NOTA TÉCNICA

Aos Deputados integrantes da
Comissão Parlamentar de Inquérito de Crimes Cibernéticos - CPICIBER

Senhores/as Deputados/as,

Este documento visa oferecer insumos à CPICIBER, tendo em conta o desafio de viabilizar o **combate aos cibercrimes** de maneira equilibrada com a **proteção de direitos fundamentais**.

É com preocupação que as organizações da sociedade civil que assinam este documento recebem o relatório final desta CPI. Acreditamos como importante **evitar que, sob a égide da segurança, o próprio Estado incorra em violações sistemáticas de direitos fundamentais** de milhões de indivíduos que usam tecnologias da informação e comunicação (TICs) para práticas cotidianas e essenciais ao exercício da democracia. Para tal, viemos por meio desta prover **informações técnicas** tanto sobre o funcionamento da rede, bem como **ressaltar de direito e deveres** já estabelecidos no que diz respeito aos usos da Internet no Brasil, para que se reavaliem algumas proposições do relatório final.

O combate ao cibercrime, cometido via ou com a ajuda de TICs, deve acatar aos limites legais estabelecidos na Constituição Federal, bem como em outras normas específicas, especialmente o Marco Civil da Internet, lei aprovada no Congresso Nacional em 2014, que, entre outros direitos, prevê garantias como **a liberdade de expressão, o sigilo de comunicações, presunção de inocência, privacidade e proteção de dados pessoais** no âmbito da Internet. Ressalta-se que o **Marco Civil da Internet é produto de um longo processo de consultas públicas e diálogo** entre os diversos setores interessados, portanto, produto de um consenso sedimentado depois de longo diálogo.

Neste sentido, **consideramos precipitadas sugestões de alterações deste texto de lei,** ainda mais quando se altera todo o balanço que se obteve após anos de negociação, **principalmente no que diz respeito à responsabilidade de intermediários por conteúdo de terceiros, neutralidade de rede e proteção da privacidade,** com todas as salvaguardas estabelecidas por termos estabelecido um regime de guarda obrigatória de registros.

1. Manutenção da neutralidade da rede, liberdade de expressão e do regime de responsabilidade limitada de Intermediários já previstos no Marco Civil

Acreditamos que a **neutralidade de rede deve ser garantida, sem exceções**, a não ser aquelas previstas no próprio Marco Civil da Internet e em sua vindoura regulamentação[1]. **Legitimar o bloqueio de aplicações no nível dos provedores de conexão** obriga tais provedores a manter **listas negras** de endereços IP, atualizadas e fiscalizadas pelas autoridades competentes, a semelhança do que ocorre com a muralha virtual da China, para assim impedir pacotes de chegar até tais endereços. Trata-se, mais uma vez, de clara **contradição ao Marco Civil da Internet**, que estabelece em seu art. 9º que "o responsável pela transmissão, comutação ou roteamento tem o dever de **tratar de forma isonômica quaisquer pacotes de dados**, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação".

Também vemos com preocupação surgirem **propostas de procedimentos específicos para a remoção de determinados tipos de conteúdo**. Lembramos que encumbir provedores e serviços de **monitorar e remover cópias de um conteúdo** de suas plataformas através de similaridade e não de links ou URL's específicos pode ser **tecnicamente custoso e desafiador**, devendo qualquer ordem judicial nesse sentido **determinar conteúdos específicos**, sendo que a aplicação em si não deveria ser alvo de bloqueios, sob pena de restringir o acesso a conteúdo e a liberdade de expressão.

No que tange o balanço hoje estabelecido para a proteção de dados dos usuários da rede, para qualquer proposta normativa que vise combater cibercrimes as previsões de **retenção e acesso a esses dados**, inclusive metadados, devem ser **excepcionais e mínimas**, devendo respeitar o princípio da presunção de inocência, pois, caso contrário, prejudica-se a privacidade das comunicações e constrange-se o exercício da **liberdade de expressão e associação**; além de se criar um alto custo de operação e segurança de centros de dados e ampliar o **risco de acesso não autorizado e de vazamentos**, trazendo, assim, mais insegurança.

Nesse contexto, o **Marco Civil da Internet já definiu o que são dados cadastrais** no contexto da provisão de serviços da rede e **já estabeleceu que número de IP não se inclui nesta definição, mas sim na definição de registros de conexão e aplicações**, que tem regimes próprios para guarda e acesso. Novamente, desconsiderar todos os anos de debate multissetorial que se teve para chegar a este regime seria uma afronta ao processo democrático do Marco Civil.

Entendemos que alterações não deveriam vir para mudar completamente a essência do que se tem hoje acordado, mas sim para melhorar sua aplicação. Nesse sentido, **parâmetros protetivos e de transparência**, presentes na Lei de Interceptação Telefônica, na Lei Geral de Telecomunicações e no Marco Civil da Internet, poderiam ser

1 Art. 4º do Decreto que passou por consulta pública: "a discriminação ou degradação de tráfego somente poderá decorrer de requisitos técnicos indispensáveis à prestação adequada de serviços e aplicações ou da priorização de serviços de emergência, sendo necessário o cumprimento de todos os requisitos dispostos no art. 9º, §2º da Lei nº 12.965, de 2014".

aprimorados para **assegurar a proteção de direitos e a integralidade dos sistemas de tecnologias de informação e comunicação**, de modo que seja sempre possível a supervisão e revisão judicial das atividades da Polícia e do Ministério Público, e até mesmo do próprio Poder Judiciário.

2. Não criminalização de tecnologias de segurança e anonimato como medida de segurança

Além do respeito ao ambiente jurídico de proteção de direitos na rede, entende-se que o reconhecimento da **legitimidade de tecnologias de proteção e segurança**, como a **criptografia**, são necessários para assegurar a confidencialidade, autenticidade e integridade nas comunicações realizadas entre pessoas e empresas, ou mesmo no âmbito do Poder Público. A **criminalização** e a imposição de quaisquer **fraquezas de chaves e algoritmos**, mesmo para combater ilícitos, abririam **portas dos fundos para criminosos e nações mal intencionadas** poderem atacar justamente aqueles inocentes que o Estado pretende defender dos cibercrimes.

Outro ponto crucial é, sem afronta à vedação constitucional, **não confundir o anonimato, por si só, com a efetiva prática de um crime**. Cabe lembrar que a **proteção da identidade é prevista em lei,** sendo a **base para viabilizar denúncias anônimas**, o sigilo de **fonte jornalística**, e outras manifestações do pensamento em contextos em que a transmissão de informação pode prejudicar a integridade física do interlocutor.

Sugere-se expressamente o entendimento e consideração de que o **anonimato também pode ser utilizado como via de exercício do direito de acesso à informação**, virtual ou presencial, sem ser identificado ou enquadrado em determinado perfil que possa ser alvo de discriminações. Igualmente, faz-se necessária a discussão sobre como práticas para **proteger a identidade** também podem servir como **mecanismo de segurança** ao debater opiniões de dissenso em ambiente seguro, contra eventuais ataques arbitrários e ilegais, como no caso de questões **pertinentes a diversos tipos de minorias** que são alvos destes ataques, inclusive em ambientes tão democráticos quanto o Brasil.

A conhecida **tecnologia Tor** viabiliza uma rede que funciona impedindo que tanto o provedor de conexão quanto o servidor de aplicações online possam ligar os pacotes de dados ao endereço IP de quem os acessou. Além de servir de ferramenta de evasão da censura, viabilizando o acesso a sites bloqueados em países mais autoritários (por exemplo, o uso de redes sociais na China e na Turquia), essa ferramenta também é usada por veículos da grande imprensa (*Washington Post, Guardian, New Yorker, Forbes*) e por ONGs, como **instrumento essencial para operar em pautas que vão desde o combate do contrabando de animais até denúncias de corrupção**. No interesse do Poder Público, muitos países se valem do Tor inclusive em **investigações policiais**.

Portanto, devem ser **incentivadas técnicas de investigação que não se oponham à natureza descentralizada desta rede**, pois qualquer quebra, invasão ou censura particular comprometeriam sua totalidade da mesma. Não se podem confundir tecnologias com eventuais **condutas ilícitas adotadas mediante o seu uso**.

Neste mesmo contexto, vemos com preocupação a criação e a ampliação de **mecanismos de identificação de acesso** à Internet e à telefonia móvel. Nas palavras do Relator para a Promoção e Proteção do Direito à Liberdade de Expressão e Opinião da ONU, obrigações como a de **vincular identificações à cartões SIM** "podem providenciar a Governos a **capacidade de monitorar indivíduos e jornalistas além de qualquer interesse legítimo**", e "a possibilidade de um Estado **obrigar provedores de conexão e aplicação a coletar e armazenar registros** documentando as atividades *online* de todos os seus usuários inevitavelmente resultou em um **Estado que possui os rastros digitais de todas as pessoas**".

3. Perigos da aplicação de um conceito vago de segurança cibernética

Também é importante ver criticamente o **conceito de "segurança cibernética"**, cujo significado, **carente de padrão ou consenso internacional**, pode abranger distintos problemas e inconvenientes, bem como ensejar falsas soluções técnicas e legislativas deletérias que envolvem desde monitoramento excessivo até censura e perseguição.

Sugere-se considerar práticas específicas ao invés de se adotar um termo tão abrangente que se esvai em si. Considerações mais específicas também tendem a levar ao entendimento de que parte de condutas que aparentam ser distintas apenas por ocorrerem no meio virtual, na realidade, já tem respaldo na legislação em vigor. Conceitos amplos podem levar até mesmo à criminalização de condutas cotidianas de usuários comuns, como é o caso da proposta de projeto de lei que trata de invasões de sistemas e que pode vir a criminalizar condutas comuns e correntes que simplesmente vão contra os termos de usos de plataformas. Termos de usos que, por sua vez, muitas vezes nem são coerentes com a legislação nacional.

4. Importância de um debate multissetorial para tratar de crimes cibernéticos

Por fim, uma estratégia nacional ou pactos multilaterais internacionais sobre o tema devem priorizar **processos de deliberação de que participem tanto governos quanto empresas, sociedade civil, academia e outros segmentos sociais**. **Caso contrário,** o debate foca-se apenas em crime e terrorismo cibernéticos, por uma **perspectiva precipitada e estritamente penal e militar da discussão de segurança pública, em detrimento de outros direitos**.

Destaca-se que, a exemplo do Comitê Gestor da Internet, das consultas públicas do Marco Civil até à realização do evento diplomático internacional NetMundial, o Brasil tem sido pioneiro no incentivo a uma **estratégia de discussão multissetorial** dos temas que dizem respeito aos direitos e deveres no uso da Internet. Tal pioneirismo deve se expandir também para promover uma discussão balanceada sobre cibercrimes e cibersegurança, bem como uma clara definição específica de seus significados.

Considerações Finais

Para maiores informações sobre cada um dos conceitos e argumentos ora apresentados, formulou-se uma **Nota Técnica, detalhada e ilustrada**, disponível integralmente no endereço http://cpiciber.codingrights.org. A nota traz discussões de conceitos chave para o desenvolvimento dos debates na CPICIBER, sob a ótica da análise jurídica e do funcionamento das tecnologias em questão.

Ademais, seguimos à disposição para quaisquer futuras eventualidades no encerramento dos trabalhos desta Comissão, bem como no debate de propostas normativas relacionadas.

Brasília, 4 de abril de 2016.

Lucas Teixeira, Diretor Técnico e
Joana Varon, Diretora Geral
Coding Rights
joana@codingrights.org (21) 98689-1313
lucas@codingrights.org (21) 99968-5003

Paulo Rená da Silva Santarém, chefe executivo de pesquisa
IBIDEM - Instituto Beta para Internet e Democracia
paulo@ibidem.org.br (61) 8334-3055

Subscrevem esta nota técnica:

Arpub – Associação Brasileira de Rádios Públicas / Associação Nacional de Pos-graduação e Pesquisa em Educação – ANPEd / Associação Software Livre.Org / Casa da Cultura Digital Porto Alegre / Centro de Estudos da Mídia Alternativa Barão de Itararé / Centro de Produção, Promoção e Formação em Arte e Cultura/ArtEstação / Centro de Tecnologia e Sociedade da FGV do Rio de Janeiro / Ciranda Internacional da Comunicação Compartilhada / Coding Rights / Coletivo Digital / FNDC – Fórum Nacional pela Democratização da Comunicação / Geledes - Instituto da Mulher Negra / IDEC – Instituto Brasileiro de Defesa do Consumidor / Instituto Bem Estar Brasil / Instituto Brasileiro de Políticas Digitais – Mutirão / Internet Sem Fronteiras – Brasil / Intervozes – Coletivo Brasil de Comunicação Social / Movimento Mega / Projeto Saúde & Alegria, Santarém, Pará / PROTESTE - Associação de Consumidores / #RedeLivre / SBPC – Sociedade Brasileira para o Progresso da Ciência / ULEPICC-Br – União Latina de Economia Política da Informação, da Comunicação e da Cultura - Capítulo Brasil