Apresentação de NOTA TÉCNICA

das Organizações da Sociedade Civil

ao Deputado Relator da Comissão Parlamentar de Inquérito de Crimes Cibernético - CPICIBER.

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**. Espera-se alcançar tal objetivo tanto por meio do provimento de **informações técnicas** sobre o funcionamento da rede, como pela **afirmação de direito e deveres** estabelecidos no que diz respeito aos usos da Internet no Brasil.

Procura-se **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.

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 **sigilo de comunicações, presunção de inocência, privacidade e proteção de dados pessoais** no âmbito da Internet.

Observados os princípios jurídicos vigentes, para qualquer proposta normativa que vise combater cibercrimes, as previsões de **retenção e acesso a dados** dos usuários da rede, inclusive metadados, devem ser **excepcionais e mínimas**, pois mitigam a privacidade das comunicações e constrangem o exercício das **liberdades de expressão e associação**; criam alto custo de operação e segurança de centros de dados; além de ampliarem o **risco de acesso não autorizado e de vazamentos**, trazendo, assim, mais insegurança.

Nesse contexto, os **parâmetros protetivos e de transparência**, presentes na Lei de Interceptação Telefônica, na Lei Geral de Telecomunicações e no Marco Civil da Internet, precisam ser 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.

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 qualquer **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 facilmente 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 circunvenção 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**.

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 à 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.

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 focam-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.

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 no debate de propostas normativas relacionadas.

Brasília, 30 de março de 2016.

Lucas Teixeira, Diretor Técnico e
Joana Varon, Diretora Geral
Coding Rights
joana@codingrights.org (21) 986891313
lucas@codingrights.org (21) 999685003

Paulo Renâ da Silva Santarém, chefe executivo de pesquisa
IBIDEM - Instituto Beta para Internet e Democracia
paulo@ibidem.org.br (61) 83343055

Apoio:
Bia Barbosa
Coletivo Intervozes
bia@intervozes.org.br (61) 99514846