades, não à sua nacionalidade. Embora percebamos que as opiniões sobre os prós e os contras da abordagem da UE possam divergir amplamente, o nosso artigo pretendeu fornecer uma abordagem um pouco mais aprofundada, incluindo também exemplos de outros regulamentos transfronteiras (futuros) que incluem extraterritorialidade, propostos por outros países ao redor do mundo (Tabela 2). Praticantes e educadores empresariais podem beneficiar-se com nossos esclarecimentos, também em suas interações com gerações digitalmente conscientes interessadas nos aspectos sociais e éticos da digitalização.

Tabela 2. Exemplos de definidores de regras (futuros) na (e fora da) UE			
	Leis (propostas)	**Escopo extraterritorial**	**Similaridades com as leis digitais da UE**
Leis e políticas digitais não europeias	Lei de Mercados Digitais e Lei de Competição e Consumidores do Reino Unido (2022)	Aplica-se também a firmas não europeias	Impõe obrigações preventivas sobre firmas com "status de mercado estratégico" (similar à LMD em relação a "gatekeepers")
	Ordem Executiva dos EUA sobre Desenvolvimento e Uso Seguro, Protegido e Confiável da Inteligência Artificial (2023)	Impõe obrigações de informação a revendedores estrangeiros de IcuS/IaaS (ex.: nuvem) dos EUA, em relação ao treinamento de MLGs/ LLMs de IA	Apesar de ser apenas uma orientação (não uma lei) para empresas privadas (diferente da LIA/AIA), mostra um compromisso com a abordagem de risco e baseada em princípios da regulação de IA, incluindo respeito a privacidade e direitos civis)
	Projeto de Lei de Inteligência Artificial e Dados do Canadá (2022)	Aplica-se também ao comércio internacional de sistemas de IA	Avaliação baseada em risco e classificação de sistemas de IA (similar à LIA/AIA)
	Proposta de regulação da IA, Brasil (2023)	Também se aplica a firmas estrangeiras que desenvolvem e/ou utilizam sistemas de IA no Brasil	Idem
	Regulação sobre Direitos dos Dados dos Consumidores, Austrália (2020)	Também se aplica a dados do consumidor gerados/coligidos fora da Austrália	Impõe obrigações de compartilhamento de dados em vários setores, a começar dos bancos (em geral se alinha à LD/DA já que pode aplicar-se a dados de IdC/IoT no futuro)
	Projeto de Lei do Brasil sobre Liberdade, Responsabilidade e Transparência na Internet (2020)	Também se aplica a serviços de mídia social, motores de busca e mensagem instantânea por firmas estrangeiras a cidadãos brasileiros	Impõe obrigações de transparência e responsibilização em relação a conteúdo sediado (similar à LSD)
Leis da UE sobre Sustentabilidade	Diretiva de Informações sobre Sustentabilidade Corporativa (2022)	Também impõe obrigações de informação a empresas não europeias	Abordagem baseada em risco das atividades digitais das firmas ao impor obrigações de transparência em relação a riscos para direitos humanos (incluindo privacidade de dados)
	Diretiva de Sustentabilidade da Diligência Devida Corporativa (2024)	Também impõe obrigações de avaliação e mitigação de risco a empresas não europeias	Ibidem, ao impor obrigações de devida diligência em relação aos riscos para os direitos humanos (incluindo privacidade de dados) nas cadeias de valor das empresas

TRADUÇÃO DAS SIGLAS

Português	Inglês	Significado
EMN(s)	MNE(s)	Empresa(s) multinacional(is)
EU	UE	União Europeia
IA	AI	Inteligência artificial
IcuS	IaaS	Infraestrutura como um serviço
IAUG	GPAI	Inteligência artificial de uso geral
IdC	IoT	Internet das coisas
LD	DA	Lei de Dados
LGD	DGA	Lei de Governança de Dados
LIA	AIA	Lei de Inteligência Artificial
LMD	DMA	Lei de Mercados Digitais
LSD	DSA	Lei de Serviços Digitais
MLG	LLM	Modelo de Linguagem Grande
NI(s)	IB(s)	Negócio(s) internacional(is)
OMC	WTO	Organização Internacional de Comércio
PMBG(s)	VLOP(s)	Plataforma(s) e motor(es) de busca online de grande dimensão
PME(s)	SME(s)	Pequenas e médias empresas
RGPD	GDPR	Regulamento Geral de Proteção de Dados

Eugénie Coche *é doutoranda na Escola de Negócios, Universidade de Amsterdã, Holanda. Com formação em direito da informação, seus interesses de pesquisa estão na intersecção entre direito e negócios internacionais, com foco particular nas implicações empresariais e sociais das políticas de digitalização. No centro do seu projeto atual, financiado pelo ABN AMRO, está explorando a tensão entre privacidade de dados, segurança e inovação, além de descobrir como as multinacionais enfrentam os desafios transfronteiriços associados.*

Ans Kolk *é professora titular na Universidade de Amsterdã, Amsterdam Business School, Holanda. Suas áreas de atuação e expertise estão em responsabilidade social corporativa, desenvolvimento e sustentabilidade, especialmente em relação a empresas internacionais e suas interações com reguladores e outras partes interessadas. Uma corrente de pesquisa, na qual ela publicou extensivamente em meios de comunicação empresariais e interdisciplinares, envolve as implicações sociais, éticas e ambientais de novas tecnologias baseadas em dados e estratégias de digitalização. Para mais informações, consulte http://www.anskolk.eu/*

As autoras, que autorizaram a publicação desta versão em português, agradecem os três revisores anônimos por seus comentários perspicazes e aprofundados sobre nossos originais e artigo revisado, e ao editor por seu apoio. Publicado originalmente em agosto de 2024. Para contato: akolk@uva.nl.

Referências

Bradford, A. 2019. The Brussels effect: How the European Union rules the world. Oxford University Press.

Bradford, A. 2023. Digital empires: The global battle to regulate technology. Oxford University Press. https://doi.org/10.1093/oso/ 9780197649268.001.0001.

Coche, E., Kolk, A., & Dekker, M. 2024. Navigating the EU data governance labyrinth: A business perspective on data sharing in the financial sector. Internet Policy Review, 13(1): 1–32.

Coche, E., Kolk, A., & Ocelík, V. 2024. Unravelling cross-country regulatory intricacies of data governance: The relevance of legal insights for digitalization and international business. Journal of International Business Policy, 7: 112–127.

EDPB. 2024. Opinion 08/2024 on valid consent in the context of consent or pay models implemented by large online platforms. Bruxelas.

European Commission. 2020. Shaping Europe's digital future. Luxemburgo: European Union Publication Office.

Geiregat, S. 2022. Who owns 'your' (business's) digital data? New EU law in the making. https://blogs.law.ox.ac.uk/oblb/blog-post/2022/12/who-owns-your-businesss-digital-data-new-eu-law-making.

Irion, K., Burri, M., Kolk, A., & Milan, S. 2021. Governing "European values" inside data flows: Interdisciplinary perspectives. Internet Policy Review, 10(3): 1–14.

Luo, Y., & Van Assche, A. 2023. The rise of techno-geopolitical uncertainty: Implications of the United States CHIPS and Science Act. Journal of International Business Studies, 54: 1432–1440.

Madan, S., Savani, K., & Katsikeas, C. S. 2022. Privacy please: Power distance and people's responses to data breaches across countries. Journal of International Business Studies, 54: 731–754.

Meyer, K. E., Li, J., Brouthers, K. D., & Jean, R.-J. "Bryan." 2023. International business in the digital age: Global strategies in a world of national institutions. Journal of International Business Studies, 54: 577–598.

OECD. 2024. Recommendation of the Council on artificial intelligence. https://legalinstruments.oecd.org/en/instruments/OECD-LEGAL-0449.

Persh, J. 2021. Google Shopping: The general court takes its position. https://competitionlawblog.kluwercompetitionlaw.com/2021/11/15/google-shopping-the-general-court-takes-its-position/.

SEC. 2023. Notice of 2023 annual meeting of stockholders and proxy statement. Califórnia: United States Securities and Exchange Commission.

Siegmann, C., & Anderljung, M. 2022. The Brussels effect and artificial intelligence: How EU regulation will impact the global AI market. Centre for the Governance of AI. https://cdn.governance.ai/Brussels_Effect_GovAI.pdf.

Stallkamp, M. 2021. After Tik Tok: International Business and the Splinternet. AIB Insights, 21(2).

https://doi.org/10.46697/001c.21943.

O nexo entre o ambiental e o digital

Rafael A. F. Zanatta, Gabriela Vergili e Pedro Saliba

A grande transformação produzida pelo uso das tecnologias da informação e sistemas de inteligência artificial tem produzido um debate novo e muito pertinente sobre a relação entre sustentabilidade ambiental e o atual modelo de capitalismo informacional (Cohen, 2019), caracterizado por datificação, acumulação e extrativismo de dados (Sadowski, 2019).

Essa relação é bastante abrangente, pois são elementos inseparáveis. Como já argumentou Stefano Quintarelli no seu livro Capitalismo Immateriale, toda a infraestrutura informacional da Internet, e sua amplíssima camada de aplicações na qual operam as grandes corporações de hoje, depende de um conjunto de infraestruturas físicas e recursos biológicos (Quintarelli, 2019). Bits e computadores exigem suportes físicos. Organizações civis como Association for Progressive Communication também têm argumentado que, pensar o avanço da tecnologia e do digital hoje (APC, 2021), implica em considerarmos as cadeias de produção de minérios e lítio que permitem a produção de microprocessadores (APC, 2023). A "nuvem", afinal, é "material" (Monserrate, 2022).

A maior capacidade computacional implica em datacenters de altíssima geração, que demandam alto consumo energético e crescente consumo de recursos hídricos (Hogan, 2015). Dados compilados pela UNCTAD mostram que, desde 2010, os usuários globais da internet mais que dobraram e o tráfego de dados se expandiu 25 vezes. Um aumento nas atividades online, como streaming de vídeos e download de arquivos, demanda mais energia e gera mais emissões. Os data centers e redes que alimentam serviços online e em nuvem geram cerca de 1% das emissões globais de gases de efeito estufa (GEE) relacionadas à energia. E dispositivos, data centers e redes de TIC respondem por 6% a 12% do uso global de energia, de acordo com o Painel Internacional sobre Mudanças Climáticas (UNCTAD, 2023).

Neste ensaio, argumentamos que a intersecção entre o ambiental e o digital na sociedade contemporânea configura-se em um "nexus" que se desdobra em múltiplas dimensões, envolvendo desde o acesso à informação até o impacto ambiental da infraestrutura digital. Este ensaio explora três dimensões centrais dessa intersecção: (1) a ampliação do acesso à informação digital e sua relação com políticas ambientais bem formuladas; (2) o consumo de recursos energéticos na produção tecnológica; e (3) a interação entre clima, recursos hídricos e datacenters.

Acreditamos que este nexus, que é complexo e envolve muitas camadas de interseção, apresenta-se como agenda a ser explorada pelas organizações da sociedade civil e pelos institutos de pesquisa no Brasil, como os mobilizados no G20 (T20 Brasil, 2024). Exploramos, a seguir, três dimensões dessa intersecção. Buscamos apresentar exemplos claros, com base na literatura especializada em estudos de ciência e tecnologia.

I. Ampliação do acesso à informação e políticas ambientais

O Acordo de Escazú é o instrumento jurídico que mais bem exemplifica a primeira dimensão desse nexus entre o ambiental e o digital, por meio dos direitos fundamentais de acesso à informação e sua relação crucial para o avanço de políticas ambientais (Cepal, 2018). Elaborado com grande participação brasileira, o Acordo de Escazú é um tratado internacional sobre acesso à justiça e sobre as condições nas quais Estados precisam se esforçar para garantir os direitos fundamentais de acesso à informação para jornalistas e lideranças ambientais (Data Privacy Brasil, 2023). A garantia do acesso à informação como direito fundamental é pré-condição dos exercícios cívicos de cidadania, que habilitam lideranças e organizações cívicas a monitorar os impactos ambientais em seus territórios, lutando por justiça climática e por responsabilização dos agentes envolvidos com processos de desflorestamento.

O acordo também considera a realidade fática ao abordar a necessidade de proteção dos defensores de direitos humanos em questões ambientais, mais um ponto em que a proteção de dados pessoais, ainda que não apresentada expressamente no texto, pode ser uma ferramenta chave para resguardar outros direitos e contribuir para avanços na pauta ambiental.

Apesar de o Brasil não ter introduzido em seu ordenamento jurídico o Acordo de Escazú, o país tem uma tradição jurídica orientada à proteção ambiental, que também influencia o campo dos direitos digitais (Zanatta, 2023). O Código Florestal é um exemplo desta tradição, que busca concretizar valores previstos na Constituição Federal (Brasil, 2012). É em razão do Código Florestal que surgiram políticas públicas como o Cadastro Ambiental Rural, que busca organizar as informações sobre propriedade rural no Brasil e permitir formas efetivas de monitoramento de cumprimento das regras de proteção das florestas no Brasil (Vergili & Saliba, 2023).

A relação entre a ampliação do acesso à informação digital e a efetividade das políticas ambientais se materializa em iniciativas como o Cadastro Ambiental Rural (CAR). Esta infraestrutura pública digital é um exemplo notável de como o acesso a dados pode potencializar a eficácia da regulação ambiental (Ministério da Gestão e Inovação em Serviços Públicos, 2023; Benelli et al., 2024). O CAR permite o mapeamento e monitoramento das propriedades rurais, facilitando a identificação de áreas desmatadas ilegalmente.

A correta interpretação da Lei Geral de Proteção de Dados Pessoais (LGPD), que não impede a divulgação de dados de proprietários envolvidos em desmatamento, mostra a possibilidade de conciliar a proteção de dados pessoais com o direito à informação (Vergili & Saliba, 2023). Nesse contexto, a transparência dos dados se torna um aliado essencial na implementação de políticas públicas ambientais, permitindo um monitoramento mais rigoroso e, consequentemente, uma maior responsabilização dos agentes envolvidos em práticas ilegais (Arcoverde; Ramos; Zanatta, 2021). Bases de dados públicas que já contém informações necessárias para o cumprimento de preceitos da legislação ambiental devem ser utilizadas para esse fim, quando a legitimidade deste uso puder ser amparada pelos requisitos da LGPD e pela persecução do interesse público.

No entanto, a prática atual do Poder Público tem sido reforçar medidas de opacidade já existentes utilizando a LGPD para justificar restrições de acesso e sigilo a dados pessoais de potenciais desmatadores, ainda que haja fortes indícios de ilegalidades (Vergili & Saliba, 2023). Nesse sentido, o Estado brasileiro limita o controle social de políticas am-

bientais ao perpetuar limites à transparência pública de bases como o CAR.

2. Consumo de recursos energéticos na produção tecnológica

A expansão da capacidade computacional, impulsionada pela crescente demanda por serviços digitais, tem gerado um aumento significativo no consumo de recursos energéticos.

Um único data center pode consumir o equivalente a eletricidade de cinquenta mil lares. A 200 terawatts-hora (TWh) anualmente, os data centers devoram coletivamente mais energia do que alguns estados-nação (Monserrate, 2022). Apenas 6–12 por cento da energia consumida é dedicada a processos computacionais ativos. O restante é alocado para resfriamento e manutenção de cadeias e mais cadeias de dispositivos de segurança redundantes para evitar tempo de inatividade dispendioso (Monserrate, 2022).

Os datacenters, que sustentam a infraestrutura digital global, são grandes consumidores de energia, o que levanta preocupações ambientais. Pesquisas apontam que, apesar do discurso de ser uma tecnologia verde, as emissões de carbono de sistemas de inteligência artificial tendem a contribuir para as mudanças climáticas diante do consumo energético (Nordgren, 2022).

Dados mostram que a operação desses centros de dados pode consumir tanta energia quanto pequenas cidades, o que tem levado a discussões sobre a necessidade de regulamentações específicas, como abertura de dados e metodologias uniformes para mensuração de eficiência energética em data centers com enfoque em sustentabilidade (De Brito et al., 2024).

Propostas de leis que visam à regulação da inteligência artificial (IA) incluem a sustentabilidade energética como um princípio jurídico fundamental (Barreto, 2024), o que pressiona órgãos reguladores, como a Agência Nacional de Energia Elétrica (ANEEL), a implementar normas que promovam a eficiência energética. Atores do campo econômico também monitoram a situação, pressionando por uma regulamentação menor para garantia de investimentos e implementação de datacenters no Brasil (Teixeira, 2024). Essa abordagem não apenas visa a reduzir o impacto ambiental da tecnologia, mas também incentivar o desenvolvimento de soluções tecnológicas mais sustentáveis.

Há diversas métricas para data centers, como o Power Usage Effectiveness (PUE - eficácia do uso de energia), o Data Center Infrastructure Efficiency (DCiE - eficiência da infraestrutura do data center), o Carbon Usage Effectiveness (CUE - eficiência do uso do carbono), Water Usage Effectiveness (WUE - eficácia do uso de água), entre muitos outros (Araújo Neto, 2023). Organizações civis como The Green Grid desenvolvem métricas para eficiência energética e há um grande interesse científico nas pesquisas sobre Green Data Center, com métricas internacionais, conectando-se com a agenda de "TI verde" no Brasil (Schulz & Silva, 2012; De Brito et al., 2023).

3. Clima, recursos hídricos e infraestruturas digitais

A relação entre clima e recursos hídricos é um fator crucial na operação de datacenters, que dependem de água para a refrigeração de seus sistemas (Hogan, 2015). O uso de IA pela Microsoft produziu um efeito notável: seus datacenters passaram a exigir maior consumo de água, com aumento de 34% no último ano (O'Brien & Fingerhut, 2023).

Este aumento da demanda por recursos hídricos tem preocupado gestores públicos e cidadãos de cidades que optaram pela atração de capital ao criar condições facilitadas de instalação de datacenters. O caso mais importante, neste sentido, é o de Oregon. Os cidadãos

enfrentaram uma batalha judicial de mais de um ano para conseguirem dados sobre o consumo de água da Google. A empresa argumentou que a informação de consumo de água é um segredo industrial que não pode ser revelado publicamente. Foi preciso uma longa batalha judicial para garantia de um direito básico de informação, que resultou em um acordo de apresentação dessas informações por um período de dez anos (Rogoway, 2022).

Em regiões com climas mais amenos e alta umidade, como Curitiba, as condições são mais favoráveis para a instalação de datacenters, pois a demanda por água para resfriamento é menor. Em contraste, cidades no Oeste dos Estados Unidos enfrentam desafios críticos, onde o consumo excessivo de água por parte de empresas de tecnologia tem causado escassez hídrica em bairros inteiros (Hogan, 2015). Isso demonstra a importância de considerar as características climáticas e a disponibilidade de recursos hídricos ao planejar a localização e a operação de infraestruturas digitais. A gestão sustentável desses recursos é essencial para evitar impactos negativos tanto para a população local quanto para o meio ambiente.

Como lembrado por Steven Montserrate, nós precisamos "desvendar as bobinas de cabos coaxiais, tubos de fibra óptica, torres de celular, condicionadores de ar, unidades de distribuição de energia, transformadores, canos de água, servidores de computador" para pensarmos as infraestruturas digitais. O capitalismo informacional depende de fluxos materiais de eletricidade, água, ar, calor, metais, minerais e elementos raros da Terra que sustentam nossas vidas digitais. Como observado por pesquisadores de orientação crítica, "o acesso a recursos hídricos baratos, como energia hidroelétrica e água para refrigeração, terras baratas e proximidade de redes submarinas criaram um ponto ideal espacial para grandes empresas de tecnologia como Google, Apple, Facebook, Microsoft e Amazon" (Levenda & Mahmoudi, 2019). ■

Rafael Zanatta *é codiretor da Data Privacy Brasil é pesquisador de pós-doutorado do Departamento de Filosofia e Teoria Geral do Direito da Faculdade de Direito da Universidade de São Paulo e doutor pelo Instituto de Energia e Ambiente da Universidade de São Paulo.*

Pedro Saliba *é advogado e sociólogo, doutorando em Teoria do Estado e Direito Constitucional (PUC-Rio) e mestre em Sociologia e Antropologia pelo PPGSA/UFRJ. Atualmente trabalha como coordenador de Assimetrias e Poder na Data Privacy Brasil.*

Gabriela Vergili *é bacharela em Direito pela Pontifícia Universidade Católica de São Paulo (PUC-SP) e pesquisadora no Data Privacy Brasil desde 2019. Atualmente é pesquisadora no projeto "Ambiente e informação: contestando a instrumentalização política da LGPD na regulação ambiental".*

Referências

ARAÚJO NETO, Antonio Palmeira. Arquitetura de Data Center. São Paulo: Senac, 2023.

ARCOVERDE, Leo; RAMOS, Maria Vitória; ZANATTA, Rafael. Transparência sob ataque, Folha de São Paulo, 09/12/2021. Disponível em: https://www.dataprivacybr.org/transparencia-sob-ataque/. Acesso em: 28 ago. 2024.

ASSOCIATION FOR PROGRESSIVE COMMUNICATION. A guide to the circular economy of digital devices. Circular Tech. 2021. Disponível em: https://circulartech.apc.org/books/a-guide-to-the-circular-economy-of-digital-devices. Acesso em: 28 ago. 2024

ASSOCIATION FOR PROGRESSIVE COMMUNICATION. APC and Coding Rights intervention at the GDC Americas Multistakeholder Consultation, APC, 08 March 2023. Disponível em: https://www.apc.org/en/pubs/apc-and-coding-rights-intervention-gdc-americas-multistakeholder-consultation Acesso em: 28 ago. 2024.

BARRETO, Elis. PL sobre "data centers" de Inteligência Artificial é proposto no Senado, O Brasilianista, 01/08/2024. Disponível em: https://obrasilianista.com.br/bastidores-de-brasilia/pl-sobre-data-centers-de-inteligencia-artificial-e-proposto-no-senado/ Acesso em: 28 ago. 2024.

BENELLI, Ana; BOTTINO, Celina; PERRONE, Christian; ALVES, Cristina. Infraestruturas Públicas Digitais. Rio de Janeiro: ITS, 2024. Disponível em: https://d26k070p771odc.cloudfront.net/wp-content/uploads/2016/12/20240411_Relatorio_InfraestruturasDigitaisPublicas_1.pdf. Acesso em: 28 ago. 2024.

BRASIL. Lei nº 12.651/2012. Dispõe sobre a proteção da vegetação nativa; altera as Leis nºs 6.938, de 31 de agosto de 1981, 9.393, de 19 de dezembro de 1996, e 11.428, de 22 de dezembro de 2006; revoga as Leis nºs 4.771, de 15 de setembro de 1965, e 7.754, de 14 de abril de 1989, e a Medida Provisória nº 2.166-67, de 24 de agosto de 2001; e dá outras providências. Diário Oficial da União, Brasília, DF, 2012 Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12651.htm. Acesso em: 28 ago. 2024.

COMISSÃO ECONÔMICA PARA A AMÉRICA LATINA (CEPAL). Acordo Regional sobre Acesso à Informação, Participação Pública e Acesso à Justiça em Assuntos Ambientais na América Latina e no Caribe. 2018. Disponível em: https://repositorio.cepal.org/entities/publication/34d8fe1b-3fe1-441d-aba5-2df15a2543ff Acesso em: 28 ago. 2024.

COHEN, Julie E. Between truth and power: the legal constructions of informational capitalism. Oxford: Oxford University Press, 2019.

DATA PRIVACY BRASIL. Ambiente e informação: contestando a instrumentalização política da LGPD na regulação ambiental. Data Privacy Brasil. 2024. Disponível em: https://www.dataprivacybr.org/projeto/ambiente-e-informacao-contestando-a-instrumentalizacao-politica-da-lgpd-na-regulacao-ambiental/. Acesso em: 28 ago. 2024.

DATA PRIVACY BRASIL. Data Privacy Brasil adere a movimento sobre informação ambiental, Data Privacy Brasil, 21/11/2023. Disponível em: https://www.dataprivacybr.org/dataprivacybrasil_movimento_escazu/. Acesso em: 28. ago. 2024

DE BRITO, José Luiz Romero; LARA DOS SANTOS MATAI, Patrícia Helena; DOS SANTOS, Mario Roberto. Data Center e Eficiência Energética: Data Center and Energy Efficiency. Brazilian Journal of Business, v. 5, n. 2, p. 786-795, 2023.

HOGAN, Mél. Data flows and water woes: The Utah data center. Big Data & Society, v. 2, n. 2, p. 2053951715592429, 2015.

MONSERRATE, Steven Gonzalez. The Cloud Is Material: On the Environmental Impacts of Computation and Data Storage. MIT Case Studies in Social and Ethical Responsibilities of Computing, no. Winter, 2022. Disponível em: https://doi.org/10.21428/2c646de5.031d4553. Acesso em: 28 ago. 2024.

LEVENDA, Anthony; MAHMOUDI, Dillon. Silicon Forest and Server Farms: the (urban) nature of digital capitalism in the Pacific Northwest, Culture Machine, 2019. Disponível em: https://api.mdsoar.org/server/api/core/bitstreams/3e914c6b-6741-47ba-94ff-d5fdf755e467/content. Acesso em 28 ago. 2024

MINISTÉRIO DA GESTÃO E INOVAÇÃO EM SERVIÇOS PÚBLICOS. Ministra reforça importância do Cadastro Ambiental Rural e cooperação com governo da Alemanha, Gov.br, 05/12/2023. Disponível em: https://www.gov.br/gestao/pt-br/assuntos/noticias/2023/dezembro/esther-dweck-reforca-importancia-do-cadastro-ambiental-rural-e-cooperacao-com-governo-da-alemanha. Acesso em: 28 ago. 2024.

NORGREN, A. Artificial intelligence and climate change: ethical issues. Journal of Information, Communication and Ethics in Society. Vol. 21 No. 1, 2023. pp. 1-15. Doi: http://dx.doi.org/10.1108/JICES-11-2021-0106. Disponível em: https://www.emerald.com/insight/content/doi/10.1108/JICES-11-2021-0106/full/pdf?title=artificial-intelligence-and-climate-change-ethical-issues. Acesso em: 28 ago. 2024.

O'BRIEN, M.; FINGERHUT, H.; THE ASSOCIATED PRESS. A.I. tools fueled a 34% spike in Microsoft's water consumption, and one city with its data centers is concerned about the effect on residential supply. 9 set. 2023. Fortune. Disponível em: https://fortune.com/2023/09/09/ai-chatgpt-usage-fuels-spike-in-microsoft-water-consumption/. Acesso em: 28 ago. 2024.

ROGOWAY, M. The Dalles settles public records lawsuit over Google's data centers, will disclose water use to The Oregonian/OregonLive. 14 dez. 2022. The Oregonian/OregonLive. Disponível em: https://www.oregonlive.com/silicon-forest/2022/12/the-dalles-settles-public-records-lawsuit-over-googles-data-centers-will-disclose-water-use.html. Acesso em: 28 ago. 2024.

QUINTARELLI, Stefano. Capitalismo immateriale: le tecnologie digitali e il nuovo conflitto sociale. Roma: Bollati Boringhieri, 2019.

SADOWSKI, Jathan. When data is capital: Datafication, accumulation, and extraction. Big data & society, v. 6, n. 1, p. 2053951718820549, 2019.

SCHULZ, Murilo Alexandre; SILVA, Tania Nunes. TI Verde e eficiência energética em Data Centers. Revista de Gestão Social e Ambiental, v. 6, n. 2, p. 121-133, 2012.

T20 BRASIL. Task Force 05 Statement. Brasília: G20 Brasil, 2024. Disponível em: https://br.boell.org/sites/default/files/2024-07/tf05_statement_t20.pdf

TEIXEIRA, Pedro. Burocracia trava investimento de R$ 100 bi em data centers só em SP, diz CEO da CPFL. 28 ago. 2024. Folha de São Paulo. Disponível em: https://www1.folha.uol.com.br/tec/2024/08/burocracia-trava-investimento-de-r-100-bi-em-data-centers-so-em-sp-diz-ceo-da-cpfl.shtml. Acesso em: 28 ago. 2024.

VERGILI, Gabriela; SALIBA, Pedro. Políticas ambientais, transparência pública e proteção de dados: a viabilidade jurídica para compartilhamento de dados pessoais no âmbito do Cadastro Ambiental Rural. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2023. Disponível em: https://www.dataprivacybr.org/wp-content/uploads/2023/06/Relatorio-Politicas-ambientais-transparencia-publica-e-protecao-de-dados-Nova-Versao.pdf. Acesso em: 28 ago. 2024

UNCTAD, Curbing the digital economy's growing environmental footprint, 07 December 2023. UNCTAD. Disponível em: https://unctad.org/news/curbing-digital-economys-growing-environmental-footprint. Acesso em: 28 ago. 2024.

ZANATTA, Rafael A. F. A proteção coletiva dos dados pessoais no Brasil: vetores de interpretação. Belo Horizonte: Letramento, 2023.

Kate Robertson

UM TRATADO GLOBAL PARA COMBATER O CIBERCRIME – SEM COMBATER O SPYWARE MERCENÁRIO[1]

O novo tratado da ONU sobre crimes cibernéticos está prestes a se tornar um veículo de cumplicidade no comércio global de espionagem mercenária.

Em 8 de agosto, a comunidade internacional concluiu suas negociações finais nas Nações Unidas sobre um tratado internacional de crimes cibernéticos. O tratado — agora pronto para ser votado na Assembleia Geral da ONU[2] — tem como objetivo alinhar as leis de crimes cibernéticos e os poderes da polícia investigativa de seus estados-partes. O processo de negociação revelou profundas falhas na comunidade global sobre o papel dos direitos humanos na era digital. Em meio a uma série de disputas, o potencial do tratado de alimentar a proliferação global de spyware mercenário[3] lança uma sombra iminente sobre sua versão final. Como a Casa Branca ressaltou,[4] os abusos estatais de spyware comercial são uma ameaça clara e urgente aos direitos humanos e aos interesses de segurança nacional dos Estados Unidos e de seus aliados.

Os proponentes do processo do tratado da ONU esperavam harmonizar os esforços globais para combater o crime cibernético transnacional.[5] No entanto, o tratado tem sido alvo de intensas críticas — da sociedade civil,[6] dos principais pesquisadores de segurança,[7] das autoridades de direitos humanos,[8] da imprensa internacional[9] e da indústria[10] — por ameaçar causar muito mais mal do que bem à segurança digital da população mundial.[11]

O mandato do projeto de tratado exige poderes de vigilância e compartilhamento de dados transfronteira sobre uma gama impressionante de conteúdos online — uma visão que, como defendida pela Rússia, China e outros adversários, ultrapassa dramaticamente um foco estreito de combate ao crime cibernético.[12] Os capítulos IV e V do projeto de tratado exigem obrigações de

1. Publicado originalmente em https://www.lawfaremedia.org/article/a-global-treaty-to-fight-cybercrime-without-combating-mercenary-spyware
2. https://undocs.org/en/A/AC.291/L.15
3. Também chamado de spyware comercial – as duas formas são usadas neste texto. Uma resenha do tema está em https://em360tech.com/tech-article/what-is-mercenary-spyware (n.t.).
4. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security
5. https://documents.un.org/doc/undoc/gen/n19/440/28/pdf/n1944028.pdf
6. https://epicenter.works/fileadmin/user_upload/Cybercrime_-_Open_Letter_to_EU-Commission_and_Member_States.pdf
7. https://www.eff.org/deeplinks/2024/02/protect-good-faith-security-research-globally-proposed-un-cybercrime-treaty
8. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/OHRC_AHC_Cybercrime_-_reconvened_concluding_session.pdf
9. https://ipi.media/ipi-calls-on-us-eu-to-reject-dangerous-global-surveillance-treaty/
10. https://uscib.org/uscib-content/uploads/2024/08/Cybercrime-Letter-FINAL.pdf
11. https://doctorow.medium.com/https-pluralistic-net-2024-07-23-expanded-spying-powers-in-russia-crime-cybers-you-607f0ab61f8a
12. https://foreignpolicy.com/2023/08/31/united-nations-russia-china-cybercrime-treaty/

vigilância e compartilhamento de dados referentes a qualquer informação digital de interesse em investigações de direito penal doméstico em cada país que seja parte do tratado. O tratado está, portanto, disposto a inundar canais de cooperação jurídica já sobrecarregados com solicitações policiais por informações digitais de baixa prioridade ou abusivas.

Esforços recentes para combater a proliferação de spyware mercenário

Se adotado pela Assembleia Geral, o tratado da ONU representaria um dos primeiros grandes retrocessos em meio aos esforços internacionais em andamento para combater spyware mercenário.[13] Após o lançamento da ordem executiva de 2023 da Casa Branca sobre spyware comercial,[14] 16 outros países se juntaram aos Estados Unidos na divulgação de uma declaração conjunta reconhecendo o spyware como uma ameaça à segurança nacional e aos direitos humanos.[15] A declaração enfatiza que o spyware é frequentemente mal utilizado por regimes autoritários e democracias — inclusive contra defensores dos direitos humanos e jornalistas. A coalizão liderada pelos EUA afirmou que eles "compartilham um interesse fundamental de segurança nacional e política externa em combater e prevenir a proliferação de spyware comercial". Os Estados Unidos deram um passo adiante ao proibir o governo federal de usar spyware comercial e lançaram uma resposta governamental para combater a tecnologia, incluindo, por exemplo, controles de exportação e sanções visando indivíduos envolvidos com entidades de spyware comercial.[16] Os Estados Unidos também se juntaram a uma iniciativa paralela na UE,[17] agora liderada pelo Reino Unido e pela França, com o objetivo de "Combater a Proliferação e o Uso Irresponsável de Capacidades Comerciais de Intrusão Cibernética".

Um quadro internacional para o comércio global de espionagem

Se o tratado prosseguir, todos os signatários seriam obrigados a adotar capacidades de vigilância e interceptação que podem ser transformadas em armas por países que buscam cobertura legal para justificar seu uso de spyware comercial. Por exemplo, o Artigo 28 da convenção obriga os signatários a obter capacidades de vigilância sobre dados eletrônicos armazenados em seu território, e os Artigos 29 e 30 obrigam os países a obter capacidades para realizar a interceptação em tempo real de dados de tráfego e dados de conteúdo. Notavelmente, as disposições não proíbem os países de recorrer a mercenários cibernéticos que lançam mão de spyware comercial para obter as capacidades necessárias. Um estado poderia, sob os artigos acima mencionados, argumentar que o tratado permite que os países recorram a fornecedores de spyware comercial para as capacidades de vigilância necessárias. A linguagem no Artigo 40, exigindo que os países forneçam

13. Uma visão convergente do tema está em https://www.techpolicy.press/new-united-nations-cybercrime-convention-sets-unprecedented-international-antihuman-rights-standard/ (n.t.)
14. https://www.whitehouse.gov/briefing-room/statements-releases/2023/03/27/fact-sheet-president-biden-signs-executive-order-to-prohibit-u-s-government-use-of-commercial-spyware-that-poses-risks-to-national-security/
15. https://www.whitehouse.gov/briefing-room/statements-releases/2024/03/18/joint-statement-on-efforts-to-counter-the-proliferation-and-misuse-of-commercial-spyware/
16. https://www.state.gov/growing-coalition-of-governments-join-the-u-s-in-countering-the-proliferation-and-misuse-of-commercial-spyware/
17. https://www.lawfaremedia.org/article/the-pall-mall-process-on-cyber-intrusion-capabilities

a "medida mais ampla" de assistência jurídica mútua em investigações policiais sob o tratado, fornece material adicional para tais alegações interpretativas. É altamente provável que os governos abusem do spyware para reforçar práticas despóticas e minar as instituições democráticas internamente e no exterior.[18] As investigações dos pesquisadores do Citizen Lab sobre a prevalência e o impacto da espionagem digital documentaram evidências de ataques direcionados, tanto internos como transfronteiras,[19] contra a sociedade civil, incluindo defensores dos direitos humanos,[20] jornalistas[21] e dissidentes políticos.[22]

Outras disposições no rascunho abrem caminho para que os países terceirizem o uso de spyware para equivalentes de aplicação da lei em países estrangeiros com controles de privacidade frouxos, ou para lavar dados obtidos de spyware por meio de canais secretos de compartilhamento de dados criados ou normalizados sob os auspícios do tratado. Por exemplo, o Artigo 46 exige que os estados "se esforcem para fornecer assistência jurídica mútua uns aos outros" na interceptação e gravação em tempo real de dados. A disposição não observa nenhuma restrição sobre se os dados em questão estão localizados no território do país que presta assistência. O Artigo 47(2) geralmente endossa o uso de redes transfronteiras que operam por meio de "acordos ou arranjos" multilaterais ou bilaterais,[23] permitindo "cooperação direta" entre agências policiais em todo o mundo. O Artigo 48 também dá sinal verde para o uso de "investigações conjuntas" transnacionais entre agências policiais, o que abre a porta para que as autoridades policiais busquem parcerias com jurisdições favoráveis a spyware. As obrigações de sigilo ilimitadas previstas no artigo 40(20) criam uma forte possibilidade de que as provas obtidas através de spyware mercenário sejam difíceis de detectar e contestar através destas redes.

A comunidade internacional já está vendo usos mais atrevidos de operações policiais transnacionais, como uma operação secreta transfronteira[24] que levou à captura subreptícia de milhões de mensagens criptografadas de celulares ao redor do mundo em uma investigação internacional conjunta, liderada por uma cooperação entre o FBI e a Polícia Federal australiana.[25] A investigação foi estruturada para situar o armazenamento das mensagens capturadas em servidores localizados em um terceiro país — mais tarde revelado como a Lituânia[26] — para evitar as barreiras legais sob as proteções constitucionais de privacidade dos EUA. A polícia dos EUA obteve assim acesso aos dados por meio de canais de assistência jurídica mútua da Lituânia. O exemplo levanta questões sobre como garantir que as proteções internacionais de direitos humanos e os controles de responsabilização sejam igualmente robustos em investigações transnacionais, especialmente devido ao potencial de que colaborações possam ocorrer com jurisdições que permitam spyware mercenário.

O Artigo 47(1) também endossa a troca rápida de informações por meio de canais

18. https://www.foreignaffairs.com/world/autocrat-in-your-iphone-mercenary-spyware-ronald-deibert
19. https://citizenlab.ca/2022/03/psychological-emotional-war-digital-transnational-repression-canada/
20. https://citizenlab.ca/2022/10/new-pegasus-spyware-abuses-identified-in-mexico/
21. https://citizenlab.ca/2020/01/stopping-the-press-new-york-times-journalist-targeted-by-saudi-linked-pegasus-spyware-operator/
22. https://citizenlab.ca/2024/05/pegasus-russian-belarusian-speaking-opposition-media-europe/
23. https://undocs.org/en/A/AC.291/L.15
24. https://www.economist.com/culture/2024/07/16/the-largest-sting-operation-youve-never-heard-of
25. https://www.crikey.com.au/2024/06/07/dark-wire-joseph-cox-afp-fbi-encrypted-phone-anom-operation-ironside/
26. https://www.404media.co/revealed-the-country-that-secretly-wiretapped-the-world-for-the-fbi/

transnacionais, incluindo quaisquer dados ou informações de localização de qualquer pessoa de interesse. Subgrupos de regimes não liberais também já estabeleceram práticas que levantaram sérias preocupações sobre riscos de compartilhamento de dados:[27] por exemplo, a unidade de contraterrorismo da Organização de Cooperação de Xangai supostamente usou tais táticas de compartilhamento de dados para atingir dissidentes[28] e circular listas de indivíduos[29] a serem presos e indiciados. Até mesmo o compartilhamento informal de informações inapropriadas ou imprecisas pode levar à prisão e tortura de pessoas inocentes.[30] Sem controles robustos de direitos humanos, redes de baixa visibilidade são particularmente propícias ao abuso por países que buscam obter e compartilhar dados coletados de spyware mercenário.

Lições difíceis do legado da INTERPOL

Potenciais estados-membros do tratado proposto pela ONU sobre crimes cibernéticos podem olhar para a Organização Internacional de Polícia Criminal (INTERPOL)[31] como um exemplo do perigo dos protocolos de compartilhamento de dados transfronteiras que não exigem e harmonizam proteções robustas de direitos humanos de todos os estados participantes.

Fundada em 1923 e reconstituída em 1946, a INTERPOL é uma organização internacional de compartilhamento de dados que faz a intermediação entre órgãos policiais membros de 196 países ao redor do mundo. Apesar de várias reformas ao longo dos anos, um compromisso com instrumentos internacionais de direitos humanos que se aplicam a investigações policiais, como o Pacto Internacional sobre Direitos Civis e Políticos,[32] nunca se tornou um pré-requisito para a filiação à INTERPOL. Na verdade, o Artigo 4 da constituição da organização — que rege a filiação — não inclui linguagem sobre conformidade com os direitos humanos ou quaisquer outros elementos de filiação. Ele exige apenas que uma solicitação de filiação venha da autoridade governamental apropriada de um país, que pode propor um "órgão policial oficial" para filiação à INTERPOL. Seu órgão dirigente, a Assembleia Geral da INTERPOL, então determina a filiação com uma votação. Além disso, o Artigo 2 de sua constituição declara que um dos objetivos da INTERPOL é promover a assistência mútua "no espírito" da Declaração Universal dos Direitos Humanos, mas não vai além para tornar obrigatório seu cumprimento para a INTERPOL ou seus membros.

O abuso crônico dos mecanismos de cooperação internacional da INTERPOL ilustra o perigo de estruturas de policiamento transfronteiriço que não exigem comprometimento compartilhado com padrões robustos de direitos humanos. Mesmo em circunstâncias de grande visibilidade, por exemplo, no caso Bill Browder — um financista conhecido por expor a corrupção no governo russo[33] — a Rússia tentou prender Browder oito vezes por meio do programa Red Notice da INTERPOL.[34] (Seu advogado, Sergei Magnitsky, foi preso em conexão com as mesmas acusações na Rússia e

27. https://www.osce.org/files/f/documents/e/8/467697.pdf
28. https://www.hrw.org/news/2006/06/14/eurasia-uphold-human-rights-combating-terrorism
29. https://www.fidh.org/IMG/pdf/sco_report.pdf
30. https://www.theglobeandmail.com/news/national/how-canada-failed-citizen-maher-arar/article1103562/
31. https://www.interpol.int/
32. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
33. https://www.cbsnews.com/news/interpol-navigates-tricky-role-assisting-worldwide-police-cooperation-60-minutes-transcript/
34. https://www.interpol.int/en/How-we-work/Notices/Red-Notices

morreu após ser espancado em uma prisão de Moscou.) Red Notices são solicitações para autoridades policiais em todo o mundo para localizar e prender um indivíduo para processamento e extradição para o país original que emitiu um mandado de prisão. O programa Red Notice e outros procedimentos de cooperação na INTERPOL[35] foram vinculados a abusos governamentais repetidos e persistentes[36] que frequentemente levam a prisões injustas, detenções, confinamento solitário[37] e, em alguns casos, extradição resultando em violações do devido processo legal[38] e tortura.[39]

O Secretário-Geral da INTERPOL, Juergen Stock, explicou que, neste estágio, a INTERPOL está limitada em sua capacidade de proteger melhor os indivíduos de abusos estatais do programa Red Notice.[40] Stock citou tensões geopolíticas e a ausência de uma definição internacional comum de terrorismo — um aceno ao perigo de países que usam indevidamente a estrutura da INTERPOL como uma ferramenta para repressão transnacional. Países autoritários frequentemente usam a lei criminal como uma espada contra a liberdade de expressão para silenciar a oposição e suprimir a dissidência, como no caso de Alexei Navalny, que foi um importante defensor anticorrupção e líder de um partido de oposição na Rússia. Moscou rotulou Navalny como um extremista criminoso, e Navalny foi preso[41] até sua morte em uma prisão russa em fevereiro.[42] Apesar do abuso repetido da estrutura da INTERPOL, no início deste ano Stock sublinhou que, embora examine as solicitações estatais de Red Notices, a organização optou por não policiar os registros de direitos humanos de seus países membros, afirmando que esse não é seu papel "como uma organização policial técnica".[43]

Mas, por mais "técnicos" que sejam os poderes policiais transnacionais, não há dúvida que seu uso indevido pode ser devastador para alguns dos interesses de direitos humanos mais sensíveis conhecidos pelo direito internacional. O posicionamento de Stock da INTERPOL como um órgão técnico também falha em reconhecer como a inadequação das salvaguardas processuais em torno da vigilância estatal e da divulgação de informações sensíveis a agências policiais não são simplesmente periféricas aos direitos humanos. As salvaguardas processuais — como autorização e supervisão judicial independente — que protegem contra abusos por funcionários estatais vão ao cerne dos padrões internacionais de direitos humanos aplicáveis a investigações policiais.[44]

Nas fases finais das negociações, vários países ressaltaram o perigo de abusos semelhantes ao tratado proposto pela ONU ao votarem para eliminar múltiplas salvaguardas do texto final do tratado, incluindo o Artigo 40(22). Este artigo estipula que os países não são obrigados a fornecer assistência jurídica a uma investigação policial estrangeira se houver "motivos substanciais" para acreditar que o propósito da investigação ou acusação estrangeira é punir uma pessoa "por conta do sexo, raça, idioma, religião, nacionalidade, origem étnica ou opiniões políticas dessa pessoa". Vinte

35. https://www.justsecurity.org/87260/after-spotlight-on-red-notices-turkey-is-abusing-another-interpol-mechanism/
36. https://www.nytimes.com/2024/02/20/world/europe/interpol-strongmen-abuse.html
37. https://thediplomat.com/2023/06/the-continued-imprisonment-of-idris-hasan/
38. https://www.theguardian.com/global-development/2022/feb/16/extradition-of-bahraini-dissident-from-serbia-calls-interpol-role-into-question
39. https://www.europarl.europa.eu/thinktank/en/document/EXPO_STU(2019)60347
40. https://www.reuters.com/world/interpol-cant-do-much-more-stop-abuse-red-notices-chief-says-2023-11-28/
41. https://www.coe.int/en/web/portal/-/european-court-of-human-rights-asks-russia-to-release-aleksey-navalnyy
42. https://www.brookings.edu/articles/the-death-of-alexei-navalny/
43. https://www.cbsnews.com/news/interpol-policing-success-failures-60-minutes/
44. https://hudoc.echr.coe.int/eng?i=002-14333

e cinco países — incluindo Rússia, China e Índia — votaram para remover o Artigo 40(22), e outros 17 países se abstiveram.

Em outras palavras, mais de 40 países endossaram ou toleraram a remoção de uma disposição que limita as obrigações de cooperação em circunstâncias em que um país estrangeiro está investigando um indivíduo com o propósito de discriminação ou punição por suas opiniões políticas. Embora a votação tenha fracassado, a tentativa serve como um alerta sobre quantos países provavelmente abordarão a implementação do tratado se ele for aprovado pela Assembleia Geral, principalmente devido às deficiências nas salvaguardas dos direitos humanos que deixam amplo espaço para abusos.

Uma oportunidade perdida para a reforma do direito internacional para atingir o spyware mercenário

Assim como a estrutura da INTERPOL, o projeto de tratado sobre crimes cibernéticos da ONU também é indiferente ao comprometimento dos estados-partes com instrumentos internacionais de direitos humanos, como o Pacto Internacional sobre Direitos Civis e Políticos (PIDCP).[45] O Artigo 6(1) faz referência à necessidade de os estados signatários garantirem que sua implementação do tratado "seja consistente com suas obrigações sob a lei internacional de direitos humanos", mas a medida é amplamente prejudicada por nações que se recusaram a assinar os principais tratados de direitos humanos ou proteção de dados. A China, por exemplo, expressou apoio ao tratado da ONU,[46] mas não é parte do PIDCP e é responsável por documentar abusos dos procedimentos de cooperação da INTERPOL.[47] Os Emirados Árabes Unidos (EAU) também participaram das negociações da ONU e são um potencial signatário do tratado da ONU. Os EAU não são signatários do PIDCP e foram vinculados a abusos do spyware Pegasus do NSO Group.[48] Os EAU também foram doadores financeiros significativos da INTERPOL[49] e foram investigados por abusos do programa Red Notice da INTERPOL.[50] Ao abrir o tratado a todos os países, independentemente de seus compromissos com os padrões internacionais de direitos humanos, como o PIDCP, o tratado da ONU abre a porta para mais abusos transnacionais.

As lacunas de direitos humanos no texto final do tratado proposto levaram a um amplo consenso entre a sociedade civil e a indústria de que o tratado deveria ser rejeitado pelos estados democráticos por não ir longe o suficiente para proteger indivíduos ao redor do mundo que serão mais impactados pelo tratado se ele for aprovado.[51] Embora haja proteções importantes no texto final do tratado proposto, a maioria de suas disposições — como o Artigo 6(1), entre outras — foram avaliadas como ausentes e vulneráveis a abusos.[52] Além do Artigo 6(1), o Artigo 6(2) inclui uma disposição que essencialmente impede que o tratado seja interpretado de uma maneira que suprima os direitos humanos e as liberdades fundamentais. O Artigo 6(2) é importante, mas também é muito amplo e, portanto, vulnerável

45. https://www.ohchr.org/en/instruments-mechanisms/instruments/international-covenant-civil-and-political-rights
46. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/First_session/Comments/Chinas_Suggestions_on_the_Scope_Objectives_and_Structure_AHC_ENG.pdf
47. https://www.hrw.org/news/2017/09/25/interpol-address-chinas-red-notice-abuses
48. https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/
49. https://www.interpol.int/en/News-and-Events/News/2017/UAE-pledges-EUR-50-million-to-support-seven-key-INTERPOL-projects
50. https://foreignpolicy.com/2018/12/03/the-scourge-of-the-red-notice-interpol-uae-russia-china/
51. https://uscib.org/uscib-content/uploads/2024/08/Cybercrime-Letter-FINAL.pdf
52. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/UN_SR_HR_Terrorism.pdf

à exploração. Por exemplo, os estados podem citar a robusta disposição de soberania conforme descrito no Artigo 5, para contestar o conteúdo específico do Artigo 6 ou a aplicabilidade de padrões internacionais de direitos humanos ao uso de intrusões cibernéticas como spyware mercenário.[53]

Outra salvaguarda fundamental encontrada no Artigo 24 exige que os Estados Partes alinhem suas leis nacionais com suas obrigações internacionais de direitos humanos ao implementar o tratado e estipula que aqueles que implementam leis devem incorporar o princípio da proporcionalidade. O Artigo 24(2) estipula a necessidade de certas condições e salvaguardas específicas, como a necessidade de revisão judicial e direitos de reparação eficazes. Apesar dessas disposições, o Artigo 24 também foi criticado por enquadrar essas obrigações essenciais de direitos humanos como opcionais e por não invocar a necessidade de outras obrigações estabelecidas de direitos humanos, como o princípio da legalidade[54] e o direito à notificação individual.[55] No geral, há muito no Artigo 24 que reforça a visão de alguns estados de que muitas de suas salvaguardas são principalmente uma questão de preferência nacional.[56] Mesmo com essas fraquezas, vários Estados ainda votaram para tentar eliminar os Artigos 6(2) e 24 do texto final do tratado.

Particularmente preocupante, dada a persistência de alguns estados no uso de spyware comercial, é que as salvaguardas do Artigo 24 também têm aplicação muito limitada às disposições de cooperação do tratado no Capítulo V.[57] Coletivamente, as disposições de cooperação nos Artigos 46 a 48 não impõem proibições expressas sobre o compartilhamento de dados hackeados ou informações obtidas de spyware comercial.[58] As disposições também não impõem nenhuma supervisão judicial independente ou obrigações de transparência para salvaguardar os direitos humanos no contexto de investigações transnacionais. Medidas de transparência e supervisão são críticas para evitar que redes transnacionais obscuras proliferem em segredo indefinido. Apesar das deficiências do tratado em exigir comprometimento com os padrões de direitos humanos, o Artigo 47(2) ainda permite que o próprio tratado atue como a "base" para a cooperação.

Os abusos estatais de spyware ilustram o perigo de delegar proteções de direitos humanos ao reino da "lei doméstica" para cada país interpretar em seus próprios termos. Autoridades internacionais de direitos humanos e acadêmicos têm chamado a atenção para a necessidade de reforma da lei internacional para confrontar a espionagem cibernética e o spyware comercial. Isso inclui a necessidade de regulamentação global que exija "ação multilateral e obrigatória com força legal"[59] contra spyware e para um tratado internacional abordando a espionagem cibernética dissidente transnacional.[60] O tratado da ONU não promoveria nenhum desses objetivos.

53. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/I.R.Iran-Explanation_of_Position-9_August_2024_NY.pdf
54. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP7/OHRC_AHC_Cybercrime_-_reconvened_concluding_session.pdf
55. https://undocs.org/CCPR/C/JPN/CO/7
56. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/MEMBER_STATES/Closing_Statement_final.pdf
57. https://www.unodc.org/documents/Cybercrime/AdHocCommittee/Reconvened_concluding_session/Written_submissions/OP8/HRW_comments_on_Rev3_20240729.pdf
58. https://www.washingtonpost.com/nation/interactive/2021/hanan-elatr-phone-pegasus/
59. https://www.ohchr.org/sites/default/files/documents/issues/terrorism/sr/statements/unsrcthr-stm-spyware.pdf
60. https://www.cambridge.org/core/journals/international-and-comparative-law-quarterly/article/regulating-transnational-dissident-cyber-espionage/8662095ACD8DB0BB32392E1BAD7DEFF6#fn54
61. https://www.coe.int/en/web/cybercrime/the-budapest-convention

Críticas semelhantes podem ser levantadas contra um tratado de cibercrime legado, originalmente desenvolvido pelo Conselho da Europa (comumente chamado de Convenção de Budapeste),[61] que também obriga os estados a manter capacidades de vigilância e não exige que os signatários assinem o Pacto Internacional sobre Direitos Civis e Políticos ou instrumentos de direitos humanos comparáveis. No entanto, o texto da Convenção de Budapeste foi desenvolvido em 2001 — muito antes de os mercenários cibernéticos desenvolverem a capacidade de manejar ferramentas poderosas, como cadeias de exploração de zero cliques,62 tornando muito mais difícil para os estados argumentarem que o tratado pretendia permitir explorações altamente invasivas que não estavam em circulação no momento da elaboração. A proliferação global de spyware comercial63 está agora diretamente diante da comunidade internacional, assim como a prevalência e a periculosidade da repressão transnacional.64 Os pesquisadores estão cada vez mais chamando a atenção para como, embora a repressão transnacional "não seja um fenômeno novo, tais táticas estão se expandindo por meio do crescimento do mercado de tecnologias digitais e da disseminação da conectividade com a Internet".65 Cada vez mais, o spyware é usado como uma ferramenta para facilitar a repressão transnacional, ou como um fim repressivo em si mesmo. Repetir erros do passado por meio do tratado cibernético da ONU consolida e piora esses problemas.

A incapacidade da comunidade internacional de gerar consenso sobre questões relativas aos direitos humanos fundamentais deixa os estados-membros da ONU com a escolha de assinar ou não o tratado sem salvaguardas essenciais de direitos humanos. No entanto, se a história é uma professora, ela diz que exigir cooperação transfronteira sem exigir compromissos robustos de direitos humanos não é um caminho sustentável para a luta contra o crime cibernético transnacional. Como o Secretário de Estado Antony Blinken pediu apenas no início deste ano,66 o uso indevido de spyware comercial tem sido associado a "detenções arbitrárias, desaparecimentos forçados e execuções extrajudiciais nos casos mais flagrantes". Para os países que buscam proteger as liberdades fundamentais, a segurança humana e a segurança nacional, esta não é uma luta que pode ser perdida. ■

Kate Robertson *é pesquisadora sênior do Citizen Lab, sediado na Munk School of Global Affairs & Public Policy, Universidade de Toronto. Este texto é publicado em português com autorização da autora e da revista Lawfare.*

Rubens Harry Born*

Informações e governança democrática em assuntos ambientais

O mundo humano apresenta desafios e situações paradoxais: o conhecimento científico e o avanço tecnológico têm oferecido contribuições importantes para o bem estar, seja na promoção da saúde e prevenção de enfermidades (por exemplo, a recente pandemia da Covid), para a produção de alimentos, de instrumentos e equipamentos em diversos segmentos econômicos, para o crescente uso de energia solar e eólica, para a comunicação por diversos meios, para a mobilidade, entre tantos outros campos das atividades econômicas, culturais, sociais etc. A evolução das tecnologias de informação e de comunicação alterou as dinâmicas das relações interpessoais, institucionais e empresariais; alavancou o conhecimento sobre a situação do planeta Terra, notadamente sobre os impactos ambientais, sanitários, migratórios e os decorrentes das várias formas de violência, entre povos, agrupamentos humanos, nações, e contra os bens e serviços ecossistêmicos essenciais à sobrevivência da Vida.

Muito se comenta sobre as atuais crises ambientais globais (mudanças do clima, poluição, degradação e perda da biodiversidade etc.) e as crises da desigualdade e da injustiça social afetam de forma diversa a sociedade. São percebidas pelo crescente número de pessoas deslocadas em razão da pobreza e da desigualdade. Essas crises se relacionam também com os desafios de gestão da sustentabilidade do desenvolvimento humano, integridade e salubridade de diversos territórios, por um lado, e com as oportunidades e barreiras para iniciativas da sociedade na governança de políticas, planos e empreendimentos. Em 1987, a Comissão Mundial de Desenvolvimento Sustentável, a Comissão Brundtland, em seu relatório "Nosso Futuro Comum", afirmara que não são crises isoladas: são facetas de uma única crise civilizatória, de padrões perversos, injustos e degradantes de sistemas econômicos, e que tornam indigna a vida de bilhões de pessoas, não obstante o progresso científico e evolução de direitos humanos.

A lista de exemplos de tais crises é longa, seja no Brasil ou no mundo: as chuvas intensas no Rio Grande do Sul, em maio deste ano e no segundo semestre de 2023, após um período de severa estiagem no mesmo ano; seca em rios da Amazônia, queimadas no Pantanal e em regiões agrícolas no estado de São Paulo; a constatação de que áreas do semi-árido nordestino se tornaram áridas, agravando os desafios de sobrevivência e convivência digna na caatinga; temporais e deslizamentos de encostas no litoral paulista. Tais fenômenos geram prejuízos às atividades educacionais, econômicas, culturais, além de dramáticas conseqüências para as vítimas sobreviventes de tais tragédias.

Em outros países, há relatos de importantes impactos e transformações ambientais: neste ano, rios do Alasca, EUA, ficando alaranjados, por decorrência de efeitos combinados da liberação de elementos químicos após o derretimento anormal do permafrost (solo congelado), afetando a biodiversidade aquática; o calor excessivo na Índia, em faixas de temperatura acima dos 50oC; a redução em proporções acima do esperado do gelo na Antártida, o que afetará o aumento do nível dos oceanos e impactos em regiões costeiras.

A OMS – Organização Mundial da Saúde, em sua recente assembléia, no final de maio de 2024, adotou resolução para reconhecer as ameaças iminentes à saúde humana decorrentes das mudanças do clima. Globalmente, segundo relatório de 2023 da Organização Meteorológica Mundial, a temperatura média do planeta no decênio 2014-2023 foi de cerca de 1,20 oC acima da média de 1850 a 1900, sendo considerado então um período decenal mais quente já avaliado pelos cientistas. Estudos científicos também apontam que no ano de 2023 o planeta teve a maior temperatura média nos últimos 125 mil anos. Dessa forma, o planeta já sofreu um aquecimento médio muito próximo do objetivo do Acordo de Paris para limitar o aquecimento global ao aumento de 1,5 oC até o fim do século.

Segundo o IPCC – Painel Científico da ONU sobre Mudanças do Clima, as emissões antrópicas de gases de efeito estufa terão que ser reduzidas em 43% até 2030, em relação aos níveis existentes em 2019, e chegar a um balanço neutro ("emissões zero", resultado da emissão e da captura de gás carbônico em atividades como recuperação de florestas) até 2050. E para que a chance de estabilizar a temperatura global do planeta, o IPCC indicou que será necessário reduzir em 60% o uso de petróleo, 45% do gás natural e 95% de carvão mineral.

Ora, as causas das mudanças do clima, da degradação da biodiversidade e da poluição são conhecidas há décadas. As convenções da ONU sobre clima, biodiversidade e desertificação são produtos da Cúpula da Terra ou Rio-92, a grande conferência realizada no Rio de Janeiro em 1992. Vinte anos depois, a Rio+20, outra conferência da ONU na mesma cidade, buscou retomar promessas e compromissos negligenciados, mediante pacto de ações para os ODS – Objetivos de Desenvolvimento Sustentável da Agenda 2030, uma "nova narrativa" para as promessas da Agenda 21, adotada na Conferência Rio-92. Esses acordos internacionais consideram como relevante a participação do público (da sociedade) nas ações e planos decorrentes e a divulgação de informações e relatórios periódicos sobre o avanço e barreiras na sua implementação, como por exemplo a Comunicação Nacional que cada país deve apresentar à Convenção Quadro de Mudanças do Clima. A internet permite conhecer planos e ações, previstas ou em curso, para a maioria dos países.

Como tantas mazelas ocorrem em uma época de sociedades cada vez mais digitalizadas, mais conectadas? Parece um paradoxo que na contemporânea sociedade digital tenhamos informações quase que instantâneas da situação do ambiente planetário, da Natureza e das violências humanas, mas obviamente os instrumentos e tecnologias digitais, não obstante a sua utilidade, não podem por si só responder pela ocorrência de tais mazelas, que se distribuem de forma desigual no planeta.

As tragédias socioambientais, entre outras, ocorrem como desdobramento de estruturas políticas, econômicas e culturais que apresentam enorme inércia às transformações necessárias para a consecução de sociedades democráticas, justas e sustentáveis. Por exemplo, a prevenção de riscos de ocorrência de desastres associados às formas insustentáveis de uso do ambiente também têm sido "esquecidas" por muitas lideranças, no Poder Público e nos setores econômicos. Os desas-

tres do rompimento de barragem de rejeitos de mineração em Brumadinho e as enchentes no Rio Grande do Sul são alguns exemplos da negligência da avaliação de riscos, da insuficiente transparência das informações e do limitado controle social das políticas públicas e atividades empresariais.

A gestão de riscos climáticos está sendo incorporada, em 2024, na elaboração do Plano Nacional para Mudanças do Clima, o conjunto de propostas de políticas e ações em mitigação das causas, adaptação aos impactos e redução de vulnerabilidades aos efeitos das alterações do sistema climático e ambiental. Mas, por outro lado, cabe destacar que a incorporação de abordagens e instrumentos de gestão de riscos deve ir muito mais além do aspecto de medidas de prevenção de desastres e conseqüências humanitárias, sanitárias e econômicas. A análise de riscos deverá necessariamente contribuir para as políticas e medidas que sejam eficazes para a segurança alimentar, a segurança hídrica (tanto para abastecimento de águas como para a geração de energia elétrica), para as infraestruturas de mobilidade e de logística, enfim para promover profunda, urgente e justa transformação do "desenvolvimento", contemplando suas diversas dimensões (cultural, tecnológica, econômica, social, ambiental, educacional).

O Acordo de Paris, de 2015, reconheceu, em seu preâmbulo, que os compromissos dos países (as NDCs – Contribuições nacionalmente determinadas), ainda que se plenamente cumpridos, não são suficientemente seguros para o objetivo de limitar o aquecimento global a 1,5 oC, e isso foi novamente reconhecido na recente 28ª Conferência das Partes (CoP 28) da Convenção da ONU sobre Mudanças do Clima, realizada em Dubai em dezembro de 2023. As emissões acumuladas de dióxido de carbono (CO2) já somam cerca de 80% do total que deveria ser o limite indicado pelos cientistas para se garantir a probabilidade de 50% de fazer o planeta não ultrapassar o limite delineado nesse Acordo.

Tal monumental esforço vai requerer, por exemplo, a recuperação de áreas que já foram florestas e outros ecossistemas de cobertura vegetal, o que nos ajudaria também a fortalecer a resiliência de áreas mais vulneráveis, a diminuir os riscos e impactos das crises ambientais. Isso é importante, sobretudo para Brasil e outros países em que o desmatamento e a perda da biodiversidade são componentes da crise ambiental. Mas só plantar árvores e proteger florestas não será suficiente. Será necessário fazer a transição para a agricultura ecológica e de baixo carbono, com produtos mais saudáveis; sistemas de mobilidade menos poluentes, de energias limpas e sustentáveis; reorientar as formas e padrões urbanísticos e das edificações, para que demandem menos energia (por ex: ar condicionado e iluminação). Também é importante a transição energética, para o mais rapidamente diminuir o uso de combustíveis fósseis, fonte de mais de 75% das emissões de gases de efeito estufa. A CoP28 sinalizou, em uma de suas decisões, tal diretriz, cujo cumprimento dependerá da "vigilância" de todas as pessoas.

Essa "vigilância" tem nome: governança democrática ambiental. Torna-se possível mediante condições de acesso a informação e participação, regras para tomada de decisão etc. que permitem à coletividade a gestão democrática dos rumos do Estado, da atividade econômica e da sociedade. Ou, como formulei o conceito, em 2007, de governança como "conjunto de iniciativas, regras, instâncias e processos que permitem às pessoas, por meio de suas comunidades e organizações civis, a exercer o controle social, público e transparente, das estruturas estatais e políticas públicas, por um lado, e das dinâmicas e das instituições do mercado, por outro lado, visando atingir objetivos comuns de bem estar, de direitos e dignidade de vidas." Meios

que precisa ser consistentes com a finalidade de sociedades justas, democráticas e sustentáveis. Enfim, ainda repetindo continuação da minha formulação, precisamos de "modos de vida e de organização social que viabilizam a vida digna de todos, da presente e das futuras gerações, com base em sistemas democráticos do exercício de direitos e deveres, para a fruição de ambientes saudáveis e com paz, conservando os processos ecológicos essenciais, os bens e serviços ecossistêmicos do planeta, assegurando a justiça e a equidade".

Um importante tratado internacional estabeleceu, em 2018, que "em caso de ameaça iminente à saúde pública ou ao meio ambiente, que a autoridade competente divulgará e disseminará de forma imediata e pelos meios mais efetivos toda informação relevante que se encontre em seu poder e que permita ao público tomar medidas para prevenir ou limitar potenciais danos". E mais, que cada país que ratificar esse tratado "deverá desenvolver e implementar um sistema de alerta precoce utilizando os mecanismos disponíveis".

Trata-se do Acordo Regional sobre Acesso à Informação, Participação Pública e Acesso à Justiça em Assuntos Ambientais na América Latina e no Caribe, conhecido como Acordo de Escazú, em vigência internacional desde 2021. Assinado pelo Brasil em 2018, o acordo somente foi encaminhado ao Congresso Nacional em maio de 2023, mas sua tramitação não foi acelerada e sequer foi aprovado ainda na Comissão de Relações Exteriores e Defesa Nacional da Câmara dos Deputados. Esse tratado determina a máxima transparência das informações ambientais, a vedação ao retrocesso e o princípio da progressividade no cumprimento de tais direitos procedimentais, essenciais para a garantia do direito ao meio ambiente saudável. Estabelece compromissos para facilitar o acesso à informação e à participação de grupos e segmentos vulneráveis, povos originários e comunidades tradicionais. Tal acordo vinculante é o primeiro tratado em todo o mundo a determinar que aos Países as medidas (políticas, normas, mecanismos) que garantam a atuação livre de ameaças e violência das pessoas, grupos e organizações que defendem direitos humanos em questões ambientais.

As principais leis ambientais do País têm dois dos quatro pilares (a saber, os três direitos de acesso e a proteção de defensores de direitos humanos em questões ambientais) do Acordo de Escazú: informação e participação social. Alguns exemplos:

• A Lei no 6.938/1981 da Política Nacional do Meio Ambiente, que criou o SINIMA – Sistema Naciona de Informações Ambientais, o Conama – Conselho Nacional do Meio Ambiente, o SINAMA Sistema Nacional do Meio Ambiente, para articular órgãos governamentais e setores da sociedade;

• A Lei no 9433/1997, da Política Nacional de Recursos Hídricos, que criou o cria o Sistema Nacional de Gerenciamento de Recursos Hídricos e o Conselho Nacional de Recursos Hídricos, contemplando membros de representantes de vários segmentos da sociedade;

• Na área de políticas de saneamento básico, a implementação recente do Sistema Nacional de Informações em Saneamento Básico, dando continuidade ao legado do anterior sistema, atendendo ao disposto na Lei de Saneamento Básico (Lei nº 11.445/2007), atualizada pelo Novo Marco Regulatório do Saneamento (Lei nº 14.026/2020);

• No campo da legislação e políticas de proteção da vegetação nativa, com destaque para a Lei no 12.651/2012, apelidada de Novo Código Florestal, destacam-se os sistemas de informações do Cadastro Ambiental (SICAR) e o Sistema Nacional de Controle da Origem e dos Produtos Florestais (Sinaflor), além do Sistema Nacional de Informações Florestais (SNIF) previsto em norma diversa.

A lista de sistemas de informações relativas ao meio ambiente é enorme; são também muitas as instâncias colegiadas, consultivas ou decisórias, com participação de interlocutores de instituições de pesquisa, de organizações da sociedade civil, de movimentos sociais e indígenas, entre outros.

Anos antes do advento da Lei de Acesso à Informação (LAI), houve a promulgação da Lei no 10650/2003 que normatizou o acesso público aos dados e informações ambientais existentes nos órgãos e entidades integrantes do Sistema Nacional do Meio Ambiente (Sisnama) e definiu que qualquer pessoa, independentemente da comprovação de interesse específico, terá acesso às informações de que trata tal Lei.

Entretanto, há muitas pendências na implementação dos vários sistemas de informações ambientais criados como instrumentos essenciais para a gestão de políticas públicas. Por serem decorrentes de políticas setoriais específicas, coordenadas por órgãos federais diversos, há desafios na integração das informações digitais desses sistemas. Alguns desses e suas normas surgiram em períodos em que as tecnologias e sistemas de informações geográficas (SIG) ainda não estavam tão avançados como atualmente.

Enfim, a existência de lacunas e barreiras na gestão das informações digitais sobre o meio ambiente nos sistemas a cargo de governos também criam dificuldades para um maior controle social e governança das políticas ambientais. É relevante que diversas instituições de pesquisa e da sociedade civil têm atuado no campo do uso e disponibilização de informações digitais, associadas aos mecanismos e referências de informações geográficas (SIG), com a produção de relatórios, mapas e cnhecimentos sobre a situação ambiental do país. Dois exemplos significativos: o primeiro é o MapBiomas, uma rede colaborativa, formada por ONGs, universidades e empresas de tecnologia, para o mapeamento anual da cobertura de uso da terra, monitoramento de desmatamento, de superfície de água e ocorrência de queimadas, valendo-se inclusive mediante sensoriamento remoto e imagens de satélite; o segundo é o Sistema de Estimativas de Emissões e Remoções de Gases de Efeito Estufa (SEEG), do Observatório do Clima, para a elaboração de estimativas anuais das emissões de gases de efeito estufa no Brasil, análises sobre tendências de tais emissões e desdobramentos à luz das políticas ambientais.

Ora, avançar a governança democrática ambiental , notadamente na eficaz aplicação dos direitos de acesso à informação, à participação e à justiça, deve ser compreendida como uma tarefa necessária e urgente, por um lado, e por outro, facilitada pelo acervo normativo da legislação de meio ambiente e por uma sociedade cada vez mais usuária de meios digitais de produção de conhecimentos e de relações sociais. Enfim, de construção de sociedade digital com responsabilidade ambiental.

Rubens Harry Born é diretor da Fundação Esquel, presidente do Conselho Diretor do Idec – Instituto de Defesa do Consumidor, membro da coordenação do FBOMS – Fórum Brasileiro de ONGs e Movimentos Sociais para o Meio Ambiente e o Desenvolvimento, colaborador do Fundo Casa Socioambiental; membro do Conama – Conselho Nacional do Meio Ambiente e da Conasq – Comissão Nacional de Segurança Química. Há 45 anos atuando em temas de Meio Ambiente. Engenheiro civil com especialização em engenharia ambiental, advogado, mestre e doutor em saúde pública ambiental. Este texto foi escrito especialmente para esta edição da poliTICs em agosto de 2024.

POLITICS

A revista POLI**TICS** é uma publicação do Nupef . ISSN: 1984-8803 [nupef.org.br] [politics.org.br]

[publicado em outubro de 2024]

Nupef nic.br cgi.br

Nupef

O Nupef é uma organização sem fins de lucro, dedicada à reflexão, análise, produção de conhecimento e formação, principalmente centradas em questões relacionadas às Tecnologias da Informação e Comunicação (TICs) e suas relações políticas com os direitos humanos, a democracia, o desenvolvimento sustentável e a justiça social.

Além de realizar cursos, eventos, desenvolver pesquisas e estudos de caso, o Nupef edita a POLITICS, a Rets (Revista do Terceiro Setor) e mantém o projeto Tiwa – um centro de serviços Internet que serve de apoio técnico aos projetos do instituto e das entidades parceiras.

https://nupef.org.br
https://politics.org.br
https://espectro.org.br
https://rets.org.br
https://tiwa.org.br