Recomendações sobre

PRIVACIDADE DAS COMUNICAÇÕES, INVESTIGAÇÕES E DIREITOS DIGITAIS

IRIS
INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

Recomendações sobre

PRIVACIDADE DAS COMUNICAÇÕES, INVESTIGAÇÕES E DIREITOS DIGITAIS

AUTORIA
Ana Bárbara Gomes Pereira
Gustavo Ramos Rodrigues
Paulo Renáda Silva Santarém
Luiza Correa de Magalhães Dutra

REVISÃO INTERNA
Wilson Guilherme Dias Pereira

REVISÃO EXTERNA
Pedro Amaral

PROJETO GRÁFICO, CAPA, DIAGRAMAÇÃO E FINALIZAÇÃO
Felipe Duarte

COMO CITAR EM ABNT
DUTRA, Luiza Correa de Magalhães; GOMES, Ana Bárbara; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renáda Silva. **Recomendações sobre privacidade das comunicações, investigações e direitos digitais**. Belo Horizonte: Instituto de Referência em Internet e Sociedade, dezembro de 2022. Disponível em: <http://bit.ly/3ViK38I>. Acesso em: dd mmm aaaa.

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE

irisbh.com.br

SUMÁRIO

Apresentação

O IRIS – Instituto de Referência em Internet e Sociedade é um centro de pesquisa independente e interdisciplinar fundado em 2015 e dedicado a produzir e comunicar conhecimento científico sobre os temas de internet e sociedade, bem como a defender e fomentar políticas públicas que avancem os direitos humanos na área digital. Sua atuação busca qualificar e democratizar os debates sobre internet, sociedade e novas tecnologias ao trazer insumos científicos aos usuários da internet e aos diferentes setores que compõem a sociedade: governo, sociedade civil, setor privado, comunidade técnica e acadêmica.

O presente documento busca contribuir com o debate regulatório sobre direitos humanos na área digital num contexto social e tecnológico marcado por transformações profundas. A privacidade das comunicações, outrora compreendida primariamente como interesse individual - e por vezes contraposta ao interesse coletivo - é crescentemente reconhecida como um pilar da ordem democrática e do exercício de outros direitos básicos, como as liberdades de pensamento, de expressão, de associação e de reunião. Os dispositivos de comunicação pessoal e as plataformas de comunicação entre indivíduos se tornaram mediadores do debate público, das dinâmicas comerciais, das relações íntimas, do acesso à saúde e da segurança pública.

No campo processual penal, esse cenário enseja uma série de esforços voltados a endereçar as novas realidades. Por um lado, observa-se uma multiplicidade de iniciativas legislativas voltadas a tratar do tema, a exemplo da reforma do Código de Processo Penal, das propostas de lei de proteção de dados aplicável à segurança pública e à persecução penal e de tentativas legislativas e judiciais de restringir o uso de criptografia forte. Paralelamente, verifica-se um recurso crescente às novas tecnologias pelas autoridades de aplicação da lei, inclusive de tecnologias de hacking governamental e de soluções de inteligência de fontes abertas. Ainda, percebe-se uma pressão progressiva sobre os provedores dos canais de comunicação para a inserção de mecanismos de monitoramento em seus sistemas, como no caso dos mecanismos de varredura pelo lado do cliente.

Com a finalidade de subsidiar representantes dos diferentes setores, sobretudo formuladores de políticas públicas, este documento apresenta oito recomendações para as políticas de governança da privacidade das comunicações no contexto da persecução penal. Cada recomendação é seguida por uma justificativa, a qual oferece argumentos e dados que a fundamentam. Desse modo, espera-se colaborar com a discussão qualificada das proposições presentemente em pauta nos contextos nacional e internacional, tendo por base a pesquisa científica multidisciplinar e a defesa dos direitos humanos na área digital.

1. O acesso de autoridades a conteúdos de dispositivos móveis, sem ordem judicial, em flagrantes ou abordagens policiais deve ser inteiramente vedado.

Justificativa: A proteção de dados pessoais é central para uma gerência social que proteja o indivíduo perante um Estado persecutório e punitivista, quando tratamos do tema de atuação de instituições de segurança pública e justiça criminal. Esse é um direito fundamental que está garantido constitucionalmente no art. 5 º, inc. LXXIX e que foi reconhecido pelo Supremo Tribunal Federal no julgamento da MPV 954/2020. Ainda que o Brasil não possua uma lei de proteção de dados aplicável às operações de tratamento para fins exclusivos de segurança pública, persecução penal, segurança de Estado e defesa nacional, a LGPD - Lei Geral de Proteção aos Dados - prevê que o devido processo, os direitos dos titulares e seus princípios gerais deverão ser observados na normatização dessa seara.

O acesso a dispositivos móveis, celulares, e a todos os dados ali pertencentes pressupõe um acesso a uma gama imensa de informações, como dados - pessoais e sensíveis - e metadados que compõem toda a intimidade e vida privada, e possibilita ações investigativas repressivas, a partir de uma lógica inquisitorial, sem qualquer resguarda a princípios constitucionais e infraconstitucionais. É nesse sentido que o acesso a celulares em flagrantes ou abordagens policiais deve ser devidamente debatido, como irá se mostrar. Trata-se, portanto, de interferência extrema em diversos direitos fundamentais, entre eles as inviolabilidades do domicílio (art. 5º, XI), da vida privada e da intimidade (art. 5º, X), do sigilo de correspondência e das comunicações telegráficas e do sigilo de dados (art. 5º, XII). Ademais, outros fundamentos constitucionais são relevantes à tutela da matéria: o respeito ao devido processo legal (art. 5º, LIV) e a inadmissibilidade das provas ilícitas (art. 5º, LVI), além do princípio da não-discriminação[1].

A severidade dessa intrusão tem sido crescentemente debatida em outros contextos jurídicos. Nos Estados Unidos, por exemplo, a Suprema Corte reconheceu, no caso Riley V. California (573 US 2014)[2], ser inconstitucional o acesso policial a dados armazenados em celulares sem ordem judicial durante a realização de prisões. Entre os fundamentos da decisão constava o entendimento de que o volume e a variedade de informações registradas em smartphones contemporâneos equivalem a um registro diário contínuo das mais diversas interações, opiniões, pensamentos e experiências do indivíduo. Nesse sentido, não haveria nenhum paralelo a ser estabelecido entre o grau de intrusividade representado pelo acesso a esses aparelhos e a quaisquer outros objetos na vida contemporânea.

A análise do contexto sociológico brasileiro também suscita preocupações quanto à observância dos ditames legais quando do acesso policial a celulares. Estudos na área da violência estatal apresentam um quadro preocupante em relação às polícias e demais

1 Cf. DERY III, George M.; MEEHAN, Kevin. A new digital divide? Considering the implications of Riley v. California's warrant mandate for cell phone searches. Univ. of Pennsylvania Journal of Law and Social Change, v. 18.4, 2015.

JACOBSEN GLOECKNER, Ricardo; DORA EILBERG, Daniela. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. Revista Brasileira de Ciências Criminais, São Paulo, v. 27, ed. 156, p. 353-393, 2019.

2 Disponível em: https://supreme.justia.com/cases/federal/us/573/373/. Acesso em: 13.10.2022

instituições de segurança pública no Brasil[3]. Em relação às formas de policiamento, extensa bibliografia nacional já vem se debruçando sobre a temática das atuações dessas instituições estatais e seus cruzamentos com diferentes marcadores sociais e com as legitimidades do agir das instituições aqui envolvidas[4]. Em se tratando de instituições policiais brasileiras, em que a lógica estatal é punitivista, arbitrária e discriminatória, não se possui qualquer amparo legal que legitime o acesso a dados pessoais em flagrante policial, ação essa que pressupõe um poder discricionário dos operadores da força, dando legitimidade a invasões domiciliares, coação para desbloqueio de dispositivos eletrônicos e uso excessivo da força, por exemplo.

Em relação às instituições policiais, nota-se, no Brasil, o aumento de modos de "segurança" que buscam, no incremento do uso da força por parte das polícias e na expansão das prerrogativas policiais de detenção e registro de cidadãos, uma forma de melhor responder à criminalidade. Ou seja, as relações entre os agentes de segurança pública e os cidadãos brasileiros ainda são muito conflituosas; isso dentro de um cenário em que grande parte da população brasileira não possui pleno acesso aos seus direitos civis, e a polícia brasileira continua valendo-se de uma lógica que combina o uso excessivo de força contra determinados grupos sociais como modo de funcionamento burocrático e bacharelesco no âmbito da investigação criminal.

A possibilidade de acesso a dados pessoais de dispositivos móveis em flagrante policial acarretaria na hipervigilância e quebra de princípios legais e constitucionais de proteção do indivíduo com relação a um Estado punitivista. Ainda, a possibilidade de acesso a dados pessoais de dispositivos móveis em flagrante policial e por meio de ordem judicial, pode aumentar a vigilância com relação à população negra, uma vez que policiais associam pessoas negras a atitudes "suspeitas", buscando tipos físicos estigmatizados, a partir de características corporais, de vestimentas, de condutas gestuais, do modo de andar e olhar, e até do corte de cabelo, que demonstram a funcionalidade da filtragem racial (submeter mais pessoas de um grupo racial a abordagens policiais, investigações e sentenças) como forma de atuação das polícias militares e do policiamento ostensivo.[5]

3 ADORNO, Sérgio; DIAS, Camila. Monopólio Estatal da Violência. In: LIMA, R. S.; RATTON, J. L.; AZEVEDO, R. G. (Orgs.). Crime, Polícia e Justiça no Brasil. São Paulo: Contexto, 2014. p. 187-197.
COSTA, Arthur Trindade Maranhão; LIMA, Renato Sérgio de. Segurança Pública. In: LIMA, R. S.; RATTON, J. L.; AZEVEDO, R. G. (Orgs.). Crime, Polícia e Justiça no Brasil. São Paulo: Contexto, 2014. p. 482-490.
KANT DE LIMA, Roberto. Éticas e Práticas na Segurança Pública e na Justiça Criminal. In: LIMA, R. S.; RATTON, J. L.; AZEVEDO, R. G. (Orgs.). Crime, Polícia e Justiça no Brasil. São Paulo: Contexto, 2014. p. 471-481.
MUNIZ, Jacqueline; JÚNIOR, Domício Proença. Mandato Policial. In: LIMA, R. S.; RATTON, J. L.; AZEVEDO, R. G. (Orgs.). Crime, Polícia e Justiça no Brasil. São Paulo: Contexto, 2014. p. 491-501.

4 LIMA, Roberto Sérgio de; BUENO, Samira; SINHORETTO, Jacqueline. A gestão da vida e da segurança pública no Brasil. Soc. estado., Brasília , v. 30, n. 1, p. 123-144, Apr. 2015.
MUNIZ, Jacqueline. Ser policial é, sobretudo, uma razão de ser. Cultura e cotidiano da Polícia Militar do Estado do Rio de Janeiro. Tese de Doutorado. Rio de Janeiro: Iuperj, 1999.
_____; PAES-MACHADO, Eduardo. Polícia para quem precisa de polícia: contribuições aos estudos sobre policiamento. Cad. CRH, Salvador , v. 23, n. 60, p. 437-447, Dec. 2010.
_____; SILVA, Washington França da. Mandato policial na prática: tomando decisões nas ruas de João Pessoa. Cad. CRH, Salvador , v. 23, n. 60, p. 449-473, Dec. 2010.

5 Disponível em: http://www.gevac.ufscar.br/wp-content/uploads/2020/09/policiamento-ostensivo-rel-raciais-2020.pdf. Acesso em: 10.10.2022.

Desse modo, é recomendada a vedação total no que tange a possibilidade de acesso a dados de dispositivos móveis pessoais em flagrante policial, tanto em casos em que ocorra a suspeição, quanto em casos de constatação de prática infracional. Similarmente, devem ser consideradas nulas as demais evidências produzidas a partir do tratamento desses dados (RHC 89.981/MG pelo STJ; ARE n° 1.042.075/RJ).[6] As garantias constitucionais e infraconstitucionais devem prevalecer perante quaisquer argumentos genéricos de segurança pública e ordem pública, que dariam legitimidade a um combate ao crime e acesso a dados pessoais excessivos e indevidos.

2. O acesso a dispositivos móveis quando da existência de ordem judicial deve ser adequadamente parametrizado.

Justificativa: A segurança e proteção de dados pessoais, em se tratando de esfera penal e de segurança pública, a partir de acesso a dispositivos pessoais móveis por instituições policiais, deve ter parâmetros adequadamente definidos e regulados, como forma de prevenção de abuso de autoridade, hipervigilância estatal, e deve direcionar mecanismos estatais que englobam princípios legais e constitucionais previamente instituídos.

Nesse sentido, **recomenda-se**, caso venha a existir o acesso a dispositivos móveis pessoais pelas autoridades policiais, que se estabeleça uma regulação legal para tanto, com debate amplo e multi institucional, envolvendo representantes da sociedade civil, demonstrando os riscos de acesso e regulação de dados pessoais existentes nesses dispositivos móveis pessoais. Isso, pois, no âmbito de atuação penal, as normas materiais e processuais devem partir do princípio de proteção do indivíduo contra o Estado, criando-se uma rede de amparo contra o poder punitivo estatal diante do desequilíbrio de poder entre as partes.

Desse modo, o acesso a dispositivos móveis por parte de instituições policiais deve ser estritamente concedido por ordem judicial, seguindo os princípios do devido processo legal, da reserva legal (fundamentada, necessária, adequada e proporcional) e do princípio da finalidade. A ordem judicial deve ser específica e fundamentada, direcionada apenas para situações estritamente indispensáveis, envolvendo crimes de natureza gravíssima, preferencialmente taxados em Lei. Para a polícia examinar dados pessoais de dispositivos móveis, deve-se ter um requerimento solicitado e examinado pelo juízo, sob prejuízo, caso isso não ocorra, de quebra de normas de sigilo e de direitos de personalidade, protegidos pela Constituição Federal[7] e de configurar qualquer prova ali produzida como ilegal.

Recomenda-se ser apreciado, do mesmo modo, o princípio da necessidade, demonstrando

6 O entendimento do Tribunal Constitucional Espanhol é no sentido de que há violação ao direito à inviolabilidade das comunicações toda vez que "existe o acesso policial aos números telefónicos das chamadas recebidas e realizadas, ou seja, quando os agentes policiais acessam, sem prévia autorização judicial, a dados derivados de um processo de comunicação" → SSTC 123/2002, FJ 6; 56/2003, FJ 3; 230/2007, FJ 2; .142/2012, FJ 3, y 241/2012, FJ 4
Caso Riley vs. Califórnia, a Suprema Corte dos Estados Unidos decidiu pela necessidade de prévia ordem judicial para que a polícia pudesse validamente acessar o conteúdo de aparelhos celulares apreendidos em buscas incidentais e prisões.

7 JACOBSEN GLOECKNER, Ricardo; DORA EILBERG, Daniela. Busca e apreensão de dados em telefones celulares: novos desafios diante dos avanços tecnológicos. Revista Brasileira de Ciências Criminais, São Paulo, v. 27, ed. 156, p. 353-393, 2019.

especificamente as razões pelas quais o acesso ao dispositivo móvel particular é indispensável para investigação criminal, delimitando quais dados serão coletados e analisados, indicando todos os meios utilizados anteriormente sem sucesso, com indicações das razões pelas quais foram insuficientes para elucidação investigativa, além da imposição de uma limitação temporal para o uso da medida e para o armazenamento dos dados coletados nos dispositivos. Caso isso não ocorra, e não se tenha a demonstração especificada das diligências necessárias, há risco de uma permissividade excessiva por parte do judiciário da liberação do acesso aos dados pessoais. Ainda, existe a possibilidade de vazamento e compartilhamento desses dados, sem a devida necessidade, o que demonstra a importância do descarte adequado dos dados.

Por fim, é de suma importância a elaboração de relatórios anuais que versem sobre a eficácia, ou não, do acesso aos dados pessoais de dispositivos móveis na resolução de investigações criminais, como forma de mapear sua real eficiência na persecução penal. Os relatórios devem especificar número de autorizações judiciais concedidas, número de medidas executadas, quantos sistemas e dispositivos foram afetados, quais dados foram coletados, quantas vezes foram usados/úteis para investigações que motivaram a coleta, assim como sua previsão de descarte. Caso não se respeite o princípio da transparência, não será possível a realização de supervisão e controle público. Ainda, importante ter a manutenção da cadeia de custódia dos dados coletados, apresentando prazos legais para a manutenção e eliminação dos dados após seu uso específico, evitando a transferência de dados para fins de hipervigilância estatal sob a escusa abrangente e generalizada de manutenção da ordem pública e segurança nacional, assim como o abuso das informações acessadas indevidamente para fins privados.

Assim, é necessária a ordem judicial para o acesso aos dados contidos em celulares por autoridade policial, mesmo após a configuração do flagrante delito, com base em elementos concretos, a necessidade e a adequação da medida e delimite a sua abrangência à luz dos direitos fundamentais à intimidade, à privacidade e ao sigilo das comunicações e dados dos indivíduos (CF, art. 5º, X e XX), sendo considerada ilícita a coleta dos dados contidos no aparelho telefônico dos investigados, sem autorização judicial, bem como das demais derivadas (RHC 89.981/MG pelo STJ; ARE nº 1.042.075/RJ).[8]

3. O uso investigativo de ferramentas de hackeamento que permitam o acesso concomitante a comunicações passadas e futuras ou a alteração de quaisquer dados é ilícito e deve ser vedado inteiramente como meio probatório.

Justificativa: o acesso a dados pessoais mantidos em dispositivos de comunicação pessoal através de ferramentas de spyware representa, por si só, uma interferência

8 O entendimento do Tribunal Constitucional Espanhol é no sentido de que há violação ao direito à inviolabilidade das comunicações toda vez que "existe o acesso policial aos números telefónicos das chamadas recebidas e realizadas, ou seja, quando os agentes policiais acessam, sem prévia autorização judicial, a dados derivados de um processo de comunicação" → SSTC 123/2002, FJ 6; 56/2003, FJ 3; 230/2007, FJ 2; .142/2012, FJ 3, y 241/2012, FJ 4

Caso Riley vs. Califórnia, a Suprema Corte dos Estados Unidos decidiu pela necessidade de prévia ordem judicial para que a polícia pudesse validamente acessar o conteúdo de aparelhos celulares apreendidos em buscas incidentais e prisões.

extrema nos direitos fundamentais das pessoas investigadas. Trata-se de uma relativização profunda da privacidade e da liberdade de expressão e de pensamento, podendo impactar também a liberdade de associação. Se esse monitoramento representa, por si só, uma grave interferência nos direitos supracitados, o recurso a ferramentas que permitem não apenas o acesso a dados, mas sua manipulação - por vezes remota e oculta - representa violação ainda mais extrema.

O mais conhecido exemplo é o software de espionagem denominado Pegasus, fornecido pela empresa israelense NSO Group para governos com a alegada finalidade de combate ao terrorismo. Além de permitir o acesso a todo o conteúdo dos smartphones comprometidos, o Pegasus possibilita ao atacante tomar o controle de suas mais diversas funcionalidades, incluindo o envio de mensagens e a ativação da câmera, microfone, geolocalização, etc. Como foi amplamente noticiado em 2022, essa ferramenta foi utilizada por dezenas de governos para monitoramento indevido e perseguição política de jornalistas, ativistas, advogados, políticos de oposição, empresários, entre outros.[9]

Conforme destaca o relatório do Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos de 2022[10], o emprego de instrumentos dessa natureza pode impactar negativamente os direitos ao devido processo e a um julgamento justo. Isso ocorre porque a possibilidade de adição, exclusão ou modificação de arquivos presentes nos dispositivos de comunicação afetados implica no risco de alteração de seu conteúdo com fins de chantagem, ou incriminação da pessoa investigada. Tal cenário representa grave rompimento da cadeia de custódia e consequente violação aos direitos da pessoa investigada.

Nesse sentido, cumpre destacar o precedente estabelecido pela Sexta Turma do Superior Tribunal de Justiça no julgamento do RHC 99.735 - SC[11] e confirmado no julgamento do RHC nº 79.848 - PE: é ilícita a prova obtida por meio de captura de imagem de mensagens espelhadas por meio de espelhamento do aplicativo WhatsApp pelo computador (WhatsApp Web).

A decisão reconheceu que o caráter simultaneamente retroativo (*ex tunc*) e progressivo (*ex nunc)* da vigilância empregada, que permite tanto o acesso a conversas passadas quanto às comunicações presentes e futuras, não encontra previsão no sistema processual penal brasileiro. Ainda, constatou que admitir a legalidade das provas produzidas quando da possibilidade de alteração, sem quaisquer vestígios, do conteúdo comunicado significaria presumir que os atos dos investigadores gozam de legitimidade absoluta, o que contrasta tanto com a doutrina, quanto com a jurisprudência atual, que reconhecem a relatividade da presunção de legitimidade dos atos de servidores públicos.

A aplicação dos entendimentos firmados por esses precedentes ao emprego de ferramentas de espionagem para fins de produção probatória implica na compreensão de que é vedada a produção probatória realizada por ferramentas de software espião que permitam: i)

9 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.

10 Disponível em: https://documents-dds-ny.un.org/doc/UNDOC/GEN/G22/442/29/PDF/G2244229.pdf?OpenElement. Acesso em: 29.09.202212.12.2018.

11 Superior Tribunal de Justiça. Recurso em Habeas Corpus nº 79.848 – Pernambuco. Rel. Min. Néfi Cordeiro. J. em 21.08.2018 – DJe de 03.09.2018.

o monitoramento simultaneamente retroativo e progressivo das comunicações; ou ii) a alteração dos conteúdos acessados. Nesse sentido, importa destacar que o processo penal deve ser regido pelo princípio da legalidade estrita: somente o que está legalmente previsto pode ser admitido, jamais o contrário.

Por fim, nota-se que a própria existência do mercado de ferramentas de software espião, tal como presentemente estruturada, é crescentemente reconhecida como nociva à democracia e aos direitos humanos. Uma vez que tal mercado depende da exploração comercial de vulnerabilidades de segurança, sua dinâmica econômica é intrinsecamente promotora da insegurança global dos dispositivos de comunicação[12]. Conforme notado pela Suprema Corte da Índia no caso Manohar Lal Sharma v. União da Índia (2021)[13] em decisão que examinou o provável uso indevido do spyware Pegasus pelo governo indiano, a autocensura decorrente da vigilância ameaça a liberdade de imprensa e, portanto, a capacidade da imprensa de fornecer informações precisas e confiáveis.

Nesse sentido, organizações internacionais e entidades civis vêm conclamando pelo estabelecimento de uma moratória sobre a comercialização desses instrumentos até que as preocupações de direitos humanos relacionadas tenham sido sanadas.[14]

4. Propostas de intervenções tecnológicas que impactem a persecução penal devem ser fundamentadas em pesquisa científica atualizada e multidisciplinar

Justificativa: Na sociedade da informação, é inevitável relacionar inovações tecnológicas a todo o complexo contexto envolvendo defesa nacional, segurança do Estado, segurança pública e atividades de investigação e repressão de infrações penais. Em alguns âmbitos, a tecnologia simplesmente se integra à mera gestão administrativa da estrutura estatal, na aquisição de dispositivos eletrônicos e na adoção de sistemas digitais. Todavia, algumas instâncias vão abarcar intervenções tecnológicas do poder público mais sensíveis, direcionadas a viabilizar atividades de persecução penal, por exemplo, na produção de provas ou investigação de suspeitos, mas sem a correspondente definição de padrões ou critérios de validade.[15]

12 SNOWDEN, Edward. The Insecurity Industry. Substack. Disponível em: https://edwardsnowden.substack.com/p/ns-oh-god-how-is-this-legal. Acesso em: 07 out. 2022.

13 Suprema Corte da Índia, *Manohar Lal Sharma v. União da Índia*, despacho de 27 de outubro de 2021, para. 39.

14 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.

15 "*Digital evidence is increasingly presented and accepted in courts without scientific validation of the digital forensic methodology or tools.* (...) *There are no European minimum standards for digital evidence to establish and enforce scientific validation in digital forensics.*" STOYKOVA, Radina. Digital evidence: Unaddressed threats to fairness and the presumption of innocence. Computer Law & Security Review, v. 42, 2021. P. 1. Disponível em https://www.sciencedirect.com/science/article/pii/S0267364921000480. DOI: 10.1016/j.clsr.2021.105575. Acesso em 26 out. 2022.

Não obstante haja evidente interesse público na constante modernização dos recursos disponíveis às autoridades estatais – de modo que se possa manter a paridade de armas com ações e ferramentas de quem comete crimes – esse propósito político não afasta a necessidade de que ingerências do Estado no campo da tecnologia venham acompanhadas de pesquisas científicas multidisciplinares para avaliar impactos e riscos, considerando os conhecimentos consolidados e verificáveis em diversas áreas do saber.

Propostas podem ser apresentadas com base apenas em um suposto clamor popular, ou expressando uma crença acrítica em um solucionismo tecnológico, de que basta a inovação digital para se atender com mais eficiência ao interesse público. A título de exemplo real, o Brasil conta hoje com vinte estados que contrataram o uso de câmeras de vigilância com sistemas de reconhecimento facial adotados,[16] sem amparo em estudos científicos prévios, e com resultados nulos na redução da criminalidade, muitos falsos positivos e baixa taxa de reconhecimento.[17]

Do ponto de vista jurídico, faz-se oportuno realizar estudos de direito comparado e até pesquisas jurisprudenciais, para se avaliarem as condições de validade das provas produzidas por meio dos novos sistemas, tais como a cadeia de custódia. Mas de modo ainda mais empírico, devem ser empregados esforços para que haja fundamentações em avaliações antropológicas, sociológicas, econômicas e, particularmente, tecnológicas. Nem todos os sistemas são adaptáveis a outros contextos de aplicação com o mesmo sucesso, ou seja, sistemas pensados para determinadas populações, ou até certas condições climáticas, podem não operar adequadamente com maior diversidade populacional ou outra luminosidade.[18]

Argumentos de convencimento são sempre pertinentes no campo da política, uma vez que faz parte da democracia o embate entre visões distintas a respeito das melhores soluções para os problemas. Mas eles não permitem, por si só, que se possam avaliar os resultados de políticas públicas de segurança, sendo necessário traçar objetivos e definir metas estratégicas, que possam não apenas ser avaliadas periodicamente, como revisadas e debatidas democraticamente. Esse cenário exige que se apontem indicadores objetivos para mensuração de sucesso ou insucesso, mediante padrões que indiquem graus de neutralização ou mesmo a eliminação de eventuais riscos.

16 DAMASCENO, Vitória; FERNANDES, Samuel. Sob críticas por viés racial, reconhecimento facial chega a 20 estados. Folha de S. Paulo. 9.jul. 2021, 23h15; atu. 10.jul.2021, 17h25. Disponível em https://www1.folha.uol.com.br/cotidiano/2021/07/sob-criticas-por-vies-racial-reconhecimento-facial-chega-a-20-estados.shtml.

17 NUNES, Pablo; SILVA, Mariah Rafaela; DE OLIVEIRA, Samuel R. Um Rio de câmeras com olhos seletivos: Uso do reconhecimento facial pela polícia fluminense. Rio de Janeiro: CESeC, 2022. Disponível em https://opanoptico.com.br/Caso/um-rio-de-cameras-com-olhos-seletivos-uso-do-reconhecimento-facial-pela-policia-fluminense/.

18 AGÊNCIA ESTADO. Reconhecimento facial identifica 20 mil pessoas 'de risco' no Galeão. Correio Braziliense, 08 set. 2016. Disponível em https://www.correiobraziliense.com.br/app/noticia/brasil/2016/09/08/interna-brasil,547797/reconhecimento-facial-identifica-20-mil-pessoas-de-risco-no-galeao.shtml; LYNCH, Jennifer. Face Off: Law Enforcement Use of Face Recognition Technology. Electronic Frontier Foundation, 2018. Disponível em https://www.eff.org/files/2018/02/15/face-off-report-1b.pdf.

5. Harmonia entre microssistemas normativos deve ser preservada e participação social em sua elaboração deve ser ampliada

Justificativa: A eventual modernização da dogmática processual penal deve observar os demais quadros normativos já consolidados, que representam a defesa de direitos importantes. A fim de preservar a harmonia entre microssistemas normativos, o direito constitucional à proteção de dados, ao sigilo das comunicações e os princípios firmados na Lei Geral de Proteção de Dados devem ser zelados independentemente das matérias que sejam debatidas.

No artigo 4º, §1º, da Lei Geral de Proteção de Dados (LGPD, Lei Nº 13.709), a norma prevê que proteção de dados em matéria penal demanda 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". Deste modo, ainda que a Lei Geral de Proteção de Dados tenha excepcionado a atividade investigativa, os parâmetros principiológicos para tratamento de dados pessoais versados em seu texto devem ser considerados.

O Brasil possui uma trajetória notória no que diz respeito às legislações sobre internet, baseada em direitos civis e fortalecida por processos participativos. A saber, o Marco Civil da Internet e a LGPD. Ambos foram construídos com amplo processo de discussão e colaboração multissetorial. O processo constitutivo de suas normas é importante para a manutenção desse ecossistema. Isso envolve, inclusive, a composição do Comitê Gestor da Internet no Brasil e o Decálogo de Princípios para a Governança da Internet, que estabelece o dever do processo acontecer de forma transparente, multilateral e democrática. Destaca-se que o caráter multissetorial e participativo da elaboração de normas favorece a identificação de potenciais conflitos entre normativas e, consequentemente, é indispensável para a preservação da harmonia entre microssistemas normativos.

Como desenvolvido em outros tópicos (a ver: recomendações 1 e 3), há um elevado risco de abuso por parte de autoridades, ao passo que o espaço de resistência do indivíduo é desproporcionalmente menor, dada a assimetria que as intrusões aos dispositivos pessoais móveis podem estabelecer. A institucionalização, por meio de normas jurídicas, de práticas de enfraquecimento de sistemas informáticos não deve ser sequer considerada sem o esforço ativo de participação multissetorial, de sustentação científica acerca da sua eficácia e seus riscos. Ademais, além dos riscos para os direitos humanos, a exploração sistemática de vulnerabilidades para fins de persecução penal é prejudicial à própria integridade dos sistemas e à economia digital, uma vez que depende da perpetuação de um ecossistema baseado na instrumentalização comercial da insegurança.

Desse modo, recomenda-se a preservação da conformação e correspondência entre microssistemas normativos, ampliando, do mesmo modo, a participação social na elaboração de políticas no campo de proteção aos dados e internet no Brasil. Dessa forma, direitos fundamentais e princípios legais serão devidamente reconhecidos e respeitados.

6. Não restringir o livre uso da criptografia forte, direta ou indiretamente

Justificativa: Considerando o amplo leque de garantias viabilizadas pelo uso difundido da criptografia, quaisquer medidas estatais tomadas a pretexto de atender a um interesse

público e que afetem a segurança e a confidencialidade das comunicações criptografadas, ou que apenas reduzam a confiança nas tecnologias de criptografia, prejudicam o pleno exercício de vários direitos humanos. Esse é o posicionamento de vários escritórios e órgãos das Nações Unidas, sintetizados pelo Gabinete do Alto Comissariado das Nações Unidas para os Direitos Humanos no relatório "*O direito à privacidade na era digital*".[19]

Ao longo das últimas décadas, a criptografia forte se desenvolveu como ferramenta crucial à proteção de sistemas computacionais em situações cotidianas da vida de bilhões de pessoas em todo o mundo. Ela permite a comunicação livre – envolvendo informações sobre saúde, finanças, identidades de gênero, orientação sexual, expressão artística e situação de minoria – com pretensão plausível de que não haja vigilância nem por autoridades estatais, nem por cibercriminosos. Além de permitir privacidade e liberdade de expressão em meios digitais, a criptografia é essencial para salvaguardar liberdade de opinião, liberdade de associação e de reunião pacífica, segurança, saúde, não discriminação e livre desenvolvimento da personalidade.

Ela se mostra importante em contextos de conflitos armados[20] e predomínio da censura prévia, mas também, em todo o mundo, no cotidiano de jornalistas e defensores de direitos humanos, e na proteção de mulheres contra ameaças de vigilância, assédio e violência. Por isso, até mesmo no contexto de crimes gravíssimos, como a detecção de conteúdo de abuso sexual e exploração infantil, as investigações de comunicações criptografadas devem se limitar estritamente pelos princípios da legalidade, da necessidade e da proporcionalidade.

Não obstante, e desconsiderando as preocupações manifestadas por muitos especialistas,[21] vários países implementam ou debatem restrições ao uso de criptografia que podem forçar empresas a optar por soluções problemáticas - como as técnicas de scanning, especialmente CSS - ou simplesmente a abandonar a criptografia forte de ponta a ponta, incluindo:[22] a criminalização do uso e da oferta da tecnologia; a limitação do desenvolvimento tecnológico; a exigência de registro e licenciamento; a obrigação de que provedores garantam portas clandestinas para acesso por autoridades estatais; a adoção de sistemas de depósito de chaves em poder do Estado ou um terceiro designado;

19 ONU - ORGANIZAÇÃO DAS NAÇÕES UNIDAS. Escritório do Alto Comissariado para Direitos Humanos. The right to privacy in the digital age: report of the Office of the United Nations High Commissioner for Human Rights. A/HRC/51/17. Genebra: ONU, 4 ago. 2022. Disponível em https://digitallibrary.un.org/record/3985679?ln=en. Acesso em 13 out. 2022.

20 A título exemplificativo, temos o caso da Ucrânia: https://www.justsecurity.org/84156/encryption-helps-ukrainians-resist-russias-invasion-but-a-european-plan-threatens-the-underlying-trust-any-tech-user-needs/

21 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em: https://irisbh.com.br/publicacoes/percepcoes-sobre-criptografia-e-investigacoes-criminais-no-brasil-mapeamento-e-analise/.

22 LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto; DOS SANTOS, Guilherme Kenzo (2018). Direito e Criptografia: tendências legislativas e debate internacional. In POLIDO, Fabrício Bertini Pasquot; DOS ANJOS, Lucas Costa; BRANDÃO, Luíza Couto Chaves (orgs.) Anais Do III Seminário Governança das Redes: políticas, internet e sociedade. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2018. Pp. 266-271. Disponível em https://irisbh.com.br/publicacoes/anais-iii-seminario-governanca-das-redes-politicas-internet-e-sociedade/. Acesso em 26 out 2022.

e a imposição de requisitos de rastreabilidade de mensagens.[23]

A maioria dessas restrições têm impactos desproporcionais, afetando não só as pessoas tidas como alvo, mas a população em geral, que – tratadas sem distinção em relação a indivíduos efetivamente suspeitos – fica indistintamente impedida de se comunicar com garantia de privacidade. O enfraquecimento da segurança e o comprometimento da integridade dos sistemas expõem as pessoas físicas e jurídicas a interferências ilegais, não apenas por eventual abuso ou erro do poder público, mas também por atores privados, incluindo redes criminosas organizadas e até mesmo interferências de agentes públicos de outros países.

Nesse sentido, também importa notar os diversos impactos econômicos negativos que normas que restringem ou limitam o uso da criptografia podem ter no ecossistema digital: aumento da insegurança do ambiente de negócios, prejuízo reputacional a provedores de serviços potencialmente afetados e diminuição da confiança nos serviços digitais[24].

Além de partir do pressuposto equivocado de que haveria uma contraposição radical entre os interesses individuais e o interesse público – esquecendo que a mesma criptografia que protege a comunicação entre particulares protege a comunicação entre agentes estatais, inclusive em relação a assuntos estratégicos –, muitas vezes essas medidas ignoram ou desconsideram outras ferramentas e abordagens disponíveis – ou que poderiam ser ao menos debatidas – na busca dos mesmos objetivos legítimos de coletar dados, produzir provas ou aplicar a lei, tais como um policiamento tradicional aprimorado e com melhores recursos, operações secretas, análise de metadados e cooperação policial internacional reforçada.

7. Sistemas de varredura pelo lado do cliente devem ser vedados inteiramente ou, quando empregados, limitados estritamente à detecção de materiais de abuso sexual infantil

Justificativa: Em uma sociedade de controle o acesso a dados pessoais e sua necessidade de proteção são veementemente questionados. A utilização de ferramentas tecnológicas demanda um olhar atento para seus aspectos jurídicos e tecnológicos. Em termos de ingerência de entidades estatais sobre a criptografia, são apresentadas técnicas para investigações de comunicações privadas que tendem, em grande medida, a aumentar de forma excessiva a vigilância em massa sobre cidadãos, o que exige medidas legislativas ou políticas de controle.

A vigilância e utilização de dados para a manutenção e ordenação social, direcionando-os

23 RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. Comunicações privadas, investigações e direitos: rastreabilidade de mensagens instantâneas. Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2022. Disponível em https://irisbh.com.br/publicacoes/comunicacoes-privadas-investigacoes-e-direitos-rastreabilidade-de-mensagens-instantaneas/. Acesso em 26 out 2022.

24 BARKER, George. LEHR, William. LONEY, Mark. SICKER, Douglas. O impacto econômico das leis que enfraquecem a criptografia. Law & Economics Consulting Associates (LECA). Tradução de Paulo Renã da Silva Santarém. 2021. Disponível em: https://isoc.org.br/noticia/o-impacto-economico-das-leis-que-enfraquecem-a-criptografia

para diversas áreas de atuação, não se trata de um campo novo nos debates acadêmicos.[25] Contudo, tem se intensificado a possibilidade de acesso a dados pessoais e à vida privada das pessoas, possibilitando ações de persecução estatal, controle irrestrito e vigilância sem controles. Em um país com altos índices de violência letal direcionada para jovens, negros e pobres,[26] a vigilância irrestrita por instituições estatais tende a ser discriminatória, elevando as preocupações com a persecução penal estatal.

Essa atenção à possibilidade de hipervigilância deve ser especial quando se trata de técnicas como a varredura pelo lado do cliente (VPLC), que escaneia dados nos dispositivos de usuário em busca, pela comparação com uma lista de *hashes* (identificadores), reconhecer materiais considerados ilícitos que possam estar sendo compartilhados de por meio de sistemas protegidos com criptografia segura, impedindo a análise durante a transmissão ou armazenamento nos servidores.

No plano tecnológico, a VPLC tem potenciais problemas de funcionamento, eficácia, segurança e escopo, dados os riscos respectivos, isolados ou cumulados, de ela ser inutilizada, não alcançar os resultados prometidos, abrir vulnerabilidades ou sofrer desvio de função. E no plano jurídico, seus possíveis efeitos negativos podem afetar privacidade, sigilo das comunicações, presunção de inocência e segurança pública, além de se questionar sua proporcionalidade e necessidade.[27]

Assim, pela falta de gerenciamento ativo para coibir vigilâncias desmedidas, considerando seus impactos potenciais, a utilização de técnicas de VPLC eleva riscos de acesso excepcional, abuso e danos de confiança no sistema digital.[28] Para a liberdade de expressão e o acesso à informação, ela pode gerar censura, uma vez que emprega métodos de filtragem padronizada de conteúdo da comunicação.[29]

---

25 Em Vigiar e punir, publicada originalmente em 1975, Michel Foucault já identificava, como um dos elementos centrais dos dispositivos de vigilância na modernidade, as técnicas de coleta, registro e classificação da informação sobre indivíduos, que ficavam sujeitos a identificação, descrição e assimilação pelas instituições. BRUNO, Fernanda. Dispositivos de vigilância no ciberespaço: duplos digitais e identidades simuladas. **Fronteiras-estudos midiáticos**, v. 8, n. 2, p. 152-159, 2006. P. 154.

26 Ver FÓRUM BRASILEIRO DE SEGURANÇA PÚBLICA. Segurança em Números 2022. Jun. 2022. Disponível em https://forumseguranca.org.br/wp-content/uploads/2022/06/anuario-2022-infografico.pdf. Acesso em 10 out. 2022.

27 PEREIRA, Wilson Guilherme Dias; RODRIGUES, Gustavo Ramos; SANTARÉM, Paulo Renã da Silva; VIEIRA, Victor Barbieri Rodrigues. **Varredura pelo lado do cliente: uma revisão sistemática.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, outubro de 2022. Disponível em: https://bit.ly/3EAhEDF. Pp. 20-24.

28 PEREIRA, Ana Bárbara Gomes; RODRIGUES, Gustavo Ramos; VIEIRA, Victor Barbieri Rodrigues. **Percepções sobre criptografia e investigações criminais no Brasil: mapeamento e análise.** Belo Horizonte: Instituto de Referência em Internet e Sociedade, 2021. Disponível em https://irisbh.com.br/publicacoes/percepcoes-sobre-criptografia-e-investigacoes-criminais-no-brasil-mapeamento-e-analise/.

29 KARDEFELT-WINTHER, Daniel; DAY, Emma; BERMAN, Gabrielle; WITTING, Sabine K.; BOSE, Anjan, on behalf of UNICEF's cross-divisional task force on child online protection (2020). **Encryption, Privacy and Children's Right to Protection from Harm**, Innocenti Working Papers, nº 2020-14, UNICEF Office of Research - Innocenti, Florence: UNICEF Office of Research – Innocenti. Disponível em https://www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html.

E mesmo se fosse aplicada de modo adequado, a VPLC poderia servir como um modelo legitimador da vigilância em massa. Ela não permite que indivíduos e a sociedade civil como um possa monitorar e fiscalizar efetivamente a real utilização das técnicas, por exemplo, se de fato houve denúncias de circulação ou alguma circunstância de impedimento na transmissão de imagens,[30] ou se houve algum uso desviante, equivocado, ou até a vigilância de dados privados sem ordem judicial.

Nessa medida, em consideração aos princípios constitucionais de presunção de inocência e proteção de dados pessoais (artigo 5º, inciso LVII e art 5 º, inc. LXXIX, CF), além das garantias à privacidade e sigilo das da criptografia de ponta a ponta, é recomendado evitar a utilização de ferramentas que possam instigar a vigilância em massa discriminatória e a quebra de criptografia de ponta a ponta.

8. Ferramentas para promover segurança do usuário devem ter tratamento distinto daquelas desenvolvidas para ambientes adversariais

Justificativa: Os dispositivos digitais, em que pese as críticas aqui já apresentadas, podem ser importantes fontes de provas eletrônicas; nesse sentido, duas perspectivas de abordagem devem ser consideradas de forma distinta. De um lado, a produção de provas em favor da defesa do interesse da pessoa detentora do dispositivo, ou usuária do sistema, cujo interesse se alinha ao do trabalho investigativo e cujo comportamento será de colaboração. Do outro lado, o dispositivo pode ser uma fonte em contraposição ao interesse da pessoa que o usa, de modo que sua vontade e sua postura serão contrárias, criando um ambiente em que ela se coloca como adversária da investigação.

Em ambientes adversariais, é importante considerar a possibilidade da pessoa investigada ter agido para atrapalhar a produção de provas (deliberadamente evitando a coleta de dados) ou, de modo mais sofisticado, para iludir ou desviar o esforço probatório (oferecendo dados que confundam ou desinformem, mais especificamente, gerando falsos positivos ou falsos negativos).

Alguns estudos, por exemplo, dedicam-se a analisar as tecnologias e medir o grau de confiabilidade dos sistemas de análise automatizada de imagens, em busca de conteúdo de abuso sexual infantil ou CSAM (iniciais do termo em inglês *child sexual abuse material*), diante da possibilidade de um adversário – após decodificar o funcionamento do algoritmo – mascarar imagens que efetivamente seriam ilegais ou forçar a correspondência de imagens inofensivas com os bancos de dados de material ilegal.

Ao mesmo tempo em que esse tipo de cuidado é crucial em ambientes adversariais, ele pode ser desnecessário quando o próprio dono do aparelho tiver interesse em colaborar, e não houver motivos para desconfiar de suas intenções, por exemplo, por ele não deter conhecimentos suficientes para interferir no funcionamento do algoritmo.

30 KARDEFELT-WINTHER, Daniel; DAY, Emma; BERMAN, Gabrielle; WITTING, Sabine K.; BOSE, Anjan, on behalf of UNICEF's cross-divisional task force on child online protection (2020). **Encryption, Privacy and Children's Right to Protection from Harm**, Innocenti Working Papers, nº 2020-14, UNICEF Office of Research - Innocenti, Florence: UNICEF Office of Research – Innocenti. Disponível em https://www.unicef-irc.org/publications/1152-encryption-privacy-and-childrens-right-to-protection-from-harm.html.

Desse modo, recomenda-se a existência de tratamento distinto entre as ferramentas para promover segurança do usuário, daquelas desenvolvidas para ambientes adversariais, ainda mais em se tratando de provas eletrônicas, sempre respeitando os princípios do devido processo legal, da presunção de inocência e da inadmissibilidade das provas ilícitas, à luz dos direitos humanos.

iris

INSTITUTO
DE REFERÊNCIA
EM INTERNET
E SOCIEDADE