

Setembro de 2026

Mapa da Criptografia na América Latina



Internet Society
Capítulo Brasil

Coordenação

Luiza Dutra

Pedro Amaral

Thobias Prado Moura

Diretoria Executiva

Flávio Rech Wagner

Pedro de Perdigão Lana

Thobias Prado Moura

Laura Gabrieli Pereira da Silva

Camila Akemi Tsuzuki

João Moreno Rodrigues Falcão

Apoio

Meta

Este relatório apresenta os resultados do levantamento comparativo sobre o tratamento jurídico da criptografia em dez países da América Latina, conduzido em parceria entre a ISOC Brasil e o IRIS.

Sumário

Sumário Executivo	2
1. O Levantamento	3
1.1 Identificação	3
1.2 Objetivo	4
1.3 Contexto regional	4
2. Metodologia	4
3. Quadro comparativo	5
4. Achados transversais	8
5. Panorama por país	9
5.1 Brasil	9
5.2 Argentina	10
5.3 Bolívia	11
5.4 Chile	12
5.5 Colômbia	13
5.6 Equador	13
5.7 Paraguai	14
5.8 Peru	15
5.9 Uruguai	16
5.10 Venezuela	16
6. Caminhos para a agenda regional	17
7. Considerações finais	18



Sumário Executivo

Este relatório consolida os resultados do levantamento comparativo sobre o tratamento jurídico da criptografia em dez países da América do Sul, conduzido pela ISOC Brasil em parceria com o IRIS, Instituto de Referência em Internet e Sociedade. O levantamento examinou Brasil, Argentina, Bolívia, Chile, Colômbia, Equador, Paraguai, Peru, Uruguai e Venezuela a partir de quatro perguntas, aplicadas a fontes primárias de cada ordenamento: (i) se existem leis que garantam o direito ao uso de criptografia ou protejam comunicações criptografadas; (ii) se existem leis ou propostas que permitam, exijam ou facilitem o acesso estatal a comunicações criptografadas; (iii) se existem obrigações legais impostas a provedores ou empresas relacionadas ao uso, à implementação ou ao enfraquecimento de criptografia; e (iv) se a legislação associa a criptografia à proteção de direitos fundamentais, como privacidade, liberdade de expressão, proteção de dados pessoais ou segurança da informação.

O quadro que emerge do levantamento é o de uma proteção à criptografia frágil e desigual. Nenhum dos dez países impõe *backdoors* ou o enfraquecimento deliberado da criptografia em lei vigente, e as obrigações dirigidas a provedores são majoritariamente protetivas, no sentido de exigir a adoção de criptografia para a segurança de dados e comunicações. A proteção, contudo, é quase sempre funcional e indireta, ancorada nos regimes de proteção de dados pessoais e nas garantias constitucionais de sigilo das comunicações, e não em um reconhecimento jurídico da criptografia em si. O Chile é a única exceção: o artigo 3º da Lei 21.663/2024, a Lei-Quadro de Cibersegurança, reconhece expressamente a toda pessoa o direito de adotar medidas de segurança, incluindo criptografia.

Essa proteção convive com vetores de pressão heterogêneos, que raramente assumem a forma de proibição direta. No Brasil, a pressão é penal, com a Lei 15.358/2026 e a Lei nº 15.487/2026 associando o uso de criptografia avançada e de VPNs a agravamento de pena. Na Colômbia, é estrutural, com a Lei 1621/2013 e o Decreto 1704/2012 organizando uma arquitetura legal de vigilância que subordina a oferta de voz criptografada ao Estado. No Equador, é de inteligência, com a Lei Orgânica de Inteligência de 2025 ampliando os deveres de colaboração de operadoras e o precedente do caso Ola Bini tratando o uso de criptografia como indício de conduta criminosa. Na Venezuela, é fática, com bloqueios de VPNs e da rede Tor em nível de rede e evidências da aquisição de ferramentas de espionagem que contornam a criptografia de ponta a ponta. A tabela a seguir sintetiza o panorama por dimensão de análise.

Dimensão	Panorama predominante	Pontos de atenção
Direito ao uso	Proteção funcional indireta na quase totalidade da amostra	Apenas o Chile reconhece um direito expresse (art. 3º, Lei 21.663/2024)
Acesso estatal	Metade da amostra sem previsão específica	Vigilância ampla ou pressão concreta na Colômbia, no Equador e na Venezuela; tensões legislativas no Brasil e no Chile
Obrigações a provedores	Obrigações de uso protetivo predominam; nenhum país exige <i>backdoors</i>	Na Colômbia, as obrigações estruturam o suporte à vigilância estatal
Direitos fundamentais	Associação avança pela via da proteção de dados	Consolidada apenas no Brasil e no Chile; no Brasil, a legislação penal recente opera em sentido oposto

1. O Levantamento

1.1 Identificação

Item	Descrição
Título	Mapa da Criptografia na América Latina
Executoras	ISOC Brasil (Capítulo Brasileiro da Internet Society) e IRIS (Instituto de Referência em Internet e Sociedade)
Escopo	Dez países da América do Sul: Argentina, Bolívia, Brasil, Chile, Colômbia, Equador, Paraguai, Peru, Uruguai e Venezuela
Dimensões de análise	Direito ao uso de criptografia; acesso estatal a comunicações cifradas; obrigações impostas a provedores; associação entre criptografia e direitos fundamentais
Corte temporal	Situação normativa apurada até julho de 2026
Licença	Creative Commons BY-NC-SA 4.0

1.2 Objetivo

O objetivo central do levantamento é oferecer uma base comparada, documentada em fontes primárias, sobre como os ordenamentos sul-americanos tratam a criptografia, por três caminhos complementares: (i) permitir a consulta rápida ao estado normativo de cada país nas quatro dimensões de análise; (ii) fornecer a jornalistas, formuladores de políticas públicas, pesquisadores e organizações da sociedade civil a fundamentação normativa necessária ao trabalho de pesquisa e incidência; e (iii)

identificar tendências regionais de proteção e vetores de pressão sobre a criptografia, de modo a orientar a agenda de *advocacy* das organizações que atuam na defesa de uma Internet aberta, globalmente conectada, segura e confiável.

Este relatório não constitui opinião jurídica, nem endossa ou se opõe a legislações específicas. Seu propósito é documentar o estado normativo de cada país, explicitar as tensões em curso e qualificar o debate público sobre criptografia e direitos digitais na região.

1.3 Contexto regional

O levantamento foi conduzido em um momento particularmente sensível da agenda regional. No Brasil, o ciclo recente combinou a aprovação da Lei 15.358/2026, a Lei Antifacção, que criou majorante pelo emprego de criptografia avançada por organizações criminosas, a aprovação pelo Senado, em julho de 2026, do PL 3066/2025 transformada na Lei nº 15.487/2026, que agrava penas pelo uso de técnicas de ocultação de IP, e a pendência, no Supremo Tribunal Federal, da ADI 5527 e da ADPF 403, que discutem a constitucionalidade de ordens de quebra de criptografia. No Chile, a implementação da Lei-Quadro de Cibersegurança inaugurou o primeiro reconhecimento expresso do direito à criptografia na região. No Equador, a Lei Orgânica de Inteligência de 2025 redesenhou os deveres de colaboração do setor de telecomunicações com o sistema de inteligência. Na Venezuela, os bloqueios de VPNs se intensificaram no contexto pós-eleitoral.

2. Metodologia

O levantamento aplicou a cada país as quatro perguntas uniformes enunciadas no Sumário Executivo, respondidas a partir de fontes primárias: textos constitucionais, leis, decretos, resoluções, regulamentos setoriais e jurisprudência. Relatórios de organizações da sociedade civil e de organismos internacionais foram utilizados subsidiariamente, sobretudo para documentar práticas estatais que não estão formalizadas em lei, como os bloqueios de rede na Venezuela, caso em que a natureza secundária da fonte está indicada na respectiva ficha. A situação normativa reflete o apurado até julho de 2026, incluindo proposições legislativas em tramitação quando relevantes para a compreensão das tensões em curso.

Para permitir a leitura comparada, as respostas foram codificadas em categorias por dimensão, apresentadas no quadro da seção 3. Na primeira dimensão, distinguem-se o direito expresso em lei, a proteção funcional indireta e os ordenamentos que regulam apenas a infraestrutura de confiança

digital, como assinaturas e certificados. Na segunda, distinguem-se os países sem previsão específica de acesso estatal, aqueles com regimes de interceptação legal atravessados por tensões em curso e aqueles em que há vigilância ampla ou pressão concreta sobre comunicações cifradas. Na terceira, separam-se as obrigações de uso protetivo, as obrigações restritas à certificação e assinatura digital e as obrigações que estruturam o suporte à vigilância estatal. Na quarta, gradua-se a associação entre criptografia e direitos fundamentais em consolidada, parcial, sobretudo via proteção de dados, e indireta ou ausente.

3. Quadro comparativo

O quadro a seguir consolida a codificação dos dez países nas quatro dimensões de análise. O sinal ▲ indica a existência de tensão legislativa, exceção setorial ou pressão fática relevante, detalhada na ficha do respectivo país na seção 5.

País	Direito ao uso	Acesso estatal	Obrigações a provedores	Direitos fundamentais
Brasil	Proteção funcional indireta ▲	Interceptação legal com tensões em curso	Obrigações de uso protetivo	Reconhecida como instrumento de proteção de direitos fundamentais ▲
Argentina	Proteção funcional indireta	Sem previsão específica	Apenas certificação e assinatura digital	Indireta ou ausente
Bolívia	Proteção funcional indireta	Sem previsão específica	Apenas certificação e assinatura digital	Parcial, via proteção de dados
Chile	Direito expresso em lei	Interceptação legal com tensões em curso	Obrigações de uso protetivo ▲	Reconhecida como instrumento de proteção de direitos fundamentais
Colômbia	Proteção funcional indireta ▲	Vigilância ampla ou pressão concreta	Obrigações de suporte à vigilância	Parcial, via proteção de dados
Equador	Proteção funcional indireta	Vigilância ampla ou pressão concreta ▲	Obrigações de uso protetivo	Parcial, via proteção de dados
Paraguai	Apenas infraestrutura de confiança digital	Sem previsão específica	Apenas certificação e assinatura digital	Indireta ou ausente

País	Direito ao uso	Acesso estatal	Obrigações a provedores	Direitos fundamentais
Peru	Proteção funcional indireta	Sem previsão específica	Obrigações de uso protetivo	Parcial, via proteção de dados
Uruguai	Proteção funcional indireta	Sem previsão específica	Obrigações de uso protetivo	Indireta ou ausente
Venezuela	Proteção funcional indireta	Vigilância ampla ou pressão concreta ▲	Obrigações de uso protetivo	Indireta ou ausente

A leitura vertical do quadro revela a assimetria entre as dimensões. Na primeira coluna, a proteção funcional indireta é a regra, com um único direito expresso, o chileno, e um único ordenamento, o paraguaio, em que a criptografia aparece apenas como pressuposto técnico da infraestrutura de assinaturas. Na segunda, a amostra se divide ao meio entre o silêncio normativo, que abrange Argentina, Bolívia, Paraguai, Peru e Uruguai, e algum grau de acesso ou pressão estatal, que abrange os demais. Na terceira, o dado mais relevante é que não foi encontrada nenhuma obrigação de enfraquecimento ou de *backdoor* em lei vigente em nenhum dos dez países. Na quarta, a associação entre criptografia e direitos fundamentais mostra-se o elo mais fraco da proteção regional, consolidada em apenas dois ordenamentos.

A seguir apresenta-se a distribuição territorial das quatro dimensões, na mesma codificação do quadro, permitindo visualizar de imediato a concentração dos vetores de pressão e o isolamento do caso chileno como único direito expresso da amostra.

Mapa da Criptografia na América Latina

Direito ao uso de criptografia



- Direito expresso em lei
- Proteção funcional indireta
- Apenas infraestrutura de confiança digital

Acesso estatal a comunicações cifradas



- Sem previsão específica
- Interceptação legal com tensões em curso
- Vigilância ampla ou pressão concreta

Obrigações impostas a provedores



- Obrigação de uso protetivo
- Apenas certificação e assinatura digital
- Obrigações de suporte à vigilância

▲ indica tensão legislativa, exceção setorial ou pressão fática relevante, detalhada na ficha do respectivo país.

Criptografia e direitos fundamentais



- Associação consolidada
- Parcial, via proteção de dados
- Indireta ou ausente

4. Achados transversais

O primeiro achado do levantamento é a ausência de *backdoors* legais na região. Nenhum dos dez países examinados impõe, em lei vigente, a criação de vulnerabilidades deliberadas, o fornecimento sistemático de chaves privadas ou obrigações de decifração dirigidas a provedores de aplicações. Esse resultado contrasta com o debate internacional, em que propostas de acesso excepcional voltam periodicamente à pauta, e constitui um patrimônio normativo regional que as organizações de defesa da criptografia têm interesse em preservar e explicitar. A exceção pontual, de alcance setorial restrito, é a Resolução 3885-EXENTA do Sernapesca chileno, que obriga fornecedores de equipamentos de gravação do setor pesqueiro a entregar chaves à agência, e que confirma, pelo seu isolamento, a inexistência de um regime geral de acesso.

O segundo achado é o caráter funcional e indireto da proteção jurídica da criptografia. Em nove dos dez países, a criptografia não é objeto de reconhecimento jurídico próprio: é protegida na medida em que serve à inviolabilidade das comunicações, garantida nas constituições, e à segurança de dados pessoais, exigida nas leis gerais de proteção de dados e em seus regulamentos, como o Decreto 8.771/2016 no Brasil, o Decreto Executivo 904/2023 no Equador e o Decreto Supremo 016-2024-JUS no Peru, que citam nominalmente a criptografia como medida de segurança. Essa arquitetura protege o uso, mas o faz por derivação, o que a torna sensível a mudanças nos regimes dos quais depende. O Chile rompeu esse padrão ao positivar, no artigo 3º da Lei 21.663/2024, o direito de toda pessoa a adotar medidas de segurança da informação, incluindo o uso de criptografia, reafirmado pelo Decreto 2/2025.

O terceiro achado é a heterogeneidade dos vetores de pressão. A erosão da proteção não segue um modelo único na região. No Brasil, avança pela via penal, com a majorante da Lei 15.358/2026 para o emprego de criptografia avançada por facções e o agravante da Lei nº 15.487/2026 para o uso de técnicas de ocultação de IP, incluindo VPNs. Na Colômbia, é estrutural e preexistente, organizada pela Lei 1621/2013 e pelo Decreto 1704/2012 em uma arquitetura de interceptação, retenção e monitoramento do espectro. No Equador, é institucional, com a Lei Orgânica de Inteligência de 2025 e com o precedente do caso Ola Bini, em que o uso de criptografia avançada e da rede Tor foi tratado pelo Ministério Público como indício presuntivo de conduta criminosa. Na Venezuela, é fática, operando por bloqueios de rede contra VPNs e Tor e pela aquisição documentada de ferramentas de espionagem, à margem do que o texto constitucional exige. Uma agenda regional de defesa da criptografia precisa, portanto, de respostas diferenciadas por país, e não de uma estratégia única.

O quarto achado é que as obrigações impostas a provedores são majoritariamente protetivas. Onde existem, elas determinam o uso de criptografia, e não o seu enfraquecimento: é o caso do Decreto 8.771/2016 e da LGPD no Brasil, da Lei 21.663 e da Lei 21.719/2024 no Chile, da LOPDP equatoriana, da Lei 29733 peruana, das resoluções da Sudeban no setor bancário venezuelano e do marco uruguaio de cibersegurança reforçado pelo Decreto 66/025. A exceção é a Colômbia, onde as obrigações dirigidas às operadoras, manutenção de infraestrutura de interceptação, retenção de dados por cinco anos, registro de IMEI e reserva da oferta de voz criptografada às agências de inteligência, estruturam o suporte à vigilância estatal, ainda que sem obrigação de quebra da criptografia de ponta a ponta.

O quinto achado é que a associação entre criptografia e direitos fundamentais avança pela via da proteção de dados, mas permanece incompleta. Na maioria dos países, a criptografia aparece nos regimes de proteção de dados como medida técnica vinculada à privacidade e à intimidade, sem alcançar a liberdade de expressão nem o estatuto de garantia autônoma. Apenas Brasil e Chile consolidaram a associação, o primeiro pela combinação entre o Marco Civil da Internet, seu decreto regulamentador e a linha inaugurada pelos votos já proferidos na ADI 5527, o segundo pela positivação expressa da Lei 21.663. No caso brasileiro, contudo, a legislação penal recente opera em sentido oposto à trajetória protetiva, associando à criptografia um sentido de periculosidade que o próprio ordenamento, em suas normas de segurança da informação, desmente.

5. Panorama por país

As fichas a seguir percorrem, para cada país, as quatro dimensões de análise, com indicação das fontes normativas e jurisprudenciais em que se apoiam.

5.1 Brasil

O ordenamento brasileiro não declara um direito explícito à criptografia, mas construiu ao seu redor uma das proteções funcionais mais densas da região. O artigo 5º, inciso XII, da Constituição Federal assegura a inviolabilidade do sigilo das comunicações, e a Emenda Constitucional 115/2022 elevou a proteção de dados pessoais a direito fundamental, no inciso LXXIX do mesmo artigo. No plano infraconstitucional, o Decreto 8.771/2016, que regulamenta o Marco Civil da Internet, cita expressamente a criptografia como medida de segurança que provedores de conexão e de aplicações devem adotar na guarda de dados e comunicações, e o ECA Digital, a Lei 15.211/2025, exige inviolabilidade técnica em produtos de monitoramento voltados a crianças e adolescentes. A jurisprudência acompanha essa arquitetura: no RHC 580.664-RJ, o Superior Tribunal de Justiça firmou

que compelir o investigado a decriptar dispositivos viola o princípio de que ninguém é obrigado a produzir prova contra si.

É no plano do acesso estatal que se concentram as tensões. A interceptação lícita de comunicações é regulada pela Lei 9.296/1996, mediante ordem judicial. Os quatro bloqueios do WhatsApp entre 2015 e 2016, determinados por juízos que exigiam dados protegidos por criptografia de ponta a ponta, foram suspensos, e o STJ assentou que provedores não podem ser sancionados por impossibilidade técnica. A questão de fundo, a constitucionalidade de ordens de quebra de criptografia, permanece pendente na ADI 5527 e na ADPF 403, cuja deliberação foi retomada em dezembro de 2024 sem decisão final. Os votos já proferidos inclinam-se a reconhecer a criptografia como expressão da privacidade e da liberdade de expressão, em julgamento que conta com IRIS, IP.rec e ISOC Brasil na condição de *amici curiae*.

Nesse sentido, as pressões mais recentes contra criptografia são de natureza penal. A Lei 15.358/2026, a Lei Antifacção, criou majorante de dois terços até o dobro da pena pelo emprego de criptografia avançada e comunicações cifradas por organizações criminosas, e o PL 3066/2025, aprovado pelo Senado em 7 de julho de 2026 e posteriormente transformado na Lei nº 15.487, de 6 de agosto de 2026, cria agravante de um terço a dois terços pelo uso de técnicas de ocultação de IP, incluindo VPNs, em crimes contra crianças e adolescentes, no artigo 226-A que acrescenta ao ECA. Nenhuma das duas normas proíbe o uso de criptografia ou de VPNs, mas ambas lhe associam um sentido de periculosidade que destoa do tratamento protetivo dado pelo restante do ordenamento, no qual as obrigações vigentes são de uso: além do Decreto 8.771/2016, a LGPD exige medidas técnicas adequadas dos agentes de tratamento, e a transformação da ANPD em agência reguladora, pela MP 1.317/2025, aprovada pelo Congresso em fevereiro de 2026, tende a reforçar a exigência de criptografia e auditorias periódicas. Não há *backdoors* em lei vigente, e a própria administração federal sinaliza na direção oposta, com a ABIN elegendo a criptografia pós-quântica como prioridade estratégica para 2026.

5.2 Argentina

A Argentina não reconhece um direito explícito à criptografia, mas seu uso é legal e as comunicações cifradas encontram proteção no artigo 18 da Constituição Nacional, que resguarda a inviolabilidade da correspondência e dos papéis privados, na Lei 25.326/2000, de proteção de dados pessoais, que exige medidas de segurança para o tratamento de dados e alcança a criptografia em determinados contextos, e na jurisprudência da Corte Suprema, que no caso Halabi, de 2009, estendeu a proteção constitucional às comunicações digitais e aos metadados.

Não foram identificadas normas que exijam *backdoors*, decifração ou acesso estatal a comunicações criptografadas. A única previsão correlata é a interceptação de comunicações telefônicas mediante ordem judicial, disciplinada pelo Código Procesal Penal, a Lei 23.984/1991, que não alcança comunicações cifradas nem prevê quebra de criptografia. No mesmo sentido, as obrigações dirigidas a provedores restringem-se à infraestrutura de confiança digital: o Decreto 2628/2002, que regulamenta a Lei de Assinatura Digital, a Lei 25.506/2001, trata de assinatura e autenticação sem exigir mecanismos criptográficos específicos, fornecimento de chaves ou enfraquecimento.

A associação entre criptografia e direitos fundamentais é muito limitada e indireta. As únicas referências identificadas remetem à Lei 25.326/2000 e à Lei 27.699/2022, que aprovou o protocolo modificatório da Convenção 108 sobre tratamento automatizado de dados pessoais. Privacidade, sigilo das comunicações e liberdade de expressão são tutelados, mas sem que a criptografia seja reconhecida como instrumento jurídico dessa tutela, o que faz da Argentina um caso de proteção sólida no plano constitucional e de dados pessoais, porém silente quanto à criptografia em si.

5.3 Bolívia

Na Bolívia, a proteção da criptografia decorre apenas de interpretação. A Lei 164/2011, a Lei Geral de Telecomunicações e TIC, garante expressa e taxativamente a inviolabilidade e o segredo absoluto das comunicações, no artigo 56, e reconhece a validade jurídica de documentos e transações eletrônicas celebrados com mecanismos criptográficos de integridade e autenticação, no artigo 43. Com o Decreto Supremo 1793/2013, ela estrutura a infraestrutura nacional de certificação digital, que inclui dispositivos de criptografia, certificados e firma digital, e a Ley de Ciudadanía Digital reforça, em seu artigo 12, a proteção de dados pessoais. Nenhuma dessas normas, contudo, cria um direito geral ao uso de criptografia em comunicações.

Inexiste legislação específica de quebra ou de acesso excepcional. A solicitação de informações sobre telecomunicações exige ordem judicial prévia e fundamentada, nos termos do artigo 175 do Decreto Supremo 1391/2012, que regulamenta a Lei 164, e a interceptação prevista no Código Penal e nas normas de telecomunicações não contempla a quebra de criptografia nem a obrigação de descriptografar (ou decifrar). As obrigações vigentes concentram-se na certificação e na soberania tecnológica: as entidades certificadoras, reguladas pela ATT e pela ADSIB, operam criptografia assimétrica, os provedores devem garantir a inviolabilidade das comunicações em suas redes e o setor estatal é impelido ao uso de software livre e padrões abertos em nome da soberania e da auditabilidade dos sistemas.

A associação com direitos fundamentais é parcial. O legislador boliviano trata a criptografia primariamente como ferramenta técnica de validade jurídica e de soberania tecnológica do Estado, e não como mecanismo autônomo de defesa de direitos. O Anteprojeto de Lei de Proteção de Dados Pessoais elaborado pela AGETIC em 2023 aponta para uma mudança: seu artigo 70 determina expressamente a adoção de criptografia por responsáveis e encarregados de tratamento, e a notificação de violações de segurança deve informar as medidas adotadas, com a criptografia como único exemplo citado, vinculando-a à segurança da informação, à proteção de dados e à privacidade, ainda sem menção à liberdade de expressão.

5.4 Chile

O Chile é o único país da amostra a reconhecer um direito expresso à criptografia. O artigo 3º da Lei 21.663/2024, a Lei-Quadro de Cibersegurança, assegura a toda pessoa o direito de adotar as medidas de segurança que estime necessárias, incluindo o uso de criptografia, direito reafirmado pelo Decreto 2/2025. A esse reconhecimento soma-se a Lei 18.168, de telecomunicações, que proíbe provedores de bloquear aplicações lícitas e, com isso, protege indiretamente o uso de VPNs.

Não há *backdoors* legais nem obrigação de quebrar criptografia de ponta a ponta. A interceptação de conteúdo exige mandado judicial fundamentado, nos termos dos artigos 222 a 226 do Código Processual Penal. A tensão em curso decorre da Lei 21.577/2023, de combate ao crime organizado, que permite ao Ministério Público requisitar dados de assinante sem mandado e que introduziu o artigo 225 bis do CPP, autorizando o acesso remoto judicial a dispositivos em investigações de crime organizado, um instrumento de *hacking* governamental circunscrito.

Por outro lado, as obrigações impostas a provedores são de implementação, e não de enfraquecimento. A Lei 21.663 obriga os operadores de importância vital a adotar criptografia e a notificar incidentes à Agência Nacional de Cibersegurança, com multas que alcançam 40.000 UTM, a Lei 21.719/2024, a nova lei de proteção de dados, exige pseudonimização e criptografia e adota *privacy by design* como princípio obrigatório, e a Comissão para o Mercado Financeiro impõe ao setor bancário criptografia robusta e duplo fator de autenticação. A exceção setorial é a Resolução 3885-EXENTA do Sernapesca, que obriga fornecedores de equipamentos de gravação do setor pesqueiro a entregar chaves à agência. O quadro geral, que a Freedom House classificou em 2024 como o de líder regional em direitos digitais, combina o reconhecimento expresso do direito, a ausência de propostas de enfraquecimento e uma institucionalidade de supervisão em consolidação.

5.5 Colômbia

A Colômbia não reconhece um direito geral à criptografia, mas oferece proteção indireta por três vias: a Lei 527/1999, que reconhece assinaturas digitais e pressupõe o uso lícito de criptografia, a Lei 1581/2012, que exige medidas técnicas de segurança para dados pessoais, e a Circular 002/2024 da Superintendência de Indústria e Comércio, que exige *privacy by design* com técnicas criptográficas. Persiste, contudo, uma restrição funcional singular na amostra: o artigo 102 da Lei 418/1997 proíbe a criptografia de conteúdo em radiocomunicações.

É no acesso estatal que o caso colombiano se destaca. O artigo 17 da Lei 1621/2013, a lei de inteligência, permite que as agências monitorem o espectro eletromagnético sem mandado judicial, autorização que a Corte Constitucional aceitou na sentença C-540/2012 e que órgãos da ONU criticam desde então. O artigo 44 da mesma lei obriga as operadoras a reter o histórico de comunicações por cinco anos e a fornecê-lo a diretores de inteligência mediante simples pedido escrito, e seu parágrafo segundo reserva a oferta de voz criptografada exclusivamente às agências de inteligência. O Decreto 1704/2012 completa a arquitetura ao exigir que as operadoras mantenham infraestrutura habilitada para interceptação, operacionalizada por plataformas como o Sistema Esperanza, da Fiscalía, o PUMA, da polícia judiciária, e o SIGDIRS, da inteligência policial, cujas sondas nas redes das operadoras suscitam preocupações documentadas de monitoramento em massa desde o relatório da Privacy International de 2015.

As obrigações impostas a provedores refletem essa orientação: manutenção de infraestrutura de interceptação, retenção de dados, registro de IMEI vinculado ao assinante, nos termos do Decreto 1630/2011 e da Resolução CRC 3128/2011, e reserva da voz cifrada ao Estado, sem que haja, contudo, obrigação de quebrar criptografia de ponta a ponta. A associação com direitos fundamentais é parcial e tensionada. O artigo 15 da Constituição protege a privacidade, a inviolabilidade das comunicações e o *habeas data*, reconhecido como direito autônomo desde a sentença T-414/1992, e o regime de proteção de dados associa a segurança da informação a técnicas criptográficas, mas o artigo 44 da Lei 1621 e o artigo 102 da Lei 418/1997 operam em sentido contrário, ambiguidade que a ONU e a sociedade civil criticam reiteradamente.

5.6 Equador

O Equador não positivou um direito explícito à criptografia, mas seu uso é legal e a proteção funcional é expressa. A Constituição de 2008 consagra, no artigo 66, a proteção de dados pessoais e a inviolabilidade das comunicações, a Lei Orgânica de Proteção de Dados Pessoais, de 2021, e seu regulamento, o Decreto Executivo 904/2023, reconhecem nominalmente a criptografia e a

pseudonimização como medidas técnicas primordiais de segurança, e a Lei de Comércio Eletrônico, a Lei 100-2002, valida mensagens de dados e firmas eletrônicas, aceitando os mecanismos criptográficos que lhes são subjacentes.

O vetor de pressão é o sistema de inteligência. A Lei Orgânica de Inteligência, de 2025, obriga as instituições públicas a fornecer quaisquer informações solicitadas pelo Sistema Nacional de Inteligência, sem exceções, no artigo 50, e impõe aos operadores de telecomunicações o atendimento a pedidos de informação histórica e em tempo real sobre comunicações, conexões, dados técnicos, localização e identificação, no artigo 52, cabendo à autoridade máxima do sistema solicitar a retenção, abertura, interceptação ou análise de documentos e comunicações. Esse desenho soma-se a dois antecedentes que preocupam: no caso Ola Bini, o Ministério Público tratou o uso de criptografia avançada e da rede Tor como indício presuntivo de conduta criminosa, e a proposta de reforma do Código Orgânico Integral Penal, de 2023, sugeriu a figura do agente secreto informacional, autorizado a infiltrar plataformas e acessar meios fechados de comunicação, com capacidade, na leitura de ativistas, de quebrar criptografia e implantar arquivos sob autorização judicial.

As obrigações dirigidas a provedores permanecem protetivas. A LOPDP exige de responsáveis e encarregados a implementação de medidas de segurança adequadas ao risco, citando expressamente a criptografia robusta, sem determinar métodos específicos nem criar obrigações de decifração ou de acesso estatal, e não foram identificadas normas exigindo *backdoors* ou enfraquecimento deliberado. A associação com direitos fundamentais existe, mas é limitada: a Constituição garante privacidade, intimidade, proteção de dados e liberdade de expressão, a LOPDP vincula a proteção de dados a esses direitos e o Decreto Executivo 904/2023 cita os mecanismos de criptografia robusta como obrigação para garantir a privacidade dos titulares de dados transferidos ou comunicados. O resultado é um ordenamento com proteção de dados avançada convivendo com um aparato de inteligência de alcance amplo, combinação cuja evolução merece acompanhamento próximo.

5.7 Paraguai

O Paraguai é o caso de maior silêncio normativo da amostra. Não há lei que reconheça a criptografia como direito nem que proteja diretamente comunicações criptografadas, e os marcos correlatos são indiretos: a Lei 4.017/10, sobre a validade jurídica de assinaturas eletrônicas e mensagens de dados, a Lei 4.610/12, que reforça o regime de assinatura digital, a Lei 4.868/13, que regula o comércio eletrônico, e a proteção constitucional geral à privacidade e ao sigilo das comunicações.

O ordenamento tampouco regula o acesso estatal a comunicações criptografadas ou mecanismos de quebra. As normas mais próximas são gerais: as garantias constitucionais de sigilo, as hipóteses de interceptação da Lei 1.286/98, o Código Processual Penal, e o marco de telecomunicações da Lei 7.280/24, nenhuma delas mencionando criptografia. As obrigações existentes vinculam-se à infraestrutura de confiança digital, com a neutralidade tecnológica das assinaturas, as regras para provedores de comércio eletrônico, os elementos setoriais de segurança da informação da Lei 6.207/18 e a cooperação digital no Mercosul das Leis 7.021/22 e 7.120/23, sem exigências de enfraquecimento, *backdoors* ou fornecimento de chaves.

A associação com direitos fundamentais não é explícita. O país protege a privacidade, a liberdade de expressão e os dados pessoais, pela Constituição e pelas Leis 4.819/12 e 6.534/20, e internalizou a Convenção de Budapeste sobre cibercrime pela Lei 5.994/17, mas a criptografia aparece apenas como ferramenta técnica implícita, sem reconhecimento jurídico como mecanismo de proteção de direitos. Desse modo, não há restrições, mas tampouco há salvaguardas que estabilizem o uso da criptografia diante de eventuais iniciativas restritivas.

5.8 Peru

No Peru, a proteção é estritamente funcional e técnica, sem um direito autônomo positivado. O artigo 2º, inciso 6, da Constituição de 1993 reconhece o direito à intimidade e ao sigilo e à inviolabilidade das comunicações e documentos privados, salvo ordem judicial nas formas previstas em lei, e é sobre essa base que se assenta o regime de proteção de dados: a Lei 29733, de 2011, e o Decreto Supremo 016-2024-JUS impõem a criptografia forte como requisito técnico inegociável para a custódia, o processamento e o tráfego de dados sensíveis.

Não existem normas ou projetos de lei obrigando a criação de *backdoors* ou de chaves de custódia estatal. A Lei 30096, de delitos informáticos, de 2013, tipifica o acesso ilícito, a interceptação e o abuso de dispositivos, sem criar regime de acesso estatal a comunicações criptografadas. As obrigações dirigidas a provedores são de segurança: o artigo 28 da Lei 29733 exige medidas técnicas, organizativas e legais dos titulares e encarregados de bancos de dados, o regulamento exemplifica a criptografia como medida para a transferência lógica ou eletrônica de dados pessoais, no artigo 52, e a Lei 27269, de firmas e certificados digitais, de 2000, pressupõe mecanismos criptográficos na infraestrutura de identidade, em nenhum caso com obrigações de enfraquecimento.

A associação com direitos fundamentais dá-se sobretudo pela via da proteção de dados, uma vez que o objeto declarado da Lei 29733 é garantir o direito fundamental previsto no artigo 2º, inciso 6, da Constituição. O Marco de Confianza Digital, o Decreto de Urgência 007/2020, embora não cite a criptografia, eleva a segurança cibernética a condição para o pleno exercício da cidadania digital e para a proteção do consumidor e da economia no ambiente online, reforçando o terreno normativo em que a exigência de criptografia forte se apoia.

5.9 Uruguai

O ordenamento uruguaio não contém um direito à criptografia e nenhuma de suas normas trata diretamente do tema. A proteção é indireta, por meio da Constituição da República, da Lei 18.331/2008, de proteção de dados pessoais, e da Lei 18.600/2009, de documento eletrônico e assinatura eletrônica, sem reconhecimento expresso do direito ao uso de criptografia.

Não foram identificadas normas que permitam ou exijam o acesso estatal a comunicações criptografadas, nem regras sobre *backdoors*, decifração ou entrega de chaves. Chama atenção, nesse silêncio, a ausência de diretrizes sobre restrições por ordem judicial ou por segurança nacional, o que gera insegurança jurídica quanto aos limites da atuação das autoridades. As obrigações existentes são limitadas e protetivas, relacionadas à adoção de medidas de segurança da informação que incluem mecanismos criptográficos em determinados contextos: a Lei 20.070/2022, de cibersegurança, o Decreto 64/020, a Circular 2280/2017 do Banco Central e, mais recentemente, o Decreto 66/025, que fortaleceu o marco nacional de cibersegurança e passou a exigir controles de segurança de órgãos públicos e de operadores de serviços críticos.

A associação com direitos fundamentais é indireta, com a Constituição, a Lei 18.331/2008, a Lei 19.307/2014, de serviços de comunicação audiovisual, e a Lei 20.070/2022 relacionando a segurança da informação, a proteção de dados, a privacidade e o sigilo das comunicações a mecanismos de segurança que podem incluir criptografia, e o Decreto 66/025 reforçando essa abordagem ao fortalecer a governança nacional de cibersegurança, sem reconhecer expressamente um direito à criptografia.

5.10 Venezuela

A Constituição da República Bolivariana da Venezuela, de 1999, garante a inviolabilidade das comunicações privadas, salvo ordem judicial com observância do devido processo, no artigo 48, e o direito à vida privada, à intimidade e à confidencialidade, prevendo a limitação do uso da informática para garantir a honra e a intimidade, no artigo 60. A Lei Orgânica de Telecomunicações reforça, no

parágrafo segundo de seu artigo 12, o direito dos usuários à privacidade e à inviolabilidade, salvo autorização constitucional ou razões de interesse público.

Embora a legislação exija ordem judicial para quebras de sigilo, há relatos recorrentes de bloqueios em nível de rede contra VPNs e contra a rede Tor, executados por meio da operadora estatal CANTV, e evidências documentais da aquisição de ferramentas de espionagem capazes de contornar a criptografia de ponta a ponta, práticas que operam em uma zona cinzenta legal e que estão registradas em fontes de sociedade civil indicadas no levantamento.

No plano das obrigações, o Decreto 3691/2018, o regulamento de proteção dos direitos dos usuários de telecomunicações, determina que os operadores estabeleçam mecanismos de proteção do sigilo e da inviolabilidade das comunicações em suas redes, no artigo 7º, e da segurança dos dados pessoais, no artigo 30. No setor bancário, a Sudeban, com base no Decreto-Lei 1402/2014, impôs pela Resolução 641-10144/2010 a implementação de criptografia forte nas comunicações e nos mecanismos de transmissão e armazenamento de informações, nos artigos 20 e 21, exigência reforçada pela Resolução 001.21/2021, no artigo 23. A associação com direitos fundamentais, por sua vez, limita-se ao vínculo entre o segredo das comunicações e a proteção da privacidade estabelecido pela Constituição e pela lei de telecomunicações, sem tratamento normativo da criptografia como instrumento de garantia de direitos.

6. Caminhos para a agenda regional

Os achados do levantamento sugerem quatro linhas de trabalho para as organizações que atuam na defesa da criptografia na região. A primeira é preservar e explicitar como achado positivo a ausência de *backdoors* legais nos dez países. A segunda é promover a migração da proteção indireta para o reconhecimento expresso, para a qual o artigo 3º da Lei 21.663/2024 chilena oferece um modelo normativo testado, compatível com marcos exigentes de cibersegurança e apto à circulação regional.

A terceira linha é diferenciar as respostas conforme o vetor de pressão de cada país. O enfrentamento da criminalização indireta no Brasil passa pelo acompanhamento da sanção e da aplicação da Lei nº 15.487/2026 e da Lei 15.358/2026 e pela atuação perante o STF na ADI 5527 e na ADPF 403; o caso colombiano exige incidência sobre uma arquitetura de vigilância consolidada há mais de uma década, com atenção às revisões periódicas da lei de inteligência; o equatoriano requer o monitoramento da regulamentação da Lei Orgânica de Inteligência de 2025 e da eventual retomada da figura do agente secreto informacional; e o venezuelano demanda documentação técnica continuada de práticas que

não passam pelo processo legislativo. A quarta linha é ocupar os espaços de regulamentação da proteção de dados, que o levantamento identifica como a via pela qual a criptografia efetivamente ingressa nos ordenamentos da região, de modo que autoridades como a ANPD brasileira, a Agência Nacional de Cibersegurança chilena e as autoridades de dados em estruturação, como a boliviana, consolidem a exigência de criptografia forte em seus atos normativos.

7. Considerações finais

O levantamento indica que a América do Sul não caminha, por ora, para a imposição legal de *backdoors*, mas tampouco consolidou a criptografia como objeto de proteção jurídica autônoma. Entre esses dois polos, o que existe é um mosaico de proteções funcionais, silêncios normativos e pressões localizadas, cuja direção dependerá de disputas em curso: a deliberação pendente do Supremo Tribunal Federal brasileiro, a implementação da Lei-Quadro de Cibersegurança chilena, a regulamentação da lei de inteligência equatoriana e a persistência da arquitetura de vigilância colombiana.

A experiência chilena demonstra que o reconhecimento expresso do direito à criptografia é normativamente viável na região. Os casos brasileiro, equatoriano e venezuelano mostram, por sua vez, que a erosão da proteção raramente ocorre por proibição direta: avança por agravantes penais, por poderes amplos de inteligência e por práticas de bloqueio à margem da lei. Acompanhar esses vetores, e não apenas a legislação dedicada ao tema, é condição para uma agenda eficaz de defesa da criptografia na América Latina.