ARTICLE 19

Brasil: Projeto de Lei de Cibercrimes

Janeiro de 2012

Legal analysis

Sumário Executivo

Em janeiro de 2012, a ARTIGO 19 analisou a Proposta Substitutiva do Senado Federal Brasileiro ao Projeto de Lei da Câmara No. 89 de 2003 (o "Projeto de Lei"). O Projeto de Lei propõe a criação de novas medidas relativas à prevenção, identificação e punição de crimes cometidos com o uso da Internet. A ARTIGO 19 está fortemente preocupada que uma parte dessas medidas sejam contrárias aos direitos à liberdade de expressão e de informação e, deste modo, faz uma série de recomendações para que o Projeto de Lei esteja em conformidade com normas internacionais.

O Projeto de Lei não oferece qualquer garantia ao direito à liberdade de expressão ou de informação. Nós também estamos preocupados com o fato dessas medidas não apenas prejudicarem esses direitos, mas de também serem incompatíveis com a legislação em tramitação no Congresso Nacional que procura assegurar os direitos fundamentais online.

O Projeto de Lei prevê uma série de medidas que transformariam as empresas privadas responsáveis pelo fornecimento de serviços de Internet em uma força policial online. É possível que o Projeto de Lei exija que essas empresas denunciem à polícia supostas violações do código penal e imponha responsabilidade penal às partes que não cumprirem esse deveres. As mesmas medidas exigem a fiscalização maciça e a retenção de dados de todas as comunicações online por essas mesmas empresas privadas, que não possuem responsabilidade jurídica necessária para tais atos, por um período de três anos, com poucas restrições nas circunstâncias sob as quais um tribunal poderia ordenar a divulgação dos dados. Medidas semelhantes já foram consideradas inconstitucionais em alguns países europeus, e o governo brasileiro se mostra ávido a enfrentar semelhante disputa em seus próprios tribunais.

O Projeto de Lei também contém proibições vagas sobre as "traições" nos casos de compartilhamento de dados eletrônicos, assim como medidas amplas para a proteção de informações pessoais. Ambas as medidas restringem potencialmente a capacidade de delatores de divulgar informações de interesse público. Outras medidas problemáticas incluem restrições ambíguas ao acesso a computadores e a obtenção e transferência de dados que não preveem a comprovação de intenção para que haja imposição de responsabilidade penal. Tais medidas potencialmente criminalizam o uso diário de computadores que não causam nenhum mal. De maneira similar, crimes relativos à "difusão de códigos maliciosos" também não preveem a necessidade de comprovar intenção.

A ARTIGO 19 solicita com urgência ao governo brasileiro que faça um revisão substancial das medidas previstas no Projeto de Lei, de forma que garanta o respeito aos direitos à liberdade de expressão e de informação no país.

Recomendações

1. O Projeto de Lei deve reivindicar a aplicação dos direitos à liberdade de expressão e de informação em todas as formas eletrônicas de comunicação, incluindo as realizadas na Internet.
2. Provedores não devem ser requisitados a monitorar ou delatar supostas violações online do código penal. Da mesma forma, tais empresas não devem ser sujeitas à responsabilidade civil ou penal por não cumprirem ou recusarem-se a cumprir tal conduta.
3. As exigências gerais para que os provedores de Internet reúnam e retenham dados relativos a comunicações online devem ser removidas.
4. Medidas que proíbam o "acesso" a sistemas de computadores e a obtenção ou transferência de dados que violem medidas de segurança devem exigir a comprovação de intencionalidade para que haja imposição de responsabilidade penal.

Índice de Conteúdos

Sobre o Programa Jurídico da Artigo 19

O programa jurídico da ARTIGO 19 defende o desenvolvimento de normas avançadas para a liberdade de expressão e o acesso à informação no cenário internacional, assim como sua implementação em sistemas jurídicos nacionais. O programa jurídico já produziu uma série de publicações para o estabelecimento de normas, que esboçam projetos de direito internacional e comparado e que melhoraram práticas em áreas como, por exemplo, leis de difamação, acesso à informação e regulamentação de transmissões.

Com base nessas publicações e na experiência geral da ARTIGO 19 em matéria jurídica, o Programa Jurídico publica uma série de análises jurídicas todos os anos, assim como comentários sobre projetos de lei e também sobre leis existentes que afetam o direito à liberdade de expressão. Esse trabalho analítico, desenvolvido desde 1998 como medida de apoio aos esforços positivos para reformas legislativas ao redor do mundo, frequentemente leva a melhoras substanciais nas legislações nacionais propostas ou existentes. Todas as nossas análises estão disponíveis online em http://www.article19.org/resources.php/legal/.

Se você deseja discutir esta análise ou se tem algum assunto para o qual você gostaria que o Programa Jurídico da ARTIGO 19 desse atenção, contate-nos via e-mail através do endereço legal@article19.org. Para mais informações sobre o trabalho da ARTIGO 19 no Brasil, por favor contate Paula Martins, Diretora da ARTIGO 19 Brasil através do e-mail paula@article19.org ou Laura Tresca, no e-mail laura@article19.org, ou pelo telefone (11) 3057 0071.

Introdução

A Proposta Substitutiva do Senado Federal ao Projeto de Lei da Câmara No. 89 de 2003 (o "Projeto de Lei")[1], de autoria do senador Eduardo Azeredo, criará uma emenda ao Código Penal brasileiro e a diversas outras leis, com o intuito de criar novos procedimentos relativos à prevenção, identificação e punição de cibercrimes. A ARTIGO 19 está fortemente preocupada com o fato de que a versão final da lei manterá medidas contrárias aos direitos à liberdade de expressão e de informação. Esta análise, portanto, faz diversas recomendações para garantir que a lei proteja adequadamente os direitos à liberdade de expressão e de informação.

A ARTIGO 19 possui ampla experiência de trabalho com liberdade de expressão e acesso à informação no Brasil. Com o nosso escritório regional na América do Sul tendo base em São Paulo, nós fazemos campanhas para diversas questões relativas à liberdade de expressão e de informação no Brasil; recentemente enviamos um relatório sobre o Brasil como parte da Revisão Periódica Universal das Nações Unidas[2] e também fizemos uma série de recomendações para auxiliar no desenvolvimento da nova lei de acesso à informação do país.[3] Também em 2011, a ARTIGO 19 acolheu bem a decisão do Supremo Tribunal Federal em defesa ao direito de defender ideias controversas.[4] Sobre a questão da legislação de crimes cibernéticos, o Programa Jurídico também produziu recentemente análises sobre tais legislações no Iraque e no Irã.[5]

Embora tenha havido desenvolvimentos positivos em relação à liberdade de expressão no Brasil recentemente, também houve uma série de decisões judiciais recentes que permitiram a censura de notícias, de postagens em blogs e de informação de interesse público. De acordo com o relatório de transparência do Google, o governo brasileiro está em quarto lugar no mundo no número de pedidos feitos ao mecanismo de busca para remover conteúdo da Internet, no período de janeiro a junho de 2011. O governo brasileiro também foi o segundo colocado no mundo no número de pedidos feitos ao Google sobre a identidade de usuários da Internet.[6] A ARTIGO 19 está preocupada que o Projeto de Lei irá encorajar o governo brasileiro a restringir ainda mais o fluxo livre de informações na Internet.

Esta análise legal aponta diversos problemas no Projeto de Lei que necessitam ser discutidos. Nenhuma medida na lei garante ou nem mesmo trata da importância de salvaguardar os direitos à livre expressão e à informação na Internet. O Projeto de Lei prevê uma série de medidas que transformariam as empresas privadas responsáveis pelo fornecimento de serviços de Internet em uma força policial online. É provável que o Projeto de Lei exija que essas empresas denunciem à polícia supostas violações do código penal e imponha responsabilidade penal às partes que não cumprirem esse deveres. As mesmas medidas exigem a fiscalização maciça e a retenção de dados

[1] Esta análise é baseada na tradução não oficial do Projeto de Lei do português ao inglês em dezembro de 2011. A ARTIGO 19 não tem responsabilidade quanto à precisão dessas traduções ou por comentários baseados em traduções errôneas ou enganosas. O texto desta tradução encontra-se disponível para análise sob pedido ao Programa Jurídico da ARTIGO 19 (legal@article19.org).

[2] ARTIGO 19 "Brasil: Submissão da ARTIGO 19 para a Revisão Periódica Universal das Nações Unidas", 29 de novembro de 2011, acesse: http://www.article19.org/resources.php/resource/2880/en/brazil:-article-19's-submission-to-the-un-universal-periodic-review

[3] ARTIGO 19 "O Brasil adota Lei de Acesso à Informação", 22 de novembro de 2011, acesse: http://www.article19.org/resources.php/resource/2862/en/brazil-adopts-access-to-information-law

[4] ARTIGO 19 "Supremo Tribunal Federal defende o direito à liberdade de expressão", 20 de junho de 2011, acesse: http://www.article19.org/resources.php/resource/1823/en/brazil:-supreme-court-defends-right-to-freedom-of-expression

[5] Estas análises estão disponíveis sob pedido ao Programa Jurídico da ARTIGO 19.

[6] Ver Relatório de Transparência do Google, acessado em 21 de dezembro de 2011: http://www.google.com/transparencyreport/governmentrequests/BR/

de todas as comunicações online por essas mesmas empresas privadas, que não possuem responsabilidade jurídica necessária para tais atos, por um período de três anos, com poucas restrições nas circunstâncias sob as quais um tribunal poderia ordenar a divulgação dos dados. Medidas semelhantes já foram consideradas inconstitucionais em alguns países europeus.

O Projeto de Lei também contém proibições vagas sobre "traição" nos casos de compartilhamento de dados eletrônicos, assim como medidas muito amplas para a proteção de informações pessoais. Ambas as medidas restringem potencialmente a capacidade de delatores de divulgar informações de interesse público. Outras medidas problemáticas incluem restrições ambíguas ao acesso a computadores e a obtenção e transferência de dados, em que não está prevista a comprovação de intencionalidade para haver imposição de responsabilidade penal. Tais medidas criminalizam potencialmente o uso diário de computadores que não causam nenhum dano. De modo similar, para crimes relativos à "difusão de códigos maliciosos" também não está prevista a necessidade de comprovação de intencionalidade.

O Projeto de Lei encontra-se atualmente nos estágios avançados da tramitação legislativa. Foi aprovado pelo Senado Federal e está atualmente sendo reanalisado pela Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados. A ARTIGO 19 ressalta que o relator do Projeto de Lei já sugeriu uma série de emendas que irão melhorar a lei de forma substancial, caso sejam adotadas. Contudo, nós também recomendamos uma série de revisões para garantir que a lei esteja em conformidade com as normas internacionais de liberdade de expressão e informação.

Normas Internacionais de Liberdade de Expressão

Os direitos à liberdade de expressão e de informação são condições fundamentais e necessárias para a realização dos princípios de transparência e responsabilidade jurídica, que, por sua vez, são essenciais para a promoção e proteção de todos os direitos humanos em uma sociedade democrática. Essa seção identifica normas internacionais e regionais para a proteção da liberdade de expressão e de informação, particularmente em relação à legislação penal sobre o uso de tecnologias de comunicação de informação (TCI). Estas normas formam a base para a análise legal conseguinte.

Declaração Universal dos Direitos Humanos

O artigo 19 da Declaração Universal dos Direitos Humanos (DUDH)[7] garante o direito à liberdade de expressão nos seguintes termos:

> "Todo o homem tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferências, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios, independentemente de fronteiras."

A DUDH, como uma Resolução da Assembleia Geral da ONU, não exige vinculação legal direta com os Estados. Entretanto, partes dela, incluindo o artigo 19, são amplamente tratadas como tendo adquirido força de lei na qualidade de direito internacional costumeiro desde sua adoção em 1948.[8]

Pacto Internacional dos Direitos Civis e Políticos

O Pacto Internacional dos Direitos Civis e Políticos (PIDCP) elabora e dá força de lei a muitos dos direitos articulados na DUDH. O PIDCP vincula seus 167 Estados partes a respeitar suas medidas e implementar seu arcabouço legal a nível nacional.[9] O Brasil aderiu ao pacto em 24 de janeiro de 1992 e está, deste modo, juridicamente vinculado ao respeito e à garantia ao direito à liberdade de expressão, conforme consta no artigo 19 do PIDCP:

1. Ninguém poderá ser molestado por suas opiniões.
2. Toda pessoa terá direito à liberdade de expressão; esse direito incluirá a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, independentemente de considerações de fronteiras, verbalmente ou por escrito, em forma impressa ou artística, ou qualquer outro meio de sua escolha.

Em 21 de junho de 2011, a Comissão de DH, como corpo de monitoramento do PIDCP, emitiu o Comentário Geral No.34 em relação ao artigo 19.[10] O Comentário Geral No.34 constitui uma interpretação oficial sobre os padrões mínimos garantidos pelo artigo 19 do PIDCP. A ARTIGO 19

[7] Resolução da Assembleia Geral da ONU 217A(III), adotada em 10 de dezembro de 1948

[8] *Filartiga v. Pena-Irala*, 630 F. 2d 876 (1980) (Circuito das Cortes de Apelações dos EUA, 2o circuito)

[9] Artigo 2o da PIDCP, res. 2200A (XXI) da AG, 21 UN GAOR Supp. (No. 16) em 52, UN Doc. A/6316 (1966); 999 UNTS 171; 6 ILM 368 (1967)

[10] Comentário Geral No. 34 da Comissão de DH, de 21 de junho de 2011, CCPR/C/GC/34

considera o Comentário Geral No.34 uma elucidação avançada e detalhada sobre o direito internacional relativo à liberdade de expressão e ao acesso à informação.[11] É contemporâneo e instrutivo a uma série de preocupações sobre a liberdade de expressão levantadas pelo Projeto de Lei.

De maneira importante, o Comentário Geral No.34 afirma que o artigo 19 da PIDCP protege todas as formas de expressão e os meios para sua difusão, incluindo todos os exemplos de formas de expressão eletrônicas e baseadas na Internet.[12] Pede-se aos Estados partes do PIDCP que acompanhem a extensão em que foram substancialmente alteradas as práticas de comunicação ao redor do mundo pelos desenvolvimentos das tecnologias de informação. O Comentário Geral No.34 exige dos Estados partes que tomem todas as medidas necessárias para promover a independência das novas mídias e assegurar o acesso dos indivíduos a elas.[13]

Como Estado parte do PIDCP, o Brasil deve assegurar que quaisquer de suas leis que procurem criminalizar ou, de outro modo, regulamentar as formas de expressão eletrônicas e baseadas na Internet, incluindo o acesso e a difusão de informação, estejam em conformidade com o artigo 19 da PIDCP.

Limitações ao Direito à Liberdade de Expressão

Embora o direito à liberdade de expressão seja um direito fundamental, ele não está garantido em termos absolutos. O artigo 19(3) da PIDCP permite que o direito seja restrito nos seguintes termos:

> 3. O exercício do direito previsto no § 2º do presente artigo implicará deveres e responsabilidades especiais. Consequentemente, poderá estar sujeito a certas restrições, que devem, entretanto, ser expressamente previstas em lei e que se façam necessárias para:
> a) assegurar o respeito dos direitos e da reputação das demais pessoas;
> b) proteger a segurança nacional, a ordem, a saúde ou a moral pública.

As restrições ao direito à liberdade de expressão devem estar estritamente adequadas e não devem colocar em risco o próprio direito. Determinar se uma restrição está estritamente adequada é normalmente feito mediante um teste de três partes. As restrições devem: i) ser previstas em lei, ii) buscar um objetivo legítimo, e iii) estar em conformidade com testes rigorosos de necessidade e proporcionalidade.[14] O Comentário Geral No.34 diz que restrições aos sistemas baseados na Internet, eletrônicos ou qualquer outro tipo de sistema de difusão de informação, sejam apenas admissíveis enquanto estiverem em conformidade com o artigo 19(3) do PIDCP.[15] Isso inclui restrições aos serviços de fornecimento de Internet.

i) "Ser previstas em lei"

O artigo 19(3) do PIDCP exige que restrições ao direito à liberdade de expressão devem ser previstas em lei. Isso exige uma determinação normativa; para ser caracterizada como lei, uma

---

[11] Pronunciamento da ARTIGO 19 sobre o Comentário Geral No.34 da Comissão de DH http://www.article19.org/resources.php/resource/2631/en/un:-article-19-welcomes-general-comment-on-freedom-of-expression

[12] Parágrafo 12, Comentário Geral No.34 da Comissão de DH

[13] Parágrafo 15, Comentário Geral No.34 da Comissão de DH

[14] Velichkin v. Belarus, Comunicado No. 1022/2001, U.N. Doc. CCPR/C/85/D/1022/2001 (2005).

[15] Parágrafo 43, HR Comentário Geral No.34 da Comissão de DH

norma deve ser formulada com precisão suficiente para permitir a um indivíduo que regule o seu comportamento de acordo.[16] Restrições ambíguas ou excessivamente amplas à liberdade de expressão e deficientes em elucidar o escopo exato de sua aplicação são, portanto, inadmissíveis de acordo com o artigo 19(3).

ii) "Objetivo Legítimo"

Interferências ao direito à liberdade de expressão devem ter um objetivo legítimo de proteção, conforme exaustivamente enumerado no artigo 19(3)(a) e (b) do PIDCP. De tal modo que seria inadmissível proibir sistemas de difusão de informação de publicarem materiais, somente pelo motivo de mostrarem uma visão crítica ao governo ou ao sistema social político endossado pelo governo.[17] Uma adequação rigorosa exige que restrições admissíveis sejam específicas quanto ao conteúdo. Por exemplo, seria inadmissível fechar um website, enquanto for possível alcançar o objetivo da proteção por meio do isolamento ou da remoção do conteúdo ofensivo. Quando um Estado limita a liberdade de expressão, ele tem o dever de mostrar uma conexão direta ou imediata entre a expressão e a razão legítima para a sua restrição.

Os Princípios de Joanesburgo sobre Segurança Nacional, Liberdade de Expressão e Acesso à Informação[18] (Princípios de Joanesburgo), um conjunto de padrões internacionais desenvolvidos pela ARTIGO 19 e especialistas internacionais em liberdade de expressão, são instrutivos em relação à restrições à liberdade de expressão com o intuito de proteger a segurança nacional. O Princípio Segundo dos Princípios de Joanesburgo afirma que as restrições justificadas por motivos de segurança nacional são ilegítimas, a não ser que seu verdadeiro propósito e efeito demonstrável sejam o de proteger a existência do país e sua integridade territorial contra o uso ou a ameaça ao uso da força, ou sua capacidade de responder ao uso ou à ameaça ao uso da força. A restrição não pode ser um pretexto para proteger o governo de situações embaraçosas ou da denúncia de maus procedimentos, nem para proteger informações sobre o funcionamento de suas instituições públicas ou se defender de uma ideologia particular. O Princípio Quinze afirma que um indivíduo não deve ser punido em nome da segurança nacional em caso de divulgação de informação, se (1) a divulgação não cause nenhum dano de fato e se ela não for possivelmente capaz de causar nenhum mal a interesses legítimos da segurança nacional, ou (2) o interesse público em tomar conhecimento de tal informação pese mais que o dano causado por sua divulgação.

O Comentário Geral No.34 também menciona que um cuidado especial deve ser tomado ao se redigirem e aplicarem leis que sirvam para restringir a expressão com a finalidade de proteger a segurança nacional. Caracterizadas como leis de traição ou não, leis sobre sigilo oficial ou sobre insubordinação, devem estar em conformidade com os requisitos estritos do artigo 19(3) do PIDCP.

iii) "Necessidade"

Estados partes do PIDCP são obrigados a garantir que restrições legítimas ao direito à liberdade de expressão sejam necessárias e proporcionadas. Para haver necessidade é preciso que haja demanda social pela restrição. O Estado parte que buscar a restrição deve mostrar uma conexão direta e imediata entre a expressão e o interesse a ser protegido. Para haver proporcionalidade é preciso que a restrição à expressão não seja muito ampla e que ela seja adequada para poder alcançar sua função protetora. Deve-se mostrar que a restrição seja específica e individual, com o intuito de obter seu objetivo de proteção e que ela não seja mais intrusiva que outros instrumentos capazes de alcançar o mesmo resultado limitado. O Comentário Geral No.34 afirma

[16] Leonardus J.M. de Groot v. Países Baixos, No. 578/1994, U.N. Doc. CCPR/C/54/D/578/1994 (1995).

[17] Observações Conclusivas da Comissão de DH sobre a República Árabe Síria CCPR/CO/84/SYR

[18] Adotados em 1o de outubro de 1995. Esses Princípios foram endossados pela Relatoria Especial da ONU para a Liberdade de Opinião e Expressão e a Comissão de Direitos Humanos das Nações Unidas refere-se a eles em cada uma de suas resoluções anuais sobre liberdade de expressão desde 1996.

que proibições gerais à operação de alguns websites e sistemas nunca são proporcionais e, deste modo, são incompatíveis com o artigo 19(3) da PIDCP.

Convenção Americana de Direitos Humanos

O marco jurídico interamericano oferece, sem dúvida, um dos maiores espaços de proteção regional para a liberdade de expressão. A Convenção Americana de Direitos Humanos (CADH) foi projetada para reduzir ao mínimo as restrições à livre circulação de informação, opiniões e ideias, como resultado da "importância que os autores da Convenção deram à necessidade de expressar e receber qualquer tipo de informação, pensamentos, opiniões e ideias".[19]

De acordo com o Escritório do Relatoria Especial da OEA para a Liberdade de Expressão, "a jurisprudência interamericana demonstrou que o marco jurídico interamericano valorizou a liberdade de expressão por ser baseado em um conceito amplo de autonomia e dignidade do indivíduo e por levar em consideração o valor instrumental da liberdade de expressão para o exercício de todos os outros direitos fundamentais, assim como o seu papel essencial dentro dos sistemas democráticos".[20]

O Brasil se tornou um Estado parte da CADH em 9 de julho de 1992, e está, desta forma, juridicamente vinculado ao respeito ao artigo 13, que garante o direito à liberdade de expressão:

> 1. Toda pessoa tem o direito à liberdade de pensamento e de expressão. Esse direito inclui a liberdade de procurar, receber e difundir informações e ideias de qualquer natureza, sem considerações de fronteiras, verbalmente ou por escrito, ou em forma impressa ou artística, ou por qualquer meio de sua escolha.
>
> 2. O exercício do direito previsto no inciso precedente não pode estar sujeito à censura prévia, mas a responsabilidades ulteriores, que devem ser expressamente previstas em lei e que se façam necessárias para assegurar:
>
> a) o respeito dos direitos e da reputação das demais pessoas;
>
> b) a proteção da segurança nacional, da ordem pública, ou da saúde ou da moral públicas.
>
> 3. Não se pode restringir o direito de expressão por vias e meios indiretos, tais como o abuso de controles oficiais ou particulares de papel de imprensa, de frequências radioelétricas ou de equipamentos e aparelhos usados na difusão de informação, nem por quaisquer outros meios destinados a obstar a comunicação e a circulação de ideias e opiniões.
>
> 4. A lei pode submeter os espetáculos públicos a censura prévia, com o objetivo exclusivo de regular o acesso a eles, para proteção moral da infância e da adolescência, sem prejuízo do disposto no inciso 2.
>
> 5. A lei deve proibir toda propaganda a favor da guerra, bem como toda apologia ao ódio nacional, racial ou religioso que constitua incitamento à discriminação, à hostilidade, ao crime ou à violência.

[19] Ver o Relatório No 11/96 Caso 11.230 (Merits) *Francisco Martorell v Chile* Com. Inter-Am de DH, 3 de maio de 1996, para 56.

[20] Escritório da Relatoria Especial para a Liberdade de Expressão, O Marco Jurídico Interamericano relativo ao Direito à Liberdade de Expressão (2010), p 2.

A Declaração Interamericana de Princípios sobre Liberdade de Expressão (2000)[21] trabalha em torno de elementos-chave do direito à liberdade de expressão no marco jurídico interamericano. Em seu quinto princípio, ela afirma que "[a] censura prévia, a interferência ou pressão direta ou indireta sobre qualquer expressão, opinião ou informação através de qualquer meio de comunicação oral, escrita, artística, visual ou eletrônica, deve ser proibida por lei."

Declaração Conjunta sobre a Liberdade de Expressão e Internet

Em junho de 2011, as quatro Relatorias Especiais Internacionais para a Liberdade de Expressão[22] produziram uma Declaração Conjunta sobre a Liberdade de Expressão e Internet (Declaração Conjunta) em consulta com a ARTIGO 19.[23] As quatro Relatorias Internacionais representam as Américas, a Europa, a África e as Nações Unidas. O parágrafo 1º(a) da Declaração Conjunta reitera a aplicação da liberdade de expressão para a Internet. O parágrafo 4º(b) da Declaração Conjunta enfatiza que a imposição de responsabilidade jurídica em casos de crimes de expressão deve levar em conta o interesse público geral de proteger tanto a expressão em si, quanto o espaço por onde ela é expressa.

Segurança Cibernética e Respeito pelos Direitos Humanos

As resoluções e os instrumentos internacionais para segurança cibernética reconhecem a importância de balancear os imperativos para a segurança com os direitos humanos fundamentais, particularmente o direito à liberdade de expressão.

A Resolução da Assembleia Geral da ONU sobre a "Criação de uma cultura global de segurança cibernética" afirma que a "segurança deve ser implementada de maneira consistente com os valores reconhecidos pelas sociedades democráticas, incluindo a liberdade de trocar pensamentos e ideias, o fluxo livre de informação, a confidencialidade de informação e comunicação, a proteção adequada da abertura, transparência e informação pessoal."[24]

De uma perspectiva comparada, a ARTIGO 19 também nota que o preâmbulo da Convenção do Conselho Europeu sobre Cibercrimes (2001) afirma que as partes devem ter em conta "a necessidade de garantir um equilíbrio adequado entre os interesses da aplicação da lei e o respeito pelos direitos fundamentais do ser humano (...) que reafirmam o direito à liberdade de opinião sem qualquer ingerência, o direito à liberdade de expressão, incluindo a liberdade de procurar, de receber e transmitir informações e ideias de qualquer natureza sem considerações de fronteiras e, ainda, o direito ao respeito pela vida privada."[25] Isso é apoiado pelo artigo 15 da Convenção de Cibercrimes, que afirma que os poderes e procedimentos previstos na Convenção "deve[m] assegurar uma proteção adequada dos direitos do Homem e das liberdades", fazendo

---

[21] Adotado pela Comissão Interamericana de Direitos Humanos em seu 108o Período Ordinário de Sessões, realizado em outubro de 2000.

[22] O Relator Especial das Nações Unidas para a Liberdade de Opinião e Expressão, Frank LaRue; a Relatora Especial para Liberdade de Expressão da Comissão Interamericana de Direitos Humanos da Organização dos Estados Americanos, Catalina Botero Marino; a Representante para Liberdade de Mídia da Organização para Segurança e Cooperação na Europa, Dunja Mijatoviæ; e a Relatora Especial para Liberdade de Expressão da Comissão Africana de Direitos Humanos e dos Povos, Faith Pansy Tlakula.

[23] Declaração Conjunta sobre a Liberdade de Expressão e Internet (1o de junho de 2011); disponível em http://www.article19.org/data/files/pdfs/press/international-mechanisms-for-promoting-freedom-of-expression.pdf

[24] Ver A/RES/57/239, 31 de jan. de 2003; disponível em http://www.itu.int/ITU-D/cyb/cybersecurity/docs/UN_resolution_57_239.pdf.

[25] Convenção sobre o Cibercrime, Budapest, 23.XI.2001; disponível em: http://conventions.coe.int/Treaty/en/Treaties/html/185.htm. http://www.coe.int/t/dghl/standardsetting/t-cy/ETS_185_Portugese.pdf

referência tanto ao PIDCP, quanto à Convenção para a Proteção dos Direitos Humanos e Liberdades Fundamentais.

É importante ressaltar que a Convenção do Conselho Europeu sobre Cibercrimes não contém nenhuma restrição baseada em conteúdos, com exceção daquelas relacionadas à pornografia infantil. A possibilidade de haver perseguição de dissidências políticas por intermédio de leis nacionais contra Cibercrimes é reconhecida na Convenção em seu artigo 27(4)(a), que permite que Estados recusem prestar assistência a outros Estados partes, caso seja percebido que o pedido está relacionado a perseguições de cunho político. Com 32 Estados partes, a Convenção possui o maior número de membros entre todos os instrumentos de direito internacional sobre a matéria. O Brasil está atualmente estudando sua adesão a essa convenção.

Vigilância de Comunicações

Garantir o direito à privacidade nas comunicações online é essencial para assegurar que indivíduos tenham segurança para exercer livremente seu direito à liberdade de expressão. Portanto, a vigilância em massa de comunicações online é uma fonte de preocupação tanto para o direito à privacidade, como para o direito à liberdade de expressão.

De uma perspectiva comparada, a União Europeia tratou a questão da proteção da privacidade das comunicações online em sua Diretiva da Privacidade Eletrônica.[26] O artigo 15 desta Diretiva prevê que qualquer infração aos direitos à privacidade devem ser "uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.o 1 do artigo 13.o da Diretiva 95/46/CE [Diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados]."

Além disso, a Resolução sobre Vigilância de Comunicações e Liberdade de Expressão, de 5 de Junho de 2009, assinada por 30 Organizações Internacionais de Liberdade de Expressão, incluindo a ARTIGO 19, afirma que:

> Os governos (devem) reconhecer totalmente que, sob leis internacionais existentes, todas as pessoas têm o direito a se comunicar em privacidade, sem interferência, com exceção em circunstâncias estritamente limitadas (...). Nenhuma vigilância deverá ser conduzida sem autorização legal.
>
> Os governos não deverão adotar leis antiterrorismo ou de proteção da ordem ou da segurança pública que permitam a vigilância de comunicações ou a obtenção de gravações de telecomunicações sem um processo legal adequado ou uma fiscalização que respeite os direitos humanos fundamentais da livre expressão e da privacidade de comunicações.
>
> Os governos não devem requisitar rotineiramente a serviços provedores de telecomunicações que gravem e guardem dados de todas as atividades de seus usuários.
>
> Os governos não devem requisitar que todas as pessoas sejam obrigadas a se pré-registrar ou a se identificar antes que sejam autorizadas a usar serviços de telecomunicações.

[26] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho Europeu, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações electrónicas (Diretiva relativa à privacidade e às comunicações; ver em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:HTML

Os governos, conforme necessário, devem revisar a legislação existente para garantir que os direitos sejam protegidos.

Análise da Lei de Cibercrimes

A Proposta Substitutiva do Senado Federal ao Projeto de Lei da Câmara No. 89 de 2003 ("o Projeto de Lei") propõe inserir uma série de medidas suplementares ao Código Penal Brasileiro que são problemáticas da ponto de vista da liberdade de expressão. O Relator do Projeto de Lei recomendou uma série de emendas que a Câmara dos Deputados decidirá agora se adotará ou não na versão final da lei. Esta análise revisa cada medida suplementar, assinalando reformas recomendadas pelo Relator do Projeto de Lei, assim como faz recomendações de outras reformas que são necessárias para deixar o Projeto de Lei em conformidade com as normas internacionais sobre liberdade de expressão e de informação.

Garantias ao Direito à Liberdade de Expressão e de Informação

O Projeto de Lei afirma que seu propósito é o de criar uma emenda ao código penal existente para "tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, de rede de computadores, ou que sejam praticadas contra dispositivos de comunicação ou sistemas informatizados e similares, e dá outras providências." Nenhuma medida no Projeto de Lei garante direitos à liberdade de expressão e de informação ou faz qualquer referência a eles.

A ARTIGO 19 acredita que, ao integrar as proteções ao direitos fundamentais ao Projeto de Lei, garantiria que sua implementação não irá prejudicar tais direitos. Conforme mencionado anteriormente, tanto a Assembleia Geral da ONU[27], como o Conselho Europeu[28] reconheceram que a segurança cibernética não deverá ser obtida ao custo da fruição dos direitos humanos fundamentais. Novamente, os quatro Relatores Especiais para Liberdade de Expressão notaram que esforços bem intencionados para regular a segurança cibernética resultam com frequência em restrições ilegais ao direito à liberdade de expressão;[29] a possibilidade que isso ocorra certamente existe no Projeto de Lei.

A ARTIGO 19 nota que um marco dos direitos civis para a Internet (também conhecido como "Marco Civil da Internet") também está atualmente sob consideração pelo governo brasileiro. Embora uma revisão do Marco dos Direitos Civis esteja além do escopo desta análise,[30] sua avaliação superficial mostra que ele prevê um marco gradual com o objetivo de atingir a harmonia adequada entre a aplicação do código penal e o respeito aos direitos humanos fundamentais.[31] Apesar da ARTIGO 19 receber bem a iniciativa do Marco Civil da Internet, nós nos mantemos preocupados, porque ela muito provavelmente será adotada posteriormente ao Projeto de Lei, que cria diversos novos crimes que restringem ilegalmente as liberdades online. Há a possibilidade das disparidades entre ambas as leis causarem confusão e indivíduos serem responsabilizados criminalmente por condutas que deveriam ser protegidas pelo Marco Civil da Internet.

Recomendações

- O propósito do Projeto de Lei deveria minimamente afirmar a proteção dos direitos humanos fundamentais, incluindo os direitos à liberdade de expressão e de informação.
- O Marco Civil da Internet deve estar em acordo com normas internacionais sobre

[27] *Ibid,* nota de rodapé 25.

[28] *Ibid*, nota de rodapé 26, Artigo 15.

[29] *Ibid,* nota de rodapé 23.

[30] A ARTIGO 19 está revisando o Marco Civil da Internet separadamente em outra análise. Para mais detalhes, contate a ARTIGO 19 Brasil.

[31] Insert link to new translation.

liberdade de expressão e de informação e deveria ser adotado previamente ou simultaneamente à criação de qualquer novo tipo de crime relacionado ao uso da Internet.

Crimes Contra a Segurança de Sistemas Informatizados

O Projeto de Lei altera o artigo 2º, Título VIII da Parte Especial do Código Penal, acrescentando o Capítulo IV, com o título "Dos Crimes Contra A Segurança Dos Sistemas Informatizados."

O artigo 285-A do Capítulo IV torna um crime "[a]cessar, mediante violação de segurança, rede de computadores, dispositivo de comunicação ou sistema informatizado, protegidos por expressa restrição de acesso." O artigo 285-B proíbe a obtenção ou transferência de dado ou informação "sem autorização ou em desconformidade com autorização do legítimo titular da rede de computadores (...) protegidos por expressa restrição de acesso." Pena de um a três anos de reclusão são previstas para ambos os crimes, além de multas sem teto especificado. As penas podem ser aumentadas da sexta parte se, em relação ao artigo 285-A, o acesso for facilitado por falsificação de identidade, ou pela terça parte se, em relação ao artigo 285-B, a informação for comunicada a terceiros.

A ARTIGO 19 considera que os seguintes aspectos da lei sejam altamente problemáticos e encontram-se em violação às garantias internacionais à liberdade de expressão.

1. **Falta de definições**: nem o artigo 285-A ou 285-B possuem clareza e acessibilidade que devem ser "previstas em lei", de acordo com o artigo 19(3) do PIDCP. Elementos-chave para os crimes não estão definidos, incluindo as definições de "acesso", "violação de segurança" ou "restrição de acesso". A ARTIGO 19 nota que, por exemplo, nas normas canadenses e britânicas equivalentes, relativas aos cibercrimes, definições precisas da terminologia técnica estão previstas no código legal, para fins de clareza.[32] É recomendado que esses termos do Projeto de Lei sejam considerados e acrescentados à lista de definições, contida no artigo 16 do Projeto de Lei**.**

2. **Intencionalidade necessária**: Adicionalmente, a intencionalidade necessária para que haja responsabilidade penal em ambos os crimes não está especificada, o que permite que uma pessoa possa ser considerada culpada sem ter tido a intenção de violar a segurança em questão ou de obter ou transferir a informação em questão. De uma perspectiva comparada, a Convenção do Conselho Europeu sobre Cibercrimes prevê o crime de "acesso ilegal" em seu artigo 2º e apenas permite que haja responsabilidade penal quando o acesso é "intencional e ilegítimo"[33]. Isso reflete fortemente a previsão canadense, que requer que o ato seja cometido "fraudulentamente" "de forma ilegítima".[34] De maneira similar, a norma penal britânica equivalente também requer a comprovação de que o acusado tenha acessado sistemas informatizados intencionalmente e que possuía conhecimento durante o acesso de que o ato não era autorizado.[35] Ambos os artigos do Projeto de Lei poderiam ser fortalecidos, ao serem requisitadas a

[32] Lei para Uso Indevido de Computador ("The Computer Misuse Act") (Reino Unido) 1990, seção 1a., Código Penal Canadense, Artigo 342

[33] Convenção sobre o Cibercrime, Budapest, 23.XI.2001, Artigo 2o – "Acesso Ilegítimo: Cada Parte adotará as medidas legislativas e outras que se revelem necessárias para estabelecer como infração penal, no seu direito interno, o acesso intencional e ilegítimo à totalidade ou a parte de um sistema informático. As Partes podem exigir que a infração seja cometida com a violação de medidas de segurança, com a intenção de obter dados informáticos ou outra intenção ilegítima, ou que seja relacionada com um sistema informático conectado a outro sistema informático."

[34] Código Penal Canadense, Artigo 342.1

[35] Lei para Uso Indevido de Computador ("The Computer Misuse Act") (Reino Unido) 1990, seção 1a. Artigo 342.1(1) do Código Penal Canadense requer comprovação de intenção fraudulenta de forma ilegítima.

comprovação de intenção durante o acesso aos sistemas informáticos e na obtenção e transferência de dado, assim como a comprovação de ter havido conhecimento da não autorização ao acesso à informação ou de ter havido conhecimento da realização do ato por meio de violação de segurança.

3. **Nenhum objetivo legítimo especificado:** a ARTIGO 19 também está preocupada que ambos os artigos 285-A e 285-B impõem limitações à liberdade de expressão e de informação sem especificarem objetivos legítimos, conforme exigido pelo teste de três partes, mencionado acima, relativo ao artigo 19 da PIDCP e ao artigo 13 do CADH. Em sua forma atual, as proibições poderiam permitir que indivíduos sejam processados por uso diário inócuo de computadores, sem propósito aparente e, desse modo, desnecessário. Além da falta de uma exigência de intencionalidade, as medidas não exigem a demonstração que um dano foi causado mediante violação de segurança ou obtenção ou transferência não autorizadas de informação. Isso contradiz a declaração do Congresso Nacional na seção de abertura do Projeto de Lei, que delineia seu objetivo como sendo o da criação de crimes relacionados a ações "*contra*" sistemas informáticos. Os objetivos legítimos para essas proibições podem ser o da proteção da privacidade e a proteção da segurança nacional (por exemplo, dos dados mantidos em computadores do governo ou militares). Entretanto, deveriam estar indicados de maneira clara tais objetivos de proteção no Projeto de Lei - para que a aplicação dessas medidas não restrinja a expressão ou o acesso à informação naqueles casos em que tais objetivos legítimos não estejam em jogo.

4. **Criminalização da burla dos Sistemas de Gestão de Direitos Digitais:** a ARTIGO 19 está preocupada que essas medidas demasiadamente amplas possam ser usadas para criminalizar o ato de burlar os sistemas de gestão de direitos digitais (GDD). Os sistemas GDD são medidas tecnológicas que permitem produtores de conteúdos eletrônicos controlar como a informação é utilizada pela perpetuidade e podem ser considerados nos termos dos "sistemas de restrição de acesso" sob os artigos 285-A e 285-B do Projeto de Lei. Os sistemas GDD são controversos do ponto de vista da liberdade de expressão, pois a legitimidade dos detentores de direitos autorais de exercerem controle absoluto sobre o compartilhamento de informação pela perpetuidade é contestado. Os sistemas GDD impedem indivíduos de praticarem atos triviais e não-comerciais de violação de direitos autorais e, deste modo, limitam a disseminação da informação e da liberdade de expressão. Eles impedem, por exemplo, que um indivíduo transfira dados entre os seus próprios aparelhos eletrônicos, ou use materiais protegidos por direito autoral em formas costumeiramente protegidas em regimes de propriedade intelectual, como o "uso justo", por exemplo, em objetivos educacionais. Essa possível aplicação dos artigos 285-A e 285-B demonstram o quanto seu escopo demasiadamente amplo podem restringir desnecessariamente a liberdade de expressão e de informação.

5. **Penas desproporcionais:** A proporcionalidade das penas impostas por essas duas medidas é também algo preocupante. Penas de reclusão de no mínimo um ano, na prática, negam ao juiz o seu critério de garantir a proporcionalidade à sentença. Como são muito amplas, essas medidas facilmente referem-se a condutas, às quais as penas de reclusão seriam, em qualquer caso, tremendamente desproporcionais. Em muitos casos, reparações ou multas seriam mais adequadas.

O Projeto de Lei insere crimes suplementares semelhantes no artigo 13, Título VII da Parte Especial do Livro I do Código Penal Militar.[36] A linguagem dos artigos No. 339 e No. 339A reflete fortemente as revisões dos artigos 285-A e 285-B do Código Penal (Civil) respectivamente. As

[36] Decreto-Lei No. 1.001, de 21 de outubro de 1969

medidas do Código Penal Militar, no entanto, contêm a cláusula "desde que o fato atente contra a administração militar". Mesmo que haja a exigência da ocorrência de dano, não está delineado qual a forma de um atentado "contra a administração militar". Isso pode facilmente incluir danos triviais; por exemplo, qualquer violação de sistemas de seguranças não intencionais poderá ser enquadrada como dano, mesmo nos casos em que ela seja uma mera inconveniência administrativa.

Recomendações

- Os artigos 285-A e 285-B do Projeto de Lei (relativos ao Código Penal Civil) e os artigos 339 e 339A do Projeto de Lei (relativos ao Código Penal Militar) deveriam exigir a comprovação de intenção do acusado durante o ato da conduta proibida, assim como a comprovação de conhecimento da violação de um sistema de segurança ou da obtenção e transferência sem autorização de informação ou dado.
- Os artigos 285-A e 285-B deveriam exigir a comprovação de dano para a imposição de responsabilidade penal, levando em conta um objetivo legítimo, de acordo com o artigo 19 (3) do PIDCP. Os artigos 339 e 339A do Código Penal Militar deveriam definir com mais precisão os termos de um atentado contra a administração militar.
- Termos chave, particularmente de linguagem técnica, em cada uma das medidas ressaltadas nessa seção, deveriam ser definidos com mais clareza no artigo 16 do Projeto de Lei.
- As sentença previstas em cada uma das medidas deveriam retirar as penas de reclusão mínimas obrigatórias e prever multas ou outras medidas menos punitivas como alternativas.

Responsabilidades dos Provedores em Assegurar a Lei

O artigo 22 do Projeto de Lei recomenda uma série de obrigações para "[o] responsável pelo provimento de acesso a rede de computadores mundial, comercial ou do setor público." Tais entes (os "provedores") fornecem a infraestrutura tecnológica para as comunicações eletrônicas e, de tal modo, desempenham um papel integral na facilitação do exercício do direito à livre expressão.

i) *Artigo 22, inciso I*

O artigo 22, inciso I do Projeto de Lei obriga os provedores a **manter dados de endereçamento da Internet que possam ser utilizados para identificar usuários de Internet:**

> I – manter em ambiente controlado e de segurança, pelo prazo de 3 (três) anos, com o objetivo de provimento de investigação pública formalizada, os dados de endereçamento eletrônico da origem, hora, data e a referência GMT da conexão efetuada por meio de rede de computadores e fornecê-los exclusivamente à autoridade investigatória mediante prévia requisição judicial.

A ARTIGO 19 acredita que a imposição de exigências de conservação generalizada de dados aos provedores seja uma violação desnecessária e desproporcionada ao direito à liberdade de expressão e ao direito à privacidade. Regimes de conservação coletiva de dados, sem a necessidade de suspeita de ato malicioso, corrompem as pré-condições a uma sociedade aberta e democrática, por enfraquecerem a confiança depositada pelos indivíduos na privacidade de suas comunicações e por criarem um risco permanente de perda e violação de dados. Parece não haver evidências que mostrem que os avanços práticos de um regime de retenção coletiva de dados não possam ser realizados de maneira tão efetiva quanto aos de restrições mais específicas, que não violam os direitos de todos os usuários de Internet de forma tão ampla. Além disso, os enormes custos de implementação de um sistema de conservação de dados nesta escala poderiam ser repassados aos consumidores, restringindo ainda mais o acesso à Internet, particularmente em relação aos indivíduos de baixa renda.

De uma perspectiva comparada, o regime de retenção de dados previsto pelo Projeto de Lei é muito mais amplo que o regime previsto pela União Europeia em sua Diretiva de Conservação de Dados (2006/2) (Diretiva da UE) - que também é muito problemática da ponto de vista da liberdade de expressão.[37] Sob a Diretiva da UE, um Estado membro poderá requisitar aos provedores a conservação de dados apenas entre seis meses e dois anos, diferentemente dos três anos obrigatórios do Projeto de Lei. Nós notamos que quanto mais tempo uma empresa for obrigada a manter dados privados de indivíduos, maior será o risco do comprometimento da privacidade dos dados. O Projeto de Lei é também muito mais amplo na medida em que não prevê restrições aos poderes dos tribunais de exigirem a divulgação dessas informações privadas. A Diretiva da UE, contudo, pelo menos restringe o uso de tais procurações judiciais para os casos de "investigações, descobertas e acusações de crimes sérios". Apesar das grandes proteções feitas pela Diretiva da UE, a Alemanha, a Romênia e a Suécia, Estados membros da UE, julgaram que as medidas da Diretiva são incompatíveis com suas constituições nacionais. A Comissão Europeia está atualmente revisando a necessidade da Diretiva de Conservação de Dados de ser parte de seus procedimentos padrões, e surgiram diversas preocupações com sua compatibilidade com os direitos humanos fundamentais. Cabe ressaltar que a Convenção sobre Cibercrimes do Conselho Europeu não coloca nenhuma confiança nos sistemas de conservação generalizada de dados para alcançar seus objetivos, o que coloca em dúvida, inclusive, a necessidade do artigo 22, inciso I.

ii) Artigo 22, inciso II

A inciso II do artigo 22 do Projeto de Lei prevê que os tribunais requisitem **imediatamente a preservação de qualquer dado eletrônico pelos provedores de Internet**, conforme requisitado "em curso de investigação". Não está claro pelo texto do artigo 22, inciso II, quais categorias de investigação podem dar competência para fazer tais requisições. Além do mais, nenhuma restrição está prevista para qual tipo de informação os provedores devem preservar. **Um provedor deve, portanto, ser requisitado a conservar conteúdo de comunicações** se o Tribunal determinar que esses sejam "requisitados em curso de investigação". A medida também falha ao não indicar sob quais critérios um Tribunal deverá determinar a requisição judicial da preservação imediata e, sob quais circunstâncias, haveria negação de tais requisições a fim de proteger os direitos fundamentais. De maneira similar, uma vez que uma requisição para a preservação for expedida, permanecem incertos quais serão os padrões adotados para as circunstâncias, sob as quais as informações preservadas sob ordem judicial poderão ser reveladas, e de que forma os direitos fundamentais estarão protegidos nessas situações. Em resumo, serão muitos os critérios deixados ao poder judiciário para determinar quando e com quais benefícios uma requisição judicial de preservação deverá ser expedida, e sem qualquer limitação à sua abrangência ou duração.

A ARTIGO 19 acredita que, embora a fiscalização judicial seja um ponto importante do artigo 22, inciso II, sua formulação presente está muito vaga para prever garantias contra abusos. De uma perspectiva comparada, o artigo 16 da Convenção sobre Cibercrimes do Conselho Europeu contém um procedimento semelhante sobre requisição de conservação, mas cuja duração é limitada a um período de 90 dias, durante os quais a parte que requisitar informações poderá requisitar a divulgação das informações mediante uma ordem judicial em separado. Apesar da ARTIGO 19 não recomendar o artigo 16 da citada Convenção como um modelo, nós recomendamos que o artigo 22, inciso II do Projeto de Lei seja reescrito, para que as circunstâncias, sob as quais um tribunal poderá expedir uma ordem judicial para a conservação de dados, estejam claras e bem definidas com um objetivo legítimo.

iii) Artigo 22, inciso III, parágrafo 2º

[37] Carta do Comissário Europeu para Assuntos Internos, assinada em conjunta pela ARTIGO 19, ver: http://www.vorratsdatenspeicherung.de/images/DRletter_Malmstroem.pdf

O Relator do Projeto de Lei recomendou a remoção da medida mais problemática do Projeto de Lei, o artigo 22, inciso III, parágrafo 2º. Se mantida, o inciso III exigirá **que os provedores de Internet realizem algumas funções policiais,** sob os seguintes termos:

> "informar, de maneira sigilosa, à autoridade competente, denúncia que tenha recebido e que contenha indícios da prática de crime sujeito a acionamento penal público incondicionado, cuja perpetração haja ocorrido no âmbito da rede de computadores sob sua responsabilidade"

O Parágrafo 2º prevê a imposição de multas entre R$ 2.000,00 e R$ 100.000,00 para os provedores de Internet que não cumprirem suas obrigações previstas no artigo 22. As sentenças serão aumentadas em casos reincidentes sem teto especificado.

A ARTIGO 19 recomenda fortemente a remoção do inciso III, parágrafo 2º do artigo 22, conforme recomendação do relator do Projeto de Lei. A adoção destas duas medidas representarão uma regressão significativa na proteção da liberdade de expressão e de informação no Brasil. As Relatorias Especiais Internacionais para a Liberdade de Expressão alertaram especificamente contra a imposição de tais obrigações aos provedores de Internet, em sua Declaração Conjunta sobre Liberdade de Expressão e Internet (2011):

> "Como mínimo, não deve ser exigido dos fornecedores que controlem o conteúdo gerado por usuários... deve-se dar uma maior atenção ao desenvolvimento de abordagens alternativas e específicas que se adaptem às características singulares da Internet, ao mesmo tempo em que reconheçam que não se devem estabelecer restrições especiais ao conteúdo dos materiais difundidos através da Internet."

De uma perspectiva comparada, o artigo 15 da Diretiva da EU sobre Privacidade Eletrônica[38] exige que qualquer restrição ao direito à privacidade seja "uma medida necessária, adequada e proporcionada numa sociedade democrática para salvaguardar a segurança nacional (ou seja, a segurança do Estado), a defesa, a segurança pública, e a prevenção, a investigação, a detecção e a repressão de infracções penais ou a utilização não autorizada do sistema de comunicações electrónicas, tal como referido no n.o 1 do artigo 13.o da Diretiva 95/46/CE [Diretiva relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados]." No contexto de violações criminais de propriedades intelectuais online, nós notamos que o Tribunal de Justiça da União Europeia recentemente determinou que um Estado violaria direitos humanos fundamentais ao requisitar a provedores de serviços de Internet que implementem sistemas de filtragem para monitorar e impedir downloads em sistemas *peer-to-peer.*[39] A imposição a provedores de exigências de monitoramento e delação no contexto previsto pelo Projeto de Lei é igualmente problemático.

Há inúmeras razões pelas quais provedores, como meros veículos de comunicação e empresas privadas, não devem ser responsáveis pela aplicação da lei em relação aos conteúdos das comunicações que eles processam. O mesmo motivo aplica-se ao proteger os serviços de correio e empresas de telecomunicações de serem responsabilizados pelo conteúdo de cartas e ligações telefônicas que eles processam. Primeiramente, há implicações significativas para os direitos à privacidade e liberdade de expressão de usuários da Internet. A vigilância em massa de comunicações online, que tais medidas requerem, colocariam em risco a confiança dos indivíduos

[38] Diretiva 2002/58/CE do Parlamento Europeu e do Conselho Europeu, de 12 de Julho de 2002, relativa ao tratamento de dados pessoais e à proteção da privacidade no setor das comunicações electrónicas (Diretiva relativa à privacidade e às comunicações; ver em http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:32002L0058:PT:HTML

[39] Para o pronunciamento da ARTIGO 19 sobre o caso de *Scarlet Extended SA v SABAM*, ver: http://www.article19.org/resources.php/resource/2872/en/landmark-digital-free-speech-ruling-at-european-court-of-justice

na privacidade de suas comunicações, desencorajando-os de exercitarem completamente seus direitos sociais e políticos online. Além disso, as multas previstas no Parágrafo 2º provavelmente incentivariam provedores a praticarem operações de vigilância ainda mais amplas do que as requisitadas e até mesmo encorajariam a censura prévia das comunicações por essas empresas, em uma tentativa de evitar processos judiciais. Essas medidas também poderão ter implicações no acesso à Internet por indivíduos de baixa renda, já que qualquer custo associado à implementação de sistemas de monitoramento e denúncia privados seriam possivelmente repassados aos consumidores. Além disso, continua incerto de que forma os provedores, como empresas privadas, seriam responsáveis juridicamente pelo exercício de suas funções e a que grau de transparência suas atividades estariam sujeitas. Ainda mais, essas empresas privadas não possuem experiência institucional para fazer determinações complexas de fatos e leis que seriam necessárias para denunciar supostos crimes online. Por fim, continua incerto a qual nível de fiscalização judicial essas funções estariam sujeitas.

Recomendações

- O artigo 22, inciso I do Projeto de Lei deveria ser removido. Provedores não deveriam ser requisitados a coletar e reter automaticamente dados relativos a todas as comunicações.
- O artigo 22, inciso II do Projeto de Lei deveria ser modificado para tornar mais claras as circunstâncias nas quais um tribunal poderá requerer a conservação de dados e para garantir que tais requisições estejam estritamente especificadas e limitadas em escopo ao seu objetivo expresso.
- O artigo 22, inciso III, parágrafo 2º do Projeto de Lei deveria ser removido, conforme recomendação do relator do Projeto de Lei. A lei brasileira deveria especificamente proteger provedores da responsabilidade jurídica pelos conteúdos de comunicações de terceiros.

Proteção de Informações Pessoais

O Projeto de Lei também altera o artigo 3, Título I do Código Penal para proteger informações e dados pessoais de "divulgação e utilização indevida." Sob o artigo 154-A, penas de retenção de um a dois anos podem ser impostas a qualquer um que divulgue, use, comercialize ou disponibilize dados e informações pessoais contidas em sistema informatizado com finalidade distinta da que motivou seu registro, salvo nos casos previstos em lei ou mediante expressa anuência da pessoa a que se referem. As penas podem ser aumentadas de sexta parte se o crime for facilitado pelo uso de falsa identidade.

Esta proibição absoluta na divulgação de informações pessoais falha em não antecipar os casos em que o interesse público em divulgar aquela informação pese mais que o direito de um indivíduo à privacidade dela. O artigo 19 do PIDCP permite limitações ao direito à liberdade de expressão para proteger o direito à privacidade de outros indivíduos, mas apenas na medida em que isso for necessário e proporcionado. Por exemplo, se a divulgação de uma informação demonstrar conduta ilegítima ou antiética de funcionários públicos corruptos, o interesse privado naquela informação deve ser considerado menos importante do que o interesse público na divulgação daquela informação.

Em seu Pronunciamento Conjunto de 2004, os Relatores Especiais Internacionais para Liberdade de Expressão requisitaram que seus governos ofereçam maior proteção àqueles que divulgarem "informações sobre violações da lei, crimes cometidos por órgãos públicos, em ameaça grave à saúde, segurança ou ao meio ambiente, ou sobre violação dos direitos humanos e das leis humanitárias, devem ser protegidos contra sanções legais, administrativas ou empregatícias, caso tenham agido de boa fé"[40] O artigo 33 da Convenção das Nações Unidas sobre Anticorrupção

[40] Declaração Conjunta do Relator Especial das Nações Unidas para a Liberdade de Opinião e Expressão, o Representante da OSCE para a Mídia e o Relator Especial da OEA para Liberdade de Expressão. Dezembro de 2004.

pede aos Estados que considerem incorporar aos seus sistemas jurídicos nacionais proteções contra qualquer tratamento injustificado dado a qualquer pessoa que relatar de boa fé e por motivos razoáveis às autoridades competentes qualquer fato relativo a crimes estabelecidos de acordo com esta Convenção.[41] O Brasil assinou essa Convenção em 9 de dezembro de 2003 e a ratificou em 15 de junho de 2005 e está, portanto, sujeito a cumprir as suas disposições na aplicação de suas leis internas.

Recomendações:

- O artigo 154-A deveria incorporar uma defesa do interesse público, que permitiria a divulgação de informações quando o interesse público sobre tal divulgação pesar mais que o interesse privado do indivíduo em manter a confidencialidade da informação.

Difusão de Códigos Maliciosos

Uma série de medidas no Projeto de Lei parecem ter sido feitas para proteger os sistemas de TCI dos indivíduos e dos militares contra os danos causados por "códigos maliciosos" (vírus de computador).

A ARTIGO 19 observa que faltam a diversas dessas medidas as exigências de comprovação de intencionalidade para a imposição de responsabilidade penal, e elas podem, deste modo, levar a processos criminais em casos em que indivíduos não transmitiram sabidamente ou intencionalmente o código malicioso. Tais medidas incluem: "inserção e difusão de código malicioso" (artigo do Código Penal 163a e do Código Penal Militar 262a) e "inserção ou difusão de código malicioso seguido de dano" (artigo do Código Penal 163a, parágrafo 1º, artigo 262A, parágrafo 1º do Código Penal Militar). Como vírus de computador são rotineiramente transmitidos via comunicações, impor sanções penais pela disseminação de vírus sem requerer a comprovação de intencionalidade para causar dano pode ter resultados arbitrários e potencialmente desencorajar indivíduos de realizarem comunicações online.

Recomendações:

- A responsabilidade civil ou penal não deve ser imposta devido a inserção ou difusão de código malicioso sem a comprovação da intenção específica de difundir tal código.

Traição

O artigo 15, incisos II e III do artigo 356 do Capítulo I, Título I do Livro II do Código Penal Militar cria dois novos crimes sob o título "favor ao inimigo":

> II – entregando ao inimigo ou expondo a perigo dessa consequência (...) dado eletrônico ou qualquer outro elemento de ação militar;
>
> III – perdendo, destruindo, inutilizando, deteriorando ou expondo a perigo (...) dado eletrônico ou qualquer outro elemento de ação militar.

Como ambas as medidas contêm referências a "dado eletrônico", elas potencialmente restringem o direito à liberdade de expressão e de acesso à informação. Ambas as medidas devem, deste modo, estar em conformidade com o artigo 19 (3) do PIDCP.

Essas medidas não contêm as qualidades de clareza e acessibilidade, que devem ser consideradas em medidas "previstas em lei" pelo artigo 19 do PIDCP. Termos chave a esses crimes não estão definidos, incluindo o que deve ser entendido como "inimigo" ou "expondo ao perigo". Novamente, tais medidas não preveem um estado mental necessário para a imposição de responsabilidade civil ou penal, o que significa que alguém pode ser considerado culpado sem que haja demonstração de sua intenção para cometer a conduta proibida.

[41] Adotado pela Resolução da Assembleia Geral 58/4 de 31 de outubro de 2003.

Conforme dito anteriormente, a proteção da segurança nacional e da ordem pública possui motivos legítimos para restringir a liberdade de expressão, enquanto as restrições forem previstas em lei - algo necessário e proporcionado em uma sociedade democrática. Os Princípios de Joanesburgo orientam a ordenação estrita de medidas relativas à segurança nacional. O segundo princípio afirma que o propósito genuíno e o efeito demonstrável de uma medida devem ser a proteção da existência de um país ou de sua integridade territorial contra o uso ou a ameaça do uso da força, ou sua capacidade de responder ao uso ou à ameaça do uso da força. Normas internacionais, refletidas nos Princípios de Joanesburgo, também exigem que haja relação causal entre as expressões proibidas e a ameaça à segurança nacional, evitada por essa proibição. O Princípio sexto provê um teste modelo de três partes para este propósito, permitindo que a expressão seja punida como uma ameaça à segurança nacional, somente se um governo for capaz de demonstrar que: (a) a intenção da expressão seja a de incitar violência iminente; (b) ela possivelmente incitará a violência; e (c) há uma conexão direta e imediata entre a expressão a probabilidade ou a ocorrência de tal violência. O artigo 15, incisos I e II não preenchem esses requisitos. "Entregando o dado eletrônico ao inimigo" ou "perdendo, destruindo, inutilizando, deteriorando (...) dado", permite-se a imposição de responsabilidade civil ou penal sem a necessidade de comprovar conexão causal entre o compartilhamento de informação e o perigo contra o qual deve-se proteger. De modo similar, a medida não especifica um nível de perigo equivalente ao incitamento de violência iminente, e, portanto, permite que o compartilhamento de informação que não ofereça perigo esteja sujeito a sanções penais severas. Isso não é necessário, nem proporcionado, e, portanto, viola normas internacionais sobre liberdade de expressão e de informação.

Além disso, os incisos II e III do artigo 356 do Código Penal Militar falham ao não fornecerem uma defesa para a divulgação do dado eletrônico sob controle militar, naqueles casos em que o interesse público na divulgação pese mais que os interesses contrários, que desejem manter essa informação confidencial. Conforme explicado anteriormente, a obrigação dos governos em proteger os delatores nessas circunstâncias está bem estabelecido em direito internacional e deve, dessa forma, ser refletido nas medidas do Código Penal Militar que procurem restringir o fluxo livro de informação.

Recomendações

- O artigo 356 deve incorporar a necessidade de comprovação de intencionalidade e requisitar uma conexão causal entre a difusão de dados eletrônicos militares e um perigo à existência do Brasil ou à sua integridade territorial.
- O artigo 356 do Código Penal Militar deve incorporar uma defesa do interesse público em divulgações de informação, nos casos em que o interesse na divulgação pese mais que interesses individuais em manter a confidencialidade da informação.