Decálogo de Recomendações sobre

Direitos Digitais e Produção de Provas

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

INSTITUTO DE PESQUISA EM DIREITO & TECNOLOGIA DO RECIFE

COALIZÃO DIREITOS NA REDE

Decálogo de Recomendações sobre Direitos Digitais e Produção de Provas

Autoria

Ana Bárbara Gomes Pereira
André Ramiro
Gustavo Ramos Rodrigues
Pedro Amaral
Victor Barbieri Rodrigues Vieira

Consultoria

Carina Quito
Paulo Renã da Silva Santarém

Revisão externa

Luiza Couto Chaves Brandão
Raquel Lima Saraiva

Projeto gráfico, capa e diagramação

Felipe Duarte

Realização

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

INSTITUTO DE PESQUISA EM DIREITO & TECNOLOGIA DO RECIFE

Apoio

COALIZÃO DIREITOS NA REDE

Apresentação

Apesar de avanços em regulações sobre a garantia de direitos fundamentais no contexto do uso da Internet e de novas tecnologias - como a promulgação da Lei Geral de Proteção de Dados (LGPD), do Marco Civil da Internet e o Decreto 8.771/2016 - o Brasil caminha lentamente na criação de uma moldura legal que sedimente procedimentos protetivos a direitos no contexto de investigações criminais. A falta de melhor delineamento sobre, por exemplo, bases legais e mecanismos de proporcionalidade para o uso de novas tecnologias na produção de provas abre margem para excessos de vigilância, arbitrariedades e prejuízos à eficácia da ação penal. Ao mesmo tempo, a conjuntura jurídica e social põe em risco a segurança do ecossistema conectado e a sociedade que o compõe.

O ano de 2021 já foi marcado por, pelo menos, duas articulações legislativas críticas para o estabelecimento de previsões legais para a produção de provas no âmbito penal: a Reforma do Código de Processo Penal e o Anteprojeto de Lei da LGPD Penal. Essas ações são sintomáticas de uma demanda capitaneada por forças de investigação, como o Ministério Público e a Polícia Federal, para que novos mecanismos de vigilância, interceptação e extração de dados sejam inseridos nas rotinas investigativas. Paralelamente, também traduzem a urgência para que uma necessária cobertura aos direitos fundamentais – cujos instrumentos protetivos deverão ir além das citadas iniciativas - seja conferida à esfera regulatória processual penal. Esses dois campos, portanto, não se dissociam e devem ser priorizados na agenda política nacional.

Será preciso que a regulação adotada observe, pelo menos, três eixos relativos à garantia de direitos fundamentais diante das novas tecnologias nesse campo: o estreito diálogo com o disciplina de proteção de dados que enderece, especificamente, a esfera das investigações criminais; salvaguardas à criptografia forte para os sistemas de comunicação e armazenamento de dados; e que o uso de ferramentas de exploração de vulnerabilidades e extração de dados seja objeto de debates públicos amplos, participativos, democráticos e multissetoriais, além de regulação detalhada e específica. Além disso, aponta-se a necessidade de fiscalização por uma entidade estrategicamente posicionada no sistema judicial brasileiro, como forma de promover regulamentação aos procedimentos investigativos e resguardar as garantias constitucionais.

Pensando nisso, o Instituto de Referência em Internet e Sociedade (IRIS) e o Instituto de Pesquisa em Direito e Tecnologia do Recife (IP.rec), como apoio da Coalizão Direitos na Rede – rede que reúne mais de 45 organizações acadêmicas e da sociedade civil em defesa dos direitos digitais - elaboraram dez recomendações que deverão ser observadas por presentes e futuras iniciativas legislativas que busquem regular procedimentos investigativos para a produção de provas. As recomendações são construídas tendo por base o instrumental jurídico e conceitual de legislações nacionais já em vigor, princípios internacionais de direitos humanos e diretrizes técnicas que prevejam um eficaz e necessário nível de segurança aos indivíduos e à coletividade diante do uso de tecnologias no processo investigativo penal.

Com isso, esperamos qualificar o debate e oferecer um conjunto de referências a formuladores de políticas públicas, como parlamentares e assessorias, entidades investigativas e de segurança pública, peritos forenses, bem como a organizações da sociedade civil, pesquisadores e especialistas em tecnologia.

1. Provedores de serviços de Internet não devem ser obrigados a implementar soluções que reduzam a segurança de seus sistemas, tampouco devem ser penalizados por impossibilidades técnicas inerentes às medidas de segurança fornecidas.

A confiança no ambiente digital é imperativa para sistemas bancários, de saúde, segurança nacional e demais áreas de interesse público. Ainda, a segurança da informação em sistemas digitais é um requisito para proteção dos direitos humanos, notoriamente o direito à privacidade e à liberdade de expressão online.

Recentemente, ataques cibernéticos no Brasil cresceram em uma taxa alarmante.[1] Serviços protegidos por técnicas criptográficas são utilizados pela vasta maioria da população conectada no país. Assim, medidas legislativas que potencialmente minam a segurança em serviços digitais representam um elevado grau de risco para os direitos dos cidadãos, a economia digital e a capacidade de inovação brasileira[3].

Em 2018, a chamada "Resolução da Internet" do Conselho de Direitos Humanos das Nações Unidas, da qual o Brasil é signatário, foi atualizada[4], passando a defender o uso de tecnologias para proteger a confidencialidade de comunicações digitais. Técnicas de criptografia e anonimato digital são citadas como medidas importantes para a manutenção dos direitos humanos nesse meio. Similarmente, na resolução "The Right to Privacy in the Digital Age"[5], o Conselho de Direitos Humanos incentiva empresas a implementarem técnicas de proteção à confidencialidade das comunicações, incluindo medidas de criptografia. Recomenda que Estados não interfiram em tais recursos e alinhem quaisquer restrições eventuais aos parâmetros internacionais direitos humanos.

Obrigações de vulneração da criptografia ou de fornecimento de assistência técnica por provedores enfraquecem o nível de segurança geral dessas aplicações e impactam toda a base de usuários desses serviços. Similarmente, a garantia de segurança de seus sistemas que inviabiliza determinada obrigação não deve resultar em multas ou demais penalidades a serviços digitais em decorrência de incapacidades técnicas inerentes às tecnologias empregadas por eles para garantir a segurança de seus sistemas.

A recomendação se alinha ao entendimento que vem sendo construído pelo Poder Judiciário no Brasil. O Ministro Edson Fachin e a Ministra Rosa Weber do Supremo Tribunal Federal (STF), ao relatarem e votarem no julgamento da ADPF 403 e da ADI 5527, consideraram inconstitucionais as decisões que determinam a quebra do sigilo de comunicação em aplicativos de mensagens instantâneas. Embora as ações ainda estejam sob pedido de vista, a tese fundamentou pelo menos duas decisões no âmbito do Superior Tribunal de Justiça.

Prevaleceu a tese do Ministro Ribeiro Dantas, no exame do RMS 60.531, no âmbito da 3ª Seção, em 09 de dezembro de 2020,6 bem como do RESP 1.871.695, julgado pela 5ª Turma, em 04 de maio de 2021,7 para anularem a aplicação de sanção pecuniária à empresa que, em virtude do uso de criptografia de ponta-a-ponta, descumpre ordem judicial de interceptação. Ressaltou-se ser impossível cumprir a ordem judicial em razão do impedimento fático criado pela criptografia e que os benefícios dessa tecnologia superam em muito seus eventuais danos.

2. Todas as operações de tratamento de dados pessoais para fins de segurança pública e persecução penal devem ser expressamente previstas em lei e vinculadas aos princípios da Lei Geral de Proteção de Dados Pessoais, mesmo que ainda não contem com a necessária previsão e disciplina em lei específica.

A esfera penal é o poder estatal mais intrusivo e detém o maior potencial lesivo para os cidadãos. Por isso, são necessários critérios de proteção de dados pessoais em qualquer matéria penal, evitando usos indevidos e consequências negativas para a sociedade. A adequação das matérias penais é urgente quando observado o nível de proteção de dados pessoais necessário para cooperação efetiva das agências brasileiras com instituições internacionais, como Europol e Interpol. O não atendimento a parâmetros internacionais de proteção de dados em investigações criminais compromete a cooperação jurídica internacional e, consequentemente, a aplicação da lei no Brasil.

Como previsto no artigo 4º, §1º, da Lei Geral de Proteção de Dados (LGPD, Lei Nº 13.709), a proteção de dados em matéria penal requer legislação específica com "**medidas proporcionais e estritamente necessárias ao atendimento do interesse público, observados o devido processo legal, os princípios gerais de proteção e os direitos do titular** previstos nesta Lei". Assim, o STF reconheceu, na ADI 6.390, sobre o compartilhamento de dados pelas empresas prestadoras de serviços de telefonia ao Instituto Brasileiro de Geografia e Estatística, a proteção de dados como direito fundamental autônomo.

Enquanto esta lei específica, o Brasil não se alinha aos principais parâmetros internacionais de proteção de dados pessoais na esfera penal. Dispõe tão somente de um "direito das quebras de sigilo"[8], isto é, um conjunto de hipóteses legalmente previstas para o afastamento do sigilo de certas categorias de dados, como bancários e de comunicações privadas. Como remédio imediato a essa situação recomenda-se que qualquer projeto de lei que afete dados pessoais no âmbito da segurança pública e da persecução penal deve, necessariamente, observar os princípios gerais da LGPD. O meio e a extensão da coleta de dados pessoais armazenados em dispositivos pessoais ou servidores de terceiros também devem obedecer aos princípios de proporcionalidade, finalidade e minimização da coleta de dados.

Igual atenção deve ser direcionada para todas as etapas da cadeia de custódia das provas digitais obtidas durante a instrução penal, desde a obtenção. Além de obtido em observância dos princípios da proteção de dados pessoais, o conteúdo probatório deve ser submetido a obrigações de guarda segura e adequada, bem como devidamente eliminado das bases de dados estatais quando tiver cumprido sua finalidade persecutória e, portanto, não for mais necessário para a efetividade do processo.

3. Dados pessoais tratados no contexto da produção de provas no processo penal devem, durante toda a cadeia de custódia, ser protegidos com as melhores técnicas de segurança da informação disponíveis como forma de impedir incidentes de segurança, violação aos direitos dos titulares dos dados e, consequentemente, comprometimento dos processos investigativos.

A rigidez dos protocolos de segurança de dados pessoais é medida preventiva basilar no estabelecimento de arquiteturas sólidas de segurança da informação. No campo penal, o comprometimento do sigilo, integridade ou disponibilidade dos dados pessoais custodiados pode gerar prejuízos tanto à eficácia da persecução penal quanto aos bens jurídicos de vítimas e suspeitos de crimes, como a privacidade, a liberdade de locomoção e até mesmo a vida. Ainda, o comprometimento da segurança pode prejudicar a confiabilidade das provas e a lisura da persecução penal.

O sigilo dos dados na cadeia de custódia, por exemplo, atravessa garantias constitucionais: o vazamento de dados do acusado e dos termos de sua acusação compromete o devido processo legal e seu amplo direito de defesa. Ainda, prejudica a presunção de inocência, pois dados não constantes na acusação podem afetar a formação de juízo durante o processo e influenciar a opinião pública; um membro do programa de proteção à testemunha[9] pode ter sua localização acessada por agentes criminosos, comprometendo sua integridade física. Favorecer a segurança da informação é fundamental no Brasil, que é o quarto país com mais senhas de órgãos públicos vazadas[10].

Incidentes de segurança envolvendo acessos indevidos igualmente podem afetar a integridade dos dados custodiados que serviriam à instrução penal e influenciar no mérito da acusação. Informações alteradas, retiradas de contexto ou alvos de outras formas de interferência acidental ou maliciosa podem enviesar o juízo criminal e afetar ambas as partes do processo e a eficácia do poder investigativo do Estado. Da mesma forma, a insegurança na cadeia de custódia pode pôr em risco a disponibilidade de informações[11] fundamentais à instrução penal, que podem ser perdidas, extraviadas ou sequestradas, resultando em absolvições ou condenações injustas.

Por fim, o respeito à segurança na custódia de provas digitais favorece a prestação de contas que comprove, de forma suficientemente transparente, as medidas e técnicas gerenciais e tecnológicas adotadas para coleta, armazenamento, acesso, compartilhamento e descarte dos dados. Em eventual auditoria por parte de órgão fiscalizador competente, o potencial de demonstração dessas informações será essencial para se medir o grau de responsabilização do agente investigativo e, assim, prestar contas à sociedade.

4. O princípio da não responsabilização da rede deve ser protegido, sob risco de dano aos direitos dos cidadãos, à inovação e à livre concorrência.

O ecossistema de provedores de serviços de Internet é complexo e heterogêneo. Sua composição abriga uma grande diversidade de agentes com variadas capacidades econômicas, naturezas jurídicas, funções desempenhadas, localizações geográficas e tipos de serviços prestados. Essa complexidade é reconhecida pelas principais normas que afetam a governança da Internet no país. O Marco Civil da Internet distingue provedores de conexão - aqueles que fornecem o acesso à Internet em geral - e provedores de aplicação - aqueles que fornecem funcionalidades específicas acessíveis por meio da rede, como sites ou aplicativos determinados -, e determina respectivas obrigações. Similarmente, a LGPD prevê a edição de normas e procedimentos simplificados e diferenciados para a adequação de micro e pequenas empresas.

Esse reconhecimento preserva o papel dos provedores de conexão enquanto intermediários que permitem a circulação dos pacotes de dados entre usuários e aplicações, sem que lhes sejam atribuídas obrigações relacionadas ao conteúdo dos pacotes trafegados. É por essa razão que o Marco Civil os proíbe de armazenar os registros de acesso a aplicações de Internet (art. 14) e estabelece sua não responsabilização por danos decorrentes de conteúdos gerados por terceiros (art. 18). Nesse espírito, o princípio sétimo[12] da Resolução CGI.br/RES/2009/003/ do Comitê Gestor da Internet no Brasil afirma que "o combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos".

Proteger o delicado equilíbrio do ecossistema de governança da Internet é essencial para a manutenção de uma Internet livre, aberta, segura e inovativa. Isso significa não compelir agentes situados nas camadas inferiores da Internet a coletar e armazenar mais dados do que o necessário para o exercício de suas funções, o que feriria os princípios da não responsabilização, da necessidade (LGPD, Art. 6º, III), da privacidade, da proteção de dados pessoais e da responsabilização de agentes conforme suas atividades (MCI, Art. 3º, I, II, VI). Além disso, geraria custos excessivos de processamento e armazenamento a micro e pequenos provedores de conexão, os quais equivalem a 91% do total brasileiro13, ferindo sua capacidade competitiva diante dos grandes e médios provedores e aumentando possivelmente a concentração de mercado.

5. Dados pessoais tratados para fins de segurança pública devem gozar do mesmo nível de proteção, independentemente de estarem em fluxo ou em repouso ou de serem ou não conteúdos de comunicações.

A natureza dos serviços tecnológicos que envolvem o armazenamento de dados e/ou comunicações realizadas via Internet torna difícil, cada vez mais, distinguir dados em trânsito e em repouso para fins de proteção legal. Além disso, não somente o sigilo do conteúdo de comunicações em fluxo é sensível, mas também (ou ainda mais) é reveladora a diversidade do conjunto de dados armazenados sobre um indivíduo, incluindo o conteúdo de comunicações pretéritas. A multiplicidade de aplicações tecnológicas usadas cotidianamente, o barateamento exponencial do armazenamento e mesmo as previsões legais para a retenção de dados são desafios crescentes para a autodeterminação informativa. A proteção ao sigilo constitucional aos dados e comunicações deve, portanto, ser atualizada.

A práxis contemporânea dos processos investigativos criminais revela uma centralidade de dados armazenados, por exemplo, em nuvem (como fotos, vídeos, arquivos, históricos de busca e localização) ou em dispositivos pessoais em detrimento da interceptação de comunicações em tempo real, como as telefônicas. Isso amplia a centralidade da proteção de dados no campo criminal - atualmente desamparada - independente de estarem ou não em trânsito ou de dizerem respeito ou não ao conteúdo de comunicações.

Como consequência, metadados também merecem plena guarida legal dado seu potencial de revelar perfis comportamentais e outras informações sensíveis sobre indivíduos e coletividades. Por isso, um corolário geral para proteção de dados, na esfera penal, é urgente e necessário. Essa compreensão deve ser norteada em conformidade com princípios e disposições já constantes no ordenamento jurídico brasileiro atinente ao uso de Internet, novas tecnologias e proteção de dados pessoais.[14]

Diante da ostensiva violação à privacidade inerente à coleta de dados para fins de investigação criminal, considerados os bens jurídicos envolvidos, como a vida e a liberdade de locomoção, apenas o mínimo necessário a uma instrução criminal previamente delimitada deve ser coletado. Para isso, as bases legais para a busca e apreensão em eventual regulação para a produção de provas digitais devem ser modernizadas e prever salvaguardas, baseadas em direitos fundamentais, como a proteção aos dados pessoais, à privacidade dos titulares e a seus direitos conexos.

6. A institucionalização de ferramentas e práticas que potencialmente afetam os direitos digitais deve ter amplo debate prévio, com ativa participação dos múltiplos setores da sociedade.

Qualquer alteração no quadro regulatório referente à produção de provas digitais deve ser precedida por amplo debate público, democrático, multissetorial e participativo, especialmente no que diz respeito à disseminação de ferramentas tecnológicas na sociedade brasileira.

O Brasil tem experiências bem sucedidas do debate de mérito de leis de forma participativa, como a LGPD e o MCI, gestado desde os debates multissetoriais do Comitê Gestor da Internet para a redação dos "Princípios para a Governança e Uso da Internet no Brasil". Entre esses princípios, consta, inclusive, o da governança democrática e colaborativa: "A governança da Internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva". Essas leis colocaram o país em posição de destaque no cenário da governança da Internet global por sua maturidade técnica, base em direitos civis e construção participativa.

A discussão sobre o uso de ferramentas digitais para fins de investigação criminal não é um consenso e qualquer iniciativa que objetive a sua institucionalização deve considerar seus riscos e fortalecer os direitos digitais coletivos. É alto o grau de invasividade à privacidade e de fragilização de sistemas informáticos provocados por novas tecnologias de vigilância, como ferramentas de extração de dados e invasão de sistemas por força bruta. O uso dessas práticas pode ser subvertido para fins de perseguição de dissidentes. A institucionalização de rotinas dessa natureza deve ser amadurecida mediante processos de oitiva e consulta pública suficientemente participativos.

Há um risco considerável de que tecnologias de vigilância fujam ao controle de entidades governamentais ou mesmo que vulnerabilidades sejam exploradas por agentes maliciosos, acarretando riscos estruturais à segurança da sociedade, aos agentes econômicos e à própria segurança nacional. Somente um debate cauteloso e participativo permite avaliar os riscos e potencialidades de tais medidas e a conveniência de institucionalizá-las, sob o risco de permitir a consolidação de seu uso indevido em contextos exploratórios, e de endossar práticas vigilantistas que conflitam com o direito à privacidade, os direitos humanos e garantias fundamentais.

7. A coleta remota de dados armazenados em dispositivos de uso pessoal só deve ser admitida como meio probatório em último caso, em hipóteses excepcionais expressamente previstas em lei específica, que estipule critérios objetivos de atendimento aos princípios da necessidade e proporcionalidade, sob supervisão pública e salvaguardas efetivas.

O uso de técnicas e ferramentas destinadas a coletar remotamente dados armazenados em dispositivos de uso pessoal pelas instituições de segurança pública tem sido objeto de crescentes preocupações entre especialistas e formuladores de políticas. Por vezes agrupadas sob o conceito de hacking governamental, essas práticas apresentam o potencial de violação excessiva da intimidade dos titulares para além do necessário à persecução penal, além de risco ao devido processo legal e dano à presunção de inocência.

Ainda, sua capacidade lesiva carrega enorme risco democrático de instrumentalização política para monitoramento e perseguição de dissidentes, ativistas, minorias sociais e defensores de direitos humanos. A extensão de tais riscos foi exemplificada pelo escândalo, de 2021, envolvendo o uso indevido do software Pegasus para monitoramento e extração de dados de ativistas de direitos humanos, jornalistas e advogados em mais de 50 países[15]. A ferramenta permitia a extração de mensagens, fotos e e-mails, além da gravação de chamadas e ativação oculta de câmeras e microfones.

A esse respeito, o Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão demonstrou preocupação com a tendência dos Estados de positivar o uso de hacking governamental através de "linguagem vaga e ambígua, que fornecem às autoridades poderes amplos com supervisão externa mínima"16. Por essa razão, recomenda expressamente que esse recurso seja utilizado somente em casos excepcionais, presentes os requisitos de previsão legal expressa, objetivo legítimo, proporcionalidade relativa aos objetivos pretendidos e inexistência comprovada de outro meio menos gravoso. Ainda, sugere que a análise desses requisitos seja realizada casuisticamente por um órgão judicial independente e imparcial.

No mesmo sentido, salvaguardas adicionais efetivas ante eventuais abusos devem estar previstas, como a reserva absoluta de jurisdição e a obrigação de reportar a uma autoridade supervisora competente caso uma operação de hacking governamental exceda o escopo de sua autorização judicial original[17]. Adicionalmente, recomenda-se parâmetros para limitação temporal de coleta de dados, prazos legais para retenção e posterior eliminação do conteúdo obtido quando este não mais for essencial para a manutenção da justiça.

Com base nos requisitos dos arts. 2 e 4 da Lei 9.296/96, o uso de tais ferramentas só deve ser possível quando forem atendidos de indícios razoáveis de autoria ou participação dos atingidos na infração penal, inexistência de outros meios para produção de prova e necessidade da medida à apuração da infração penal com base em elementos concretos da investigação - preferencialmente a indicação exaustiva de diligências já realizadas e os respectivos resultados. As hipóteses dessas medidas devem ser limitadas à persecução de infrações penais gravíssimas legalmente enumeradas, cuja persecução justifique tamanha gravidade da medida.

8. O processo de contratação de ferramentas ou serviços de interceptação, extração, coleta e análise de dados de dispositivos eletrônicos, remoto ou não, para fins de investigação criminal, deve atender aos princípios da administração pública, exigida transparência sobre o uso e auditabilidade da ferramenta ou serviço, bem como a reputação do agente econômico no âmbito dos Direitos Humanos, proibida a contratação sigilosa e a dispensa de licitação.

Antes de serem consideradas alternativas viáveis à produção de provas, ferramentas de extração, coleta, análise e interceptação de dados de dispositivos eletrônicos constituem tecnologias de vigilância que oferecem elevado grau de pervasividade e envolvem, necessariamente, a violação da privacidade e a exploração de brechas de segurança que podem danificar serviços e produtos,[18] bem como afetar bilhões de usuários.

O banimento, moratória ou proibição da contratação de ferramentas de extração, coleta, análise e interceptação de dados de dispositivos eletrônicos são amplamente defendidos por especialistas e entidades internacionais de direitos humanos[19] e organismos multilaterais. Em 2019, o então Relator para a Liberdade de Expressão e Opinião da ONU, David Kaye, pediu a moratória da venda, transferência e uso de ferramentas do gênero,[20] por sua frequente associação das violações aos direitos humanos e perseguição de dissidentes políticos e jornalistas em regimes autoritários, inclusive com risco à vida.[21]

Considerada a restrição e excepcionalidade de seu uso, sua contratação, compra ou licenciamento devem passar por amplo escrutínio, atender a critérios pré-determinados e aos princípios da administração pública, com base no Art. 37 da Constituição Federal, aplicáveis ao conjunto de tecnologias associadas ao processo penal. Por isso, o processo administrativo deverá justificar suficiente necessidade para embasar a contratação, fundamentada sua proporcionalidade e comprovado que o instrumento seria o último recurso disponível à entidade investigativa. Essa diretriz é respaldada pelo regime pré-definido na LGPD, art. 4º, § 1º, à legislação sobre o tratamento de dados pessoais para fins de segurança pública.

Considerada a probabilidade de que as provas produzidas por tais expedientes sejam fundamento de condenações na esfera criminal, é imprescindível que a administração pública exija, no processo de contratação, a auditabilidade da tecnologia. Caso contrário, além da possibilidade de contestação da integridade da prova em juízo, afetando a cadeia de custódia e incorrendo em nulidade do processo e ineficácia do trabalho investigativo,[22] será violado o direito constitucional ao contraditório e ampla defesa previsto no Art. 5, LV, da Constituição Federal.

Além disso, o trâmite de contratação dos referidos serviços e ferramentas sem chamada pública de licitação distancia-se de critérios específicos que a administração pública poderia exigir dos agentes econômicos,[23] como os listados acima. Isso afasta a transparência do processo do ponto de vista do acesso à informação, sobrepõe as regras do mercado privado de tecnologias de vigilância em detrimento do interesse público e abre margem a arbitrariedades e a seu uso para fins políticos[24]. Por isso, recomenda-se que, nos casos excepcionais que justifiquem a contratação, o processo ocorra mediante licitação pública e acessível, conforme princípios e procedimentos da Lei de Licitações e garantia de transparência aos atos administrativos.

9. As atividades investigativas que objetivem a produção de provas mediante meios tecnológicos que ofereçam riscos a direitos deverão estar sujeitas à fiscalização, supervisão e a diretrizes administrativas instituídas pelo Conselho Nacional de Justiça (CNJ).

Modelos de governança de novas tecnologias passam pela instituição de instâncias administrativas imparciais e especializadas que atuem nos processos de normatização e fiscalização de procedimentos de tratamento de dados pessoais. São ainda mais prementes a supervisão e o monitoramento de tecnologias de vigilância e produção de provas na esfera investigativa criminal, que oferecem consideráveis chances de impactos a direitos.

O CNJ, responsável pela observação aos princípios da administração pública por parte das entidades do sistema de justiça (Art. 103-B, § 4º, inciso II, da Constituição Federal), coloca-se em posição estratégica para garantir salvaguardas aos direitos fundamentais em expedientes investigativos. Além de ser destinado à promoção de controle e transparência, possui pluralidade representativa em sua composição e dispõe de estrutura financeira, administrativa e pessoal para a finalidade.

Considerando que o estabelecimento de políticas de segurança pública encontra diretrizes administrativas variadas em níveis estaduais, o CNJ oferece a possibilidade de uniformizar procedimentos a nível nacional, por exemplo, em processos de contratação e uso de tecnologias de vigilância e destinadas à produção de provas, parâmetros de segurança da informação e integridade da cadeia de custódia. O poder regulamentar do CNJ dialoga e articula com corregedorias da polícia locais, secretarias de segurança pública, varas criminais estaduais, Ministério Público e outras instâncias judiciárias de responsabilidades perante a justiça criminal. Esse modelo fortalece a padronização de procedimentos e dá sustentabilidade, a longo prazo, às salvaguardas processuais e à cadeia de custódia de provas.

Da mesma forma, poderá instituir rotinas de produção de estatística sobre o uso de tecnologias de alto risco, instruindo o juízo de magistrados e oferecendo possibilidade de transparência perante a sociedade.[25] Adicionalmente, poderá estabelecer procedimentos administrativos necessários à mensuração de eficácia, proporcionalidade e legalidade sobre o uso de tecnologias de alto risco aos direitos fundamentais, como aquelas que visam a suspensão do sigilo dos dados e comunicações, direito fundamental sedimentado no art. 5º, inciso XII da Constituição Federal.

A atuação do CNJ diante do histórico de transgressões dos poderes investigativos brasileiros por ferramentas de suspensão do sigilo de comunicações - que renderam ao Brasil, por exemplo, condenação pela Corte Interamericana de Direitos Humanos[26] - deu origem à instituição de mecanismos de controle social e transparência, como o Sistema Nacional de Controle de Interceptações Telefônicas (SNCI). Para além do necessário aperfeiçoamento de estruturas de fiscalização já existentes, o CNJ possui o ferramental funcional e administrativo necessário à regulamentação e supervisão de novos recursos tecnológicos de produção de provas que ofereçam riscos à garantia de direitos fundamentais.

Por fim, a atividade de controle e fiscalização passa também pela capacitação técnica dos agentes públicos, como promotores e magistrados, para melhor executar e compreender as potencialidades e riscos de tecnologias de vigilância e produção de provas - uma demanda expressa pelas próprias instituições policiais e judiciárias. Isso aumenta a segurança jurídica e eficácia do processo investigativo e reduz margens para arbitrariedades.

10. A legislação nacional que versa sobre a instrução criminal e a obtenção de provas no meio digital deve observar, criticamente, a experiência internacional pertinente a esta temática, bem como os instrumentos internacionais relativos à proteção de direitos humanos e fundamentais.

A experiência internacional contém instrumentos de instrução penal destinados à obtenção de provas digitais. A Convenção de Budapeste sobre o Cibercrime[27] enuncia dispositivos sobre a atuação estatal em investigações de crimes cibernéticos, estabelece salvaguardas para garantir a legitimidade do procedimento penal e evitar abusos, apesar das discussões[28] quanto aos seus limites estruturais e à ineficácia prática de seus enunciados em situações graves.

Em sua Seção 2, Título 1, a Convenção enuncia os limites da atuação investigativa estatal, aplicáveis a todas as demais previsões relativas ao Direito Processual Penal. O Título 1, nesse sentido, representa um sistema de balanceamento dos instrumentos do Título 2 da mesma Seção. Tais salvaguardas implicam a observância das normas jurídicas internas e de tratados internacionais para proteção de direitos humanos e fundamentais, conforme o item 1 do artigo 15º. Dentre os instrumentos, há a Carta de Direitos Humanos da ONU[29], o Pacto de San José da Costa Rica,[30] as obrigações contraídas pelo Brasil na Declaração da Internet[31] e a Resolução do Conselho de Direitos Humanos da ONU quanto ao direito à privacidade na era digital[32] [vide Recomendação 1].

A necessidade de observância da legislação nacional também condiciona o Estado ao respeito dos princípios norteadores da proteção de dados pessoais no Brasil, definidos pela LGPD [vide Recomendação 2]. Assim, importante ressaltar a necessidade de que sejam positivados instrumentos jurídicos sobre a cadeia de custódia das provas digitais utilizadas na persecução penal e criados mecanismos para regular sua obtenção, uso, guarda segura [vide Recomendação 3] e eliminação.

O artigo 15º da Convenção de Budapeste, ainda, estabelece em seu item 2 a necessidade de um controle sobre as atividades investigativas do Estado, que pode ser realizado de forma judicial ou independente e deve incluir a fiscalização e a supervisão das atividades desempenhadas no procedimento de instrução criminal [vide Recomendação 9]. Por fim, o artigo 21º da Convenção, em seu item 1, define como único respaldo legal para a interceptação de conteúdo de comunicações para a persecução penal procedimentos que visam investigar infrações graves. Nesse sentido, a obtenção de provas dessa natureza – além de depender de mecanismos de auditabilidade [vide Recomendação 8] e de fundamentação comprovando a ineficácia de meios de prova menos gravosos – deve estar sujeita a tipos penais de maior periculosidade [vide Recomendação 7].

Não obstante as quase duas décadas de aplicação da Convenção de Budapeste, não se deve ignorar as sérias ressalvas existentes quanto ao tratado. Conforme representantes da sociedade civil e da comunidade técnico-científica[33], a adesão do Brasil exige a adoção de salvaguardas que garantam a proporcional aplicação de suas previsões. Do ponto de vista legislativo, por exemplo, são necessários mecanismos próprios para a proteção de dados pessoais na persecução penal, em observância aos princípios da LGPD, e que definam garantias procedimentais pertinentes ao uso de metadados e dados cadastrais como meios de prova [vide Recomendações 4, 5 e 6].

Esses seriam passos cruciais para suprir as lacunas atuais da Convenção, notadamente quanto ao estabelecimento de limites legais para o acesso legítimo aos conteúdos de comunicações eletrônicas, para a integridade da cadeia de custódia de dados digitais, entre outros aspectos inerentes ao devido processo legal.

Notas

1. KASPERSKY. **Home office motiva aumento de mais de 330% em ataques usando sistemas de acesso remoto no Brasil**. 2020. Disponível em: https://www.kaspersky.com.br/about/press-releases/2020_home-office-motiva-aumento-de-mais-de-330-em-ataques-usando-sistemas-de-acesso-remoto-no-brasil. Acesso em: 16 jul. 2021.

2. VENTURA, Felipe. WhatsApp chega a 99% dos celulares no Brasil; Telegram cresce. 2020. **Tecnoblog**. Disponível em: https://tecnoblog.net/326932/whatsapp-chega-a-99-por-cento-celulares-brasil-telegram-cresce/. Acesso em: 16 jul. 2021.

3. Internet Society. **O impacto econômico das leis que enfraquecem a criptografia**. 08/07/21 Disponível em <https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia>, acesso em 16 ago. 2021.

4. Conselho de Direitos Humanos das Nações Unidas. **The promotion, protection and enjoyment of human rights on the Internet**. 04 de julho de 2018. Disponível em: https://ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1. Acesso em: 16 jul. 2021.

5. Conselho de Direitos Humanos das Nações Unidas. **The right to privacy in the digital age**. 26 de setembro de 2019. Disponível em: https://digitallibrary.un.org/record/3837297?ln=en. Acesso em: 18 ago. 2021.

6. BRASIL. Superior Tribunal de Justiça. Informativo nº 684, 5 de fevereiro de 2021. Disponível em https://processo.stj.jus.br/jurisprudencia/externo/informativo/?acao=pesquisar&livre=RMS+60531&operador=e&b=INFJ.

O Recurso Extraordinário interposto foi admitido em 08 de março de 2021 (BRASIL. Superior Tribunal de Justiça. RE no RMS 60.531/RO, Rel. Ministro Jorge Mussi, 05/03/2021. Disponível em https://processo.stj.jus.br/processo/dj/documento/mediado/?tipo_documento=documento&componente=MON&sequencial=121797957&num_registro=201900993927&data=20210308),

e hoje tramita no STF sob o nº RE 1317341 (BRASIL. Supremo Tribunal Federal. Página de Acompanhamento Processual RE 1317341. Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=6134575).

7. Superior Tribunal de Justiça. Recurso especial Nº 1.871.695 - RO (2020/0095443-3). Relator: Ministro Ribeiro Dantas. Disponível em https://processo.stj.jus.br/processo/revista/documento/mediado/?componente=ITA&sequencial=2051239&num_registro=202000954433&data=20210510&peticao_numero=202100264529&formato=PDF; hoje tramita no STF sob o nº ARE 1330950 (BRASIL. Supremo Tribunal Federal. Página de Acompanhamento Processual. Agravo em Recurso Extraordinário. Disponível em http://portal.stf.jus.br/processos/detalhe.asp?incidente=6193418.)

8. ABREU, Jacqueline. [9º FórumBR] Proteção de dados e segurança pública no Brasil. Youtube. Disponível em: https://www.youtube.com/watch?v=aOiLKoKhm3k. Acesso em: 27/07/2021.

9. **Trend Micro.** Data Breach Compromised 250,000 PII of U.S. Department of Homeland Security Employees. 2018. https://www.trendmicro.com/vinfo/us/security/news/cyber-attacks/data-breach-250k-pii-of-dhs-employees-witnesses. Acesso em 27 de julho de 2021.

10. Brasil é o quarto país que mais tem senhas de órgãos públicos vazadas. **CNN Brasil**. 2021. Disponível em: https://www.cnnbrasil.com.br/tecnologia/brasil-e-o-quarto-pais-do-mundo-que-mais-tem-senhas-vazadas-de-orgaos-publicos/. Acesso em 18 ago. 2021.

11. **Security Management: Asis International**. Police Departments Hit by Ransomware. 2021. Disponível em https://www.asisonline.org/security-management-magazine/latest-news/today-in-security/2021/april/Police-Departments-Hit-by-Ransomware/. Acesso em 27 de julho de 2021.

12. Comitê Gestor da Internet no Brasil. **Princípios da governança e uso da Internet no Brasil**. São Paulo: CGI.br, 2009.

13. Comitê Gestor da Internet no Brasil. Resumo Executivo - Pesquisa sobre o Setor de Provimento de Serviços de Internet no Brasil - **TIC Provedores 2020**. São Paulo: CGI.br, 2020.

14. BRASIL. Marco Civil da Internet, **LEI Nº 12.965, DE 23 DE ABRIL DE 2014**. Art. 10, caput e § 1º, Art. 11, §º 1, Art. 13, §5º, Art. 15, § 3º e Art. 22; e LGPD, Art. II, incisos ! ao VII, Art. 6º, incisos I ao X. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em 18 ago. 2021.

15. BBC. Pegasus: o que é o sistema que espionou jornalistas, ativistas e advogados. **BBC News Brasil**, 19 jul. 2021. Disponível em: https://www.bbc.com/portuguese/internacional-57885795. Acesso em 09 ago. 2021. SHU, Catherine. Federal court rules WhatsApp and Facebook's malware exploit case against NSO Group can proceed. Techcrunch, 2020. Disponível em: https://techcrunch.com/2020/07/16/federal-court-rules-whatsapp-and-facebooks-malware-exploit-case-against-nso-group-can-proceed/. Acesso em 05 de agosto de 2021.

16. ORGANIZAÇÃO DAS NAÇÕES UNIDAS. **Relatoria de acompanhamento sobre criptografia e anonimato do Relator Especial para a Promoção e Proteção do Direito à Liberdade de Opinião e Expressão**. Genebra, 2018. Disponível em:https://www.ohchr.org/Documents/Issues/Opinion/EncryptionAnonymityFollowUpReport.pdf. Acesso em: 05 ago. 2021. p. 18.

17. STEPANOVICH, Amie et al. A Human Rights Response to Government Hacking. **Access Now**, set. 2016. Disponível em:https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Acesso em: 05 ago. 2021.

18. LEETARU, Kalev. As EternalBlue Racks Up Damages It Reminds Us There Is No Such Thing As A Safe Cyber Weapon. **Forbes**. Disponível em: https://www.forbes.com/sites/kalevleetaru/2019/05/25/as-eternalblue-racks-up-damages-it-reminds-us-there-is-no-such-thing-as-a-safe-cyber-weapon/?sh=4cf03407603d Acesso em 20 ago. 2021.

19. PEGG, David & LEWIS, Paul. Edward Snowden calls for spyware trade ban amid Pegasus revelations. **The Guardian**, 2021. Disponível em: https://www.theguardian.com/news/2021/jul/19/edward-snowden-calls-spyware-trade-ban-pegasus-revelations. Acesso em 06 de agosto de 2021. STEPANOVICH, Amie & et al. A HUMAN RIGHTS RESPONSE TO GOVERNMENT HACKING. **Access Now,** 2016. Disponível em: https://www.accessnow.org/cms/assets/uploads/2016/09/GovernmentHackingDoc.pdf. Acesso em 06 de agosto de 2021.

20. KAYE, David. UN expert calls for immediate moratorium on the sale, transfer and use of surveillance tools. **Office of the High Commissioner for Human Rights**, 25 de junho de 2019. Disponível em: https://www.ohchr.org/EN/NewsEvents/Pages/DisplayNews.aspx?NewsID=24736. Acesso em 05 de agosto de 2021.;

LAKHANI, Nina. Revealed: murdered journalist's number selected by Mexican NSO client. **The Guardian**, 2021. Disponível em: https://www.theguardian.com/news/2021/jul/18/revealed-murdered-journalist-number-selected-mexico-nso-client-cecilio-pineda-birto. Acesso em 05 de agosto de 2021.

21. RUECKERT, Phineas. PEGASUS: THE NEW GLOBAL WEAPON FOR SILENCING JOURNALISTS. **Forbidden Stories**, 2021. Disponível em: https://forbiddenstories.org/pegasus-the-new-global-weapon-for-silencing-journalists/. Acesso em 06 de agosto de 2021.

22. ROPEL, Lucas. Cellebrite Hack Is Already Causing Grief for the Law. **Gizmodo**, 27 de abril de 2016. Disponível em: https://gizmodo.com/signals-cellebrite-hack-is-already-causing-grief-for-th-1846773797. Acesso em 06 de agosto de 2021.

23. MENDES, Vinícius. Sem licitação, Ministério Público contrata empresa de tecnologia por R$ 2,6 milhões. **Olhar Jurídico**, 2020. Disponível em: https://www.olharjuridico.com.br/noticias/exibir.asp?id=45141&noticia=sem-licitacao-ministerio-publico-contrata-empresa-de-tecnologia-por-r-26-milhoes. Acesso em 05 de agosto de 2021.

24. **Istoé**. Além do Pegasus, Carlos Bolsonaro queria outra ferramenta para espionagem dentro do governo. 2021. Disponível em: https://istoe.com.br/alem-do-pegasus-carlos-bolsonaro-queria-outra-ferramenta-para-espionagem-dentro-do-governo/ Acesso em 18 ago. 2021.

25. A exemplo do Sistema Nacional de Controle de Interceptações Telefônicas (SNCI), instituído pela Resolução/CNJ n. 59/2009. Disponível em https://atos.cnj.jus.br/atos/detalhar/101. Acesso em 13 de agosto de 2021.

26. CORTE INTERAMERICANA DE DIREITOS HUMANOS. CASO ESCHER E OUTROS VS. BRASIL: SENTENÇA DE 6 DE JULHO DE 2009. Disponível em: https://www.corteidh.or.cr/docs/casos/articulos/seriec_200_por.pdf. Acesso em 17 de agosto de 2021.

27. **Conselho da Europa**. Convention on Cybercrime (CETS 185). 23 de novembro de 2001. Disponível em: https://rm.coe.int/1680081561. Acesso em: 16 ago. 2021.

28. EILBERG, Daniela Dora; ZANATTA, Rafael A. F.; SANTOS, Bruna Martins dos; SALIBA, Pedro; VERGILI, Gabriel; CUNHA, Brenda. Os cuidados com a Convenção de Budapeste: objetivo da norma é a criação de vias para cooperação internacional em matéria penal e de procedimentos para combate aos cibercrimes. Objetivo da norma é a criação de vias para cooperação internacional em matéria penal e de procedimentos para combate aos cibercrimes. **JOTA** 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021. Acesso em: 16 ago. 2021.

29. Assembleia Geral das Nações Unidas. Universal Declaration of Human Rights. 10 de dezembro de 1948. Disponível em: https://www.ohchr.org/EN/UDHR/Pages/Language.aspx?LangID=por. Acesso em: 16 ago. 2021.

30. **BRASIL**. Decreto nº 678, de 06 de novembro de 1992. Promulga a Convenção Americana sobre Direitos Humanos (Pacto de São José da Costa Rica), de 22 de novembro de 1969. Brasília, DF, Disponível em: http://www.planalto.gov.br/ccivil_03/decreto/d0678.htm. Acesso em: 16 ago. 2021.

31. Conselho de Direitos Humanos das Nações Unidas. **The promotion, protection and enjoyment of human rights on the Internet**. 04 de julho de 2018. Disponível em: https://

ap.ohchr.org/documents/dpage_e.aspx?si=A/HRC/38/L.10/Rev.1. Acesso em: 16 jul. 2021.

32. Conselho de Direitos Humanos das Nações Unidas. **The right to privacy in the digital age**. 26 de setembro de 2019. Disponível em: https://digitallibrary.un.org/record/3837297?ln=en. Acesso em: 18 ago. 2021.

33. EILBERG, Daniela Dora; ZANATTA, Rafael A. F.; SANTOS, Bruna Martins dos; SALIBA, Pedro; VERGILI, Gabriel; CUNHA, Brenda. Os cuidados com a Convenção de Budapeste: objetivo da norma é a criação de vias para cooperação internacional em matéria penal e de procedimentos para combate aos cibercrimes. Objetivo da norma é a criação de vias para cooperação internacional em matéria penal e de procedimentos para combate aos cibercrimes. **JOTA** 2021. Disponível em: https://www.jota.info/opiniao-e-analise/colunas/agenda-da-privacidade-e-da-protecao-de-dados/os-cuidados-com-a-convencao-de-budapeste-08072021. Acesso em: 16 ago. 2021. ;

RODRIGUES, Katitza. ISRAEL, Tamir. Global Law Enforcement Convention Weakens Privacy & Human Rights. **Electronic Frontier Foundation**, 8 jun. 2021. Disponível em: https://www.eff.org/pt-br/deeplinks/2021/06/global-law-enforcement-convention-weakens-privacy-human-rights. Acesso em: 18 jul. 2021.

Realização

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE

INSTITUTO DE PESQUISA EM DIREITO & TECNOLOGIA DO RECIFE

Apoio

COALIZÃO DIREITOS NA REDE