ARTICLE 19

Brasil: Análise da Estratégia de Cibersegurança

Abril de 2016

Legal analysis

Sumário Executivo

Neste documento, a ARTIGO 19 analisa a Estratégia de Segurança de Segurança da Informação e Comunicações e da Segurança Cibernética da Administração Pública Federal do Brasil para 2015-2018.

A Estratégia está vinculada ao arcabouço mais amplo de planejamento estratégico geral do Governo brasileiro. Ela foi desenvolvida a partir da instrução normativa GSI/PR nº 01/2008 do antigo Gabinete de Segurança Institucional da Presidência da República – GSI/PR – relacionada à gestão da segurança da informação e das comunicações da Administração Pública Federal, tendo sido preparada e aprovada pelo já mencionado Gabinete. O texto tem o objetivo de buscar as melhores práticas na área de segurança da informação e cibersegurança, além estabelecer as principais metas e objetivos estratégicos para os próximos quatro anos, que deverá inspirar e guiar ações futuras e específica.

A ARTIGO 19 acredita que essa Estratégia é importante para a proteção de uma ampla gama de direitos humanos e, em particular, a liberdade de expressão. Por essa razão ela deve ser avaliada para que possam ser observada a conformidade com os padrões internacionais e, não obstante, com as leis domésticas de direitos humanos e liberdade de expressão. A Estratégia propõe princípios relevantes relacionados à proteção de direitos, abordagem multissetorial, acesso à informação e participação. Entretanto, nossa análise identifica que existem sérias deficiências. Em particular:

- O governo falha em fundamentar de maneira firme a Estratégia em padrões nacionais e internacionais de proteção aos direitos humanos. Existe referenciamento mínimo à proteção doméstica de direitos, principalmente aqueles relacionados à liberdade de expressão e às tecnologias digitais.
- Dentre as metas da Estratégia está obtenção de determinados resultados para beneficiar a sociedade, dentre os quais estão incluídos a transparência, a proteção à privacidade, a democratização do acesso à informação e a salvaguarda de informações confidenciais. Este objetivo é relevante e em consonância com os padrões legais aplicáveis nacionais e internacionais. Porém, o documento falha ao não elaborar recomendações mais profundas e específicas na área. Ademais, a enumeração dos diferentes objetivos estratégicos concretos na parte central da Estratégia sequer menciona ou leva em consideração estes importantes valores e direitos.
- Na medida em que a execução de algumas das orientações determinadas no documento vão requerer o envolvimento de diferentes grupos de atores privados, os responsáveis primários pela aplicação e acompanhamento das diretivas serão os vários departamentos e agências da

Administração Federal. Significativamente, a imprecisão das disposições que guiam as ações destes atores públicos é a parte mais problemática da Estratégia, com severas implicações para os direitos humanos.

- No desenvolvimento da Estratégia não houve consultas relevantes com as diferentes partes interessadas. Houve consultas apenas no interior da administração federal e ao CGI.br. Consideramos problemático que a sociedade civil, organizações, indivíduos e outros *stakeholders* não tiveram a oportunidade de analisar e fazer contribuições ao documento. Apesar do texto formalmente estabelecer a estratégia de cibersegurança da administração federal e reconhece as principais responsabilidades das instituições públicas, ele não deve ser confundido como um mero conjunto de regras "internas". Também notamos que este tipo de consulta já foi organizado previamente ao redor de questões importantes, principalmente em legislações, como na elaboração do Marco Civil da Internet; tais consultas foram amplamente apreciadas como uma abordagem positiva.

A ARTIGO 19 solicita ao governo brasileiro que revise o a Estratégia à luz das recomendações destacadas nessa análise, a fim de garantir que uma maior variedade de atores da sociedade em geral sejam envolvidos no processo.

Resumo das Recomendações

- Como uma questão de princípio, políticas públicas – incluindo aquelas relacionadas à segurança da informação e comunicações e cibersegurança – devem ser abertas à uma discussão ampla e compreensível a todas as partes interessadas relevantes. A discussão deve basear-se em documentos e propostas elaborados por órgãos governamentais competentes que sejam claros e inteligíveis; as propostas também devem levar em consideração todos os parâmetros legislativos relevantes estabelecidos em nível nacional, bem como os padrões internacionais;
- Respeito aos direitos humanos, especialmente aos direitos de liberdade de expressão e proteção à privacidade, deveriam ser apropriadamente incorporados no conjunto dos princípios e objetivos que orientam a Estratégia, assim como referências a participação pública, à prestação de contas à sociedade e ao acesso à informação de interesse público. Uma visão de cibersegurança para além das dinâmicas internas administrativas também deveria ser integrada às premissas e propósitos do documento;
- Todos os princípios norteadores e objetivos deveriam ser esboçados de maneira mais precisa, incorporando os valores estabelecidos de maneira clara na legislação nacional, bem como a linguagem e as metas presentes nos diversos documentos internacionais;
- Devem ser introduzidas e desenvolvidas diretrizes para as discussões multissetoriais que envolvem decisões sobre investimentos nacionais em SIC e SegCiber;

- Qualquer treinamento ou programa de formação na área não deve dar importância desproporcional à defesa da soberania nacional como constituinte da cibersegurança. As preocupações relacionadas à segurança nacional devem ser propriamente balanceadas com os direitos humanos, necessidade de transparência e o acesso à informação;
- Pesquisas em SIC e SegCiber devem ser inteligíveis e completas e, portanto, devem ir além de questões tecnológicas para cobrir áreas como os direitos humanos e políticas públicas, no sentido mais amplo desses termos;
- O modelo de governança a ser implementado relacionado à SIC e à SegCiber deve ser definido apropriadamente; mais especificamente, deve ser desenvolvido em consulta com diferentes atores e deve incorporar dentre suas prioridades a proteção adequada aos direitos humanos, a prestação de contas à sociedade e a adotação de uma abordagem multissetorial.
- Referências a parcerias para aperfeiçoar a confidencialidade ou integridade das informações deve ser acompanhado de diretivas mais claras e específicas *vis-à-vis à* proteção da privacidade e ao exercício adequado do direito à liberdade de expressão.
- A Estratégia deve ser mais específica nas ações sugeridas relacionadas à proteção de infraestruturas críticas; em particular, ela deve focar nas elaboração de busca de envolvimento com os diferentes atores, do direito à informação dos cidadãos nestas questões e, também, no estabelecimento de salvaguardas apropriadas para a proteção adequada aos direitos humanos. Ela também precisa delimitar diretrizes claras relacionadas à cooperação entre instituições públicas e atores privados na área.
- Com o objetivo de atingir o objetivo estratégico de promover a conscientização dos cidadãos nas temáticas de SIC e SegCiber, a Estratégia precisa estabelecer mecanismos para a disseminação adequada e compreensível de informação, particularmente as relacionadas ao exercício e proteção efetivos dos direitos humanos, e aos diferentes mecanismos disponíveis para a realização de tais metas.

Índice

Introdução

Em abril de 2016, a ARTIGO 19 analisou a Estratégia de Segurança de Segurança da Informação e Comunicações e da Segurança Cibernética da Administração Pública Federal para 2015-2018. [1]

A Estratégia é um documento vinculante[2] unido ao arcabouço mais amplo de planejamento estratégico geral do Governo brasileiro. Foi desenvolvida a partir da instrução normativa GSI/PR nº 01/2008 do então Gabinete de Segurança Institucional da Presidência da República – GSI/PR – relacionada à gestão da segurança da informação e das comunicações da Administração Pública Federal, tendo sido preparada e aprovada pelo já mencionado Gabinete.

O propósito da Estratégia é estabelecer uma série de princípios gerais estratégicos para o provimento de proteção para os sistemas do governo; além disso, estabelece as principais metas para os próximos quatro anos, que deverão inspirar e guiar novas ações, com mais especificidade, para o cumprimento dos objetivos estratégicos de forma geral.

É esperado que os princípios estabelecidos inspirem e guiem futuramente ações mais específicas. Espera-se que estas ações atinjam as metas e objetivos estratégicos propostos para os próximos quatro anos na área de segurança da informação e cibersegurança.

A ARTIGO 19 acredita que a Estratégia – como uma política pública direcionada à cibersegurança - é relevante para a proteção de uma ampla gama de direitos humanos e, em particular, a liberdade de expressão e o direito à privacidade. Principalmente ao garantir a segurança de transações online de agências e departamentos públicos, agindo como facilitador da efetiva proteção de uma ampla gama de direitos humanos, tendo em vista que diversos sistemas de serviços públicos relevantes (como saúde, segurança, informações públicas, transporte, etc) são desempenhados via conexão à internet.

Consequentemente, nesta análise, a ARTIGO 19 avalia a Estratégia focando em observar a sua conformidade com os padrões internacionais e indicando de que forma estes devem ser adequadamente refletidos nela. Também acreditamos ser importante considerar como a Estratégia é aplicada subsequentemente na prática. Na análise destas questões, a ARTIGO 19 busca de maneira ativa oferecer recomendações construtivas em como a Estratégia pode ser aperfeiçoada.

A ARTIGO 19 solicita ao governo brasileiro que revise a Estratégia à luz das recomendações destacadas nessa análise. Nós nos colocamos à disposição para o provimento de assistência adicional no processo.

---

1 A análise legal é baseada na versão original da Estratégia, disponível em http://bit.ly/22T8EOs.

2 A natureza vinculante do documento deve ser entendida como não prejudicial às ferramentas de planejamento que promovem o plano de fundo geral para esta Estratégia, bem como os princípios e direitos estabelecidos pela legislação nacional e os padrões internacionais.

Padrões internacionais relevantes

A proteção da liberdade de expressão sob a legislação internacional

O direito à liberdade de expressão é protegido por inúmeros instrumentos internacionais de direitos humanos vinculantes a Estados, inclusive o Brasil; particularmente pertinentes são os Artigos 19 da **Declaração Universal dos Direitos Humanos *(UDHR)***[3] e o artigo 19 do **Pacto Internacional dos Direitos Civis e Políticos *(ICCPR)***.[4]

Adicionalmente, o **Comentário Geral No 34**,[5] adotado pela Comissão de Direitos Humanos da ONU, em setembro de 2011, explicitamente reconhece que o artigo 19 do *ICCPR* protege todas as formas de expressão e meios de disseminação, incluindo todas as formas de expressão por meios eletrônicos e baseados na internet.[6] Em outras palavras, a proteção da liberdade de expressão é aplicada online da mesma maneira que é aplicada offline. Estados signatários da *ICCPR* também são exigidos a considerar a extensão dos desenvolvimentos nas tecnologias da informação, como a disseminação da internet e de sistemas de informação eletrônicos móveis, mudaram dramaticamente as práticas de comunicação ao redor do mundo.[7] O arcabouço legal que regula as mídias de massa deve, também, considerar as diferenças entre as mídias impressas e de radiodifusão com relação à internet, sem deixar de observar as maneiras com que estas podem vir a convergir.[8]

De maneira similar, os quatro mandatos especiais para a proteção da liberdade de expressão destacaram, em sua **Declaração Conjunta sobre Liberdade de Expressão e Internet** de junho de 2011, que as abordagens regulatórias apropriadas aos setores de telecomunicações e radiodifusão não podem ser simplesmente transpostas para a internet.[9] Em particular, recomendam o desenvolvimento de abordagens regulatórias adaptadas a conteúdos ilegais na internet, enquanto destacam que restrições específicas para materiais disseminados ao redor da rede são desnecessárias. Também fomentam o uso de autorregulação como uma ferramenta efetiva para a reparação de discursos nocivos.

Como Estado signatário do *ICCPR*, o Brasil deve garantir que qualquer tipo de lei que tente regular as modalidades de expressão eletrônicas e baseadas na internet deve obedecer ao artigo 19 do *ICCPR*, como já interpretado pela Comissão de Direitos Humanos da ONU, além de estar alinhada às recomendações dos mandatos especiais.

---

3 *UN General Assembly Resolution 217A*(III), adotada em 10 de dezembro 1948.

4 GA res. 2200A (XXI), 21 UN GAOR Supp. (No. 16) at 52, UN Doc.

5 CCPR/C/GC/3, adotada em 12 de setembro de 2011, disponível em http://bit.ly/1xmySgV.

6 *Ibid.*, para 12.

7 *Ibid.*, para 17.

8 *Ibid.*, para 39.

9 Declaração Conjunta sobre Liberdade de Expressão e Internet, Junho de 2011, disponível em http://bit.ly/1CUwVap.

Limitações ao direito de liberdade de expressão

Apesar do direito à liberdade de expressão ser um direito fundamental, ele não é garantido em termos absolutos. Restrições a esse direito devem, entretanto, ser estritamente e rigorosamente adaptadas e não devem colocar em risco a liberdade de expressão em si. A determinação acerca de quando uma restrição é estritamente adaptada é geralmente determinada através de um teste de três partes. As restrições devem:

- **Serem prescritas pela lei**: isso significa que uma norma deve ser formulada com precisão suficiente para permitir um indivíduo possa regular a sua conduta de acordo com ela.[10] Restrições à liberdade de expressão ambíguas, vagas ou amplas em demasia são, portanto, inadmissíveis;

- **Terem um objetivo legítimo:** estes objetivos legítimos são exaustivamente enumerados no Artigo 19(3)(a) e (b) do *ICCPR* como: respeito aos direitos ou reputações de outros; proteção à segurança nacional; ordem pública; saúde pública ou morais. Dessa maneira, seria inadmissível proibir a expressão ou informação apenas sob o fundamento de que ela lança uma luz crítica sobre um governo ou sistema sociopolítico defendido pelo governo;

- **Serem necessárias e proporcionais:** Necessidade requere que deva existir uma demanda social para que ocorra a restrição. A parte que evoca deve demonstrar uma conexão imediata entre a expressão e o interesse protegido. Já a proporcionalidade requere que uma restrição à liberdade de expressão não seja ampla demais e que seja apropriada para alcançar sua função protetiva. Deve ser demonstrado que a restrição é específica para alcançar esse resultado protetor e não é mais intrusiva do que outros instrumentos disponíveis e capazes de alcançar o mesmo resultado limitado.[11]

Os mesmos princípios se aplicam às formas eletrônicas de comunicação ou expressão disseminadas por toda a internet.[12]

Segurança nacional e liberdade de expressão

Os **Princípios de Johannesburgo sobre Segurança Nacional, Liberdade de Expressão, e Acesso á informação**[13] (Princípios de Johannensburgo), um conjunto de padrões internacionais desenvolvidos pela ARTIGO 19 e especialistas em liberdade de expressão internacionais, são instruções relativas a restrições em liberdade de expressão que tem como fim a proteção da segurança nacional.

O Princípio 2 dos Princípios de Johannensburgo afirma que restrições justificadas na seara da segurança nacional são ilegítimas, a não ser que exista um propósito genuíno e o efeito demonstrável seja proteger a existência do país ou sua integridade territorial contra o uso da força ou ameaça de força, ou sua capacidade de responder ao uso ou ameaça de força. A restrição não pode servir como

10 Comissão de DH ONU, *L.J.M de Groot v. The Netherlands,* No. 578/1994, UN Doc. CCPR/C/54/D/578/1994 (1995).
11 Comissão de DH ONU, *Velichkin v. Belarus*, No. 1022/2001, UN Doc. CCPR/C/85/D/1022/2001 (2005).
12 Comentário Geral no. 34, *op.cit.*, para 43.
13 Adotado em 1º de Outubro de 1995. Os Princípios foram endossados pela Relatoria Especial para Liberdade de Expressão da ONU e foram referidos à Comissão de DH da ONU em suas resoluções anuais.

pretexto para a proteção do constrangimento de um governo ou exposição de uma transgressão, ocultando informações sobre o funcionamento de suas instituições públicas, ou a supressão de uma ideologia em particular.

O Princípio 15 determina que um indivíduo não pode ser punido por ameaça à segurança nacional por revelação de informações se:

- a revelação não necessariamente causa dano e provavelmente não causará dano a um interesse de segurança nacional legítimo, ou
- o interesse público da informação prevalece sobre os perigos de sua divulgação.

Ademais, os **Princípios Globais sobre Segurança Nacional e o Direito a Informação** (Príncipios de Tschwane)[14] também consideram de maneira extensiva os tipos de restrições que podem ser impostos ao acesso à informação.

Proibição de incitação à discriminação, hostilidade e violência

Também é importante observar que o Artigo 20(2) do *ICCPR* prevê que qualquer tipo de defesa ou apoio de ódio de caráter nacional, racial ou religioso que constitui incitação à discriminação, hostilidade ou violência deve ser proibido por lei. Ao mesmo tempo, "incitar violência" significa mais do que simplesmente expressar visões que pessoas desaprovem ou achem ofensivas:[15] é o discurso que encoraja ou solicita que outras pessoas se envolvam com violência através de retóricas veementemente discriminatórias. No âmbito internacional, a ONU desenvolveu o Plano de Ação de Rabat, um processo interregional e multissetorial envolvendo as instâncias de direitos humanos da organização, ONGs e a academia – e que fornece a definição mais próxima do que constitui uma lei sobre incitação de acordo com o previsto no Artigo 20(2) do *ICCPR*.[16]

Vigilância das Comunicações

O direito à privacidade complementa e reforça o direito à liberdade de expressão. O direito à privacidade é essencial para garantir que indivíduos possam se manifestar livremente, inclusive de forma anônima[17] caso façam essa escolha. A vigilância em massa das comunicações online, portanto, impõe preocupações significantes tanto para o direito à privacidade quanto à liberdade de expressão.

O direito a comunicação privada é firmemente protegido pelas leis internacionais através do Artigo 17 do *ICCPR*,[18] que determina que nenhum indivíduo deve ser submetido a interferências arbitrárias ou

14 Princípios de Tschwane, disponível em http://osf.to/1jag6nW.

15 *C.f.* European Court, *Handyside v the UK*, julgamento de 6 de julho 1976, para 56.

16 Ver *UN Rabat Plan of Action* (2012), disponível em http://bit.ly/1T2efOV. Ele esclarece a questão dizendo que devem ser dados seis fatores para avaliar quando um discurso deve ou não ser considerado incitação, incluindo o contexto geral, o interlocutor, a intenção, conteúdo, a extensão do discurso e a probabilidade de ocorrer prejuízo, incluindo sua iminência.

17 *Ibid.*, para 84.

18 Artigo 17 diz: 1) Ninguém será objecto de intervenções arbitrárias ou ilegais na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem de atentados ilegais à sua honra e à sua reputação. 2) Toda e qualquer pessoa tem direito à proteção da lei contra tais intervenções ou tais atentados.

ilegais à privacidade pessoal, de sua família ou de sua correspondência. No **Comentário Geral no. 16** sobre o direito à privacidade,[19] a Comissão de Direitos Humanos da ONU esclarece que o termo "ilegal" significa que nenhum tipo de interferência deve ocorrer, exceto em casos previstos pela lei. Interferência autorizada por Estados apenas pode ocorrer com base na lei, a qual deve estar em consonância com as provisões, alvos e objetivos do *ICCPR*. O Comentário Geral ainda ressalta que:

> Mesmo no que diz respeito a interferências que estão em conformidade com o Pacto, legislações relevantes devem especificar em detalhes as circunstâncias precisas em que tais intereferências podem ser permitidas. Uma decisão que faz uso de tal interferência autorizada deve apenas ser feita por uma autoridade designada pela lei e na base de análise caso-a-caso.[20]

O Relator Especial da Onu para promoção e proteção de direitos humanos e liberdades fundamentais no combate ao terrorismo enfatizou, enquanto se referia sobretudo ao "ciberespaço", que apesar de ser um direito em si, a privacidade também serve como base para o exercício de outros direitos:

> A privacidade é necessária para criar espaços que permitam que indivíduos e grupos possam pensar e desenvolver ideias e relacionamentos. Outros direitos, como a liberdade de expressão, de associação e de movimento, requerem privacidade para que possam se desenvolver de maneira efetiva.[21]

Ele também argumentou que, assim como as restrições à liberdade de expressão sob o Artigo 19, as restrições ao direito à privacidade sob o Artigo 17 do *ICCPR* devem ser interpretadas à luz do teste de três partes:

> O Artigo 17 do Pacto também deve ser interpretado como detentor dos ditos elementos de um teste de limitações permissivo. Restrições que não estejam previstas pela lei são "ilegais" no sentido do Artigo 17 e, restrições que ficam aquém da necessidade ou não servem como fim legítimo acabam por ser interferências "arbitrárias" com os direitos providos pelo Artigo 17.[22]

Em termos de vigilantismo (com o contexto de terrorismo neste caso), ele definiu parâmetros de restrições legítimas no direito à privacidade de acordo com os seguintes termos:

> Estados devem poder fazer uso de medidas de vigilância direcionadas, previsto que sejam interferências em casos específicos, com base em um mandato emitido por um juíz que demonstra causa provável em âmbito razoável. Deve haver alguma base factual, relacionada ao comportamento de um indivíduo que possa justificar a suspeita de que ele ou ela estar envolvido ou envolvida na preparação de um ataque terrorista. [23]

O Relator Especial também salientou que:

---

19 Comentário Geral 16, adotado em 8 Abril de 1988.

20 *Ibid.*, para 8.

21 Relatório do Relator Especial da ONU sobre a promoção e proteção dos direitos humanos e liberdades fundamentais no combate ao terrorismo, Martin Scheinin, A/HRC/13/37, 28 Dezembro de 2009, para 33; disponível em http://bit.ly/23NMPpo.

22 *Ibid.*, para 17.

23 *Ibid.*, para 21

> O direito à privacidade é usualmente compreendido como um requisito essencial para a refetivação do direito à liberdade de expressão. Interferência indevida com a privacidade de um indivíduo pode tanto diretamente quanto indiretamente limitar o livre desenvolvimento e a troca de ideias[24].

Ademais, ele observou:

> O direito à privacidade pode estar sujeito a restrições ou limitações sob determinadas circunstâncias excepcionais. Estas podem incluir medidas de vigilância estatal que envolvem a administração da justiça criminal, prevenção de crimes ou combate ao terrorismo. Porém, tal interferência só é permissível se os critérios para limitações admissíveis sob as leis internacionais de direitos humanos forem cumpridos. Consequentemente, deve haver uma lei que identifique de maneira clara as condições em que o direito à privacidade de indivíduos pode ser restringido em situações com circunstâncias excepcionais. Além disso, medidas que usurpem esse direito devem ser tomadas com base de uma decisão específica de uma autoridade estatal com competência expressa para tomar tal, normalmente o judiciário, com o objetivo de proteger os direitos de terceiros como, por exemplo, na recolha de provas para prevenir o cometimento de um crime, respeitando o princípio da proporcionalidade.

Cibersegurança e proteção de direitos humanos

Cibersegurança, liberdade de expressão e privacidade estão claramente entrelaçados. Entretanto, não existe definição clara de cibersegurança em nível internacional. Abordagens nacionais para tais conceitos, enquanto isso, podem variar; elas também podem coincidir ou ao mínimo parcialmente se sobrepõem com outros conceitos similares, como ciberdefesa, segurança de TI ou prevenção de cibercrimes.

O Relator Especial para Liberdade de Expressão da Organização dos Estados Americanos (OEA) recomenda a adoção de padrões claros e definições não demasiadamente amplas de cibersegurança, limitadas à salvaguarda de dados de computadores e sistemas ou, em outras palavras, a integridade da rede e da infraestrutura da internet, incluindo a confidencialidade da informação que elas contém.[25] De acordo com o Relator da OEA, qualquer ação estatal relacionada à segurança no ciberespaço.

> Deve ser limitada e proporcional, além de desenhada para cumprir fins legítimos específicos que não põem em risco as virtudes democráticas que caracterizam a rede.[26]

O Relator da OEA ainda enfatizou que natureza aberta e descentralizada da internet requer não só uma abordagem de governança multissetorial, bem como o reconhecimento de que as responsabilidades relacionadas à proteção das comunicações e infraestrutura devem ser compartilhadas. Adicionalmente,

[24] O relatório da Relatoria Especial em LibEx, A/HRC/23/40, 2013, para 2; disponível em http://bit.ly/1XMsDgk.

[25] Liberdade de Expressão e Internet, 2013, paras 118 and 119, disponível em http://bit.ly/1SyvDM3. Ver também capítulo de intersecção entre vigilantismo, cibersegurança, cibercrimes e ciberguerra em ARTIGO 19, *Da cibersegurança à ciberguerra. O desenvolvimento de políticas de vigilança no Brasil*, disponível em http://bit.ly/1YKG7cJ.

[26] *Ibid.,* para 120.

os Estados devem estar atentos ao impacto de qualquer tipo de medida nessa área nos direitos humanos e, particularmente, na liberdade de expressão. Os Estados também:

> Deveriam visar ter uma política que garanta a integridade da infraestrutura e da informação online, a fim de garantir a proteção de usuários de ataques cibernéticos que violam o direito à privacidade ou liberdade de expressão e direitos correlatos.[27]

Qualquer tipo de política, ou objetivo legal, de cibersegurança deve ser pesada em contraposição aos direitos humanos antes de sua adoção.[28]

- À luz dos objetivos especificados na Estratégia, os seguintes princípios internacionais também são relevantes: uma reunião de alto nível da Assembleia Geral, revisando a implementação dos resultados da *World Summit on the Information Society* de 2015 *(WSIS +10)*, onde claramente está reconhecido o papel de liderança que governos e outras autoridades estatais tem na nas questões de cibersegurança relacionadas à segurança nacional, reconhecendo também a importância das contribuições de todos os atores, em seus respectivos papéis e responsabilidades. Também é salientado que a construção de confiança e de segurança no uso de informações e nas tecnologias das comunicações também devem ser consistentes com os direitos humanos.[29]

- O Relator Especial para Liberdade de Expressão da OEA também enfatizou que políticas e medidas de cibersegurança devem ser completamente passíveis de fiscalização, escrutínio público e debate. Essa recomendação também faz referência a ações adotadas por atores privados e intermediários no caso de auxiliarem o Estado em tais políticas. A prestação de contas e responsabilidade para com a sociedade não só deve respeitar o princípio geral de transparência, mas também garantir o envolvimento dos cidadãos, sociedade civil e outros atores relevantes na tarefa de definição e implementação de políticas. Por último, mas não menos importante, decisões e ações públicas – mesmo aquelas delegadas a terceiros – precisam estar sujeitas ao controle apropriado das normas jurídicas e ao judiciário, em particular.[30]

- Embora não exista padrão internacional em cibercrimes, alguns padrões regionais foram adotados. Dentre esses padrões regionais, a Convenção sobre o Cibercrime de 2001 do Conselho Europeu se tornou a mais reconhecida e relevante.[31] A Convenção prevê definições para termos relevantes, incluindo: dados de computador, sistemas de computador, tráfego de dados e provedores de serviço. Ela demanda que Estados participantes criem infrações contra a confidencialidade, integridade e disponibilidade de sistemas informáticos e dados informáticos; delitos relacionados à informática, incluindo falsificação e fraude; e infrações relacionadas a conteúdos, como por

---

27 *Ibid.,* para 121.

28 *Ibid.* para 124.

29 Esboço da resolução submetida pelo presidente da GA, A/70/L.33, para 50, disponível em http://bit.ly/1VGHJH2.

30 Relatório em Liberdade de Expressão e a Internet *op.cit.*, paras 126-129. Em particular, o relatório diz que "Os Estados têm o dever de informar, entre outras coisas, sobre as diretrizes gerais das políticas e sobre as agências encarregadas e suas responsabilidades. Diante de ataques ou riscos iminentes, os Estados devem prestar contas ou ordenar investigações que permitam conhecer a dimensão do ocorrido."
."

31 Convenção sobre Cibercrimes do Conselho Europeu, CETS No. 185, desde Julho de 2004. Em Maio de 2015, 46 estados haviam ratificado e ainda oito outros assinaram a Convenção mas não ratificaram-na.

exemplo a criminalização da pornografia infantil. A Convenção sobre o Cibercrime, então, define um número de exigências procedimentais para a investigação e acusação para cibercrimes, incluindo requerimentos de guarda de dados, injunções para produção de provas e busca e apreensão de dados de computadores. Finalmente, é importante ainda que a Convenção estabelece de maneira clara que as medidas acima devem respeitar todas as condições e salvaguardas para a proteção de direitos humanos e liberdades, consistentes com o *ICCPR* e outros instrumentos de direito internacional aplicáveis.

A Estratégia e seu contexto

Conforme observado acima, a Estratégia é um documento vinculante dentro de uma estrutura mais ampla de planejamento do Governo brasileiro, tendo sida preparada e aprovada pelo então GSI/PR. Uma estratégia geral sobre cibersegurança já havia sido aprovada previamente pelo Governo em 2010 (o Livro Verde sobre Segurança Cibernética no Brasil[32]). A preparação da minuta do texto foi realizada por um grupo de trabalho no âmbito do Gabinete de Segurança Institucional, em consulta com o Comitê Gestor de Segurança da Informação e Comunicações. Este comitê é um órgão consultivo da Presidência da República, formado por representantes de diferentes ministérios e várias grandes instituições do Estado brasileiro.[33]

Os fatos a seguir irão fornecer um contexto geral útil sob o qual será mais fácil compreender o contexto e os objetivos da Estratégia:

- O Brasil vem desempenhando um papel bastante ativo no âmbito internacional, relacionado ao estabelecimento de novos princípios e parâmetros nas áreas de cibersegurança, proteção da privacidade e governança multissetorial da internet. A origem deste posicionamento político é rigorosamente conectada às famosas revelações de Edward Snowden a respeito da vigilância em massa praticada por agências de inteligência dos EUA;
- Recentemente o Brasil esteve no centro da atenção internacional como sede da Copa do Mundo FIFA de 2014; ainda continuará sob os holofotes como sede dos Jogos Olímpicos de 2016. Tais eventos levantam desafios importantes relacionados ao acesso à internet, segurança e outras questões online.
- A Administração Pública Federal no Brasil tem um tamanho considerável. Diferentes agências e escritórios públicos acabam por fazer uso extensivo da internet, criando uma estrutura grande e e potencialmente vulnerável. De acordo com a Estratégia, a Administração Federal cobre 39 Ministérios,[34] por volta de 6000 órgãos públicos, mais de 1 milhão de servidores públicos, 320 redes digitais e 12 milhões de websites. Atualmente parecem haver algumas deficiências na coordenação das ações de SIC e SegCiber, sem que exista uma autoridade central implementando uma abordagem sistêmica e multissetorial.

[32] Presidencia da República, GSI, Secretário Executivo, Departamento de Segurança da Informação e Comunicações, Livro Verde: Segurança Cibernética no Brasil, 2010, disponível em http://bit.ly/1l5AtRt.

[33] O Comitê foi criado pelo Decreto nº 3505, de 13 de Junho de 2000; Mais informações disponíveis em http://bit.ly/1SomJhX.

[34] O Ministério do Planejamento, Orçamento e Gestão lançou um plano para reduzir o número de ministérios. Uma recente remodelação do gabinete de fato eliminado 8 deles.

- O chamado "Plano Brasil 2022" (o grande plano estratégico para o Brasil para a década)[35] inclui dentre seus objetivos implantação de redes de banda larga, a universalidade do acesso à cultura, a proteção adequada do direito à informação pública, bem como a consolidação da Internet como uma plataforma para a liberdade de expressão.

Além disso, existem diversas leis nacionais que proporcionam uma estrutura normativa para a Estratégia:

- **O Marco Civil da Internet**[36] define uma série de princípios básicos, salvaguardas, direitos e responsabilidades relacionados à internet no Brasil. Ele ganhou reconhecimento proeminente para além das fronteiras brasileiras e sua aprovação foi apresentada como um forte comprometimento político em favor de uma internet aberta, diversa e democrática. A lei estabelece que a regulação relacionada à internet no Brasil deve estar fundamentada no respeito à liberdade de expressão, nos direitos humanos em geral, além da ideia de cidadania[37]. A internet tem um papel social claro que deve ser, portanto, preservado. A liberdade de expressão e a privacidade são estabelecidas como princípios básicos que governam a rede e a necessidade de preservar sua estabilidade, segurança e funcionalidade é reconhecida. Responsabilidades nessas áreas precisam ser proporcionalmente divididas por todos os atores, preservando sempre a natureza multiparticipativa da internet. A web também é reconhecida como uma peça chave na promoção do acesso à informação e à participação nos assuntos públicos. A lei estipula que a proteção adequada dos direitos à privacidade e à liberdade de expressão é uma pré-condição para o pleno exercício do direito ao acesso à internet.[38] Por último, a lei estabelece uma série de princípios bastante claros e aplicáveis para políticas e atividades de órgãos públicos com relação à rede. Particularmente, o Marco Civil define que:[39]

  - Autoridades públicas precisam estabelecer mecanismos multissetoriais, transparentes, colaborativos e democráticos para a governança da internet, com participação do Governo, o setor privado, a sociedade civil e a academia;

  - Os dados e informações do setor público devem ser publicizados e disseminados de maneira aberta e estruturada.

  - A participação dos cidadãos nas políticas públicas deve ser fortalecida.

---

35 Governo Federal, a Presidência da República, Secretaria de Assuntos Estratégicos, Brasil 2022, disponível em http://bit.ly/1VpRSaH.

36 A Lei No. 12.965 de 23 Abril de 2014 (conhecido como Marco Civil da Internet).

37 *Ibid.,* Artigos 2-4.

38 *Ibid.,* Artigo 8.

39 *Ibid.,* Capítulo IV.

- **A Lei de Acesso à Informação**[40] também é um instrumento importante que deve ser levado em consideração. A lei surgiu com o foco de mudar o comportamento a cultura do sigilo do governo brasileiro e de outros órgãos públicos, fruto de um legado negativo e autoritário do período ditatorial; entretanto, ainda existem sérios desafios para a sua efetiva implementação. A lei estabelece um princípio geral de publicidade, tornando dados secretos e confidencias a exceção dentro dos termos legais; ela também promove o uso de tecnologias da informação como fins para facilitar a transparência e o acesso à informação, assim como a fiscalização civil sob a administração pública.[41]

  A lei também:

  - Atribui uma série de responsabilidades às autoridades públicas ao mesmo tempo em que visa garantir a disponibilidade, integridade e autenticidade das informações públicas e a confidencialidade de dados pessoais (artigo 6);

  - Proporciona ao cidadão o direito de obter informação acerca de todas as atividades realizadas por órgãos públicos, incluindo aqueles relacionados à própria organização e serviços internos dos mesmos; por essa lei, os cidadãos também tem o direito de ter conhecimento a respeito da implementação e resultados de programas, projetos e ações desempenhadas pelos órgãos públicos, bem como seus objetivos e intenções (artigo 7);

  - Aborda o nível de sigilo ou confidencialidade de determinadas informações sensíveis relacionadas à defesa nacional, relações internacionais e outros assuntos (artigos 23-29). A lei busca definir o escopo de tais exceções à publicidade e também determina um procedimento apropriado para a adoção e o escopo das decisões dentro deste quesito. Também insiste que informações só devem ser declaradas secretas ou confidenciais após o balanço entre o interesse público de determinadas informações e a necessidade de adoção à medida menos restritiva possível. No entanto, em particular, a adoção destes tipos de medidas tem sido bastante problemática.

40 Lei No. 12.527 de18 Novembro 2011 (Lei de Acesso à Informação).
41 *Ibid,* Artigo 3.

Metodologia, metas, valores e princípios orientadores da Estratégia

A ARTIGO 19 faz as seguintes observações gerais a respeito da Estratégia:

- **A falta de disposições claras que orientam as ações dos organismos públicos**: Embora a Estratégia seja um documento vinculativo, ela não é um texto jurídico normativo: não estão incluídas regras claras ou disposições diretas. Essencialmente, o documento visa estabelecer uma série de princípios estratégicos gerais que inspiram e orientam as ações futuras e mais específicas. Apesar de que, como será mostrado, a execução de algumas das suas orientações exigirá o envolvimento de diferentes grupos de atores privados, aqueles que deverão aplicar primariamente e seguir as diretrizes da Estratégia serão os diferentes departamentos e órgãos da administração federal. Significativamente, a imprecisão das disposições que orientam as ações desses agentes públicos é a questão mais problemática deste documento, com fortes implicações para os direitos humanos.

- **A metodologia específica utilizada na elaboração da Estratégia**: o documento refere-se ao planejamento e metodologia estratégica chamada *Balanced Scorecard* (ou "placar balanceado"), desenvolvido por Robert Kaplan e David Norton. Esta é uma ferramenta gerencial, que faz uso de procedimentos e parâmetros técnicos aplicáveis a uma vasta gama de organizações; é uma metodologia essencialmente destinada a melhorar a eficácia e eficiência de planos estratégicos. Aqui, tem sido adaptada ao contexto específico da política pública, e um dos principais objetivos definidos pela Estratégia refere-se ao cumprimento de determinados resultados para beneficiar a sociedade. Estes objetivos sociais incluem a transparência, a proteção da privacidade, a democratização do acesso à informação e a salvaguarda de ativos de informações confidenciais (páginas 35-36). Estes objetivos são relevantes e bastante alinhados com as normas jurídicas nacionais e internacionais aplicáveis, conforme já detalhado acima. No entanto, é difícil encontrar na Estratégia um plano mais específico para atingir essas metas. Além disso, o estabelecimento dos diferentes objetivos estratégicos concretos na parte central da Estratégia sequer menciona ou mesmo leva em consideração qualquer um destes importantes valores e direitos.

- **Objetivo principal:** O principal objetivo da Estratégia é garantir o uso do ciberespaço, impedindo ou obstruindo ações que vão contra os interesses do país ou da sociedade. Este objetivo geral parece ser legítimo. No entanto, as referências à proteção e exercício dos direitos humanos, além de uma ampla participação dos cidadãos também são necessários neste contexto.

- **Objetivo geral:** Outro objetivo principal da Estratégia foca-se em medidas e ações assumidas pelas autoridades públicas. Estes não só se relacionam com a organização e coordenação

interna, mas também incluem mudanças legislativas e outras normativas. Por esta razão, embora o documento não contenha disposições elaboradas como normas específicas, o fato de que ele trata enfaticamente do estabelecimento de uma série de princípios, valores e direitos que devem ser protegidos na adoção de novas medidas administrativas e legislativas é muito importante.

- **A falta de participação pública no desenvolvimento da Estratégia:** A seção de metodologia da Estratégia contém uma breve explicação das diferentes fases da elaboração do documento, detalhando os atores que participaram em cada estágio (p 36). De acordo com a descrição, o processo foi essencialmente realizado internamente na Administração Federal, com a formação de um comitê técnico composto por funcionários do Gabinete de Segurança Institucional; foram realizadas consultas em conjunto com o Comitê de Gestão de Segurança da Informação. Transparece nos fatos que, na elaboração de um importante documento como este, não houve consultas pertinentes a atores de fora da Administração Federal. As organizações da sociedade civil, os mais diferentes atores da Internet, além do público em geral, não tiveram a oportunidade de analisar e fazer contribuições para a Estratégia. Conforme explicado acima, acreditamos que este não é um mero conjunto de diretivas "internas" e que, portanto, tal documento não deveria ser elaborado sem consulta externa.

- **Fracasso em situar a Estratégia na proteção dos princípios dos direitos humanos:** os valores e os princípios orientadores das estrategia (páginas 37-41) se concentram exclusivamente em preocupações administrativas e de gestão, tais como a ética profissional, colaboração, eficácia, liderança e apoio para políticas públicas. Não existem referências claras à cidadania, direitos humanos, abordagem multissetorial para segurança da internet, acesso a informações ou à participação pública. A ARTIGO 19 considera decepcionante o fato de que os princípios orientadores só referem-se às implicações de cibersegurança em termos de soberania nacional, da centralização das decisões, resiliência, ou o envolvimento de órgãos públicos com capacidade de influência. Vagas referências à necessidade de uma "forte ligação entre múltiplos atores" e a promoção da cooperação com o "setor produtivo e a academia" não parecem um compromisso adequado à complexidade das estratégias necessárias para a cibersegurança. Finalmente, esta parte da Estratégia salienta o fato de que o documento terá uma influência direta na elaboração de novos instrumentos jurídicos para a área, deixando claro, mais uma vez, a importância vital de uma abordagem abrangente para estas questões e a influência negativa que as deficiências do documento podem ter sobre futuras medidas.

A ARTIGO 19 também destaca que a única referência na Estratégia à Lei de Acesso à Informação (ver acima) é feita em razão do tratamento especial de "os ativos de informação sigilosos cuja publicidade seja sensível para o país" (página 17). A Estratégia sublinha que esta "dinâmica impacta diretamente na estratégia adotada pelo governo para a SIC e a SegCiber". Assim, é relevante notar que a Estratégia

parece dar legitimidade às decisões secretas sobre medidas e ações de segurança cibernética. Apesar de algumas informações nesta área realmente poderem ser sensíveis e requerem um certo grau de confidencialidade, existe uma clara desproporção entre a atenção dada a estas considerações e a total ausência de referências à transparência, o acesso à informação e a princípios de prestação responsável de contas à sociedade incluídas na lei.

Como observação final, apesar da Estratégia referir-se apenas às questões de cibersegurança do aparato da administração federal, a ARTIGO 19 aproveita a oportunidade para enfatizar que nem este nem qualquer outro documento poderiam ser usados para legitimar quaisquer ações que possam envolver o uso massivo e injustificado vigilância contra os cidadãos. Além disso, as preocupações refletidas na Estratégia não podem ser utilizadas para justificar a implementação de práticas de vigilância contra a sociedade brasileira, a fim de evitar a mobilização social e obstruir o direito de protesto.

Recomendações:

- Como um questão de princípio, políticas públicas – incluindo aquelas relacionadas à segurança da informação e das comunicações e cibersegurança – devem ser abertas à uma discussão ampla e compreensível a todas as partes interessadas relevantes. A discussão deve basear-se em documentos e propostas elaborados por órgãos governamentais competentes que sejam claros e inteligíveis; as propostas também devem levar em consideração todos os parâmetros legislativos relevantes estabelecidos em nível nacional, bem como os padrões internacionais;
- Respeito aos direitos humanos, especialmente aos direitos de liberdade de expressão e proteção à privacidade, deveriam ser incorporados apropriadamente no conjunto dos princípios e objetivos que orientam a Estratégia, assim como referências a participação pública, à prestação de contas à sociedade e ao acesso à informação de interesse público. Uma visão de cibersegurança para além das dinâmicas internas e administrativas também deveria ser integrada às premissas e ao espírito do documento;
- Todos os princípios norteadores e objetivos deveriam ser esboçados de maneira mais precisa, incorporando os valores estabelecidos de maneira clara na legislação nacional, bem como a linguagem e as metas presentes nos diversos documentos internacionais;
- Referências à sigilo e necessidade de proteção de informações sensíveis precisam ser colocadas em contexto com as regras gerais de publicidade, acesso à informação e prestação responsável de contas à sociedade das questões relacionadas às políticas de cibersegurança.

Análise dos objetivos estratégicos específicos

Institucionalização da SIC e SegCiber como parte do planejamento nacional e das decisões orçamentárias federais

Priorização e consideração apropriada da SIC e da SegCiber dentro do contexto das decisões políticas majoritárias parece ser um objetivo geral positivo. Também vale mencionar que a Estratégia faz referência à necessidade de ampliar as discussões para "atores chave do governo, da academia, do setor privado e do terceiro setor" sobre qual porcentagem do PIB deveria ser estabelecida como investimento mínimo nestas áreas. Estes podem ser vistos como princípios gerais bons, mas não existem diretrizes procedimentais mencionadas, muito menos existe algum detalhe sobre quais fatores poderiam ser levados em consideração em tais debates.

Recomendação:

- Diretrizes para participação multissetorial em decisões relacionadas ao investimento nacional em SIC e SegCiber necessitam ser introduzidas e desenvolvidas.

Aperfeiçoamento quantitativo e qualitativo dos envolvidos nas ações de SIC e SegCiber

A Estratégia indica a necessidade de desenvolver programas de treinamento para aperfeiçoar a dedicação e expertise dos oficiais públicos nestas áreas. O documento sugere o estabelecimento de um diploma específico de SIC e SegCiber no setor público. Também declara que essas áreas pertencem exclusivamente ao Estado, tendo em vista a sua importância estratégica na proteção da segurança nacional.

Recomendações:

- As referências à formação de pessoal no campo da SIC e SegCiber devem necessariamente incorporar um forte componente de direitos humanos e invocar questões mais amplas de cidadania, incluindo a responsabilização e prestação de contas dos funcionários públicos;
- Qualquer treinamento ou programa de formação nesta área não deve dar importância desproporcional ou demasiadamente ampla à defesa da soberania nacional como um componente de cibersegurança. As preocupações de segurança nacional devem ser devidamente equilibradas com os direitos humanos, prestação de contas e transparência, além de acesso à informação.

Promoção da pesquisa nas áreas de SIC e SegCiber

A Estratégia faz uma referência geral para o reforço e priorização de pesquisa, desenvolvimento e inovação nas áreas da SIC e SegCiber. Refere-se também à necessidade de criar parcerias entre

universidades, o setor privado e a administração pública, a fim de desenvolver as melhores soluções. O fato de que a pesquisa tecnológica irá melhorar a confidencialidade das comunicações e, portanto, facilitar uma melhor proteção da privacidade também é mencionado. No entanto, a promoção da pesquisa mencionada é limitada à tecnologia e gestão; mesmo nessas áreas, a Estratégia é extremamente vaga com relação à identificação e promoção de temas e objetivos específicos da investigação. A ARTIGO 19 reitera que a segurança cibernética exige a consideração de perspectivas mais amplas e que o desenvolvimento deverá exigir uma abordagem multidisciplinar que envolve direitos humanos e políticas públicas, no sentido mais amplo desses termos.

Recomendações:

- Pesquisas em SIC e SegCiber devem ser abrangente e completas e, portanto, devem abranger áreas que vão além das questões tecnológicas, tais como os direitos humanos e políticas públicas, no sentido mais amplo destes termos;
- O documento deve promover a elaboração multiparticipativa de uma agenda de pesquisa completa, com indicação dos instrumentos e recursos disponíveis para o desenvolvimento de projetos e atividades específicas.

Melhoria da governança pública e coordenação relacionada a SIC e SegCiber, incluindo a presença de órgão "central"

A Estratégia destaca a necessidade de adoção de um modelo de governança eficaz nestas áreas. Esse modelo terá um órgão de coordenação central e deverá basear-se numa série de prioridades de políticas: apoio à gestão, acordos sobre diretivas, busca de harmonização, aumento de maturidade, melhorar a resiliência, reforçar a segurança dos ativos de informação e proteger infraestruturas críticas. A ARTIGO 19 considera problemático que estas prioridades não contemplem a natureza participativa e multissetorial de governança da cibersegurança, nem as suas implicações para os direitos humanos.

Recomendação:

- A Estratégia tem de definir de maneira adequada o modelo de governança que deverá ser implementado em áreas SIC e SegCiber. Este modelo de governança deve ser elaborado com a participação de diferentes atores e deve incluir entre as suas prioridades a proteção adequada aos direitos humanos, a plena transparência e prestação de contas e a adoção de uma abordagem multissetorial;
- Apesar da necessidade de algum tipo de coordenação de um órgão centralizado, os modelos de governança da cibersegurança devem ser apropriadamente adaptados à natureza diversa e plural da internet. Transparência e acesso à informação devem ser os princípios fundamentais.

Alinhamento com o planejamento estratégico de outros órgãos e entidades que pertencem à Administração Pública Federal

A Estratégia ressalta que, além de um bom planejamento nas áreas SIC e SegCiber dentro da administração pública federal, também é necessário que essas ações sejam coordenadas com o planejamento geral e as políticas estratégicas do governo. A ARTIGO 19 reitera a necessidade de que o

alinhamento das ações SIC e SegCiber com a estratégia federal deve incorporar referências específicas para políticas públicas e para a proteção dos direitos humanos, o acesso à informação, a melhoria da participação dos cidadãos e da prestação de contas das autoridades públicas.

Recomendação:

- A Estratégia também deve incorporar referências a políticas públicas específicas relacionadas à proteção de direitos humanos, acesso à informação, aumento de participação popular e à capacidade de prestação de contas das autoridades, ao lado do alinhamento com políticas e planejamentos estratégicos em nível federal.

Reforço de parcerias públicas com o setor privado e a sociedade civil, ambos em nível nacional e internacional

De acordo com a Estratégia, o objetivo principal de tais parcerias seria a troca de experiência de melhores práticas para assegurar a disponibilidade, integridade, confidencialidade e autenticidade da informação, garantindo a disponibilidade e continuidade dos serviços públicos. A ARTIGO 19 considera que estes são princípios muito amplos – apresentados nesta parte do documento como objetivos estratégicos – que já foram repetidos em partes anteriores do documento, mas não são objeto de nenhum desenvolvimento ou especificação posterior.

Recomendação

- Referências à parcerias para garantir a confidencialidade e integridade da informação devem ser acompanhadas de diretivas mais claras e específicas que estejam em conformidade com a proteção à privacidade e ao adequado exercício da liberdade de expressão.

Aumento de foco em SIC e SegCiber nos departamentos da Administração Pública Federal

A Estratégia prevê que os diferentes departamentos e agências da administração pública irão estabelecer os seus próprios planos em relação às questões SIC e SegCiber, envolvendo uma série de mecanismos de autodiagnóstico. Tais mecanismos serão geralmente definida pelo órgão central com responsabilidade nesta área. No entanto, a ARTIGO 19 acredita que planos específicos de SIC e SegCiber e os mecanismos de autodiagnóstico precisam incorporar os direitos humanos, prestação de contas e componentes de participação pública. A Estratégia deve ser mais clara e detalhada nesta área.

Recomendação

- A Estratégia deveria desenvolver mais as seções específicas sobre como os planos de SIC e SegCiber e os mecanismos de auto-diagnóstico irão incorporar os direitos humanos, prestação de contas à sociedade e outros componentes democráticos

Reforço de que SIC e SegCiber devem ter prioridade elevada na agenda do Governo

ARTIGO 19 observa que, mais uma vez, a Estratégia refere-se à importância da SIC e SegCiber para a atividade política do governo. Nesta seção, especificamente aponta para o artigo 91 da Constituição, que diz respeito às funções do Conselho de Defesa Nacional. No entanto, nenhum tipo de menção de outros valores constitucionais importantes, em matéria de direitos humanos, participação e prestação de contas, é feita.

Recomendação

- Objetivos estratégicos em relação ao planejamento de políticas e à estratégia do Governo nas áreas da SIC e SegCiber também devem incluir referências e incorporar os mandatos constitucionais relativos aos direitos humanos, participação e responsabilidade dos funcionários públicos.

Aperfeiçoamentos para o fortalecimento da segurança de infraestruturas críticas

Este objetivo estratégico trata de uma área muito significativa e que desperta preocupação: a proteção das infraestruturas críticas. A questão é complicada, porque essas infraestruturas de informação não são exclusivamente de posse e gestão do Estado, mas também por atores privados (telecomunicações, eletricidade, etc). A Estratégia reconhece a necessidade de realizar "ações de cooperação" com a academia e o setor privado, em conjunto com a implementação de medidas de investimentos adequadas para garantir a segurança das infraestruturas públicas.

ARTIGO 19 observa, porém, que este objetivo é formulado em termos muito vagos, e que não é feita qualquer referência específica aos mecanismos das políticas, como a discussão e participação pública que será adotada ou direitos humanos. Questões de responsabilização e transparência não são nem mesmo mencionados. Além disso, a eventual imposição de deveres específicos para atores privados é uma questão muito sensível: de um lado, pode-se prejudicar o investimento; por outro lado, este processo pode delegar para mãos de entes privados poderes importantes, que podem interferir diretamente nos direitos e nas atividades dos cidadãos.

Recomendação:

- A Estratégia precisa ser mais específica em relação a ações que serão tomadas em relação à proteção das infraestruturas críticas, sobretudo sobre o envolvimento de diferentes atores, ao direito dos cidadãos de acesso à informações sobre estas questões, bem como o estabelecimento de garantias adequadas para a proteção adequada dos direitos humanos. Também precisam ser estabelecidas diretrizes claras sobre como se dará a cooperação entre as instituições públicas e os agentes privados nesta área.

Promoção de mecanismos para aumentar a conscientização dos cidadãos com relação à SIC e à SegCiber

ARTIGO 19 considera que a sensibilização dos cidadãos é, sem dúvida, uma poderosa forma de melhorar a cibersegurança, reduzir os riscos e aumentar a eficácia das medidas adotadas pelas autoridades públicas. No entanto, observamos também que esta política deve, em primeiro lugar, basear-se na divulgação de informações completas e facilmente compreensíveis e, em segundo lugar, fazer referência às diferentes perspectivas e considerações que estão envolvidas na noção de cibersegurança. Esta segunda preocupação é mencionada de maneira bastante vaga no documento, em relação à prevenção de crimes cibernéticos e à proteção da privacidade.

Recomendação:

- A implementação efetiva deste objetivo estratégico, que consiste em promover a conscientização dos cidadãos sobre a SIC e a SegCiber, requer o estabelecimento de mecanismos para a divulgação de informações completas entre os cidadãos, a informação que inclui referências ao efetivo exercício e à proteção dos direitos humanos.

Sobre a ARTIGO 19

A ARTIGO 19 advoga em prol do desenvolvimento de padrões progressistas de liberdade de expressão e liberdade de informação em nível internacional e regional, além da implementação destes nos sistemas legais domésticos. O *Law Programme* produziu uma série de publicações de definição de padrões que para traçam um perfil do direito internacional e do direito comparado, além das boas práticas em áreas como a leis de difamação, acesso à informação e regulamentação de radiodifusão.

Com base nestas publicações e a expertise jurídica geral da ARTIGO 19, a organização publica uma série de análises jurídicas a cada ano, além de comentários sobre propostas legislativas e leis existentes que afetam o direito à liberdade de expressão. Este trabalho de análise, realizado desde 1998 como forma de apoiar os esforços positivos de reforma legislativa em todo o mundo, frequentemente leva a melhorias substanciais nas legislação nacionais propostas ou existentes. Todas as nossas análises estão disponíveis em http://www.article19.org/resources.php/legal.

Caso você queira discutir esta análise de maneira mais aprofundada, ou caso você tenha uma questão que gostaria direcionar ao *Law Programme* da ARTIGO 19, você pode nos contactar por e-mail em legal@article19.org. Para obter mais informações sobre o trabalho da ARTIGO 19 no Brasil, entre em contato com Paula Martins, Diretora da ARTIGO 19 Brasil e América do Sul, em paula@article19.org.