COALIZÃO DIREITOS NA REDE

contato@direitosnarede.org.br
DIREITOSNAREDE.ORG.BR

Brasília, 24 de fevereiro de 2023

A Sua Excelência
Ministro de Estado de Justiça e Segurança Pública
Senhor Flávio Dino

Aos cuidados do Ministério da Justiça e Segurança Pública

Assunto: Propostas da Coalizão Direitos na Rede (CDR) para áreas de justiça e segurança pública do Governo Federal

Estimado Senhor Flávio Dino,

A Coalizão Direitos na Rede (CDR) é uma rede de entidades que reúne 52 organizações acadêmicas e da sociedade civil em defesa dos direitos digitais. As entidades que integram o coletivo participaram ativamente da construção de políticas públicas de Internet de grande relevância para o Brasil, como o processo de discussão e elaboração do Marco Civil da Internet e de seu decreto regulamentador, bem como a Lei Geral de Proteção de Dados Pessoais.

O Grupo de Trabalho em Privacidade e Vigilância (GTPV) da CDR advoga para que ninguém esteja sujeito à vigilância (estatal ou privada), à interceptação de comunicações ou coleta arbitrária e ilegal de dados pessoais, nem mesmo para fins de segurança nacional. As diversas organizações que compõem o GTPV possuem substrato teórico e prático que baseiam as propostas apresentadas. Este documento tem como objetivo contribuir para o diagnóstico e oferecer recomendações aos problemas a serem enfrentados no que se refere à vigilância e ao controle sobre a população.

A CDR segue em defesa dos direitos digitais, tendo como temas principais de atuação a defesa do acesso à internet, soberania nacional, liberdade de expressão, proteção de dados pessoais e privacidade na Internet. Esperamos que o mandato

2023-2026 do Governo Federal seja desempenhado de forma transparente, diversa e democrática, com a participação da CDR e demais organizações da sociedade civil.

Atenciosamente,

Fabricio Solagna
Secretário Executivo
Coalizão Direitos na Rede

Contatos
E-mail: secretariaexecutiva@direitosnarede.org.br
Telefone: 51 99281-9425

Diagnóstico:

Nos últimos anos houve a ampliação da vigilância estatal no Brasil, o que viola os direitos fundamentais à privacidade e à proteção de dados dos cidadãos. Sob a justificativa de combate à criminalidade, os órgãos estatais (i) criaram aparatos institucionais sem o devido controle social, (ii) adquiriram aparatos tecnológicos de vigilância e (iii) fragilizaram o aparato normativo em matéria de privacidade. Ocorre que essas ferramentas são frequentemente utilizadas para fins ilegítimos, com forte viés racista, sexista, classista e para reprimir e vigiar opiniões críticas ou dissidentes de jornalistas, adversários políticos e ativistas sociais.

Por aparato institucional de vigilância nos referimos a órgãos subordinados principalmente à Presidência da República, ao Ministério da Justiça e às Secretarias Estaduais de Segurança Pública que têm como função desenvolver atividades investigação e/ou de inteligência e promover o intercâmbio de dados. Esses órgãos têm pouco ou nenhum controle social e mantêm suas atividades e estruturas opacas. Além disso, esse aparato é constituído por uma multiplicidade de atores, como agentes de inteligência, de investigação, forças armadas, agências reguladoras e etc., com atividades e funções que extrapolam seus respectivos âmbitos de atuação.

Já por aparato tecnológico, nos referimos a ferramentas utilizadas para ampliar a capacidade do poder público de vigilância e de controle sobre a população. Essas ferramentas se utilizam, por exemplo, da quebra de criptografia, do reconhecimento facial massivo e indiscriminado, do acesso a conteúdos de dispositivos móveis e do levantamento de informações públicas para "catalogar" pessoas. Exemplo notório do uso de tecnologias de vigilância em violação às garantias e direitos fundamentais é o escândalo do Dossiê Antifacista elaborado pela então Secretaria de Operações Integradas (SEOPI) do Ministério da Justiça para catalogar e mapear servidores federais e estaduais de segurança pública ditos "antifascistas".

Por aparato normativo nos referimos às leis esparsas aplicáveis à proteção de dados na área penal, mas que não são devidamente adequadas à transformação digital ocorrida nas últimas décadas, constituindo verdadeiro cenário de vácuo legislativo sobre o tema no Brasil. Por isso, ao não haver regulação, o uso do aparato tecnológico acima mencionado pelo poder público fere o princípio básico da legalidade ao não haver autorização legal expressa apta a subsidiar a atividade do Estado.

Portanto, a partir do cenário acima descrito, as propostas elencadas a seguir se distinguem em 3 dimensões. É preciso (i) reformar o aparato institucional existente criado para a vigilância massiva dos cidadãos, (ii) desmobilizar a aquisição

e o uso do aparato de vigilância e (iii) aprimorar o arcabouço normativo sobre o tema.

Propostas:

1. **Reforma aparato institucional de vigilância existente**

1.1. **Revisar o Decreto nº 8.793, de 29 de junho de 2016,** que fixa a Política Nacional de Inteligência.

Justificativa: A Política Nacional de Inteligência teria como função definir parâmetros e limites para a atuação dos órgãos que realizam inteligência, mas não o faz. O decreto se limita a definir a competência do Gabinete de Segurança Institucional para coordenar as atividades de inteligência no âmbito da administração pública federal (art. 2º). Além disso, o decreto menciona um amplo campo de atuação para as atividades de inteligência, incluindo atividades denominadas como "contrárias ao Estado Democrático de Direito". Ocorre que nos últimos anos houve uma ampliação do aparato estatal de inteligência decorrente da crescente transformação digital e da realização de eventos internacionais no Brasil, como a Copa das Confederações, a Copa do Mundo e as Olimpíadas. Essa ampliação não foi acompanhada de um devido estabelecimento de normas e procedimentos de controle e de fiscalização, além de não prever limitações expressas para as atividades de inteligência no Brasil. O mesmo aparato que em governos democráticos pode ser utilizado para fins legítimos foi facilmente cooptado por esforços e práticas autoritárias dos últimos governos para a perseguição política de detratores.

Proposta: Revisar a Política Nacional de Inteligência de forma a limitar o âmbito de atuação dos órgãos de inteligência e criar mecanismos de controle, fiscalização e transparência.

1.2. **Prover transparência e controle social à área de inteligência e operações integradas**

Justificativa: O aparato institucional revestido de poderes nas áreas de inteligência e operações integradas, a Secretaria de Operações Integradas do Ministério da Justiça (SEOPI) no governo Bolsonaro, hoje Diretoria de Operações Integradas e de

Inteligência, serviu como centro para a execução das atividades de vigilância antidemocrática e irregular nos últimos 4 anos de governo Bolsonaro. Em 24 de julho de 2020, por exemplo, foi revelado que a Secretaria colocou em prática uma ação sigilosa que monitorou 579 servidores públicos federais que seriam, supostamente, antifascistas e opositores do governo Jair Messias Bolsonaro, incluindo professores e policiais. Nesse período, a SEOPI adquiriu robusto aparato tecnológico e se engajou em atividades ilegais de vigilância com as secretarias estaduais de segurança pública. Por isso, é importante que sejam criados mecanismos que garantam a transparência e controle social das atividades, estruturas e recursos da Diretoria de Operações Integradas e de Inteligência.

Proposta: criar mecanismos que garantam a transparência e controle social das atividades, estruturas e recursos da Diretoria de Operações Integradas e de Inteligência.

1.3. **Revogar a Portaria nº 26, de 9 de julho de 2020**, que aprova o Protocolo do Projeto Excel, que visa estabelecer os critérios para adesão e utilização de ferramentas de extração e análise de dados de dispositivos móveis e compartilhamento dos dados obtidos sem os devidos controles.

Justificativa: Segundo informações do próprio sítio eletrônico do Ministério da Justiça e Segurança Pública, o Projeto Excel engloba o fornecimento de softwares forenses e hardwares para dar mais celeridade na extração e análise de celulares apreendidos de indivíduos envolvidos com o crime organizado. Trata-se de equipamento que quebra de sigilo telemático no âmbito de inquéritos policiais. A Portaria prevê ainda a criação de uma base de dados constituída por dados extraídos por ferramenta própria e compartilhados com a Diretoria de Inteligência da então SEOPI (art. 2º). As soluções adquiridas no Projeto Excel possibilitam a extração de dados dos aparelhos, cruzamento desses dados e análise de informações na nuvem. A portaria não se limita à previsão do uso do aparato institucional para o combate às organizações criminosas (art. 2º, §2º, inc. I), como também prevê de forma vaga o uso das ferramentas para "hipóteses excepcionais" (art. 2º, §2º, inc. I). É preocupante que o mesmo equipamento e a base de dados que são utilizados para combater o crime organizado possam ter seu uso desvirtuado e utilizado para espionar adversários políticos do governo, como já ocorreu em diversos outros países, inclusive naqueles considerados "desenvolvidos" e democráticos.

2. Desmobilizar e descontinuar o uso do aparato tecnológico existente

Justificativa: O aparato institucional acima mencionado se utiliza de ferramentas tecnológicas capazes, por exemplo, de quebra de criptografia, de reconhecimento facial massivo e indiscriminado, de acesso a conteúdos de dispositivos móveis e do levantamento de informações públicas para "catalogar" pessoas. São centenas de contratos que visam adquirir as mais variadas ferramentas de vigilância[1]. Dentre as soluções utilizadas, menciona-se (i) as câmeras de reconhecimento facial utilizadas para o tratamento massivo de dados biométricos faciais[2]; (ii) a solução tecnológica da empresa israelense Cellebrite, que possibilita o acesso a todas as fotos, vídeos, mensagens, registros de localização e Wi-Fi, dados e metadados apagados, informações de mais de 1.000 aplicativos, conteúdos na nuvem, acesso a aparelhos e aplicativos bloqueados e quebra de senhas[3]; (iii) os produtos oferecidos pela empresa Harpia Tech, que utiliza-se Inteligência de Fontes Abertas é capaz de detectar, analisar e produzir relatórios que detalham vínculos entre pessoas, quais as mídias utilizadas por um indivíduo a partir de informações públicas[4]; e (iv) o Córtex, uma tecnologia de inteligência artificial que usa a leitura de placas de veículos por milhares de câmeras viárias espalhadas por rodovias, pontes, túneis, ruas e avenidas país afora para rastrear alvos móveis em tempo real[5]. Não existe propósito legítimo que justifique o emprego de ferramentas de hacking e tratamento de biometria facial na segurança pública por autoridades públicas. Para que tais ferramentas possam ser utilizadas, é necessário que falhas de segurança em dispositivos e provedores tenham sido identificadas e não sejam corrigidas. Ou seja, investir em tal aparato tecnológico significa despender grande aporte de recursos públicos em um mercado baseado na identificação e na exploração de vulnerabilidades em sistemas de segurança. Os recursos despendidos pelas autoridades públicas brasileiras para a exploração de vulnerabilidades em sistemas de terceiros termina por beneficiar um mercado responsável pelo aproveitamento de vulnerabilidades nos próprios sistemas do governo brasiliero, que ameaçam a segurança e estabilidade do Estado, como no caso dos ataques hackers ao Superior Tribunal de Justiça e ao Ministério da Saúde. É inconcebível a existência de uma política de Estado que promova a vulnerabilização de sistema de terceiros ao invés de investir na correção das falhas

[1] https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf
[2] https://tiremeurostodasuamira.org.br/carta-aberta/
[3] https://theintercept.com/2022/03/21/ministerio-da-justica-equipa-policias-para-vasculhar-celulares-em-troca-de-dados/
[4] https://www.dataprivacybr.org/o-que-sabemos-sobre-a-harpia-tech/
[5] https://theintercept.com/2020/09/21/governo-vigilancia-cortex/

de segurança dos sistemas usados por instituições, agentes públicos e seus cidadãos. Essa prática fomenta uma indústria que aumenta a insegurança, além de municiar governos autoritários no Brasil e no mundo.

Proposta: Desmobilizar a aquisição e o uso de aparato tecnológico de vigilância, já que não há garantias legais, administrativas e procedimentais que assegurem limitações às atividades do poder público frente às garantias e direitos fundamentais dos cidadãos.

3. Fortalecer arcabouço normativo

3.1. Aprovar Lei Geral de Proteção de Dados Pessoais para o âmbito penal

Justificativa: Há um vácuo normativo na regulação da privacidade e da proteção de dados pessoais no âmbito da segurança pública, defesa nacional, segurança do Estado e atividades de investigação e repressão de infrações penais. A Lei Geral de Proteção excetua seu âmbito de aplicação para os fins acima elencados, mas define que futura legislação sobre o tema deve conter medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados os princípios gerais de proteção e os direitos do titular previstos na própria LGPD. Em 2020 foi elaborado um Anteprojeto de Lei por uma comissão de juristas da Câmara dos Deputados que buscou equilibrar a tutela dos direitos de titulares de dados pessoais, a eficácia na atuação das autoridades públicas e a inserção brasileira nas cadeias de cooperação jurídica internacional. No entanto, em setembro de 2022 foi protocolado o PL 1515/22, que replicou a estrutura geral do Anteprojeto, porém desmontou o arcabouço garantista nele proposto.[6]

Proposta: Propõe-se, portanto, a aplicação de esforços do Governo Federal para que seja formalmente proposto um projeto de lei, que possa ter sua redação discutida, aprimorada e aprovada como legislação específica para a proteção de dados pessoais no âmbito penal, nos moldes do Anteprojeto de Lei elaborado pela Comissão de Juristas.

3.2. Aprovar novo Código de Processo Penal que discipline as provas digitais

6 https://irisbh.com.br/publicacoes/analise-comparativa-entre-o-anteprojeto-de-lgpd-penal-e-o-pl-1515-2022/

Justificativa: É necessário que o arcabouço normativo processual penal no Brasil se adeque ao cenário de transformação digital que tem afetado as investigações criminais de forma a proteger os direitos e garantias fundamentais dos cidadãos. Ocorre que o anteprojeto que tramita no Congresso Nacional segue sentido contrário e incorre em 4 principais problemas. O texto (i) expande de forma desproporcional a retenção massiva, ilegítima e insegura de dados para futuras investigações; (ii) retrocede em garantias no âmbito de acesso a dados em investigações, como a exclusão da exigência de ordem judicial para o acesso a dados cadastrais; (iii) cria exigências aos provedores que podem requerer a introdução de vulnerabilidades e redução da segurança em seus sistemas e serviços; e (iv) legitima a exploração de vulnerabilidades em sistemas realizado por agentes estatais.

Proposta: Propõe-se, a aplicação de esforços do Governo Federal eleito para que uma futura legislação no âmbito processual penal seja aprovada sob a égide dos princípios da legalidade, da proporcionalidade, do devido processo legal e do devido processo informacional.

3.3. Reforma da Lei de Organizações Criminosas para a transparência na aquisição de aparato tecnológico

Justificativa: A Lei nº 13.097/2015 alterou a Lei de Organização Criminosas, Lei nº 12.850/2013, para prever a possibilidade de dispensa de licitação para contratação de serviços técnicos especializados, aquisição ou locação de equipamentos destinados à polícia judiciária para o rastreamento e obtenção de provas. No entanto, tal dispositivo tem justificado a contratação e utilização de aparato tecnológico sem a devida transparência. Muitas das tecnologias adquiridas são utilizadas por autocracias ao redor do mundo para a vigilância massiva dos cidadãos e opositores. Portanto, é premente que seja alterado o regime de contratação de tecnologia na segurança pública e persecução penal para dar mais transparência à capacidade de vigilância do Estado.

Proposta: Propõe-se, a aplicação de esforços do Governo Federal eleito para que seja modificado o regime de contratação e utilização de tecnologias de vigilância na segurança pública e persecução penal, com especial atenção ao dispositivo da Lei de Organizações criminosas que possibilita a contratação de serviços sem a devida publicidade.

Entidades que integram a Coalizão Direitos na Rede

1. Ação Educativa – Assessoria, Pesquisa e Informação
2. Actantes
3. Amarc Brasil – Associação Mundial de Rádios Comunitárias
4. ANPED – Associação Nacional de Pós-Graduação e Pesquisa em Educação
5. AqualtuneLab – Cruzando o Atlântico
6. Artigo 19
7. ASL – Associação Software Livre
8. Associação Brasileira de Pesquisadores e Profissionais em Educomunicação – ABPEducom
9. Associação Data Privacy Brasil de Pesquisa
10. Casa da Cultura Digital de Porto Alegre
11. Casa Hacker
12. Centro de Estudos da Mídia Alternativa Barão de Itararé
13. Centro de Pesquisa em Comunicação e Trabalho – CPCT-ECA/USP
14. Ciranda da Comunicação Compartilhada
15. Coding Rights
16. Colaboratório de Desenvolvimento e Participação-COLAB-USP
17. Coletivo Digital
18. Coolab – Laboratório Cooperativista de Tecnologias Comunitárias
19. Creative Commons Brasil
20. data_labe
21. Diracom - Direito à Comunicação e Democracia
22. Fórum Nacional pela Democratização da Comunicação – FNDC
23. Garoa Hacker Clube
24. Grupo de Pesquisa em Políticas Públicas para o Acesso a Informação/GPoPAI da USP
25. Idec-Instituto Brasileiro de Defesa do Consumidor
26. Instituto Aaron Swartz
27. Instituto Bem-Estar Brasil
28. Instituto Beta: Internet & Democracia
29. Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec
30. Instituto Educadigital
31. Instituto Igarapé
32. Instituto de Referência em Internet e Sociedade – IRIS
33. Instituto Nupef

34. Instituto Observatório do Direito Autoral – IODA
35. Instituto SIGILO
36. Instituto Telecom
37. Instituto Vero
38. Internet Sem Fronteiras Brasil
39. InternetLab – Centro de pesquisa em direito e tecnologia
40. Intervozes-Coletivo Brasil de Comunicação Social
41. ITS-Rio-Instituto de Tecnologia e Sociedade do Rio de Janeiro
42. LAPCOM – UnB – Laboratório de Políticas de Comunicação da UnB
43. LAPIN – Laboratório de Pesquisa em Políticas Públicas e Internet
44. LAVITS-Rede latina-americana de estudos sobre vigilância, tecnologia e Sociedade
45. Me Representa
46. Movimento Mega
47. NUREP – Núcleo de Pesquisas em Direitos Fundamentais, Relações Privadas e Políticas Públicas
48. O Panóptico – CESeC
49. Observatório da Ética Jornalística – objETHOS
50. Open Knowledge Brasil
51. Instituto Alana
52. Projeto Saúde e Alegria
53. PROTESTE-Associação de Consumidores
54. Transparência Brasil
55. Wiki Movimento Brasil