Instituto de Pesquisa em Direito & Tecnologia do Recife

Internet Society
Capítulo Brasil

Hacking governamental e criptografia no Brasil: oposições em redes e narrativas

Hacking governamental e criptografia no Brasil: oposições em redes e narrativas.
Agosto de 2025.

Instituto de Pesquisa em Direito e Tecnologia do Recife – IP.rec

Internet Society Capítulo Brasil – ISOC Brasil

Este estudo faz parte do projeto Criptografia e Direitos Digitais no Brasil: Capacitação, Diálogo e Incidência Política, iniciativa apoiada pela ISOC Foundation por meio do programa Beyond the Net.

Pesquisa e redação

Mariana Canto

Pedro Silva Neto

Thobias Prado Moura

Coordenação e revisão

Raquel Saraiva

Projeto gráfico

Estúdio Puya

Sumário Executivo

Sumário Executivo

Este estudo teve como objetivo investigar o ecossistema do hacking governamental no Brasil, combinando análise de redes sociais (ARS) com entrevistas realizadas com representantes do governo, setor privado, mídia, academia, comunidade técnica e sociedade civil. A pesquisa buscou identificar os fluxos de poder, a centralidade de atores, os vínculos de colaboração ou conflito e as percepções sobre os riscos e as salvaguardas relacionados ao uso estatal de ferramentas de intrusão digital.

A análise das redes revela um cenário de escassos espaços de diálogo multissetorial. Existe um ecossistema fortemente centralizado em instituições governamentais, especialmente aquelas ligadas à segurança, justiça e inteligência, no qual o setor privado aparece como parceiro técnico relevante, mas internamente dividido entre empresas que fornecem soluções de segurança e plataformas preocupadas com privacidade. Em contraste, a sociedade civil, a mídia e a comunidade técnica e academia possuem menor centralidade, sendo frequentemente excluídas das instâncias centrais de decisão, embora desempenhem papéis essenciais na fiscalização e na produção de conhecimento.

As entrevistas evidenciam um consenso dos atores entrevistados sobre a opacidade institucional e a assimetria informacional que caracterizam a aquisição e o uso de tecnologias de intrusão, especialmente nos níveis subnacionais. A ausência de métricas públicas, a fragmentação regulatória e a prática recorrente de intermediação por empresas que ocultam a origem das tecnologias dificultam a supervisão e favorecem práticas abusivas. A combinação entre baixa transparência, terceirizações mal reguladas e frágil cultura de proteção de dados coloca em risco o direito à privacidade e às liberdades fundamentais, como a liberdade de expressão, de imprensa e de reunião.

Diante desses desafios, esse estudo propõe sete eixos de ação: (1) institucionalizar mecanismos permanentes e vinculantes de governança intersetorial; (2) aprovar um pacote legislativo robusto voltado à proteção de dados e à soberania digital, incluindo uma Lei Geral de Proteção de Dados penal; (3) combater a opacidade nas contratações públicas, com rastreabilidade total e proibição de

empresas laranja e violadoras de direitos humanos; (4) desenvolver métricas auditáveis sobre o uso e os impactos das tecnologias de intrusão; (5) fortalecer controles *ex-ante* e *ex-post*, com autorizações específicas e supervisão independente; (6) consolidar a segurança cibernética como um direito democrático, com defesa da criptografia forte e educação digital; e (7) fomentar a produção científica aplicada e parcerias com centros de pesquisa para orientar políticas públicas e decisões judiciais com base em evidências.

Essas recomendações buscam construir uma governança legítima, transparente e proporcional do uso estatal de tecnologias de intrusão, promovendo a proteção de direitos, a responsabilização pública e a autonomia tecnológica do país.

Definições e conceitos

Hacking governamental: Refere-se ao uso, por parte de órgãos estatais, de técnicas de intrusão digital com o objetivo de acessar, monitorar, interceptar ou manipular dados armazenados em dispositivos ou sistemas informáticos, geralmente no contexto de investigações criminais, inteligência ou segurança nacional. Essa prática pode envolver o uso de malwares, vulnerabilidades e outros métodos que permitem o controle remoto de dispositivos-alvo.

Ferramentas de intrusão digital: São softwares ou sistemas utilizados para acessar dispositivos, redes ou sistemas computacionais sem o conhecimento ou consentimento do usuário, com a finalidade de coleta de dados, vigilância, interceptação de comunicações ou manipulação de informações. Essas ferramentas podem ser empregadas por agentes públicos ou privados e variam em grau de sofisticação e potencial invasivo.

Hardening: Conjunto de práticas e técnicas voltadas ao reforço da segurança de sistemas, dispositivos ou aplicações, por meio da redução da superfície de ataque. Isso inclui a desativação de serviços desnecessários, aplicação de patches de segurança, configuração segura de sistemas operacionais, segmentação de privilégios e adoção de políticas de controle de acesso, com o objetivo de dificultar ações maliciosas ou intrusivas.

Criptografia forte: Refere-se à utilização de algoritmos criptográficos robustos e atualizados que garantem a confidencialidade, integridade e autenticidade das informações, mesmo diante de tentativas avançadas de quebra. Em contextos de segurança digital, a criptografia forte é aquela cuja implementação segue padrões reconhecidos internacionalmente, sem *backdoors* ou fragilidades conhecidas, e que resiste a ataques computacionais viáveis com os recursos tecnológicos disponíveis.

1. Introdução

O avanço de tecnologias utilizadas para práticas de hacking governamental tem gerado profundas implicações para a privacidade, os direitos humanos e a governança democrática. No Brasil, a crescente adoção de ferramentas de intrusão digital por parte de entes do setor público exige uma análise aprofundada sobre os atores envolvidos, os interesses em disputa e os caminhos regulatórios em construção.

Mapear as partes interessadas e os seus posicionamentos nesse debate é fundamental para compreender a dinâmica de poder e influência que molda as decisões políticas e legais sobre o uso de tecnologias invasivas. Identificar quem são os principais agentes (desde formuladores de políticas públicas e forças de segurança até representantes da sociedade civil e setor privado) e como se posicionam em relação ao hacking governamental permite revelar não apenas as tensões e alianças, mas também as lacunas de representação e participação no processo decisório.

Além disso, a compreensão dos cenários político e regulatório no Brasil é essencial para avaliar se a formulação de normas e práticas está alinhada com princípios democráticos e com uma abordagem baseada na preservação de direitos fundamentais. Considerando a natureza sensível e controversa das ferramentas de intrusão digital, garantir a transparência e o debate público sobre sua adoção é uma necessidade urgente.

O objetivo geral do relatório é compreender o grau de influência e poder de determinados atores (e setores) na regulação de hacking governamental no Brasil. Dessa forma, o estudo contribui para o fortalecimento do debate público informado, a promoção da prestação de contas institucional e o desenvolvimento de políticas públicas mais equilibradas, participativas e comprometidas com a proteção de direitos fundamentais.

2. Metodologia

A pesquisa adota uma abordagem qualitativa e exploratória, combinando métodos de mapeamento de partes interessadas, análise de redes sociais (ARS) e entrevistas semiestruturadas. A metodologia foi elaborada para permitir uma compreensão aprofundada do ecossistema em torno do hacking governamental e da criptografia no Brasil, considerando tanto aspectos estruturais quanto percepções subjetivas dos atores envolvidos.

A primeira etapa da pesquisa consistiu no mapeamento de partes interessadas. Essa etapa teve como objetivo identificar os principais atores envolvidos direta ou indiretamente na formulação, implementação ou contestação de políticas relacionadas ao hacking governamental e à criptografia. A identificação foi feita a partir de critérios específicos, tais como a atuação direta no tema (por exemplo, participação em audiências públicas, proposição legislativa ou decisões judiciais), poder de influência política ou institucional, produção de conhecimento técnico ou jurídico relevante, atuação em defesa de interesses públicos ou privados afetados por essas tecnologias e contribuição para a construção de narrativas públicas sobre o tema.

Com base no mapeamento realizado, a ARS foi executada com o objetivo de identificar quais atores ocupam posições centrais na rede, quais estão mais isolados e como se organizam possíveis coalizões ou alianças de posicionamento semelhantes. A análise permitiu a visualização das relações entre os atores e possibilitou uma maior compreensão da estrutura de poder e influência existente no campo regulatório. Além disso, também permitiu a identificação de lacunas de representação e dinâmicas de exclusão. A ferramenta de visualização utilizada foi o software de código aberto Gephi, que considera parâmetros como grau de centralidade, centralidade de intermediação, densidade da rede e identificação de comunidades. As conexões entre os atores foram traçadas com base em interações observáveis, tais como participação conjunta em eventos ou documentos públicos, colaborações institucionais e posicionamentos públicos convergentes.

Por fim, entrevistas semiestruturadas foram conduzidas com atores considerados partes interessadas e relevantes para o estudo. Foram selecionados representantes de diversos setores, incluindo mídia, sociedade civil, academia/comunidade técnica, setor privado e órgãos governamentais, com o intuito de captar uma diversidade de perspectivas, experiências e interesses em torno do tema. As entrevistas buscaram explorar percepções sobre os impactos do hacking governamental na sociedade, desafios regulatórios, estratégias de atuação e possíveis conflitos ou convergências entre os diferentes grupos de interesse. As entrevistas possibilitaram uma compreensão multifacetada do ecossistema, ao articular dimensões técnicas, políticas e sociais. Além disso, a metodologia adotada permitiu incorporar as vozes de atores frequentemente marginalizados nos processos formais de tomada de decisão.

3. Panorama do hacking governamental no Brasil

O ano de 2013 foi um divisor de águas nas políticas de cibersegurança no Brasil. Internamente, as Jornadas de Junho evidenciaram a força de mobilização digital em meio à insatisfação popular. Externamente, as revelações de Edward Snowden mostraram que a presidenta Dilma Rousseff fora alvo direto da NSA. A divulgação de Glenn Greenwald evidenciou que o Brasil estava entre os países mais monitorados, o que colocou a pauta da soberania digital no centro da agenda política[1]. Em agosto de 2013, o Congresso instaurou a CPI da Espionagem, que concluiu pela necessidade de investir em tecnologias nacionais, criptografia e profissionais especializados. Como ressaltam os autores do estudo *The construction of a sociotechnical surveillance network in Brazil*, a CPI resultou na criação de um amplo aparato estatal de vigilância da Internet[2].

Esse processo coincidiu com os “megaeventos” – a Copa do Mundo de futebol masculino de 2014 e as Olimpíadas de 2016 – que catalisaram investimentos em segurança. O Ministério da Justiça gastou cerca de 360 milhões de dólares em

[1] GREENWALD, Glenn. The NSA's mass and indiscriminate spying on Brazilians. The Guardian, [S.l.], 6 jul. 2013. Disponível em: https://www.theguardian.com/commentisfree/2013/jul/07/nsa-brazilians-globo-spying. Acesso em: 20 ago. 2025.

[2] BRAGA, Pedro et al. The construction of a sociotechnical surveillance network in Brazil. First Monday, [S.l.], v. 27, n. 8, 2022. DOI: 10.5210/fm.v27i8.12410. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/12410. Acesso em: 20 ago. 2025.

cinco anos com tecnologias de vigilância, incluindo centros de comando, drones e softwares importados[3]. Como o estudo de Pedro Braga et al. (2022) aponta, embora justificados como medidas antiterrorismo, esses instrumentos foram usados contra manifestantes, jornalistas e ativistas. Como observa Sérgio Amadeu, a lógica de segurança voltada a inimigos externos passou a ser empregada internamente, mirando movimentos sociais e defensores de direitos[4].

O período consolidou um modelo de governança cibernética fragmentado e securitário. O Gabinete de Segurança Institucional (GSI) já coordenava a política de segurança da informação, supervisionando o CTIR Gov, enquanto o Exército estruturava o ComDCiber e a Polícia Federal criava delegacias próprias de crimes digitais. O resultado foi sobreposição de agendas e disputas interinstitucionais. Para Louise Marie Hurel (2022), essa governança é “fragmentada e paradoxal”, marcada pela militarização[5]. Segundo a pesquisadora, o GSI mantém uma forte herança institucional militarizada. Para ela, essa verticalização resultou em pouca transparência e baixa integração da sociedade civil e de outros setores.

Apesar do Marco Civil da Internet (2014) e da Lei Geral de Proteção de Dados (2018), a proteção de dados em investigações criminais permanece em limbo. A LGPD exclui explicitamente esse campo, e a proposta de uma “LGPD penal” nunca avançou. Nesse vácuo, órgãos de segurança recorrem a técnicas de intrusão digital sem parâmetros claros. Em 2015, o WikiLeaks mostrou que a Polícia Federal negociava com a empresa italiana Hacking Team a compra de um software espião capaz de ativar câmeras e microfones, capturar senhas e infectar redes inteiras[6]. O caso evidenciou a dependência de tecnologias estrangeiras e a fragilidade de controles democráticos sobre aquisições de alto risco.

---

[3] VIANA, Natalia; ROZA, Gabriele. Loja de souvenirs tecnológicos: Um guia para as compras da vigilância. Agência Pública, 31 jan. 2017. Disponível em: https://apublica.org/vigilancia/loja-de-souvenirs-tecnologicos/. Acesso em: 20 ago. 2025.

[4] TATEMOTO, Rafael. Vigilância em massa e inversão dos princípios democráticos, afirma pesquisador. Brasil de Fato, 4 ago. 2016. Disponível em: https://www.brasildefato.com.br/2016/08/04/vigilancia-em-massa-e-inversao-dos-principios-democraticos-afirma-pesquisador/. Acesso em: 20 ago. 2025.

[5] HUREL, Louise Marie. Mapping Cyber Policy in Latin America: The Brazilian Case. [S.l.]: Centro LATAM Digital, 2022.

[6] VIANA, Natalia. Hackeando o Brasil. Agência Pública, 27 jul. 2015. Disponível em: https://apublica.org/2015/07/hackeando-o-brasil/. Acesso em: 19 set. 2025.

Esse ambiente favoreceu a chamada “indústria da insegurança” no Brasil. Como aponta o relatório *Mercadores da Insegurança*, empresas privadas passaram a vender soluções de vigilância ao Estado sob a lógica da mercantilização do medo, firmando contratos sigilosos e sem licitação transparente[7]. Muitas contratações atendiam mais a interesses comerciais do que a necessidades legítimas de investigação, capturando políticas públicas e deslocando o foco da proteção de direitos para uma lógica mercadológica e punitivista.

Os riscos dessa ausência de controle ficaram claros no escândalo da “ABIN paralela”, revelado em 2023, quando investigações da Polícia Federal apontaram que softwares de espionagem foram usados ilegalmente contra adversários políticos, jornalistas e ministros do STF, sem autorização judicial[8]. O episódio expôs como ferramentas de intrusão podem ser instrumentalizadas para perseguição política, corroendo a confiança democrática.

Em 2025, o governo buscou atualizar a regulação. A Portaria nº 634/2025 do Ministério da Justiça regulamentou o uso de tecnologias de investigação, incluindo de intrusão cibernética[9]. Embora pioneira e necessária, essa medida carece de força de lei e não prevê mecanismos eficientes de auditoria externa. Em agosto, o Decreto nº 12.573/2025 instituiu a Estratégia Nacional de Cibersegurança, com diretrizes para proteção de infraestruturas críticas e estímulo à indústria nacional de defesa digital[10]. Ambos, porém, foram criticados por não enfrentarem os riscos à privacidade e à liberdade, reproduzindo a lógica securitária.

No Congresso, a consolidação da Frente Parlamentar de Apoio à Cibersegurança e à Defesa Cibernética (FrenCyber)) em 2025 ampliou essa

---

[7] Instituto de Pesquisa em Direito e Tecnologia do Recife - IP.rec. Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil. Recife: IP.rec, nov. 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 20 ago. 2025.

[8] GALISI, Juliano. O que é a investigação da ‘Abin paralela’, que indiciou Carlos Bolsonaro e Alexandre Ramagem. Estadão, São Paulo, 17 jun. 2025. Disponível em: https://www.estadao.com.br/politica/o-que-e-investigacao-abin-paralela-indiciou-carlos-bolsonaro-alexandre-ramagem-nprp/. Acesso em: 20 ago. 2025.

[9] BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 634, de 10 de junho de 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-em-investigacoes-criminais-e-inteligencia-de-seguranca-publica. Acesso em: 19 ago. 2025.

[10] BRASIL. Presidência da República. Decreto nº 12.573, de 4 de agosto de 2025. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2023-2026/2025/decreto/D12573.htm. Acesso em: 19 ago. 2025.

tendência. Composta majoritariamente por militares e parlamentares de viés punitivista, a Frente atua a portas fechadas, sem participação da sociedade civil e da comunidade científica, discutindo projetos que expandem a vigilância sem salvaguardas[11]. A pauta da cibersegurança, assim, permanece concentrada em grupos restritos, comprometidos com a ampliação do aparato de vigilância.

O resultado é um cenário paradoxal: o Brasil ostenta marcos avançados, como o MCI e a LGPD, mas mantém práticas opacas de hacking governamental. Estados e municípios usam, de forma crescente, recursos federais para contratar ferramentas de intrusão sem transparência, em um ambiente jurídico instável que permite interpretações subjetivas sobre os limites dessas técnicas. Diante disso, jornalistas, ativistas e defensores de direitos humanos recorrem a estratégias de autodefesa digital, como criptografia de ponta a ponta e servidores descentralizados, para se proteger do próprio Estado[12].

A experiência brasileira evidencia que o uso de ferramentas de hacking governamental, quando ocorre sem regulação e mecanismos de *accountability*, pode gerar riscos tanto individuais quanto coletivos, além de afetar a confiança entre Estado e sociedade. Desde 2013, observa-se no país uma tensão permanente entre a busca por soberania digital e a ampliação da vigilância interna. O futuro da política de cibersegurança estará relacionado à forma como a legislação sobre tecnologias invasivas será construída e em que medida incorporará participação social e garantias de direitos fundamentais. Caso contrário, há indícios de que se consolide um aparato de vigilância pouco transparente e distante do controle democrático, com impactos relevantes para a qualidade da democracia brasileira.

4. Mapeamento de partes interessadas

O debate brasileiro sobre hacking governamental, criptografia e vigilância estatal compõe um campo de disputa com atores, interesses e assimetrias bem definidos. Desse modo, o presente mapeamento resulta do próprio processo de

[11] SILVA NETO, Pedro; SARAIVA, Raquel. As portas fechadas da bancada da cibersegurança. ObCrypto – Observatório da Criptografia, 11 abr. 2025. Disponível em: https://obcrypto.org/as-portas-fechadas-da-bancada-da-ciberseguranca/. Acesso em: 20 ago. 2025.
[12] BRAGA, Pedro et al. The construction of a sociotechnical surveillance network in Brazil. First Monday, [S.l.], v. 27, n. 8, 2022. DOI: 10.5210/fm.v27i8.12410. Disponível em: https://firstmonday.org/ojs/index.php/fm/article/view/12410. Acesso em: 20 ago. 2025.

investigação, combinando levantamentos quantitativos e percepções qualitativas que permitiram identificar grupos relevantes, posições e motivações a partir do material empírico colhido[13].

4.1. Setor Governamental

Nos achados da pesquisa, o setor governamental aparece como ocupando posição central por reunir simultaneamente a demanda por ferramentas de vigilância e a responsabilidade regulatória. Foram encontradas instituições com papéis distintos que convergem para esse centro decisório, entre elas o Supremo Tribunal Federal — especialmente no âmbito da ADPF 1143 —, o Ministério da Justiça e Segurança Pública, a Agência Brasileira de Inteligência e a Polícia Federal.

A atuação estatal, no entanto, mantém um de opacidade, observável em negativas a pedidos de acesso a informações amparadas em alegações de segredo comercial e de segurança nacional, o que restringe a fiscalização externa e dificulta a construção de parâmetros públicos de avaliação de risco[14]. Mesmo iniciativas recentes do Executivo, como a Portaria nº 634/2025[15], que são percebidas como um movimento inicial de ordenação do setor, permanecem aquém do necessário por carecerem de mecanismos proibitivos efetivos voltados às tecnologias de intrusão mais invasivas. No Legislativo, a tramitação de proposições como o PL 4939 de 2020[16] e o PL 402 de 2024[17] sinaliza presença de debate formal, porém avaliações

---

[13] [1] Trata-se, portanto, de um recorte analítico que reflete as dinâmicas observadas na pesquisa, sem a pretensão de abarcar a totalidade dos atores e perspectivas existentes no campo. Conforme se observa, o ARS inclusive aponta contraposições a algumas das tendências destacadas nas entrevistas, o que reforça a necessidade de compreender este mapeamento como fotografia situada de um processo em movimento.

[14] IP.REC. Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil. Recife: IP.rec, nov. 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 20 ago. 2025.

[15] BRASIL. Ministério da Justiça e Segurança Pública. Portaria nº 634, de 10 de junho de 2025. Disponível em: https://www.gov.br/mj/pt-br/assuntos/noticias/portaria-do-mjsp-regulamenta-uso-de-tecnologia-em-investigacoes-criminais-e-inteligencia-de-seguranca-publica. Acesso em: 19 ago. 2025.

[16] CÂMARA DOS DEPUTADOS. Projeto de Lei n. 4939, de 15 out. 2020, do Deputado Hugo Leal (PSD-RJ), que dispõe sobre as diretrizes do direito da Tecnologia da Informação e as normas de obtenção e admissibilidade de provas digitais na investigação e no processo, além de outras providências. Disponível em: <https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2264367>. Acesso em: 29 ago. 2025.

[17] SENADO FEDERAL. Projeto de Lei n.º 402, de 22 fev. 2024, de autoria do Senador Alessandro Vieira (MDB-SE), que disciplina a utilização de ferramentas de monitoramento remoto de terminais de

colhidas junto a atores do campo indicam baixo horizonte de efetividade diante de um ambiente permeado por *lobby*. Subjaz a esse quadro a leitura de que não se verifica vontade política consolidada para impor proibições significativas, já que diferentes espectros de governo percebem utilidade estratégica nessas ferramentas e tendem a relativizar a crítica quando resultados imediatos se mostram convenientes, prática que termina por normalizar a exceção e enfraquecer a responsabilização pública.

A complexidade aumenta quando se considera a dinâmica federativa que introduz assimetrias regulatórias e operacionais entre União, estados e municípios. Na esfera subnacional observa-se menor densidade institucional para controle e auditoria do ciclo de aquisição e uso de tecnologias de vigilância, o que abre espaço para práticas mais permissivas e contratação com escrutínio reduzido[18]. Essa heterogeneidade produz um mosaico regulatório difícil de harmonizar e dificulta a aplicação uniforme de salvaguardas técnicas e jurídicas. A fragmentação repercute sobre a transparência dos contratos, sobre a padronização de relatórios e sobre a possibilidade de aferição independente em relação à proporcionalidade e à necessidade dos meios empregados[19]. O resultado é uma ambiência em que a soma de lacunas incrementa riscos coletivos e torna mais custosa a construção de mecanismos de supervisão que sejam comparáveis, replicáveis e auditáveis em todo o território nacional.

4.2. Mídia

A Mídia aparece ocupando posição estratégica *accountability* e atua como amplificador público de práticas e riscos associados ao hacking governamental e à vigilância. Foram mencionados veículos de jornalismo investigativo — com destaque para iniciativas como o *The Intercept Brasil* — que enfrentam um ambiente descrito como hostil, no qual profissionais e fontes figuram como “potenciais alvos de

---

comunicações pessoais por órgãos e agentes públicos, civis e militares. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/162146>. Acesso em: 29 ago. 2025.

[18] IP.REC. Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil. Recife: IP.rec, nov. 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 20 ago. 2025.

[19] IP.REC. Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil. Recife: IP.rec, nov. 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 20 ago. 2025.

hacking governamental". Nessa conjuntura, a criptografia de ponta a ponta é vista não como mera preferência tecnológica, mas como condição operacional indispensável. Plataformas como o Signal foram citadas como integrando protocolos de rotina voltados à preservação do sigilo da fonte, pilar do exercício jornalístico em contextos de alta sensibilidade.

A atuação editorial, segundo as percepções reunidas, não se limita à função de denúncia: incorpora também uma dimensão de "educação política" ao traduzir riscos técnicos e jurídicos em consequências concretas para a cidadania e para liberdades comunicacionais. Nesse processo, constrói enquadramentos que esclarecem como ferramentas de intrusão se conectam a práticas de poder e a impactos cotidianos sobre a esfera pública.

Outro ponto levantado é que a cobertura ainda se depara com obstáculos informacionais que decorrem de opacidade estatal e de práticas comerciais que dificultam o rastreamento do ciclo de aquisição e de uso de tecnologias de vigilância. Negativas a pedidos com base na Lei de Acesso à Informação sob justificativas de segredo comercial e de segurança nacional restringem a checagem de contratos, de interlocutores e de especificações técnicas, impondo às reportagens a tarefa de compor narrativas verificáveis com fragmentos parciais e com documentação incompleta.

Mesmo diante dessas condições adversas, a Mídia foi descrita como continuando a desempenhar papel de vitrine pública do debate, ao dar forma compreensível a riscos que, de outro modo, permaneceriam abstratos e afastados do radar social. Com isso, cria as bases para que discussões técnicas circulem no espaço público e possam informar decisões políticas e institucionais.

4.3. Sociedade Civil

Nos achados da pesquisa, a Sociedade Civil aparece como sustentando a discussão intelectual, técnica e de incidência que mantém o tema em circulação permanente, inclusive quando a cobertura jornalística enfrenta limites de audiência e de recursos. Foram mencionadas organizações como IP.rec, InternetLab, SaferNet e Coalizão Direitos na Rede, além de iniciativas internacionais como a Electronic Frontier Foundation e a Access Now, descritas como produtoras de diagnósticos

setoriais, mapeamentos de cadeias de fornecedores e tipologias de risco que permitem qualificar o debate público.

De acordo com os dados coletados, estudos de fôlego oferecem base empírica para reportagens, para interlocução com o Legislativo e para diálogo com órgãos de controle, reduzindo a assimetria informacional que costuma favorecer aquisições opacas e adoção de tecnologias intrusivas. Entre os produtos mencionados, destacou-se o relatório Mercadores da Insegurança, referido como "divisor de águas" por sistematizar a opacidade do mercado de vigilância no Brasil e por apresentar evidências verificáveis sobre práticas comerciais e arranjos contratuais que operam em baixa transparência[20].

Esse tipo de produção foi percebido como viabilizando agendas de *advocacy* com pretensão de continuidade, diminuindo a dependência de ciclos de notícia e oferece linguagem acessível para explicar riscos técnicos a públicos não especializados. Nesse sentido, a atuação de *advocacy* aparece mobilizando instrumentos complementares e operando em múltiplas frentes. Observou-se a realização de monitoramento contínuo de proposições legislativas, elaboração de notas técnicas e participação em audiências públicas com o objetivo de qualificar salvaguardas e de enfrentar narrativas que normalizam a exceção em nome de segurança[21].

No campo judicial as intervenções de diversas entidades como *amicus curiae* em casos paradigmáticos como a ADPF 1143 inserem argumentos técnicos e de direitos humanos na arena decisória e dificultam a adoção de soluções simplistas que ignorem proporcionalidade, necessidade e adequação. Em paralelo, programas de capacitação em segurança digital e em avaliação de impacto oferecem ferramentas práticas a jornalistas defensores de direitos, comunidades vulnerabilizadas e agentes públicos, fortalecendo capacidades locais e construindo redes de confiança. Essas rotinas criam pontes entre especialistas técnicos e

[20] IP.REC. Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil. Recife: IP.rec, nov. 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 20 ago. 2025.

[21] IP.REC. Mercadores da Insegurança: conjuntura e riscos do hacking governamental no Brasil. Recife: IP.rec, nov. 2022. Disponível em: https://ip.rec.br/wp-content/uploads/2022/11/Mercadores-da-inseguranca.pdf. Acesso em: 20 ago. 2025.

formuladores de políticas, o que melhora a qualidade do desenho regulatório e a factibilidade de mecanismos de fiscalização.

Ainda assim, persistem desafios estruturais apontados como condicionantes do alcance e da velocidade de entrega de resultados. A assimetria de recursos frente a fornecedores de vigilância e a órgãos de Estado impõe escolhas difíceis de priorização e torna estratégica a construção de alianças com imprensa e academia. Também foi ressaltado que a fragmentação federativa adiciona camadas de complexidade, na medida em que práticas permissivas em níveis subnacionais tendem a escapar de escrutínio concentrado na esfera federal.

Por fim, medidas de *due diligence* em direitos humanos, avaliações de impacto e auditorias independentes foram destacadas como compondo o núcleo de salvaguardas defendidas por essas organizações. Tais medidas são percebidas como instrumentos voltados a transformar evidências coletadas em obrigações verificáveis e em rotinas institucionais capazes de reequilibrar a relação entre segurança e liberdade em um ambiente marcado por opacidade persistente.

4.4. Academia e comunidade técnica

De acordo com as percepções levantadas na pesquisa, em centros e grupos de pesquisa vinculados a instituições como a Fundação Getúlio Vargas e a Universidade Federal do ABC, bem como em entidades do setor técnico, como o CERT.br e a ISOC Brasil, observam-se esforços de consolidação de métodos de análise que conectam aspectos técnicos de criptografia e de vigilância a parâmetros normativos e a impactos sobre direitos fundamentais. Esse movimento é aqui interpretado como capaz de fornecer terreno comum para comparação entre casos e para um escrutínio público mais consistente.

Ainda segundo esse recorte, a produção acadêmica e técnica se materializa em artigos, estudos e pareceres que estruturam linhas de raciocínio replicáveis e oferecem critérios de avaliação a jornalistas, organizações cívicas e formuladores de política. A interlocução com diferentes públicos ocorre por meio de sínteses e de traduções de conceitos técnicos para linguagem acessível sem perda de rigor, o que amplia o alcance social do debate e fortalece a compreensão coletiva sobre riscos e salvaguardas.

Segundo os achados da pesquisa, esse circuito acadêmico e técnico é percebido como capaz de reduzir ruídos entre o que é tecnicamente demonstrável e o que pode ser narrado de modo compreensível para a sociedade, conferindo lastro às denúncias e prevenindo conclusões apressadas que possam deslegitimar investigações ou enfraquecer a confiança do público. Observou-se também a percepção de que, ao validar com rigor metodológico as preocupações levantadas por imprensa e sociedade civil e ao conectar evidências a teorias consistentes, a academia e a comunidade técnica emprestam peso de autoridade que dificulta a desqualificação do debate como mera disputa ideológica. Esse papel é igualmente associado à capacidade de fortalecer a contestação informada de apelos genéricos à segurança nacional, ao exigir demonstrações concretas de necessidade e adequação e ao expor custos institucionais e sociais de soluções que relativizam direitos sem benefícios comprovados.

Dessa forma, dentro do recorte analisado, a função acadêmica e técnica aparece como duplamente relevante: de um lado, por aprofundar o debate; de outro, por legitimar a crítica pública em ambientes marcados por opacidade estatal e por práticas comerciais que dificultam a rastreabilidade. Essa mediação técnica e normativa é descrita como nutrindo a frente de *accountability* composta por Mídia e Sociedade Civil, ao oferecer linguagem comum para reportagens, peças de *advocacy* e diálogo com o sistema de justiça e com o Legislativo.

Em conjunto, tais aportes são apresentados como fatores que transformam a discussão sobre *hacking* governamental e criptografia de um embate retórico em um campo de avaliação pública baseado em evidências, em que argumentos se submetem a padrões de prova e decisões podem ser testadas contra princípios e resultados — condição vista como indispensável para reequilibrar a relação entre segurança e liberdade em um Estado Democrático de Direito.

4.5. Setor Privado

Por fim, os achados da pesquisa indicam que o setor privado apresenta configuração heterogênea e ambígua, na qual motivações predominantemente comerciais se combinam com efeitos complexos sobre o ecossistema de vigilância.

De um lado, foram mencionados fornecedores de tecnologias de intrusão e monitoramento, que vão de grupos globais a revendedoras e integradoras nacionais com presença recorrente em compras públicas. Segundo os dados coletados e analisados, o desenho contratual frequentemente recorre a cláusulas de confidencialidade abrangentes, terceirizações sucessivas e fragmentação de objetos técnicos, o que pode diluir a aderência a padrões de *due diligence* e torna menos visível a identificação de beneficiários finais e de responsáveis por suportes e atualizações. Esse quadro é descrito como terreno fértil para aquisições com baixa transparência e para o uso de funcionalidades intrusivas sem trilhas de auditoria adequadas.

No outro polo, a pesquisa identificou a percepção de que grandes plataformas de tecnologia passaram a apresentar a proteção criptográfica como atributo central de segurança para usuários e como sinalizador de valor reputacional. Essa leitura situa tais empresas em um movimento de posicionamento público em defesa de criptografia forte, o que, em determinados contextos, gera fricções com demandas governamentais por acesso a conteúdo e metadados. Observou-se ainda a compreensão de que, embora o interesse declarado permaneça predominantemente comercial e vinculado à diferenciação competitiva, a agenda de privacidade impulsionada por essas plataformas acaba produzindo externalidades positivas tanto para a proteção de direitos quanto para a elevação de padrões de segurança comunicacional.

Foram também identificadas situações em que a defesa pública de privacidade convive com escolhas de desenho que privilegiam metas de negócio ou compatibilidades regulatórias e que não necessariamente coincidem com referências mais amplas de direitos humanos. Essa percepção reforça a necessidade de avaliação caso a caso e de métricas auditáveis para aferir impactos reais de promessas de segurança e de compromissos de criptografia ponta a ponta.

Esse jogo de narrativas e de incentivos, conforme encontrado nos documentos e nos conteúdos analisados, ajuda a explicar variações de engajamento, a neutralizar leituras simplistas de alinhamento automático com agendas de direitos e a indicar que, mesmo quando contribuem para elevar o

padrão de proteção criptográfica, as plataformas tendem a fazê-lo em termos compatíveis com seus objetivos estratégicos.

Desse modo, o quadro resultante, segundo a análise empreendida, é de uma tensão dialética sustentada por duas forças que se retroalimentam: de um lado, um aparato estatal inclinado ao secretismo e, de outro, um mercado que lucra com a opacidade e que organiza operações para reduzir visibilidade pública sobre fluxos de tecnologia, de dados e de decisões. Essa interação é percebida como estabelecendo barreiras cumulativas à construção de *accountability* e deslocando o ônus probatório para jornalistas, organizações cívicas e pesquisadores, que precisam recompor trilhas informacionais fragmentadas.

O setor privado permanece, assim, descrito nos achados da pesquisa como vetor decisivo na determinação do grau de opacidade ou de transparência do ecossistema, seja pela forma como desenha e comercializa tecnologias de vigilância, seja pela maneira como plataformas moldam a narrativa pública sobre criptografia e segurança — com efeitos concretos sobre a qualidade do controle social e sobre a possibilidade de alinhamento entre segurança e liberdade em um ambiente democrático.

5. Análise de Influência e Participação

5.1. Contextualização

A ARS utiliza a teoria dos grafos, ou seja, estruturas matemáticas para descrever relações entre objetos, compostas por vértices ou entidades individuais (também chamados de nós) e arestas (que representam a conexão entre os nós). Essa abordagem metodológica permite uma atenção detalhada aos mecanismos que conectam as partes, tornando possível analisar atores individuais, subgrupos e a rede como um todo. **É importante observar que o conceito de "rede social" refere-se a um conjunto de relações (que podem incluir tanto vínculos positivos quanto negativos) entre um número definido e finito de atores.**

De modo geral, a análise de redes sociais foca nas relações entre atores sociais, na interdependência entre eles e nos efeitos que emergem da estrutura geral. No contexto das discussões relacionadas ao hacking governamental no

Brasil, a ARS também foi utilizada para apoiar a identificação e demonstração dos níveis de representação e participação de entidades e grupos na discussão da matéria e de marcos regulatórios.

As conexões entre os atores foram definidas a partir de uma base de dados construída com informações públicas e observáveis, incluindo registros de participação conjunta em eventos, documentos oficiais, colaborações institucionais, posicionamentos divulgados por organizações em espaços públicos de debate, bem como notícias e matérias jornalísticas que registram interações relevantes. Essa base foi sistematizada e catalogada especificamente para este estudo, servindo como referência para a aplicação da Análise de Redes Sociais (ARS) no contexto do hacking governamental no Brasil. Para assegurar transparência e possibilitar a verificação por outros pesquisadores, a base de dados poderá ser disponibilizada mediante solicitação. O peso das relações pode ser visualizado a partir da espessura das arestas conectando os pontos da rede. Quanto mais grossa a aresta, mais elevado o peso daquela relação pode ser entendido.

Peso	Descrição	Indicador
Alto	Interações regulares e contínuas ao longo do tempo, com envolvimento constante ao longo dos últimos 5 anos (2020-2025).	Publicações conjuntas, projetos conjuntos, eventos e conferências em conjunto, assinaturas de cartas e documentos em conjunto, troca de informações e recursos.
Médio	Trocas que ocorrem com menos frequência, mas com uma colaboração significativa em ocasiões pontuais ao longo dos últimos 5 anos (2020-2025).	Colaborações pontuais, eventos esporádicos, assinatura em documentos e cartas
Baixo	Trocas raras, sem um compromisso constante ou profundo ao longo dos últimos 5 anos (2020-2025).	Comunicação superficial e referências ocasionais.

As cores das conexões entre os atores representam a natureza das relações no contexto do hacking governamental no Brasil. As arestas vermelhas indicam conflitos ou tensões, como disputas técnicas ou desacordos políticos; as verdes representam relações positivas e de cooperação, comuns em parcerias institucionais ou operacionais; as cinzas apontam relações neutras ou técnicas,

marcadas por interações protocolares ou informacionais; e as amarelas sinalizam relações voláteis, que oscilam entre colaboração e conflito conforme o contexto.

Marcador	Descrição	Indicador
Positiva (Colaboração ou Apoio Mútuo)	Interações onde os atores se apoiam ou colaboram ativamente, compartilhando objetivos e trabalhando em conjunto para alcançar metas comuns.	Troca de recursos, apoio explícito em projetos, colaborações contínuas, troca de informações sem interesses pessoais em detrimento do outro.
Negativa (Conflito, Oposição ou Desacordo)	Interações onde os atores estão em desacordo, competindo ou criticando um ao outro, com um foco em diferenças de opinião ou em estratégias conflitantes.	Críticas abertas, discordâncias em políticas ou propostas, oposição direta a iniciativas do outro ator, relações tensas.
Neutra ou N/A (Referências Informativas ou Sem Julgamento Claro)	Quando os atores se relacionam de forma mais distante, com interações limitadas à troca de informações sem envolvimento emocional ou posição clara.	Relacionamentos baseados em trocas informativas sem tomar partido, menções neutras ou factuais sem conclusões claras.
Volátil (Relações Ambíguas ou Temporárias)	Interações que não são claras quanto à sua natureza e podem mudar com o tempo, sendo difíceis de categorizar devido à incerteza sobre a continuidade ou profundidade.	Relações que flutuam entre colaboração e conflito, críticas indiretas, alianças temporárias com objetivos mutáveis, ou colaborações que se dissolvem rapidamente.

Essa codificação permite identificar rapidamente os tipos de interação predominantes e compreender a complexidade das dinâmicas entre os diferentes setores envolvidos.

5.2. Métricas-chave

No contexto desta pesquisa, três métricas estabelecidas da ARS foram empregadas para examinar a estrutura das interações e da influência entre as partes interessadas no ecossistema regulatório que envolve o hacking governamental no Brasil.

5.2.1. Centralidade de grau

A primeira métrica refere-se ao número de conexões diretas que um ator (ou nó) possui dentro da rede. É um indicador primário do nível de atividade de um ator e de sua influência imediata em uma estrutura relacional. Uma alta centralidade de grau sugere que o ator está altamente envolvido com os demais, seja como organizador de determinada iniciativa regulatória ou como signatário de diversos documentos relevantes. Em redes voltadas para políticas públicas, atores com alta centralidade de grau são frequentemente percebidos como participantes-chave ou vozes influentes no discurso regulatório.

5.2.2. Densidade da rede

A densidade da rede é uma métrica que representa o quão conectados estão os atores dentro da rede. Quanto maior a densidade, maior a probabilidade de que a rede tenha comunicação eficaz e construção de consenso em relação à formulação de políticas. Por outro lado, uma baixa densidade pode sugerir fragmentação ou um ambiente desafiador para a cooperação entre diferentes atores. No contexto deste estudo, a densidade serve como um indicador da inclusão no ecossistema regulatório.

5.2.3. Agrupamento (clustering)

Por fim, a métrica de agrupamento está relacionada à probabilidade de que os atores formem grupos altamente conectados dentro da rede maior. Esses agrupamentos muitas vezes refletem coalizões ou alianças de atores que colaboram com mais frequência entre si. A identificação desses agrupamentos é útil para entender as dinâmicas de subgrupos e a presença de pautas coordenadas de incidência ou políticas públicas. Neste relatório, a análise de agrupamento visa

identificar padrões de colaboração e o surgimento de alianças temáticas ou ideológicas.

5.3. Análise e achados

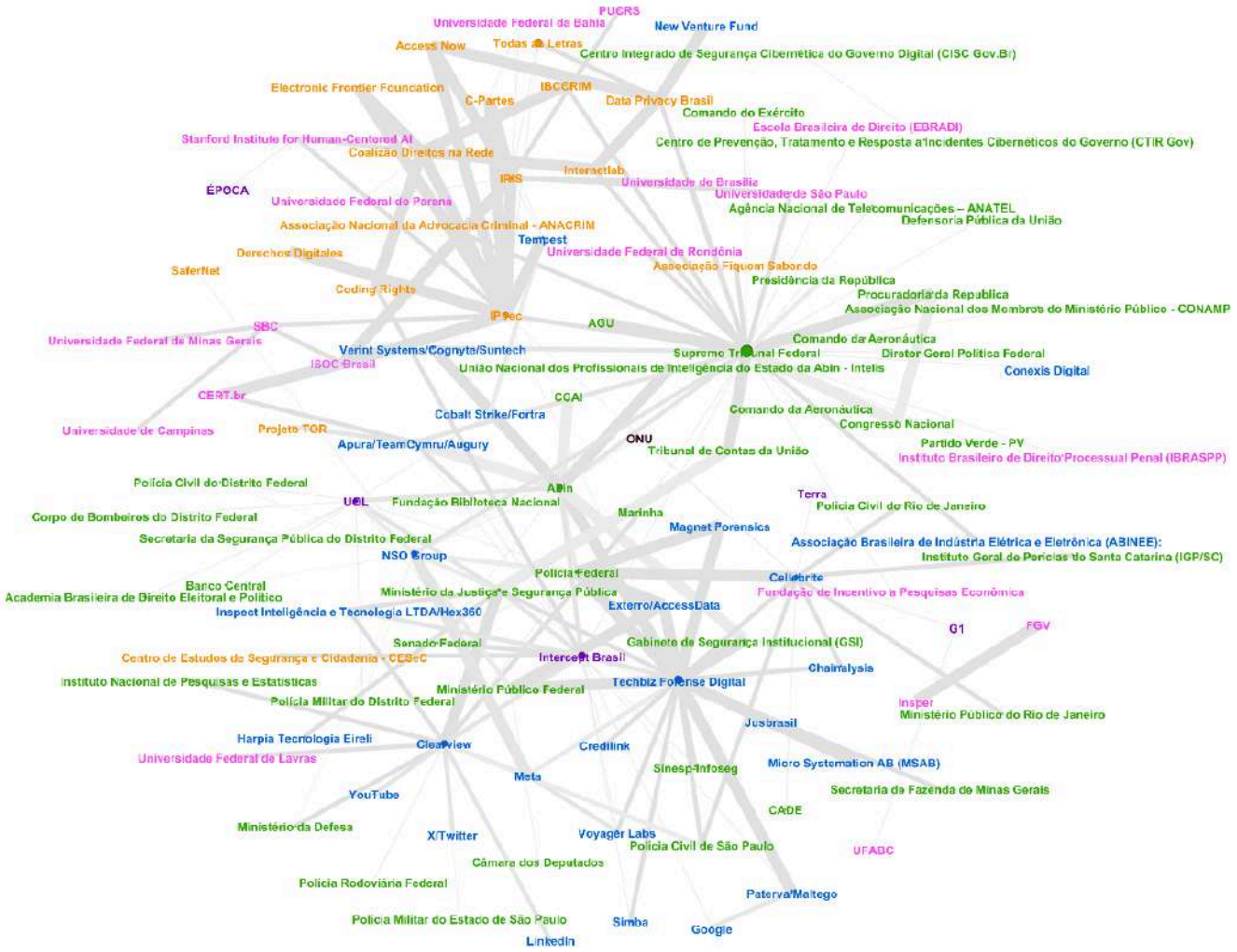


Figura 1. Rede de interações relacionadas ao hacking governamental entre atores no Brasil, representada por Análise de Redes Sociais (ARS). As cores do vértice e rótulo de cada ator representam os seus respectivos setores. Em verde, atores do setor público; em azul, membros do setor privado; em rosa, membros da academia e comunidade técnica; em laranja, membros de organizações da sociedade civil; e em roxo, representantes de veículos de comunicação e mídia.

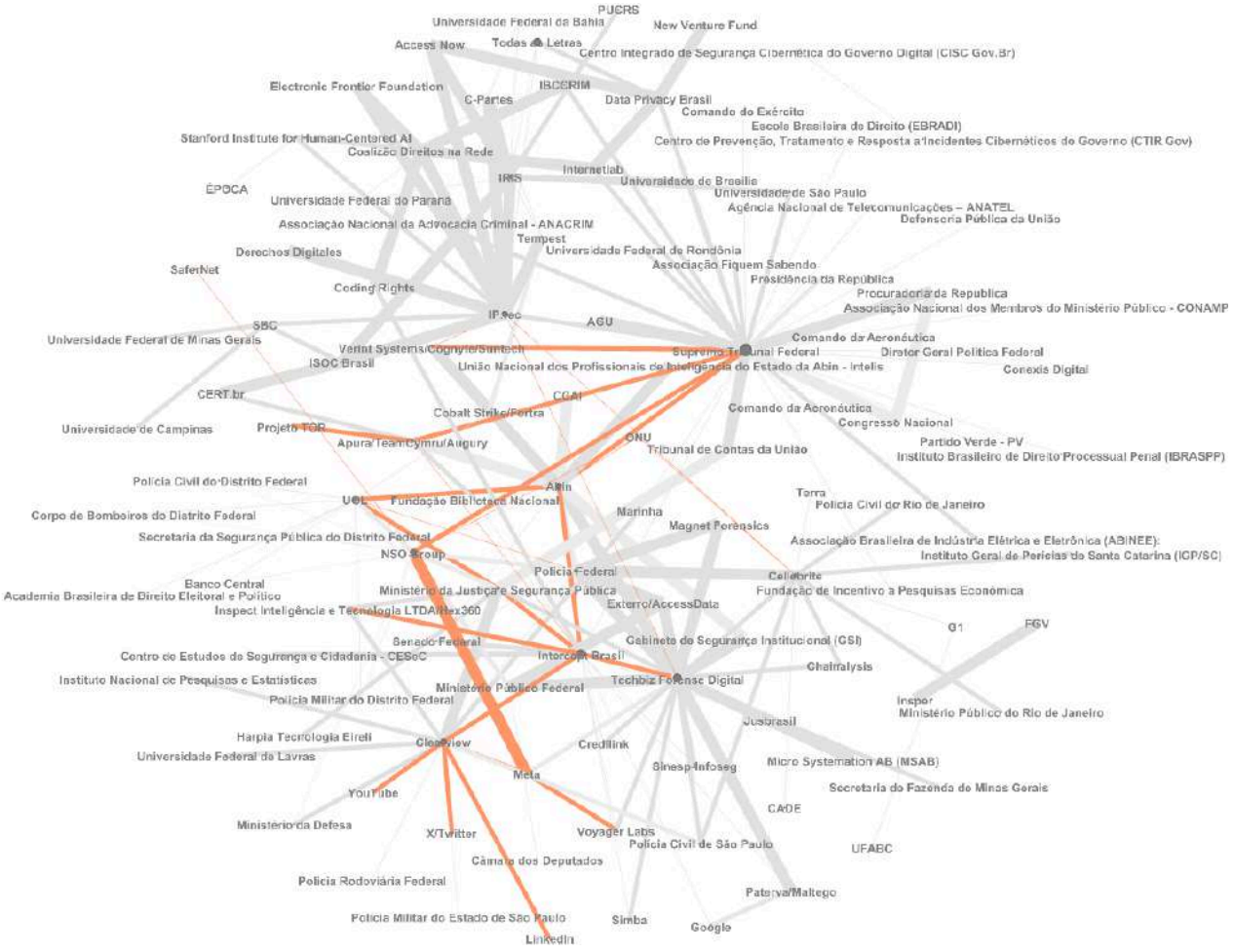


Figura 2. Rede de interações negativas relacionadas ao hacking governamental entre atores no Brasil, representada por Análise de Redes Sociais (ARS).

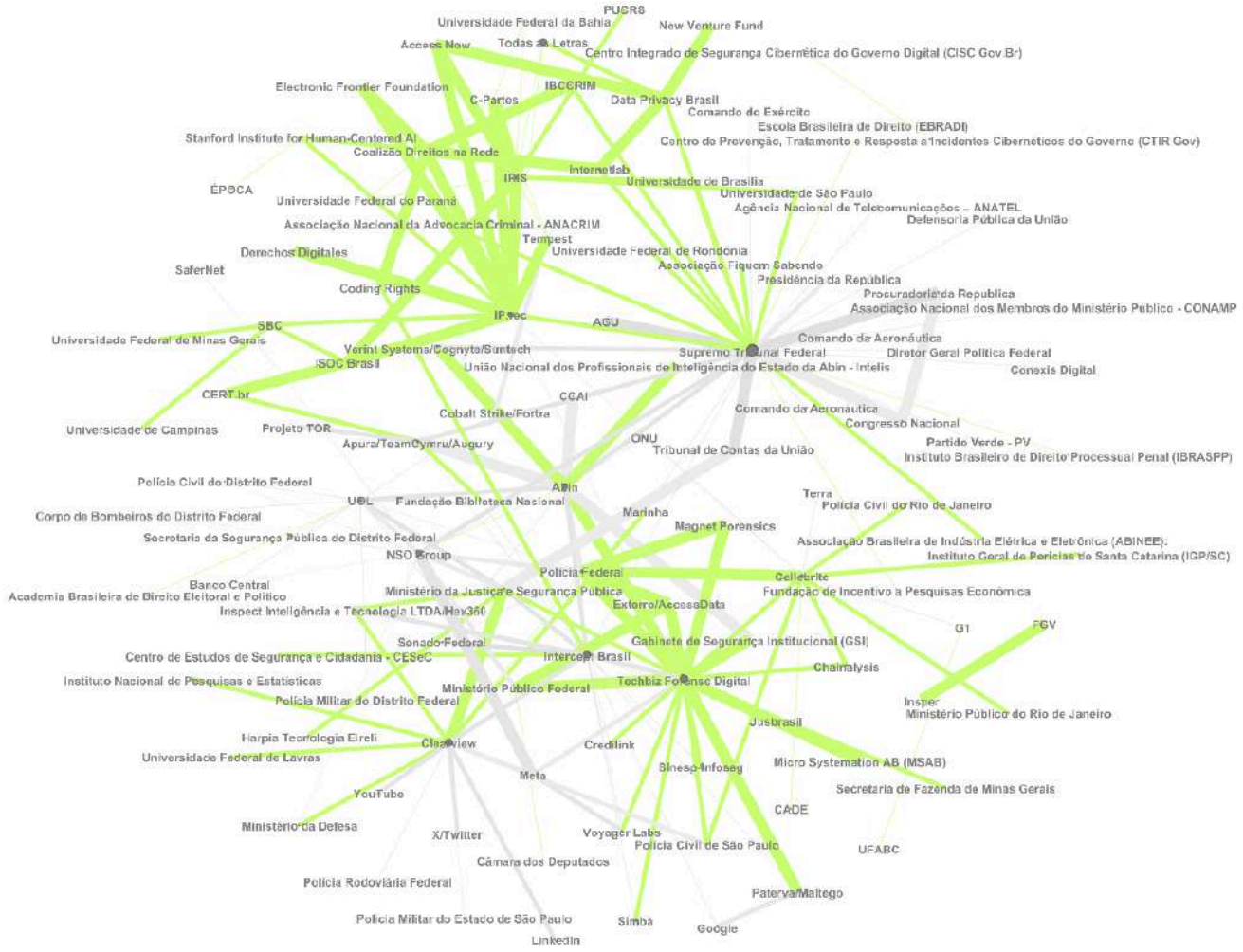


Figura 3. Rede de interações positivas relacionadas ao hacking governamental entre atores no Brasil, representada por Análise de Redes Sociais (ARS).

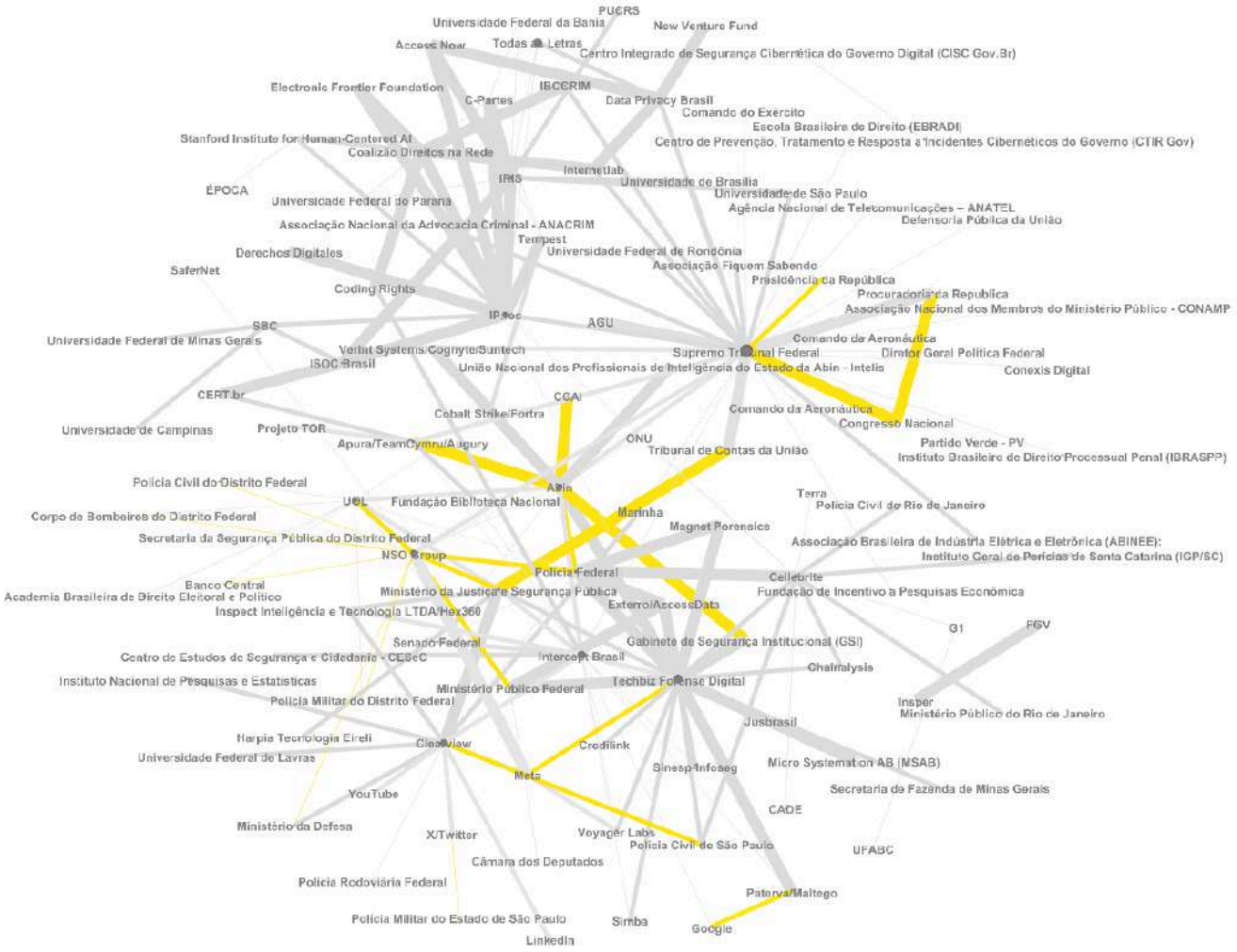


Figura 4. Rede de interações voláteis relacionadas ao hacking governamental entre atores no Brasil, representada por Análise de Redes Sociais (ARS).

5.3.1 Centralidade

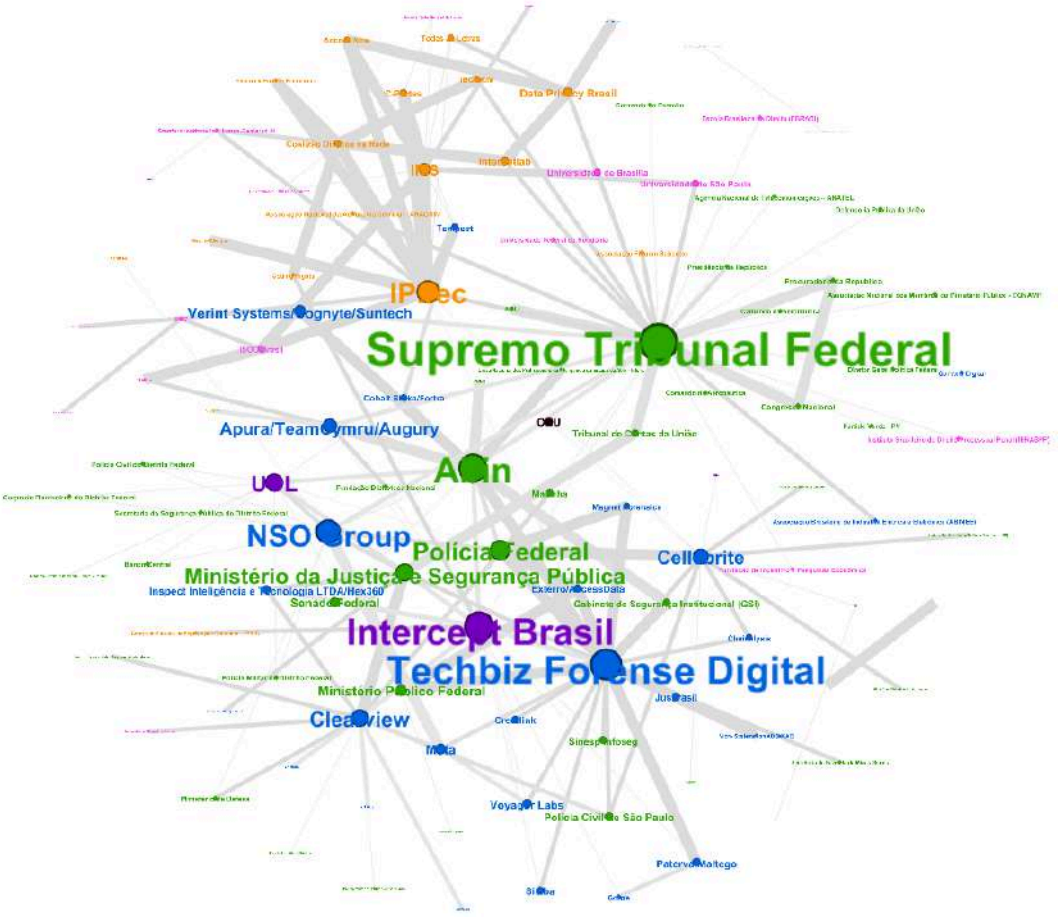


Figura 5. A rede indica o nível de centralidade de grau: quanto maior o nó e rótulo, maior o número de conexões diretas daquele ator com outros na rede. Assim, atores maiores ocupam papel mais influente ou central no debate.

A centralidade de grau é uma das métricas mais intuitivas da ARS e, neste estudo, revela com clareza quais são os atores mais conectados e, portanto, mais influentes na rede de relações relacionadas ao hacking governamental no Brasil. Na rede analisada, o **setor governamental** aparece com destaque, ocupando posições centrais e com um elevado número de conexões diretas com diversos outros setores, incluindo o setor privado, academia, comunidade técnica, sociedade civil e organismos internacionais. Esse padrão indica que as instituições públicas, em especial órgãos ligados à segurança, justiça e defesa, exercem papel central na formulação, implementação e discussão de políticas relacionadas ao hacking. Assim, a análise da rede evidencia uma forte centralidade dos atores do governo, que ocupam posições estratégicas e concentram grande parte das conexões na visualização. Entre os nós mais centrais, destaca-se o Supremo Tribunal Federal

(STF), que atua como hub de influência, além do Ministério da Justiça e Segurança Pública (MJSP) e da Polícia Federal, que reforçam a centralidade do aparato estatal no tema. O papel central da Agência Brasileira de Inteligência (Abin), no entanto, é definido por meio de casos envolvendo o uso de ferramentas de intrusão de forma irregular.

O **setor privado** também apresenta alta centralidade de grau, o que indica uma participação significativa e ativa nas dinâmicas relacionadas ao hacking governamental. Empresas de tecnologia e fornecedores de soluções de intrusão digital, como Techbiz Forense Digital, Cellebrite, NSO Group e Clearview, mantêm vínculos diretos com órgãos governamentais, evidenciando tanto a dependência do Estado em relação a serviços corporativos quanto o protagonismo dessas empresas no desenvolvimento e oferta de tecnologias intrusivas no Brasil. Além de atuarem como parceiras do setor público, também é possível identificar relações de conflito (representadas previamente em vermelho na Figura 2) entre diferentes atores do setor privado como, por exemplo, entre plataformas de mensageria privada e empresas que desenvolvem ferramentas de intrusão. Esses conflitos geralmente decorrem do risco de que tais ferramentas comprometam a segurança e a integridade dos sistemas e dispositivos oferecidos por outras empresas. Em muitos casos, há um embate direto entre o interesse comercial em oferecer proteção e privacidade aos usuários e o desenvolvimento de tecnologias que buscam justamente romper essas barreiras de segurança. Esses posicionamentos divergentes são relevantes para revelar os múltiplos interesses e disputas internas que coexistem dentro do próprio setor privado, mostrando que ele não é um bloco monolítico, mas sim um campo de tensões e negociações tecnológicas e comerciais.

No campo da **mídia**, destaca-se o papel do The Intercept Brasil, que exerce influência significativa na rede ao atuar como um ator central na revelação de abusos relacionados ao uso de ferramentas de intrusão e vigilância. A atuação da mídia no Brasil não apenas expõe práticas questionáveis de órgãos estatais e empresas privadas, mas também amplia a pressão por mecanismos de transparência e accountability. Embora a **sociedade civil** apareça com menor centralidade de grau, há nós específicos que ocupam posições estratégicas com

múltiplas conexões, inclusive em posições conflitantes (em vermelho na Figura 2), especialmente com atores do setor privado e governamental. Isso sinaliza sua atuação crítica e fiscalizadora, além da tentativa de influenciar a formulação de políticas públicas que respeitem os direitos digitais, a privacidade e os princípios democráticos. Contudo, o menor número de conexões diretas também pode indicar uma exclusão parcial desses setores nos processos decisórios centrais. Ainda que organizações da sociedade civil atuem de forma crítica e ativa na defesa dos direitos digitais e na promoção da transparência, sua distância estrutural dos atores centrais da rede evidencia desafios em acessar os espaços onde se definem as políticas públicas sobre hacking governamental. Isso reforça a necessidade de mecanismos mais inclusivos e transparentes de governança, capazes de equilibrar os interesses em jogo e garantir que a regulação dessas tecnologias esteja alinhada com os princípios democráticos e com a proteção dos direitos fundamentais.

Finalmente, a **academia e comunidade técnica** aparecem como grupos de alta relevância, ainda que o seu posicionamento seja mais periférico em relação ao núcleo decisório representado pelo setor público. Seu papel não se limita à produção de conhecimento teórico ou à formação de especialistas, mas também envolve a mediação entre diferentes atores, funcionando como uma ponte que pode aproximar perspectivas divergentes e facilitar a circulação de ideias. Quando conectada a organizações do terceiro setor e ao próprio governo, a academia e a comunidade técnica contribui para o debate normativo e para a qualificação técnica das discussões, oferecendo análises fundamentadas e propostas que buscam equilibrar inovação tecnológica, interesses econômicos e direitos fundamentais. Além disso, a comunidade técnica ocupa uma posição estratégica na validação e no questionamento de soluções tecnológicas voltadas para a segurança digital. Essa atuação crítica fortalece a sociedade civil, amplia a capacidade de monitoramento de práticas estatais e privadas e gera subsídios para a formulação de políticas públicas mais sólidas. Em relação ao contexto brasileiro, a academia e a comunidade técnica apresentam um número expressivo de conexões fortes com organizações da sociedade civil, reforçando seu papel de suporte e legitimidade técnica nas disputas políticas e jurídicas. Assim, mesmo em posição periférica, sua relevância se manifesta pela capacidade de articular diferentes setores, tensionar

narrativas dominantes e abrir espaços de participação em um campo historicamente restrito aos interesses governamentais e corporativos.

Em resumo, a análise da centralidade de grau revela um sistema altamente centralizado no governo, com influência relevante do setor privado, e menor, porém estratégica, participação de atores da academia, comunidade técnica, mídia e sociedade civil.

5.3.2. Densidade

A densidade da rede, ou seja, o nível de interconexão entre os nós, é um indicador-chave para entender o grau de coesão e colaboração entre os atores envolvidos no ecossistema do hacking governamental no Brasil. Na rede analisada, percebe-se que a rede como um todo não é homogênea em termos de densidade. A visualização da rede também indica que os atores tendem a se conectar mais fortemente com instituições do mesmo setor. Essa segmentação reforça a ideia de que há poucos espaços de diálogo estruturados entre os diferentes grupos de interesse, o que pode dificultar a construção de consensos e a formulação de políticas públicas participativas.

O **setor público**, por exemplo, com a exceção do Supremo Tribunal Federal, aparece como um bloco denso e interconectado, com pouca abertura para conexões com o terceiro setor, o que sugere uma dinâmica interna autorreferente, onde decisões são tomadas majoritariamente dentro do próprio aparato estatal. Apesar da falta de diálogo com membros da sociedade civil, o bloco governamental e o setor privado apresentam alta densidade, o que sugere um ambiente de comunicação frequente, acordos institucionais e fluxos contínuos de informação e decisão. Isso é especialmente visível nos fortes vínculos verdes entre ministérios, forças de segurança, agências de inteligência e empresas de tecnologia.

O **setor privado** demonstra baixa densidade relacional interna e limitada inserção nas articulações com a sociedade civil, o que pode ser explicado por diferentes fatores. Empresas de tecnologia, apesar de serem afetadas diretamente por regulações sobre hacking e criptografia, muitas vezes atuam com baixa transparência e pouca articulação com a sociedade civil, preferindo canais institucionais diretos com o governo ou optando por posições discretas no debate

público. Essa ausência de engajamento mais aberto pode enfraquecer a construção de políticas equilibradas, especialmente em um contexto em que soluções técnicas e comerciais impactam diretamente a proteção de dados e os direitos dos cidadãos.

No agrupamento da **mídia**, **sociedade civil, academia** e **comunidade técnica**, a densidade interna é relativamente boa, mas as conexões externas, com o governo e o setor privado, são frágeis e, em vários casos, marcadas por tensão (arestas vermelhas). Isso revela uma atuação crítica, porém marginalizada, onde esses atores exercem papel de alerta, *advocacy* e produção de conhecimento, mas com limitada influência direta na formulação de decisões. Isso reforça a percepção de que o ecossistema regulatório brasileiro de hacking governamental ainda necessita fortalecer os canais formais de participação social e de garantir espaços de escuta qualificada no processo regulatório.

Apesar da cooperação identificada entre entes públicos e empresas do setor privado, é preciso destacar que a rede como um todo apresenta baixa densidade intersetorial. Isso aponta para uma estrutura relativamente fragmentada, com blocos que operam quase de forma autônoma e com pouco diálogo entre si. A baixa densidade entre grupos com posições divergentes pode dificultar a construção de políticas equilibradas, especialmente em temas sensíveis como privacidade, vigilância, segurança digital e direitos fundamentais.

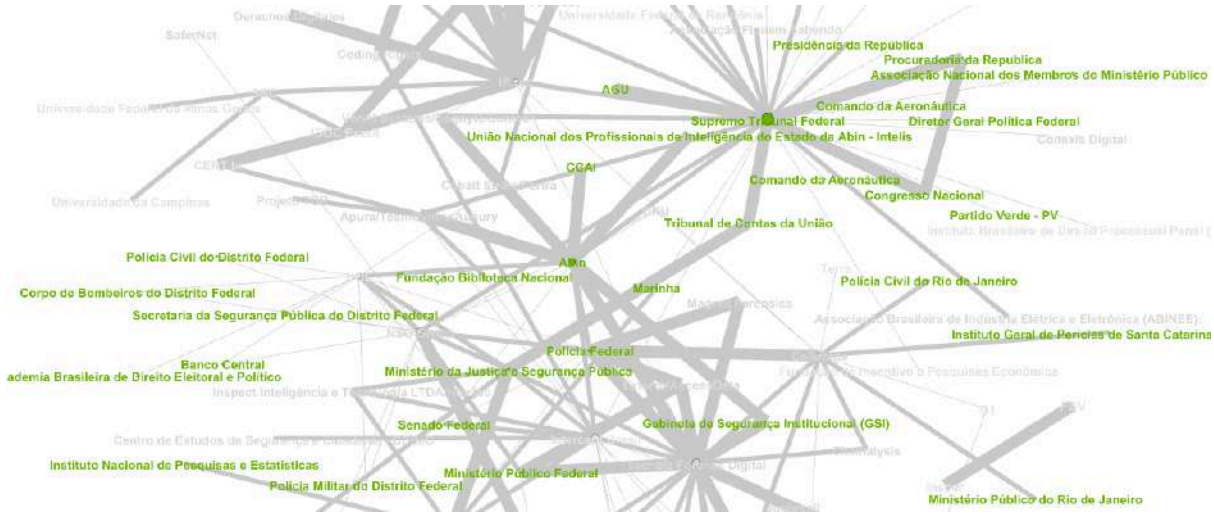
Portanto, a densidade da rede reflete tanto forte articulação operacional entre governo e empresas, quanto fragilidade no envolvimento de setores que representam a sociedade civil e o controle democrático. Para avançar em um modelo de governança mais inclusivo, ético e eficiente no uso de ferramentas de hacking, seria necessário promover conexões mais densas e produtivas entre todos os atores, incluindo canais institucionais de diálogo, participação pública, e transparência nas relações Estado-empresa. Em termos práticos, essa fragmentação compromete a construção de consensos e a governança participativa.

Políticas públicas que envolvem hacking governamental e criptografia não podem ser desenhadas exclusivamente por atores estatais sob pena de comprometer os direitos fundamentais e os princípios do Estado de Direito. A visualização da rede aponta para a urgência de mecanismos intersetoriais

permanentes, com participação equilibrada de diferentes setores, especialmente daqueles que hoje se encontram marginalizados ou pouco conectados aos centros de decisão. Um ambiente regulatório saudável exige transparência, pluralismo e *accountability*, valores que só podem ser garantidos com a ampliação das conexões entre os diversos atores que compõem esse ecossistema.

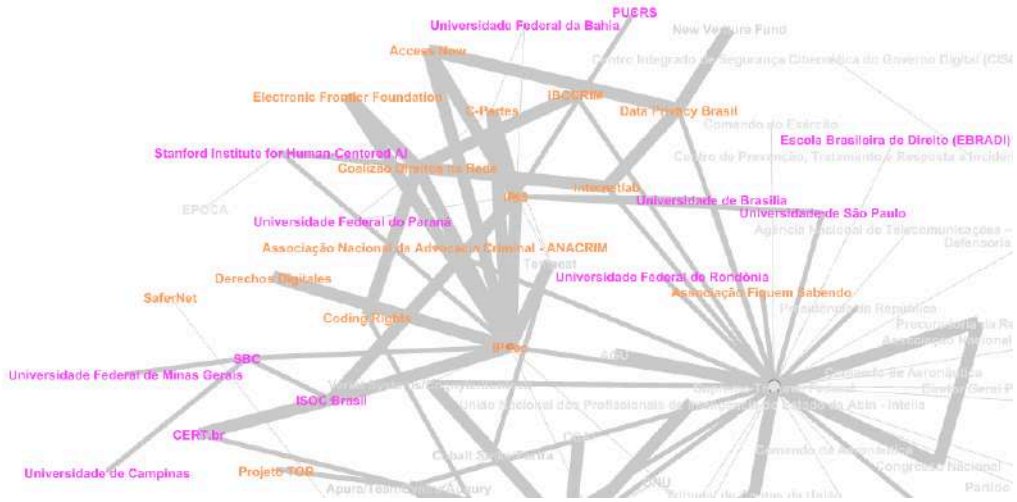
5.3.3 Agrupamentos

A métrica de agrupamento (ou *clustering*) permite identificar subgrupos de atores que se relacionam mais intensamente entre si, formando coalizões ou blocos de influência. Na rede, é possível observar claramente pelo menos três grandes *clusters*: um governamental, um acadêmico-civil e um privado. Esses agrupamentos revelam afinidades ideológicas, interesses compartilhados ou simplesmente práticas recorrentes de colaboração. O ***cluster* governamental**, por exemplo, é, em grande parte, denso e coeso, o que sugere forte cooperação institucional. As relações conflitantes identificadas no cluster, no entanto, estão relacionadas a investigações iniciadas devido a identificação do uso abusivo de ferramentas de intrusão por parte de entes públicos e agências brasileiras, como por exemplo, a Abin.

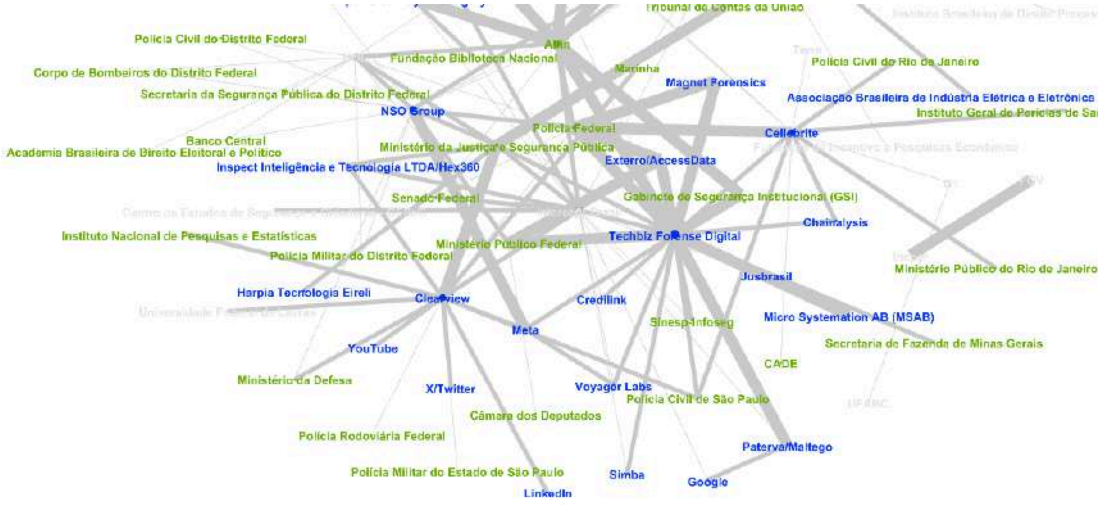


O ***cluster* da sociedade civil, da academia** e **comunidade técnica** apresenta outro tipo de dinâmica. Formado por universidades públicas, ONGs nacionais e internacionais, institutos de pesquisa e centros de direitos digitais, esse grupo tende a desenvolver laços mais fortes entre si do que com o centro governamental. Com exceção das relações com o Supremo Tribunal Federal, suas

conexões com o setor público ou privado, quando existem, são frequentemente marcadas por relações negativas ou neutras, indicando posições críticas, de oposição ou monitoramento. O agrupamento reflete, portanto, uma rede paralela de atores preocupados com os impactos éticos, legais e sociais do uso de ferramentas de hacking por parte do Estado.



No caso do ***cluster* do setor privado**, observa-se uma relação intensa com os entes governamentais, mas também com outras empresas e fornecedores internacionais de tecnologia. A presença desses atores mostra como o mercado global de tecnologias de vigilância influencia o cenário brasileiro, e como essas empresas disputam espaço como fornecedoras de soluções de hacking e monitoramento para o governo brasileiro. A articulação entre essas empresas, muitas vezes em parceria com o governo, levanta preocupações em relação à privacidade, abuso de poder e falta de transparência.



Esses agrupamentos revelam, portanto, um ecossistema dividido em três frentes principais: uma institucional e operacional (governo), uma mercadológica e tecnológica (privado) e uma crítica e normativa (sociedade civil, comunidade técnica e academia). A falta de interconectividade entre esses blocos indica baixa capacidade de diálogo transversal, o que pode dificultar a criação de consensos sobre limites éticos e jurídicos no uso de hacking por parte do Estado. Ao mesmo tempo, reforça a necessidade de mecanismos de participação mais inclusivos e transparentes.

6. Percepções e perspectivas sobre o hacking governamental

As entrevistas realizadas neste estudo revelam um conjunto diverso de percepções, caracterizado por diagnósticos convergentes sobre a opacidade do tema e por divergências quanto às prioridades de enfrentamento e constituem uma nova fonte de dados, distinta do levantamento utilizado para a ARS. Esse cenário reforça a importância de uma leitura articulada entre os aspectos técnicos, jurídicos e operacionais envolvidos.

Foram convidados ao todo 18 pessoas para um universo de 15 entrevistas, com a intenção de assegurar equilíbrio entre diferentes setores — três representantes de cada um dos seguintes segmentos: governo, setor privado, mídia, academia/ comunidade técnica e sociedade civil. Entretanto, houve recusas ou ausência de resposta (uma em tempo hábil) de alguns atores: dois representantes do governo (considerando Executivo, Legislativo e Judiciário), um do setor privado, um da academia/ comunidade técnica e dois da sociedade civil.

As entrevistas utilizadas neste estudo foram conduzidas sob compromisso de confidencialidade. Por isso, os(as) participantes não serão identificados nominalmente, e todos os pronunciamentos foram anonimizados, com destaque apenas para o setor de atuação e um número de referência (por exemplo: Mídia 1, Governo 1, Sociedade civil 1). Essa abordagem visa proteger a identidade dos(as) entrevistados(as) e permitir maior liberdade na exposição de diagnósticos e percepções sensíveis sobre o tema investigado.

6.1. Governança e controles institucionais

Há um consenso entre os entrevistados de que a assimetria informacional favorece a aquisição e o uso de tecnologias de intrusão com baixo grau de controle institucional. Ao mesmo tempo, a compreensão limitada da sociedade sobre privacidade reduz os incentivos à transparência. O risco, entretanto, vai além da interceptação de comunicações: abrange o comprometimento de dispositivos, terceirizações sem mecanismos adequados de auditoria e a dependência de tecnologias estrangeiras, elementos que elevam significativamente a complexidade regulatória e investigativa. Tomadas em conjunto, as entrevistas revelam um cenário de equilíbrio precário entre o sigilo necessário à persecução penal e o dever democrático de transparência, com alertas recorrentes sobre a normalização de exceções sob o argumento de eficiência.

Além disso, a análise aponta uma clivagem institucional entre esferas federais e subnacionais: enquanto o nível federal tende a ter estruturas mais densas de controle, muitos estados operam com menor capacidade institucional e rotinas de contratação mais permissivas, comprometendo a harmonia regulatória. A interação entre jornalismo investigativo, organizações cívicas, academia, comunidade técnica, setor privado e governo constitui um circuito de contrapesos ainda incompleto, marcado pela ausência de métricas públicas padronizadas e falta de mecanismos contínuos de avaliação de proporcionalidade e necessidade. Nesse contexto, os entrevistados destacam a necessidade de fortalecer práticas de documentação, custódia de evidências e publicação de dados agregados sobre aquisição e uso, como forma de reduzir zonas cinzentas e viabilizar auditorias independentes.

Com relação à legitimidade e controle institucional das ferramentas de intrusão, os depoimentos sugerem que legitimidade depende de lastro normativo claro e de governança capaz de comprovar necessidade, adequação e proporcionalidade em cada etapa do ciclo de vida das ferramentas. Isso inclui avaliação prévia, autorização específica e motivada, registros técnicos detalhados, cadeia de custódia verificável e mecanismos de controle posterior com possibilidade de auditoria externa. A referência a ambientes subnacionais “muito mais várzeas” sugere necessidade de parâmetros mínimos nacionais com aplicação uniforme e com sanções por descumprimento. A desconfiança em relação à produção

normativa ordinária aparece em sentimentos de “zero otimismo” no âmbito legislativo, associados à influência de lobby e à dificuldade de consolidar comandos inequívocos para hipóteses excepcionais.

Dessa forma, a tensão entre celeridade investigativa e prestação de contas perpassa todos os relatos dos entrevistados. Há defesa de relatórios públicos periódicos com dados agregados sobre aquisições, tipos de ferramentas, finalidades, indicadores de efetividade e impactos sobre direitos, preservando sigilos legalmente protegidos[22]. Também aparece a demanda por instâncias independentes de supervisão com competência técnica e autonomia para inspeções, bem como por cláusulas de expiração, avaliações de impacto em direitos humanos e auditorias de código e de configuração quando cabível. Essas salvaguardas são apresentadas como instrumentos para reduzir arbitrariedade e para prevenir expansão silenciosa do perímetro de intrusão sem debate público qualificado.

Mídia 1 descreve negativas recorrentes a pedidos de acesso a informações com justificativas de “segredo comercial” e “segurança nacional”, o que impede escrutínio jornalístico e restringe a capacidade de aferir proporcionalidade e necessidade na aplicação de ferramentas de intrusão. A prática de intermediação por “empresas laranja” e por revendedoras que “omitem os nomes das empresas originais ou as tecnologias utilizadas” surge como vetor crítico de assimetria informacional que dificulta fiscalização e responsabilização. Governo 1 reconhece que controles estão em processo de amadurecimento e que transparência sobre finalidade, uso e resultados deve orientar mecanismos de controle prévio e posterior.

Cabe ainda destacar que Governo 1 distingue controle interno e externo, relembra que o debate decisório migra entre Legislativo e Supremo e indica que a transparência sobre finalidade, uso e resultados deve ser operacionalizada em rotinas, com atenção à extensão a entes federativos. Finalmente, Mídia 2 adiciona que o Congresso opera sob “contaminação por lobby” e que comissões de controle muitas vezes se movem pouco, o que torna indispensável a presença de dados

[22] Ressalte-se que essa convergência reflete o recorte de atores ouvidos na pesquisa e não a totalidade do campo. Na análise ARS anterior pode-se registrar resistências a mecanismos de transparência e controle, especialmente em alguns segmentos governamentais e privados, o que evidencia a complexidade do debate.

verificáveis e de coalizões intersetoriais para contrabalançar pressões por flexibilização.

6.2. Impactos sobre direitos e liberdades

As entrevistas apontam efeitos inibidores sobre liberdades de expressão, reunião e imprensa quando ferramentas de intrusão operam em ambientes de baixa previsibilidade. O medo de exposição e de retaliação alcança fontes sensíveis e profissionais que dependem de sigilo para atuação legítima, o que reforça a afirmação de que jornalistas e fontes são “potenciais alvos de hacking governamental”. Somam-se riscos de viés e de discriminação quando integrações massivas de dados ocorrem sem balizas claras, gerando assimetrias que recaem de forma desproporcional sobre populações vulnerabilizadas. O quadro é agravado por indiferença cívica em relação à privacidade sinalizado por diversos entrevistados, com relatos de que pautas de vigilância “vão muito mal” em relação a audiência de veículos de imprensa, o que diminui a pressão social por reformas e preserva incentivos para opacidade.

Além disso, os depoimentos de Sociedade civil 1 e Academia 1/ Comunidade Técnica 1 enfatizam um vazio normativo que fragiliza garantias processuais, pedem parâmetros estritos para o uso estatal de intrusão e associam a proteção criptográfica à própria possibilidade de exercício de liberdades. Já Governo 1 reconhece tensões entre segurança e privacidade, aponta amadurecimento institucional em curso e menciona esforços para formular balizas de finalidade, uso e transparência em instrumentos administrativos, com desafios acrescidos quando a discussão se desloca para entes subnacionais.

Mídia 1 relata que jornalistas e suas fontes passaram a ser tratados como “potenciais alvos de hacking governamental”. Esse cenário fez com que a criptografia de ponta a ponta se tornasse essencial para o exercício do jornalismo investigativo, levando à adoção de práticas mais seguras no trato de informações sensíveis, como o uso prioritário de aplicativos como Signal, a substituição de canais mais vulneráveis e a redução de pontos de exposição ao risco. Na mesma linha, Mídia 2 destaca que a ameaça se agrava em contextos com infraestrutura digital frágil e alto nível de desinformação, especialmente quando esses fatores são

usados para obter ganhos econômicos ou políticos. Nesse ambiente, a proteção digital se torna uma necessidade diária, exigindo desde o uso redundante de VPNs até cuidados físicos específicos para evitar violações.

Sociedade civil 1 sustenta que a ausência de lei orgânica para dados penais e a falta de uma LGPD penal abrem margem para usos abusivos, especialmente no inquérito, quando meios ocultos de obtenção de prova se expandem sem balizas claras e sem integridade assegurada dos sistemas informáticos. Academia 1/ Comunidade Técnica 1 qualifica esses vetores como “risco sistêmico”, já que a quebra seletiva de salvaguardas corrói garantias de todos, e alerta para discursos que criminalizam a criptografia ao associá-la a obstrução de justiça, quando sua função consiste em proteger o espaço de pensamento e de expressão.

Os entrevistados apontam a necessidade de definição de limites substantivos e procedimentais para o uso de intrusão pelo Estado e a urgência de deslocar a discussão de respostas casuísticas para parâmetros estáveis. Mídia 1 defende que é preciso estabelecer “uma linha” que separe usos legítimos de usos excessivos, inclusive quando finalidades declaradas são nobres, e que essa linha não pode aguardar novas crises para ser traçada. Enquanto isso, Sociedade civil 1 propõe balizas “as mais estritas possíveis” e uso em “hipóteses extremas, crimes gravíssimos”, sempre com base legal clara, integridade dos sistemas informáticos, registro padronizado de operações e preservação do contraditório. Finalmente, Academia 1/ Comunidade Técnica 1 reivindica pacote legislativo robusto, com LGPD penal e regras para entrega de dados privados ao Estado, e enfatiza produção de ciência aplicada para orientar decisões judiciais e políticas públicas.

6.3. Criptografia, soberania tecnológica e segurança

Os riscos à soberania digital e à dependência tecnológica ganham destaque quando soluções críticas são adquiridas por meio de contratos opacos, frequentemente mediados por intermediários que ocultam a origem das tecnologias, prática descrita como uso de “empresas laranja”. Esse cenário é agravado pela percepção de que há “passagem de pano” quando os resultados políticos são convenientes, além da ideia de que “todo mundo quer tirar uma casquinha”, o que enfraquece a responsabilização e amplia a tolerância a exceções. A combinação de

baixa transparência, fragmentação federativa e déficit de letramento digital cria um ambiente propício à expansão silenciosa da vigilância, com pouca resistência institucional ou social. Isso gera efeitos cumulativos sobre direitos fundamentais, como a proteção de dados, o devido processo legal e a confiança nas instituições públicas.

No setor privado, Setor Privado 1 defende que os serviços de mensageria devem permanecer privados e que a proteção da criptografia forte é fundamental para garantir a segurança dos usuários e a confiabilidade do ecossistema digital, mesmo sob pressões para flexibilizá-la. Já Setor Privado 2 alerta que, em situações de comprometimento do dispositivo, “pouco importa a criptografia”, pois atacantes buscam acesso direto ao sistema, exigindo camadas adicionais de proteção e práticas de hardening que ultrapassem o ciframento de conteúdo. Mais ainda, Setor Privado 2 reforça que ofensores e Advanced Persistent Threat (APTs) priorizam acesso no nível de dispositivo e que a criptografia, isoladamente, não cobre esse vetor, o que demanda políticas públicas e práticas organizacionais que integrem camadas técnicas e procedimentos auditáveis.

Esse ponto é reforçado por Mídia 2, que destaca como a falta de proteção física e lógica nos ambientes institucionais, somada a terceirizações pouco criteriosas, amplia significativamente a superfície de ataque. Situações como a presença de *backdoors* e dependência de tecnologias externas fora do controle local também agravam o risco.

Ainda em relação à criação de *backdoors*, Setor Privado 1 relata sofrer pressões frequentes para criar acessos excepcionais e desconfigurar sistemas criptográficos. Apesar da resistência, Setor Privado 1 afirma que cumpre ordens legais quando estas não implicam a criação de *backdoors*, desde que haja justificativa de benefício público demonstrado — situação que, ainda assim, acarreta custos tanto para os usuários quanto para a segurança geral do ecossistema. Ainda assim, a criptografia é tratada como um elemento central de segurança e liberdade comunicacional, inserido em uma arquitetura mais ampla que envolve dispositivos, processos e governança técnica. Setor privado 2 defende que a definição de regras

técnicas e de governança centralizada, inspirada em órgãos como CISA e ENISA[23], pode reduzir fragmentação, criar padrões mínimos e aumentar previsibilidade, o que melhora a supervisão e a resposta a incidentes.

A importância da criptografia de ponta a ponta como ferramenta de proteção do jornalismo investigativo é enfatizada por Mídia 1, que a considera essencial para resguardar o sigilo da fonte e garantir a circulação segura de informações sensíveis. Setor Privado 1 também expressa otimismo com ferramentas criptográficas baseadas em princípios matemáticos, que impedem o acesso mesmo por parte dos provedores, garantindo controle total aos usuários, embora isso gere tensões com demandas legais e expectativas de privacidade. Já Setor Privado 2 e Mídia 2 alertam que, diante de comprometimento de dispositivo, ciframento de conteúdo não basta, já que ofensores buscam privilégios de *root* e exploram vetores laterais, exigindo defesa em profundidade que inclua hardening, políticas de atualização, segmentação e práticas seguras de *endpoint*.

Apesar da centralidade da criptografia, os entrevistados concordam que ela não basta por si só. A defesa da segurança digital requer práticas organizacionais robustas, contra medidas físicas e uma governança eficaz dos dados. O alerta recorrente de que “pouco importa a criptografia” quando o dispositivo é invadido reforça a necessidade de uma abordagem sistêmica para proteção digital.

A compreensão pública sobre o tema é limitada. Segundo Mídia 1, a percepção das pessoas é fortemente moldada pela narrativa das grandes empresas, o que dificulta o debate público informado e reforça a urgência de educação digital e transparência técnica. Todos os entrevistados apontam o déficit de compreensão pública, com Mídia 1 relatando que o entendimento do tema é “muito ditado pelo que as empresas, a narrativa pública em torno das empresas passa”, o que torna “tudo muito mais difícil” e reforça a importância de educação digital e de transparência técnica.

[23] CISA (Cybersecurity and Infrastructure Security Agency) é a agência do governo dos Estados Unidos responsável pela proteção de infraestruturas críticas e pela promoção de boas práticas em cibersegurança. ENISA (European Union Agency for Cybersecurity) é a agência da União Europeia voltada para a melhoria da segurança de redes e sistemas de informação nos Estados-membros, fornecendo orientação, apoio técnico e políticas de cibersegurança.

Sociedade Civil 1 e Academia1 / Comunidade Técnica 1 qualificam a criptografia como pilar da democracia e da liberdade individual, mas alertam que a fragmentação regulatória favorece soluções excepcionais e compromete a aplicação de garantias. Já Governo 1 reconhece a criptografia como atributo legítimo de serviços digitais e como direito, inclusive com amadurecimento social e estatal sobre o tema, e sugere que o debate deve levar em conta a diversidade de ferramentas e níveis de invasividade, de modo a calibrar controles proporcionais.

Por fim, os relatos introduzem uma dimensão de economia política no debate criptográfico. De um lado, há pressões constantes por acessos excepcionais; de outro, existem incentivos de mercado para proteger a privacidade de forma mais robusta. A visão de que “a cripto é apenas uma camada” reforça a necessidade de integrá-la a práticas técnicas e organizacionais seguras. Já a afirmação de que “o limite é o técnico” revela a importância de projetar sistemas nos quais o acesso extraordinário simplesmente não seja possível, evitando assim que a exceção se torne a regra e preservando a integridade do ecossistema digital como um todo.

6.4. Recomendações dos atores chave

As recomendações colhidas nas entrevistas convergem em três eixos principais: (i) ampliação da transparência ativa, (ii) fortalecimento de salvaguardas técnicas e jurídicas, e (iii) aprimoramento da capacidade institucional de controle.

Mídia 1 defende o banimento imediato da prática de intermediação por “empresas laranja”, como medida essencial para revelar a origem das tecnologias utilizadas, identificar os beneficiários finais e permitir fiscalização pública efetiva. A mesma fonte reconhece que regulações por meio de portarias administrativas podem representar “um bom primeiro passo”, mas alerta que, sem proibições claras, tendem a funcionar apenas como “pano quente”. Por isso, reforça a necessidade de processos legislativos com comandos inequívocos.

Mídia 2 propõe a criação de grupos intersetoriais permanentes de resposta a incidentes cibernéticos, com participação do Ministério Público, universidades, setor privado, sociedade civil, Polícia Federal e organizações independentes. Também recomenda a elevação dos padrões de segurança em infraestruturas críticas e a

implementação de políticas obrigatórias de uso de ferramentas seguras no setor público.

Setor Privado 1 defende a importância de uma educação pública ampla sobre os fundamentos da criptografia, especialmente seus princípios matemáticos, bem como a adoção de padrões de transparência voltados à comunidade técnica. A empresa também defende mecanismos de governança fortes, que garantam que nem mesmo funcionários internos dos provedores tenham acesso às comunicações protegidas. Além disso, recomenda o engajamento em coalizões multissetoriais, como a Global Encryption Coalition[24], para resistir a narrativas que associam proteção digital à impunidade.

Setor Privado 2 sugere a criação de um órgão centralizado de cibersegurança, responsável por definir, aplicar e fiscalizar regras técnicas. Entre as propostas estão: adoção de padrões únicos de configuração e de criptografia, fortalecimento de validações independentes de algoritmos e implementações, e reconhecimento de que a criptografia é apenas "uma das camadas" de proteção, devendo ser complementada por outras medidas.

Sociedade Civil 1 recomenda a aprovação de legislação estruturante, como uma LGPD penal, e regras estritas para o uso estatal de técnicas de intrusão, restritas a hipóteses excepcionais. Defende também garantias de integridade dos sistemas, litigância estratégica para consolidar precedentes protetivos, criação de canais de denúncia contra práticas abusivas e formações voltadas à magistratura e ao público em geral.

Academia 1/ Comunidade Técnica 1 propõe um programa integrado de ação legislativa e produção de conhecimento aplicado, com foco na formulação de critérios claros de necessidade, adequação e proporcionalidade, além da implementação de métricas auditáveis de impacto sobre direitos. Sugere ainda parcerias com organizações especializadas para subsidiar decisões judiciais e políticas públicas com base em evidências.

[24] A Global Encryption Coalition é uma iniciativa internacional que reúne organizações da sociedade civil, setor privado, setor técnico e academia para promover e defender o uso da criptografia forte no mundo todo, contrapondo-se a propostas de enfraquecimento de sistemas de segurança digital.

Governo 1 destaca a importância de uma procedimentalização clara dos mecanismos de controle, incluindo definição de quando, como e por quem a fiscalização deve ser exercida. Defende a distinção entre controle prévio e posterior e enfatiza a transparência sobre finalidade, uso e resultados, como forma de equilibrar agilidade investigativa e prestação de contas.

Por fim, de maneira transversal, os depoimentos ressaltam a necessidade de um processo de responsabilização contínuo, imparcial e independente de mudanças no cenário político. Apontam ainda a urgência de combater a leniência institucional diante de práticas irregulares ou politicamente convenientes, bem como a importância de promover uma educação pública estruturada desde os níveis escolares iniciais. Essa formação deve consolidar uma cultura de proteção capaz de sustentar, no longo prazo, políticas públicas estáveis e aderentes aos direitos fundamentais.

7. Considerações finais e recomendações

O estudo evidencia que o ecossistema do hacking governamental no Brasil opera de forma altamente centralizada, com forte protagonismo do Estado e participação estratégica, porém assimétrica, do setor privado. Ao mesmo tempo, revela a marginalização de atores da sociedade civil, academia, comunidade técnica e mídia, que enfrentam obstáculos significativos para influenciar políticas públicas, mesmo atuando em defesa de direitos fundamentais.

A combinação entre opacidade institucional, lacunas normativas e baixa densidade intersetorial cria um ambiente de risco para a democracia, no qual práticas excepcionais podem se tornar silenciosamente normativas. A governança atual carece de mecanismos robustos de controle, transparência e prestação de contas. A ausência de salvaguardas claras amplia a possibilidade de abusos, sobretudo em contextos de baixa capacidade institucional e dependência tecnológica externa.

Por isso, uma abordagem sistêmica que integre regulação, fiscalização e capacitação pública é essencial para garantir que tecnologias de intrusão não comprometam direitos fundamentais nem corroam o Estado de Direito. Diante desse cenário, o estudo propõe um conjunto de recomendações urgentes para reequilibrar

o uso estatal de tecnologias intrusivas e fortalecer a governança democrática do setor. Entre elas destacam-se:

Recomendações

1. **Institucionalizar mecanismos intersetoriais permanentes de governança**
   Criar instâncias formais e contínuas de diálogo entre governo, setor privado, academia, comunidade técnica e sociedade civil para a formulação, monitoramento e revisão de políticas públicas sobre hacking governamental, com representatividade equilibrada e participação multissetorial vinculante.

2. **Aprovar um pacote legislativo robusto e orientado à soberania digital**
   Avançar em marcos legais que fortaleçam a proteção de dados e regulem de forma clara o uso de tecnologias de intrusão, estabelecendo critérios objetivos de necessidade, legitimidade e proporcionalidade e exigências de controle prévio e posterior com base em registros técnicos auditáveis. Nesse sentido, a consolidação de uma LGPD penal e de normas específicas deve ser articulada com a promoção da soberania digital, de forma a reduzir dependências externas e assegurar que as soluções adotadas respeitem os direitos humanos e fundamentais e fortaleçam a autonomia tecnológica do país.

3. **Combater a opacidade nas contratações públicas**
   Banir a contratação com empresas laranja e empresas envolvidas na violação de direitos humanos e liberdades civis. Atualização de portais de transparência de maneira a garantir uma transparência total sobre fornecedores, tecnologias contratadas, cadeias de responsabilidade e finalidades de uso, permitindo auditorias independentes e fiscalização multissetorial. Diante da crescente distribuição de ferramentas e recursos para estados e municípios, implementar um controle rigoroso sobre esse fluxo, assegurando o rastreamento do tráfego, a legitimidade, necessidade e a proporcionalidade no uso das tecnologias conforme as capacidades e funções dos órgãos.

4. **Desenvolver métricas públicas e auditáveis de uso e impacto**
   Publicar relatórios de transparência periódicos com dados sobre aquisições, finalidades, frequência de utilização, efetividade, impacto sobre direitos, riscos detectados e ações corretivas, garantindo *accountability*.

5. **Fortalecer o controle *ex-ante* e *ex-post* do uso de ferramentas de intrusão**
   Criar sistemas de autorização judicial específica e motivada, com registros obrigatórios, cadeia de custódia verificável e supervisão técnica por órgãos independentes, além de comissões de controle com transparência pública e poder efetivo. Garantir também o direito a remédios eficazes contra o uso ilegal ou abusivo desse tipo de tecnologia.

6. **Consolidar a segurança cibernética como um direito e pilar democrático**
   Fortalecer a segurança cibernética de forma abrangente, combinando uma defesa pela criptografia forte, a proibição do uso de backdoors, a exigência de padrões mínimos de proteção em dispositivos e sistemas, e a promoção de educação pública para ampliar a compreensão social sobre a privacidade e os riscos correlatos.

7. **Fomentar produção científica e cooperação com centros de pesquisa**
   Estimular parcerias entre o poder público, a comunidade técnica, a comunidade acadêmica e organizações de pesquisa independentes para subsidiar decisões com evidências, construir *benchmarks* regulatórios e desenvolver inovações em segurança, privacidade e governança digital.

Instituto de
Pesquisa em
Direito & Tecnologia
do Recife

Internet Society
Capítulo Brasil