INTERMEDIAÇÃO DA VIGILÂNCIA DO ESTADO NO BRASIL E PROTEÇÃO DE DADOS ENTRE COOPERAÇÃO, LITÍGIOS E CONSTRIÇÃO DE AGENTES PRIVADOS: HISTÓRICO, FUNDAMENTOS E REGULAÇÃO

Jacqueline de Souza Abreu

Doutora em Direito pela Universidade de São Paulo. Mestre em Direito pela Universidade da Califórnia, Berkeley e pela Ludwig-Maximilians-Universität, Munique. Advogada. *E-mail*: jacqueline.abreu@alumni.usp.br.

Resumo: O artigo se debruça sobre o fenômeno da intermediação de atividades de vigilância do Estado no Brasil: a cooperação, no mais das vezes forçada, de agentes privados para acesso a dados pessoais interessantes à instrução de processos, investigações e políticas de segurança pública. Primeiro, reconta os primeiros grandes litígios movidos por empresas privadas contra ordens de colaboração, de forma tanto a ilustrar que debates atuais são uma versão contemporânea de discussões antigas quanto a mostrar que possuem influência para a demarcação da compreensão sobre limites do poder do Estado. Segundo, localiza o fundamento dessa atuação em deveres fiduciários que empresas acionadas como intermediárias de vigilância possuem junto a seus clientes e aponta como a regulação de fluxos de dados entre essas empresas e o Estado é crucial para controle do poder corporativo e estatal, em respeito a direitos e expectativas de justiça. Terceiro, com ênfase em questões postas pelo avanço tecnológico sobre o sigilo telemático, apontam-se os limites da regulação brasileira atual e o que precisa ser aperfeiçoado tendo em vista o rápido avanço tecnológico.

Palavras-chave: Vigilância. Privacidade. Segurança. Proteção de dados. Compartilhamento.

1 Introdução

Em 1995, ao abrir divergência em um julgamento do Supremo Tribunal Federal (STF) com repercussões históricas sobre a compreensão do escopo constitucional da privacidade, o Min. Francisco Rezek defendeu que não se pode exigir autorização judicial prévia para quebra de sigilo de dados bancários (envolvendo recursos públicos) porque não faria parte da "estrita privacidade pessoal", diferente de interceptações telefônicas, que afetam a comunicação pessoal. Como razão

adicional, o Ministro ainda pontuou que escutas telefônicas precisariam de "abono judiciário" porque nelas a polícia "é, ela mesma, a executora do grampeamento" e que "se faz sempre sob o véu do sigilo".[1] É o tipo de medida que poderia dar lugar a muitos abusos, por isso a exigência. No caso da quebra de sigilo bancário requisitada pelo Ministério Público, isso não ocorreria: dependem da formalização de requisições e as informações obtidas devem ser resguardadas em sigilo, sob pena de responsabilização civil e criminal.

Como as razões de seu voto no caso MS 21729/DF[2] de 1995, que fizeram parte da maioria no julgamento apertado por 6x5, capturaram a prática do tempo e agora fazem recordar, houve um momento histórico em que, para que que a polícia realizasse um *grampo*, havia efetivamente a necessidade de que houvesse a instalação de dispositivos de gravação por agentes do próprio Estado em torres e linhas de telefonia. Essa necessidade diminui a partir do momento em que se exige das próprias empresas responsáveis pelo serviço de telefonia que sejam capazes de fazer interceptações, desviando conversas a agentes de investigação.[3] A maior parte das interceptações telefônicas são feitas hoje obrigando-se empresas de telefonia a retransmitir ligações através de sistemas próprios de vigilância.[4] Nesse aspecto, portanto, há algum tipo de formalização que dificulta o uso desregrado e escuso da medida. Não fosse pela consideração sobre invasividade anterior, portanto, até parece que o Ministro poderia admitir as interceptações telefônicas intermediadas por empresas sem autorização judicial nos dias de hoje.

---

1 BRASIL. Supremo Tribunal Federal. MS 21729/DF, Rel. Min. Marco Aurélio. Redator p/ acórdão Min. Néri da Silveira, Tribunal Pleno, j. 05/10/1995, *DJ* 19/10/2001, voto do Min Francisco Rezek, p. 121-2: "Acima de tudo, entretanto, vale considerar que a escuta telefônica, se autorizada à máquina policial sem abono judiciário, induziria abusos dos quais é improvável que algum dia transparecessem e se pudessem punir. Não afirmo, em absoluto, que o magistrado seja essencial e necessariamente melhor do que qualquer outro servidor do Estado. O que sucede é que a polícia é, ela mesma a executora do grampo telefônico que lhe pareça útil à investigação criminal, e que se faz sempre sob o véu do sigilo. O aval do juiz é a garantia de que a quebra da privacidade, nesse caso, parece necessária, e ficará registrada nos autos, sob a responsabilidade conjugada de quem a pediu e de quem a autorizou, sem espaço algum para capricho e para o arbítrio. Estes, de outro modo, haveriam de incorporar-se à rotina, como ao tempo das últimas sombras na história política do Brasil, quando os esbirros do sistema de informações se comprazia na escuta telefônica não só de supostos subversivos e corruptos, mas também na de ministros de Estado e membros desta mesma casa".

2 BRASIL. Supremo Tribunal Federal. MS 21729/DF, Rel. Min. Marco Aurélio. Redator p/ acórdão Min. Néri da Silveira, Tribunal Pleno, j. 05/10/1995, *DJ* 19/10/2001.

3 TICOM, Miguel Ângelo Duarte; PEREIRA NETO, Wanderson de Freitas; ALBUQUERQUE, Silde Monteiro de; CARVALHO, Israel Carbone de; SILVA JR., Arnaldo Rosa. "Histórico, implementação e uso do Sistema Guardião® de interceptação de dados de informática e telemática nas garantias do cidadão". *Cadernos de Segurança Pública,* 12 de setembro de 2020.

4 TICOM, Miguel Ângelo Duarte; PEREIRA NETO, Wanderson de Freitas; ALBUQUERQUE, Silde Monteiro de; CARVALHO, Israel Carbone de; SILVA JR., Arnaldo Rosa. "Histórico, implementação e uso do Sistema Guardião® de interceptação de dados de informática e telemática nas garantias do cidadão". *Cadernos de Segurança Pública,* 12 de setembro de 2020.

Atualmente, compelir empresas a assistir investigações, quebrando-se sigilo sobre dados que possuem de seus clientes, é prática usual. Tão comum que fez inclusive nascer um certo senso de prerrogativa de que se o Estado sempre pode interceptar comunicações, não poderia existir uma tecnologia que viabilizasse comunicações não interceptáveis – isto é, um formato em que a empresa não fosse capaz de acessar comunicações para entregar ao Estado em tempo real, mesmo que o devido processo legal para o caso fosse observado e as condições de legitimidade estivessem presentes. Foi esse o debate sobre o uso de criptografia de ponta a ponta em aplicações de comunicações a distância como o WhatsApp, por exemplo.[5]

Ao mesmo tempo em que grandes empresas dos mais diversos setores recebem o escrutínio devido sobre as suas práticas de uso de dados pessoais tendo em vista a defesa do consumidor e o direito da concorrência, devem também ser estudadas, avaliadas e reguladas sob a perspectiva de se transformarem nos novos "intermediários de vigilância"[6] do Estado. Isso coloca desafios e oportunidades da perspectiva regulatória para preservação da privacidade. Nessa modalidade, como foi e ainda é para bancos e operadoras de telefonia, agentes de aplicação da lei não executam medidas diretamente, mas são *assistidos* – em geral forçadamente – por empresas que desenvolveram produtos baseados em coleta e uso massivo de dados pessoais. A "era de ouro da vigilância"[7] é um grande baú do tesouro para registro documental de fatos que se transformam em evidências para prevenção e repressão criminal.[8]

Este artigo parte da provocação, surgida da leitura do voto do Min. Rezek, de que há algo relevante, do ponto de vista regulatório, no fato de o Estado precisar de alguns agentes externos, separados e movidos por outros interesses, se quiser praticar medidas de vigilância – isto é, de acesso a informações pessoais. Essa fricção oferece a possibilidade de um nível adicional de controle da legalidade da vigilância e, por isso mesmo, deve ser reconhecida como um elemento de arranjos regulatórios. Numa era com empresas que praticam coleta e uso cada vez mais intensivo de dados pessoais, a convergência – quando e se acrítica, inescrutável e desregulada – entre o Estado e empresas para o exercício de vigilância torna-se preocupante, pelo acúmulo de poder e potencial de risco que

5 LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. "Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil". *Revista da Faculdade de Direito UFPR* 63, nº 3, 2018, pp. 135-61. Disponível em: https://doi.org/10.5380/rfdufpr.v63i3.59422.

6 ROZENSHTEIN, Alan Z. "Surveillance Intermediaries". *Stanford Law Review,* vol. 70, 2018, pp. 102-89.

7 SWIRE, Peter. The FBI doesn't need more access: we are already in the golden age of surveillance". *Just Security,* 17 de novembro de 2014. https://www.justsecurity.org/17496/fbi-access-golden-age-surveillance/.

8 FERGUSON, Andrew. Structural Sensor Surveillance. *Iowa Law Review*, vol. 106, 2021, pp. 47-112.

dela decorre. A possibilidade de tensão entre Estado e agentes privados quando se fala em intermediação de medidas de vigilância é bem-vinda, ainda que não suficiente para exaurir o quadro regulatório, ao contrário do que o Min. Rezek parecia sugerir.

O artigo se divide em três partes.[9] Primeiro, reconta os primeiros grandes litígios de intermediários da vigilância do Estado no Brasil e aponta as suas manifestações atuais, de forma a mostrar sua atuação de longa data em litígios que envolvem preocupações com alcance do poder do Estado sobre dados e informações. Segundo, com ênfase em questões postas pelo avanço tecnológico, fundamenta os deveres fiduciários que empresas acionadas como intermediárias de vigilância possuem junto a seus clientes e que ajuda a explicar e justificar sua atuação litigiosa. Nesse sentido, mostra como a regulação de fluxos de dados entre essas empresas e o Estado é crucial para controle do poder corporativo e estatal, em respeito a direitos e expectativas de justiça. Terceiro, aponta os limites da regulação brasileira atual diante do rápido avanço tecnológico, a importância da litigância de empresas para suscitar esses limites e as inconsistências e abusos a que podem dar vazão e a necessidade de aperfeiçoar o quadro jurídico aplicável.

2 Histórico

A tarefa de intermediar medidas de vigilância do Estado não é nem foi aceita voluntária e silenciosamente por agentes privados. Pelo contrário, envolve já historicamente atuação litigiosa em nome de seus deveres de sigilo perante as informações de seus clientes, de preservação de parâmetros de legalidade e segurança jurídica. O repositório eletrônico do STF aponta que bancos foram as primeiras instituições que levaram casos sobre seus deveres de guarda de sigilo com respeito a informações de clientes até a mais alta corte do país.[10]

[9] Tendo em vista que o artigo trata de questões relacionadas à atuação de empresas privadas e embora o artigo reflita sobre questões que estuda como acadêmica em privacidade há mais de uma década, a autora considera importante declarar que atualmente atua como advogada no setor privado de tecnologia. As opiniões são pessoais e não refletem as de seu presente empregador, de antigos clientes, nem de qualquer instituição a que esteve vinculada.

[10] O repositório eletrônico do STF contempla os acórdãos publicados após 06/07/1950. Cf. BRASIL, Supremo Tribunal Federal, Dicas de Pesquisa, disponível em: https://portal.stf.jus.br/textos/verTexto.asp?servico=jurisprudenciaPesquisaGeralNovoPortal&pagina=Dicas_de_pesquisa Acessado em 17.12.2023. Pode, no entanto, conter alguns acórdãos mais antigos. O encontro dos acórdãos citados abaixo se deu buscando os acórdãos mais antigos que retornassem a partir de buscas por "sigilo", "intimidade", "privacidade" e "inviolabilidade". O primeiro foi encontrado por ser referido em acórdãos antigos e, diante disso, requisitado à biblioteca do STF. Esta pesquisa foi primeiramente feita no âmbito de programa de doutorado: ABREU, Jacqueline de Souza. *Privacidade, segurança e tecnologia*. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2022.

No MS nº 1047-SP, julgado em 6 de setembro de 1949,[11] o STF apreciou recurso de três bancos – Banco do Comércio e Indústria de São Paulo, Banco Financial Novo Mundo e Banco Central de São Paulo – contra ordem judicial da 16ª Vara Cível de São Paulo que determinou o fornecimento de informações sobre a conta de um cliente, para fins de prova em um processo de natureza cível de que este era parte, por ato ilícito. O juízo impetrado defendeu a validade da ordem ferrenhamente: sustentou que (i) o sigilo profissional de banqueiros não pode ser absoluto, devendo ceder "quando se trata de auxiliar a justiça, pois o interesse da sociedade prima sobre o dos indivíduos"; (ii) "bancos são organizações de caráter coletivo" e "não podem desenvolver suas atividades de maneira ante-social", de modo que não se compreende como possam "negarem-se a colaborar com a descoberta da verdade, e assumindo o risco de concorrerem para o erro do judiciário, que gera a desconfiança do cidadão e estimula a revolta"; e (iii) o "banqueiro deve guardar o segredo até que o interesse coletivo, apreciado pelo poder judiciário, exija a informação". O Tribunal de Justiça de São Paulo manteve a decisão:

> [T]rata-se de ação de indenização de dano causado por estelionato ou furto. Logo, é evidente o interesse público, em frente do qual não há que se falar em segredo de profissão nem direito líquido e certo, para não se informar à autoridade pública. O que se pretende não constitui devassa dos negócios dos bancos, hipótese em que seria legítima a recusa dos impetrantes, circunscrito como está o pedido a determinados pontos das contas de seus clientes, envolvidos legitimamente na demanda.

Segundo o relatório do acórdão, os bancos recorreram sustentando que (a) pela natureza da profissão estão obrigados a sigilo e a hipótese em questão não seria excepcional (art. 154 do Código Penal[12]); (b) se a determinação consistia em exibição de documentos, deveria ter sido observado o procedimento do art. 220 do Código de Processo Civil;[13] (c) a medida violaria os arts. 17, 18 e 19 do Código

[11] BRASIL. Supremo Tribunal Federal. MS 1047, Min. rel. Ribeiro da Costa, Tribunal Pleno, j. 06.09.1949.

[12] Código Penal (Decreto-Lei nº 2.848/1940): "Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: (...)".

[13] Código Civil de 1940: "Art. 220. Quando documento necessário à formação de prova se achar em poder de terceiro obrigado a exibi-lo, por ser comum ao requerente, poderá o juiz, ouvido o terceiro, ordenar o respectivo depósito, a expensas do requerente. Parágrafo único. Si o terceiro negar a posse do documento, ou o dever de exibi-lo, poderá o juiz designar audiência especial, afim de, ouvidos o requerente e o terceiro, proferir despacho".

Comercial,[14] que resguardam o sigilo comercial, pois resultaria no fornecimento de livros comerciais.

No STF, entretanto, não conseguiram reverter o entendimento já fixado até ali. O relator Min. Ribeiro da Costa entendeu que o segredo profissional não é violado, como previsto no Código Penal, quando há "justa causa na sua revelação". Os bancos não se equivaleriam a médicos, advogados, sacerdotes e parteiras – categorias às quais a lei concederia inviolabilidade. Não poderiam, portanto, se "sobreporem à determinação judicial, no sentido de prestarem, na causa, esclarecimentos essenciais, necessários ao julgamento e desenlace da demanda. As razões de interesse público tanto ocorrem no Juízo Criminal como no processo civil". Seguindo o relator, o Min. Marcelo Lundolf registrou que nunca tinha visto um banco negar tal informação em sua experiência como juiz cível: "desde que o pedido não tenha caráter de devassa, não é possível negar-se à Justiça essa colaboração necessária, essencial ao esclarecimento da verdade". Por fim o recurso foi negado por unanimidade.

Quatro anos depois o raciocínio foi reafirmado no RE 2172, julgado em 10 de julho de 1953.[15] O Banco do Brasil entrou com ação contra um devedor por uma operação que representava fraude. Pessoas que participaram dessa operação entraram como litisconsortes e pediram para o banco apresentar informações sobre outras operações realizadas por esse devedor, o que o juiz do caso deferiu no despacho saneador. O banco então se recusou ao fornecimento alegando sigilo profissional bancário – art. 154 do Código Penal.[16] No STF, foi mantido o entendimento de que o banco tinha o dever de entregar as informações, tendo o juiz entendido necessário para esclarecimento do objeto. Nas palavras do relator Min. Nelson Hungria "banqueiros são 'confidentes necessários' e, como tais, obrigados a sigilo

[14] Código Comercial de 1850: "Art. 17. Nenhuma Autoridade, Juizo ou Tribunal, debaixo de pretexto algum, por mais especioso que seja, póde praticar ou ordenar alguma diligencia para examinar se o commerciante arruma ou não devidamente seus livros de escripturação mercantil, ou nelles tem commettido algum vicio".

"Art. 18. A exhibição judicial dos livros de escripturação commercial por inteiro, ou de balanços geraes de qualquer casa de commercio, só póde ser ordenada a favor dos interessados em gestão de successão, communhão ou sociedade, administração ou gestão mercantil por conta de outrem, e em caso de quebra".

"Art. 19. Todavia, o Juiz ou Tribunal do Commercio, que conhecer de huma causa, poderá, a requerimento da parte, ou mesmo *ex officio*, ordenar, na pendencia da lide, que os livros de qualquer ou de ambos os litigantes sejão examinados na presença do commerciante a quem pertencerem e debaixo de suas vistas, ou na de pessoa por elle nomeada, para delles se averiguar e extrahir o tocante á questão. Se os livros se acharem em diverso districto, o exame será feito pelo Juiz de Direito do Commercio respectivo, na fórma sobredita; com declaração, porém, de que em nenhum caso os referidos livros poderão ser transportados para fóra do domicilio do commerciante a quem pertencerem, ainda que elle nisso convenha".

[15] BRASIL. Supremo Tribunal Federal, RE 2172, Min. rel. Nelson Hungria, Tribunal Pleno, j. 10.07.1953.

[16] Código Penal (Decreto-Lei nº 2.848/1940): "Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: (...)".

sobre tudo que sabem a respeito de seus clientes, em virtude da relação contratual que com estes mantém; mas tal obrigação não pode ser invocada quando se trata de prestar esclarecimentos exigidos pela Justiça". O que se proíbe é que o banqueiro seja obrigado a depor como testemunha, o que não seria o caso.

Como se vê, as duas decisões, provocadas pela atuação de bancos, destacam a necessidade de se "habilitar a justiça" pela prestação de informações e colocam na autoridade judiciária a capacidade de balizar a validade da obrigação de fornecer a obrigação. Os acórdãos não tratam de direito à privacidade do cliente que seria atingido, mas do alcance do sigilo profissional de bancos, considerando as suas obrigações (dever de confidencialidade) com esses clientes – perspectiva que não é particularmente significativa considerando que a discussão foi suscitada por bancos que assim o podem ter feito por razões processuais e que a proteção à intimidade e à vida privada só foi consagrada na Constituição Federal de 1988. No entendimento mantido pelo STF, o banco não carrega segredos absolutos e autoridades judiciais podem determinar sua colaboração para esclarecimento da verdade, conquanto sirva a esse propósito e o pedido não constitua devassa. Ao mesmo tempo, entretanto, não há qualquer linguagem que descarte que, como regra, clientes possam e devam esperar sigilo de suas informações e transações financeiras mantidas junto ao banco, o que tanto respeita como lhes confere a prerrogativa de, no dia a dia, compartilhar tais informações apenas com quem queiram e no contexto específico de comércio e negócio com certas pessoas e empresas.

Esse velho embate entre empresas preocupadas com seus deveres na preservação de dados de seus clientes e interesses do Estado na "habilitação da justiça" pela produção de prova perdura em novas versões até hoje. Se não há precedente claro nem previsão legal explícita que esclareça os termos e as circunstâncias em que pode haver transferência de dados de clientes a autoridades do Estado, há discussão. O debate em geral pode se dar em quatros níveis: (i) se a medida é constitucionalmente possível em tese; (ii) se a medida tem previsão legal; (iii) se a medida depende de autorização judicial prévia; (iv) se a medida tinha justa causa para ocorrer no caso concreto.

Atualmente, por exemplo, há ações diretas de inconstitucionalidade propostas por entidades representativas de empresas de telefonia contra leis ambíguas e que estabeleceram prerrogativas a autoridades policiais de acesso a dados – cadastrais e, pontualmente, metadados – sem ordem judicial. Por exemplo, na Ação Direta de Inconstitucionalidade (ADI) 5063/DF, questionam-se dispositivos da Lei das Organizações Criminosas (Lei nº 12.850/13), cuja leitura combinada seria usada para requerer registros telefônicos (histórico de ligações) sem autorização

judicial; na ADI 4906, discute-se o art. 17-B da Lei de Lavagem de Dinheiro (Lei nº 9.613/98), que permite a autoridades e ao Ministério Público acesso a dados cadastrais mantidos por certas entidades públicas e privadas, sem autorização judicial prévia; e na ADI 5642, debruça-se sobre os art. 13-A e 13-B incluídos no CPP pela Lei nº 13.344/16, que, para investigações de crimes de tráfico de pessoas, permitem acesso a dados cadastrais e, em certas circunstâncias, também a dados de geolocalização, sem ordem judicial, entre outros problemas da redação ambígua.[17] A primeira pende de julgamento; a segunda teve o julgamento virtual suspenso, já com desfecho aparente[18] pela improcedência; e o julgamento da terceira foi interrompido por pedido de vista após voto inicial pela improcedência.

Empresas de internet também já fazem a mesma atuação litigiosa. Na Ação Declaratória de Constitucionalidade nº 51, entidade de classe do setor de empresas de tecnologia buscou do STF a declaração de constitucionalidade do Decreto nº 3.810/2001, que rege acordo de cooperação judiciária entre Brasil e Estados Unidos (MLAT), bem como de dispositivos acerca de cartas rogatórias nos Códigos de Processo Civil e Penal. A alegação era de que tribunais e autoridades do Brasil frequentemente desconsideram tais mecanismos diplomáticos e forçam empresas, com multas e ameaças de prisão e bloqueio, a fornecerem no Brasil dados (conteúdo de comunicações) regidos por lei estrangeira. A discussão é de jurisdição na internet, mas no fim envolve também proteções de privacidade em face do Estado: soluções unilaterais, que desconsideram mecanismos internacionais, tendem a acelerar um processo de "vale tudo" entre as nações: o país com a pior lei de privacidade do mundo vai reger como pode acessar dados controlados por empresas que possuem presença global na internet. Em 2023, o STF decidiu que

[17] ABREU, Jacqueline de Souza; ANTONIALLI, Dennys Marcelo. *Vigilância sobre as comunicações no Brasil*: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf.

[18] O relator Min. Nunes Marques votou pelo conhecimento em parte da ação e, na parte conhecida, pela improcedência, declarando constitucional o art. 17-B da Lei nº 9.613/1998. Foi acompanhado dos Min. Alexandre de Moraes, Cármen Lúcia, Luiz Fux e Luís Roberto Barroso. Na divergência, o Min. Marco Aurélio votou para conhecer da ação apenas quanto a concessionárias de telefonia fixa e, nessa extensão, julgar procedente, pela inconstitucionalidade do dispositivo. Já os Min. Gilmar Mendes, Edson Fachin, Dias Toffoli e Rosa Weber votaram para conhecer parcialmente da ação e, nessa parte, julgar parcialmente procedente, para excluir do âmbito de incidência do dispositivo questionado a possibilidade de requisição de qualquer outro dado além daqueles de qualificação pessoal, filiação e endereço. O julgamento foi suspenso para aguardar voto de novo Ministro a ser integrado à Corte (no caso, o voto do Min. Cristiano Zanin). Tendo em vista que o art. 17-B trata explicitamente de dados cadastrais de "qualificação pessoal, filiação e endereço", na prática o grupo que formou a maior divergência aparenta ter apenas exercido zelo contra possíveis excessos em interpretações e igualmente entendido pela constitucionalidade do dispositivo.

o art. 11 do Marco Civil da Internet autoriza requisições diretas de dados, sem a necessidade de recorrer a tais meios diplomáticos.[19]

Também no STF, pende o julgamento do Recurso Extraordinário nº 1.301.250, tema de repercussão geral nº 1.148 reconhecido em 2021, levado pelo Google, em que se debate a constitucionalidade de ordens judiciais que determinam a quebra de sigilo de dados de pessoas indeterminadas a partir de termos de busca que tenham pesquisado na internet[20] ou de lugares que tenham passado, para fins de instrução de investigações criminais. A empresa alega que tais ordens violam a Constituição Federal porque a proteção constitucional da privacidade e da proteção de dados pessoais exige algum tipo de justa causa contra as pessoas afetadas e que não há previsão legal que autorize medidas investigativas sobre pessoas não suspeitas. Na prática, isso significaria permitir que os serviços de busca e localização da empresa sejam transformados em mecanismos de vigilância. Em setembro de 2023, a relatora Min. Rosa Weber votou pelo provimento do recurso, seguida de pedido de vista do Min. Alexandre de Moraes, que retirou o caso da pauta virtual.

Como se percebe, há uma aparente tendência do Judiciário em afirmar que empresas devem sim ter uma postura colaborativa com o Estado no compartilhamento de informações pessoais de seus clientes para "habilitar a justiça". Isso não necessariamente significa derrota da perspectiva regulatória de proteção a direitos de privacidade e proteção de dados pessoais. Os casos não deixam de demarcar aspectos relevantes sobre limites do poder do Estado, explorando contornos de deveres de sigilo, trazendo à luz como ambiguidades podem ser exploradas e alcançando a reafirmação de razões jurídicas que salientam a importância da existência de justa causa para a restrição de um direito à privacidade na área de prevenção e repressão criminal, e a impossibilidade de devassas, excessos e práticas não previstas em lei. A atuação litigiosa de empresas convocadas para intermediar vigilância acaba por mostrar que a camada de controle e fricção que decorre da necessidade de acionar agentes privados para executar medidas de vigilância, a que apelava o Min. Rezek, de fato existe – e não é sem valor do ponto de vista de proteção da privacidade. Como se passa a ver a seguir, é esperado e justificável que seja assim.

[19] BRASIL. Supremo Tribunal Federal. ADC 51, Rel. Min. Gilmar Mendes, Plenário, j. 18.04.2023, *DJe* 28.04.2023.

[20] BRASIL. Superior Tribunal de Justiça, RMS 60698, Rel. Min. Rogério Schietti Cruz, Terceira Seção, j. 26.08.2020, *DJe* 04.09.2020.

3 Uma relação fiduciária e a separação informacional dos poderes

Os dados que bancos, empresas de telefonia e empresas de tecnologia em geral possuem foram originalmente coletados para finalidades completamente diversas do que servir a investigações e instrução processual: no caso de bancos, formar o histórico de transações, registrar valores de um depósito; no caso de empresas de telefonia, registrar ligações para fins de cobrança; no caso de empresas de tecnologia, para prover seus serviços de troca de *e-mail*, troca de mensagens, *microblog*, compartilhamento de fotos e vídeos, de localização e rotas de trajetos, de pesquisa por informações e notícias. A colaboração exigida pelo Estado é, portanto, um específico *uso secundário* forçado mediante *transferência* e/ou *análise* dessas informações coletadas e mantidas por tais empresas.[21] Diante disso, não é sem razão que existem iniciativas até hoje de questionamento daquilo que aparente ser abuso, desrespeitar as regras do jogo até então, ou que seja novo, não ainda testado – isto, sem clareza se possui amparo legal.

Proponho aqui reconhecer – tanto para dar conta do fenômeno de questionamento por empresas quanto para elaborar seus fundamentos – que nós temos relações fiduciárias com essas empresas. Esperamos delas tratamento que seja respeitoso de nossa privacidade e atenta aos danos morais que o desrespeito pode provocar – que preservem nossos dados com segurança contra terceiros, que impeçam mau uso interno, que não façam uso fora daquilo previamente combinado e razoável para o contexto do serviço contratado, que atuem na forma da lei.[22] Nós contamos com isso para exercer práticas de privacidade em torno da acessibilidade de aspectos de nossa vida pessoal, de nossa identidade e de nossas relações sociais, a outras pessoas.[23] Se entregar dados para bancos, empresas de telefonia e empresas de internet significasse abrir mão desses dados e dos dados gerados no uso desse serviço a qualquer pessoa, a relação em si de confiança com a empresa que viabiliza o negócio seria fragilizada e colocada

[21] Para referências do direito da proteção de dados pessoais, ver DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006; MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014; BIONI, Bruno R. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

[22] Hartzog e Richards vêm desenvolvendo essa ideia já em vários trabalhos e falam em um dever de "lealdade". Ver HARTZOG, Woodrow; RICHARDS, Neil. "Taking Trust Seriously in Privacy Law", *Stanford Technology Law Review*, vol. 19, 2016, pp. 431-472; HARTZOG, Woodrow; RICHARDS, Neil. "A Duty of Loyalty for Privacy Law", *Washington University Law Review*, vol. 99, 2021, pp. 961-1021.

[23] Para uma perspectiva nessa linha dentro da jurisprudência americana sobre alcance do poder de busca e apreensão do Estado, ver BRENNAN-MARQUEZ, Kiel. "Fourth Amendment Fiduciaries", *Fordham Law Review*, vol. 84, nº 2, 2015, pp. 611-659.

em xeque. Isso significa que essas empresas podem e devem poder questionar o Estado quando são forçadas a atuar fora dos parâmetros legais, de forma excessiva ou abusiva, e que devem preservar a privacidade de seus clientes.

No passado, já reconhecemos que relações profissionais com advogados, médicos, padres poderiam estar cobertas de uma expectativa de privacidade sobre o que é dito e compartilhado no contexto dessas relações, inclusive a ponto de ser tutelado especialmente pelo direito: garantias de sigilo médico, de sigilo sacramental, do sigilo cliente-advogado, que visam proteger os valores constitutivos dessa relação (permitir a ampla defesa com devido processo legal, garantir o melhor tratamento médico possível, preservar a busca de harmonização com o sagrado). Essas garantias permitem que seja resguardado o "sigilo" de dados e informações que compartilhamos com algum terceiro que venha ter acesso a elas por alguma relação legítima socialmente relevante. Não perdem o seu caráter "privado", não caem em domínio público apenas por isso. Nesse contexto, não há nenhum impedimento *a priori* para reconhecer relações ou interesses análogos, ainda que não coincidentes: bancos servem à facilitação da vida no mercado; empresas de telefonia, à comunicação interpessoal a distância; serviços digitais, a um enorme universo de atividades humanas no domínio virtual. Não é porque interagimos com esses serviços que estamos abandonando interesses legítimos de privacidade.[24] Não há por que negar, portanto, que seja importante preservar as condições válidas de manutenção da relação fiduciária entre tais empresas e seus clientes.

Paralelamente, a história confirma que a preocupação com os limites do poder do Estado está na base da existência de qualquer Constituição democrática que preserve direitos fundamentais. Notadamente, se há alguma lição a ser extraída de garantias clássicas como as insculpidas no art. 5º, inciso XI (inviolabilidade do domicílio) e do art. 5º, XII (inviolabilidade de comunicações), é um interesse em não admitir que o Estado tenha acesso irrestrito, fora de balizas concretas, nem possa transformar estruturas de comunicação e casas em máquinas de facilitação de vigilância que anulem a privacidade. Igualmente, o desenvolvimento de práticas jurídicas como o direito da proteção de dados pessoais reforça uma perspectiva contrária à unificação de bases de dados – colocando ênfase na "separação informacional dos poderes",[25] dentro de estruturas do próprio Estado, mas também,

[24] Demonstrando a importância da perspectiva contextual, ver NISSENBAUM, Helen. "Privacy as Contextual Integrity", *Washington Law Review,* vol. 79, pp. 119-158, 2004. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10. Também SELBST, Andrew D. "Contextual Expectations of Privacy", *Cardozo Law Review*, vol. 35, 2013, pp. 643–709.

[25] "Toda tentativa de enxergar a administração pública como uma unidade informacional é incompatível com uma proteção eficiente de dados'. Se saber é poder, o Estado não pode saber tudo, porque um Estado que tem conhecimentos ilimitados tem também um poder ilimitado. O direito de proteção de dados, que começa como direito subjetivo, mostra-se, ao menos em boa parte, como garantia institucional, relativa à

naturalmente fora dele: não deixando poderes econômicos e políticos acumularem-se pelo intercâmbio desregrado de dados.

A aprovação de leis de proteção de dados pessoais, que impõem obrigações a controladores de dados, reforça esse ponto.[26] Tais leis exigem que cada operação e processo que implique tratamento de dados pessoais seja justificada, tendo em vista sua finalidade. Transferências de dados de uma empresa a uma entidade externa, após decisão judicial ou requisição administrativa, por exemplo, até podem ter base legal em tese ("cumprimento de obrigação legal ou regulatória" é uma das hipóteses de legalidade, a exemplo do art. 7º, II da Lei nº 13.709/18), mas a validade dessa base precisa ser segura: se a validade da decisão ou da requisição é controversa, é igualmente controverso se a base legal para a transferência da empresa para o agente externo existe. Isso se aplica inclusive quando requisições e ordens são dirigidas a pretexto de servir para investigações criminais e segurança pública.

Neste ponto, cabe uma breve nota mais dogmática: ainda que uma entidade policial venha a se dizer isenta de atender a Lei Geral de Proteção de Dados Pessoais (LGPD) para fim exclusivo de atividade de investigação criminal (art. 4º, III, *d*), por exemplo, a empresa privada está sujeita à LGPD e deve justificar tais fluxos de transferência, uma vez que os dados em questão não foram tratados exclusivamente para tal fim e agentes privados não podem ser controladores de dados para tais fins (art. 4º, III, §2º). Impedir que empresas suscitem preocupações acerca da possível ausência de interesse público, de proporcionalidade, de respeito aos princípios da lei (art. 4º, §1º), em favor de uma cooperação forçada representaria anular um mecanismo de controle – um sistema de freios e contrapesos – inerente às preocupações que deram origem a tal legislação.[27]

própria estrutura da sociedade e do Estado. Nesse nível macro o direito se transforma em uma exigência de separação informacional dos poderes" (GRECO, Luís. O inviolável e o intocável no direito processual penal: considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência). *In*: WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal*: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. São Paulo: Marcial Pons, 2018, pp. 21-82).

[26] Sobre a perspectiva da distribuição do poder como um dos aspectos centrais do direito da proteção de dados pessoais, ver RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Organizado por Maria Cecilia Bodin de Moraes. Traduzido por Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008, p. 24 e RICHARDS, Neil; HARTZOG, Woodrow. "A Relational Turn for Data Protection?", *European Data Protection Law Review*, vol. 6, nº 4, 2020, pp. 492-497.

[27] Ver também o tipo de análise depurada que ANPD faz (BRASIL, Autoridade Nacional de Proteção de Dados Pessoais (ANPD). *Nota Técnica nº 175/2023/CGF/ANPD, SEI 00261.001722/2023-13*, [sobre acordo de cooperação entre MJSP e CBF], 25 de outubro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf. Acesso em: 30 jan. 2024).

É de se esperar, portanto, a preservação do compromisso básico com o controle do poder coercitivo estatal também em uma sociedade caracterizada pelas novas "tecnologias de informações e comunicação" (TICs) que acabam facilitando intermediação de atividades de vigilância.[28] Se hoje parte do nosso "domicílio" consta em uma conta de computação em nuvem, as mesmas razões que nos levaram a proteger o domicílio devem ser consideradas para proteger novos "territórios".[29] Se hoje as TICs carregam e geram muito mais dados que conteúdo de comunicações e fazem muito mais do que só viabilizar a privacidade de comunicações, mas acumulam diversos outros dados que informam nossa identidade e nossas relações sociais e compõem o exercício de nossa autonomia, não há por que descartar proteções de plano; pelo contrário. Não se desconhece que tais empresas usam os mesmos dados para seus próprios fins econômicos e que há concentração no mercado. A análise jurídica do assunto, no entanto, merece tratamento direcionado e analítico: o direito do consumidor e da proteção de dados deve lidar com as questões consumeristas e de justiça nas relações informacionais entre privados; o direito concorrencial com controle de condutas e estruturas. A existência de vício em outras áreas não autoriza, por sua vez, que haja abuso do poder do Estado na intermediação de vigilância. O fato de que a existência de grandes empresas pode ser conveniente ao Estado em seus propósitos de vigilância merece olhos críticos.

A importância da demarcação dessa relação fiduciária à base de nossas práticas de privacidade e o reconhecimento da relevância da separação informacional dos poderes não significa, por outro lado, e como já se viu, que o Estado não possa legitimamente acessar informações em condições preestabelecidas. O combate ao crime, a responsabilização correta daqueles responsáveis por ilícitos e a instrução adequada de processos com vistas a evitar a punição de inocentes está entre os interesses e razões primordiais da instituição do Estado. Considerando que o acúmulo de poder político do Estado, por outro lado, também sujeita pessoas a abusos, erros e excessos no exercício desse poder, é natural que existam salvaguardas processuais para quando e como restrições de direitos podem ocorrer e mesmo a delimitação de limites duros sobre o que o Estado não pode fazer, a partir de nossos compromissos básicos com princípios morais de proteção à dignidade, à liberdade e à igualdade.[30]

[28] HILDEBRANDT, Mireille. Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology. Cheltenham, UK: Edward Elgar Publishing, 2015, p. 155.

[29] Explorando esse ponto, ver STRANDBURG, Katherine J. "Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change". *Maryland Law Review*, vol. 70, 2011, pp. 614-680.

[30] Ver também GUTWIRTH, Serge; DE HERT, Paul. "Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power". *In*: CLAES, Erik; DUFF, Antony; GUTWIRTH, Serge. *Privacy and the Criminal Law*. Antwep/Oxfor: Intersentia, 2006, pp. 61-104.

O próximo item debate esse ponto a partir da relevância de questões atinentes ao sigilo telemático. Comunicações privadas são documentadas em escala como nunca foram antes. Pessoas deixam vestígios, pegadas virtuais de suas atividades como nunca deixaram antes.[31] E de atividades que nunca antes deixaram registros tão precisos e detalhados – ex.: de batimentos cardíacos, de leituras feitas, de informações buscadas, de emoções, de trajetos. Em um universo em que empresas de tecnologia controlam um volume cada vez maior de informações de usuários – e se tornam baús de tesouro e máquinas do tempo no âmbito de investigações –, é imprescindível que a regulação de interações e compartilhamentos de dados com autoridades públicas para fins de investigação estejam balizados em lei e que não haja uma convergência silenciosa entre poderes econômico e político. Esse aspecto torna a litigância de empresas contra medidas de vigilância do Estado potencialmente abusivas, excessivas ou sem previsão legal ainda mais importante, embora esteja longe de ser suficiente para satisfazer o quadro regulatório. O próximo item se debruça sobre esse último ponto.

4 Regulação atual e necessidade de aperfeiçoamento

A Constituição Federal brasileira de 1988 manifesta seu compromisso com a proteção da privacidade notadamente por meio de um conjunto de incisos: um que protege a inviolabilidade da intimidade e da vida privada, outro que garante a inviolabilidade do domicílio, bem como um terceiro que protege a inviolabilidade do sigilo de comunicações (art. 5º, incisos X, XI e XII). Mais recentemente, também o direito à proteção dos dados pessoais, inclusive nos meios digitais, foi incluído na Constituição (art. 5º, LXXIC) e reforçou esse compromisso.

Já o escopo da proteção constitucional ao "sigilo telemático", que aqui vou usar para me referir à proteção de dados eletrônicos, em particular no contexto de questionamentos das situações e condições em que autoridades estatais podem acessar tais informações, é controverso de longa data.[32] Em síntese, embora haja

[31] SCHNEIER, Bruce. *Data and Goliath*: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton & Company, 2015, pp. 13-19.

[32] Ver também ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. "A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência". *Revista de Investigações Constitucionais*, vol. 4, nº 3, 2017, pp.167-200; ABREU, Jacqueline de Souza; ANTONIALLI, Dennys Marcelo. *Vigilância sobre as comunicações no Brasil*: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf; QUEIROZ, Rafael Mafei Rabelo. "Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de trocas de mensagens". *In*: *Caderno Especial* – A Regulação da Criptografia no Direito Brasileiro, organizado por Danilo Doneda, 13–26. São Paulo: Thomson Reuters Brasil, 2018.

hoje certo reconhecimento jurisprudencial de que "comunicações de dados" são protegidos pela Constituição no sentido de exigir ordem judicial prévia para acesso por autoridades estatais, há uma discussão pendente e acentuada pelo avanço tecnológico sobre em que medida a proteção se estende e deve se estender a "dados armazenados". Isso porque, se só dados em trânsito (em "comunicação") estão ou estivessem protegidos, nenhum dado estacionado, já estático, inclusive aqueles salvos em um celular, estariam. Diante da desconexão normativa que isso gera, há uma tendência[33] a reconhecer a proteção a *conteúdo* de comunicações – no sentido de também exigir uma autorização judicial prévia para acesso para fins de investigações, ainda que o tal conteúdo já esteja armazenado. Por exemplo, para que uma autoridade policial possa fazer uma busca que inclua acesso ao aplicativo WhatsApp (que inclui *conteúdo* de comunicações) mantido em um dispositivo celular, seria preciso obter decisão judicial. Por outro lado, nessa lógica, seria possível acessar histórico de chamadas e fotos sem autorização judicial prévia.[34]

Essa discussão às vezes chega a empresas convocadas a fazer intermediação da vigilância e em certa medida é antecipada pela lei infraconstitucional mais específica aplicável a essas relações. O Marco Civil da Internet (Lei nº 12.965/14) é hoje o principal regime jurídico aplicável a empresas de tecnologia e que regula as condições em que podem ser requeridos dados de usuários delas. Oferece importantes parâmetros: estabelece que a disciplina do uso da internet no Brasil tem como princípio, entre outros, a proteção da privacidade, a proteção dos dados pessoais, na forma da lei (art. 3º, II e III). Também resguarda direitos à "inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação"; "inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei"; "inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial"; "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei" (art. 7º, I, II, III e VII, respectivamente).

---

[33] *Vide* BRASIL. Superior Tribunal de Justiça. RHC 51.531, rel. Min. Nefi Cordeiro, Sexta Turma, j. 19.04.2016, *DJe* 09.05.2016; BRASIL. Supremo Tribunal Federal, HC 168052, rel. Min. Gilmar Mendes, Segunda Turma, j. 20.10.2020.

[34] A discussão se a necessidade de autorização judicial para acesso a dados armazenados que não são conteúdo de comunicação se perfaz no ARE 1042075, tema 977 de repercussão geral do STF, ainda está pendente de julgamento. No STJ, alguns julgados já delimitam essa diferença, ver ABREU, Jacqueline de Souza. Comentário ao REsp 1.782.386/RJ – STJ (Acesso a agenda de contatos de celular por autoridade policial sem autorização judicial). *Revista dos Tribunais*, vol. 1026, pp. 371-406, 2021.

Embora se refira a "hipóteses previstas em lei", a principal ferramenta da lei para balizar fornecimentos desses dados é a referência à necessidade de ordem judicial. Pelo art. 10, §1º, "O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º". Já "O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º" (art. 10, §2º). Mas ressalva: "O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição" (art. 10, §3º).

O requisito formal da ordem judicial é explicitamente acompanhado de um tipo claro de *padrão de justificação* no Marco Civil da Internet para o caso de fornecimento de registros de conexão e acesso a aplicações de internet (art. 22[35]): o requerimento deve conter fundados indícios da ocorrência do ilícito, justificativa motivada da utilidade dos registros solicitados e período ao qual se referem. Essas informações se referem a endereços de IP, acompanhados de data e hora, informações que são cruciais para *rastrear* a origem de atividades praticadas na internet: o usuário pode ter praticado algum crime usando contas falsas e usando pseudônimos, mas com o rastreamento de IPs é ainda, em tese, possível avançar nas investigações. O padrão de justificação desenhado pelo dispositivo leva em conta o propósito a que foi concebido em seu histórico legislativo:[36] permitir a obtenção de dados relativos a ilícitos praticados na internet como forma de identificar alguém – sobre quem se tem suspeita individualizada – junto aos únicos agentes capazes de auxiliar com o fornecimento de tais dados.

[35] Marco Civil da Internet (Lei nº 12.965/14): "Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet. Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade: I – fundados indícios da ocorrência do ilícito; II – justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e III – período ao qual se referem os registros".

[36] SANTARÉM, Paulo Renã da Silva. "O direito achado na rede: a emergência do acesso à Internet como direito fundamental no Brasil". Dissertação de Mestrado, Faculdade de Direito da Universidade de Brasília, 2010. Disponível em: https://repositorio.unb.br/handle/10482/8828; BRITO CRUZ, Francisco Carvalho de. *Direito, democracia e cultura digital*: a experiência de elaboração legislativa do Marco Civil da Internet. Dissertação de Mestrado, Universidade de São Paulo, 2015. Disponível em: https://doi.org/10.11606/D.2.2016.tde-08042016-154010.

Como se vê, o Marco Civil da Internet divide o universo de dados e de hipóteses de regulação entre conteúdo de comunicações em fluxo, conteúdo de comunicações privadas armazenadas, registros de IP e outras informações que possam contribuir para identificar alguém. Exceto ao que parecem ser referências pontuais à Lei nº 9.296/96 (Lei de Interceptações), que exige indícios de autoria ou participação para deferimento da medida sobre alguém e ao art. 22 do próprio Marco Civil, basicamente não se fala em requisitos materiais para a quebra de sigilo/fornecimento desses dados. Também não trata de todo o universo de dados que não são conteúdo de comunicações nem registros de IP ou dados de identificação. Diante disso, e do impasse de interpretação constitucional, há um amplo espectro de dados cuja proteção é controversa no contexto de pedidos de acesso por autoridades estatais.

Tendo em vista o que até aqui se apresentou sobre intermediação de vigilância, há de se reconhecer que a legislação até o momento parece deixar de fora um amplo espectro de informações que podem ter implicações a direitos fundamentais e merecerem ser protegidas como parte de um direito constitucional ao sigilo telemático, inclusive quando, a princípio, controladas por empresas. Imagine-se serviços de montagem de árvore genealógica e ancestralidade. Também serviços de geolocalização e de assistentes domésticos como o Amazon Echo. Atualmente, a fragilidade da regulação dá lugar a muitas controvérsias sobre hipóteses de acesso a essas informações. Se colocar um robô doméstico para auxiliar em atividades em casa viesse a significar que garantias da inviolabilidade do domicílio e o respeito à privacidade pudessem ser dribladas por autoridades porque os dados estão armazenados e não são comunicações, a direção em que estamos indo é diluição de proteções constitucionais e não de reafirmação delas também numa sociedade digital.

A intermediação de vigilância não pode ser naturalizada para contextos novos como se normal fosse: não é porque podem passar a existir empresas ou novos serviços que capturam algum tipo de registro sobre nossas atividades (e até pensamentos) que instantaneamente o Estado deve ganhar a capacidade de extrair essas mesmas informações para um universo irrestrito e indiscutido de usos no processo penal e na segurança pública e por regras judiciais. As regras do jogo sobre produção de provas são e devem ser debatidas e fixadas legislativamente: sem elas, é patente o risco de ter um direito à privacidade violado erroneamente, sem um nível apropriado (publicamente debatido e fixado) de justa causa, de ter sua privacidade exposta em excesso ou mesmo efetivamente abusada (caso de uma quebra de sigilo sem razão legítima ou por razões escusas). E pior: sem regulação, o casuísmo leva ao tratamento desigual de pessoas em situações análogas.

Nesse contexto, empresas podem e devem suscitar problemas ou mesmo questionar decisões, pedidos e leis que não aparentem ter passado por um teste

constitucional, ter previsão legal ou preencher os requisitos legais. A partir do que foi visto, torna-se inevitável concluir que é saudável do ponto de vista da privacidade e do regime da proteção de dados pessoais que exerçam essa fricção. Do contrário, esse enorme universo novo de dados e de possibilidades de vigilância estatal por "esticadinho" representaria enorme acúmulo de poder e, assim, de riscos de abusos e excessos. Nesse sentido, inclusive, do ponto de vista regulatório, é importante que empresas não se acomodem a ponto de perder o interesse em questionar medidas potencialmente ilícitas e que, obviamente, e ao contrário do que o Min. Rezek parecia sugerir, a mera separação Estado-empresa não seja vista como suficiente para mitigar riscos.

Embora a atuação litigante de empresas privadas seja importante, certamente não é suficiente. O Judiciário tem opções limitadas no tratamento dessas questões jurídicas: a discussão tende a se reduzir a se é necessária autorização judicial prévia para acesso ou não a certo dado. Há, no entanto, um amplo espectro de ferramentas regulatórias existentes[37] para lidar com medidas de vigilância e uso de dados, que vão além da exigência ou não de uma autorização judicial prévia: como regras de minimização, de expiração, de barreiras e balizamentos a encontro fortuito,[38] de padrão de justificação, de controle interno, de supervisão e contenção preventiva de riscos. O foro para projetá-las e desenhá-las é o processo legislativo. A melhor estratégia regulatória depende da medida concreta em análise. Assim, embora na esfera judicial de litigância possa ser reconhecido que certa ordem ou pedido é inconstitucional, ilegal ou inválido, inclusive por provocação de intermediários da vigilância, não é lá o foro ideal do debate regulatório.

Um contra-argumento frequente é de que impedir ou dificultar o uso de novas tecnologias não reguladas deixaria o Estado despreparado para combater criminosos que não têm o mesmo limite e usam toda e qualquer nova tecnologia a seu favor. A rapidez do avanço tecnológico em comparação com a velocidade de mudanças legislativas não pode servir de justificativa para que o princípio da legalidade seja abandonado: o reconhecimento judicial de que a matéria precisa passar por debate público, pois não tem previsão legal, deve na verdade catalisar tais debates – e se houver vontade política de autoridades a que a medida venha

[37] OHM, Paul. "The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause". *In*: *The Cambridge Handbook of Surveillance Law*, organizado por David Gray e Stephen Henderson, p. 491-508. Cambridge: Cambridge University Press, 2017.

[38] A possibilidade e ampla admissão do encontro fortuito confere interesses secundários (senão principais, disfarçados) para quebras de sigilo. Em muitas oportunidades, o interesse no acesso a dados digitais é descobrir *outros crimes* para além do investigado. A exemplo disso, ver: VILALTA, Luís Antônio; MACHADO, Talles Amaral. "Novos Paradigmas da Investigação Criminal". *Revista Brasileira de Ciências Policiais* 9, nº 1 (8 de novembro de 2018): 13-41. p. 30 Disponível em: https://doi.org/10.31412/rbcp.v9i1.542.

ser admitida, o projeto de lei será proposto e a discussão acontecerá.[39] Como sociedade, podemos decidir que a prerrogativa de privacidade em questão é preciosa demais para comportar riscos de uso abusivo, excessivo e errado, mesmo que isso signifique que processos judiciais não terão acesso a esse novo tipo de informação. Podemos tomar a decisão coletiva de não permitir certa medida de vigilância mesmo a custo de não ter máxima eficiência em processos preventivos e repressivos, de modo que deve existir um canal para tal decisão.

Em termos de transparência, cabe ainda levar a essa área de intermediação da vigilância do Estado a exigência legal de publicação de relatórios sobre quantos pedidos de fornecimento de dados foram feitos, quantos foram deferidos/indeferidos, da parte de autoridades, e de quantos pedidos foram recebidos e quantos foram atendidos, da parte de empresas, para que possam ser cruzados e a acurácia das informações e eventuais estudos sobre qualidade de revisão judicial possam ser viabilizados. Pode também ser dada transparência a medidas de maneira anonimizada e por amostragem, para permitir estudo crítico de arranjos sem prejuízo ao sigilo de casos concretos, além do escrutínio de órgãos de controle interno e externo. Tais mecanismos são cruciais para avaliar se as salvaguardas estão funcionando e para permitir debate público qualificado periódico sobre tanto.

Por fim, devemos avançar discussões sobre como ampliar mecanismos de *accountability* e notificação dos titulares de dados nessa área que sejam capazes de vencer o segredo de justiça sobre quase tudo que se faz e que só é questionado, *post facto*, quando alguém é acusado. Usuários afetados por quebras de sigilo podem nunca ficar sabendo que foram alvo de pedidos abusivos e ilegais (por contra de determinações de silenciamento – *gag orders*) – essa era, aliás, uma das preocupações do Min. Rezek com escutas ilegais. Também não "veem" as devassas de que foram alvo, sem possibilidade de questionarem responsabilização pelos danos, ao contrário da ciência que tomam quando a medida é física e diretamente visível. Muitas medidas são feitas sob segredo de justiça. Nessas condições, devemos buscar mecanismos institucionais que façam as vezes do controle que esperamos em respeito à dignidade.[40]

[39] FRIEDMAN, Barry. *Unwarranted: policing without permission*. New York: Farrar, Straus, Giroux, 2017, p. 215 (e-book).

[40] Pensando em uma instituição que pudesse oferecer contraditório na fase de investigações, ver, por exemplo: FRAGOSO, Nathalie; RODRIGUES, Gabriel Brezinski. "Protodefesa à Brasileira: Contraditório e Ampla Defesa em Investigações Sigilosas". *Direito Público* 18, nº 100 (2021): 581-605.

5 Conclusão

Empresas controladoras de dados pessoais foram historicamente e continuarão sendo acionadas para atuarem em assistência ao Estado na "habilitação da justiça". Como visto ao longo do trabalho, diante disso, em certas ocasiões foram levadas a questionar ordens de quebra de sigilo ou mesmo leis que pareciam incoerentes com a Constituição. Isso mostra que podem trazer questionamentos importantes sobre o teor, natureza e amplitude das ordens antes que a violação irreversível à privacidade ocorra pela instrumentalização de seus serviços, o que é especialmente valioso caso sejam ordens abusivas e/ou não previstas em lei.

Há vários ânimos que podem mobilizar empresas a embarcar em disputas sobre privacidade e proteção de dados pessoais em face do Estado – modelos de negócios das empresas, estruturas técnicas de produtos e serviços, interesses de usuários (comuns ou corporativos).[41] Esse artigo buscou explorar e demonstrar aqueles que se alinham a esforços de proteção de dados pessoais: o dever fiduciário que é exigível dessas empresas que possuem um relacionamento específico baseado no compartilhamento de dados pessoais com as pessoas atingidas – fundamento para autorizar questionamentos e parâmetro de cobrança de sua própria atuação – e a necessidade de contenção de poder. Permitir o intercâmbio desregrado de dados entre setores público e privado ou mesmo a cumplicidade entre agentes públicos e privados mesmo diante de ordens ilegais está desalinhado com propósitos básicos do direito.

Aperfeiçoamento regulatório é mais que necessário. A regulação atual dá lugar a falsas diferenças de tratamento a partir de alguma suposta natureza imanente de certos tipos de dados e não está preparada para lidar com ferramentas novas e abrangentes de vigilância baseadas em enormes volumes de dados. A incorporação naturalizada desses novos serviços ao braço de intermediação da vigilância contraria os propósitos básicos de contenção do poder do Estado que norteiam não só o direito da proteção de dados pessoais, mas todo o direito constitucional, administrativo e processual. O ferramental regulatório deve se expandir e se fortalecer para manter-se alinhado com os fundamentos da proteção de dados pessoais.

Intermediation of State surveillance in Brazil and data protection between cooperation, litigation and constriction of private agents: history, foundation and regulation

Abstract: The article focuses on the phenomenon of intermediation of State surveillance activities in Brazil: the cooperation, most often forced, of private agents to obtain personal data of interest to the instruction of processes, investigations and public security policies. First, it recounts the first major

[41] "Developments in the Law – More Data, More Problems – Chapter 1 – Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance", *Harvard Law Review*, nº 131, 2018, pp. 1715-1741.

litigations of state surveillance intermediaries in Brazil, in order to show that current debates are a contemporary version of old discussions, and to illustrate the influence they had in demarcating the limits of the state's prerogatives. Second, it locates the foundation of these actions on the fiduciary duties that companies operating as surveillance intermediaries have with their clients and it shows how the regulation of data flows between these companies and the State is crucial for control of corporate and state power, in respect of fundamental rights and expectations of justice. Third, with an emphasis on questions posed by technological advances on telematic secrecy, the article points out the limits of current Brazilian regulation and what needs to be improved in view of the rapid technological advances.

Keywords: Surveillance. Privacy. Security. Data protection. Sharing.

Referências

ABREU, Jacqueline de Souza. Comentário ao REsp 1.782.386/RJ – STJ (Acesso a agenda de contatos de celular por autoridade policial sem autorização judicial). *Revista dos Tribunais*, vol. 1026, pp. 371-406, 2021.

ABREU, Jacqueline de Souza. Privacidade, segurança e tecnologia. Tese (Doutorado em Direito) – Faculdade de Direito da Universidade de São Paulo. São Paulo, 2022.

ABREU, Jacqueline de Souza; ANTONIALLI, Dennys Marcelo. *Vigilância sobre as comunicações no Brasil*: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais. São Paulo: InternetLab, 2017. Disponível em: http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf.

ÁVILA, Ana Paula Oliveira; WOLOSZYN, André Luis. "A tutela jurídica da privacidade e do sigilo na era digital: doutrina, legislação e jurisprudência". *Revista de Investigações Constitucionais*, vol. 4, nº 3, 2017, pp. 167-200.

BRASIL. Autoridade Nacional de Proteção de Dados Pessoais (ANPD). *Nota Técnica nº 175/2023/CGF/ANPD, SEI 00261.001722/2023-13*, [sobre acordo de cooperação entre MJSP e CBF], 25 de outubro de 2023. Disponível em: https://www.gov.br/anpd/pt-br/documentos-e-publicacoes/documentos-de-publicacoes/nota-tecnica-no-175-2023-cgf-anpd-acordo-de-cooperacao-mjsp-e-cbf.pdf. Acesso em: 30 jan. 2024.

BRASIL. Superior Tribunal de Justiça. RMS 60698, Rel. Min. Rogério Schietti Cruz, Terceira Seção, j. 26.08.2020, *DJe* 04.09.2020.

BRASIL. Superior Tribunal de Justiça. RHC 51.531, rel. Min. Nefi Cordeiro, Sexta Turma, j. 19.04.2016, *DJe* 09.05.2016.

BRASIL. Supremo Tribunal Federal. ADC 51, Rel. Min. Gilmar Mendes, Plenário, j. 18.04.2023, *DJe* 28.04.2023.

BRASIL. Supremo Tribunal Federal. HC 168052, Rel. Min. Gilmar Mendes, Segunda Turma, j. 20.10.2020.

BRASIL. Supremo Tribunal Federal. HC 170376 AgR, Rel. Min. Rosa Weber, Primeira Turma, j. 08.06.2020.

BRASIL. Supremo Tribunal Federal. MS 1047, Rel. Min. Ribeiro da Costa, Tribunal Pleno, j. 06.09.1949.

BRASIL. Supremo Tribunal Federal. MS 21729/DF, Rel. Min. Marco Aurélio. Redator p/ acórdão Min. Néri da Silveira, Tribunal Pleno, j. 05.10.1995.

BRASIL. Supremo Tribunal Federal. RE 2172, Rel. Min. Nelson Hungria, Tribunal Pleno, j. 10.07.1953

BIONI, Bruno R. *Proteção de dados pessoais*: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BRENNAN-MARQUEZ, Kiel. "Fourth Amendment Fiduciaries". *Fordham Law Review*, vol. 84, nº 2, 2015, 611-659.

BRITO CRUZ, Francisco Carvalho de. *Direito, democracia e cultura digital*: a experiência de elaboração legislativa do Marco Civil da Internet. Dissertação de Mestrado, Universidade de São Paulo, 2015. https://doi.org/10.11606/D.2.2016.tde-08042016-154010.

DEVELOPMENTS in the Law – More Data, More Problems – Chapter 1 – Cooperation or Resistance?: The Role of Tech Companies in Government Surveillance", Harvard Law Review, nº 131, 2018, pp. 1715-1741.

DONEDA, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006;

FRAGOSO, Nathalie; RODRIGUES, Gabriel Brezinski. "Protodefesa à Brasileira: Contraditório e Ampla Defesa em Investigações Sigilosas". *Direito Público* 18, nº 100 (2021): 581-605.

FRIEDMAN, Barry. *Unwarranted: policing without permission*. New York: Farrar, Straus, Giroux, 2017.

GRECO, Luís. O inviolável e o intocável no direito processual penal: considerações introdutórias sobre o processo penal alemão (e suas relações com o direito constitucional, o direito de polícia e o direito dos serviços de inteligência). *In*: WOLTER, Jürgen. *O inviolável e o intocável no direito processual penal*: reflexões sobre dignidade humana, proibições de prova, proteção de dados (e separação informacional de poderes) diante da persecução penal. São Paulo: Marcial Pons, 2018, pp. 21-82.

GUTWIRTH, Serge; DE HERT, Paul. Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power. *In*: CLAES, Erik; DUFF, Antony; GUTWIRTH, Serge. *Privacy and the Criminal Law*. Antwep/Oxfor: Intersentia, 2006, p. 61-104.

HARTZOG, Woodrow; RICHARDS, Neil. "Taking Trust Seriously in Privacy Law". *Stanford Technology Law Review*, vol. 19, 2016, p. 431-472.

HARTZOG, Woodrow; RICHARDS, Neil. "A Duty of Loyalty for Privacy Law". *Washington University Law Review*, vol. 99, 2021, p. 961-1021.

HILDEBRANDT, Mireille. *Smart Technologies and the End*(s) *of Law*: Novel Entanglements of Law and Technology. Cheltenham, UK: Edward Elgar Publishing, 2015.

LIGUORI FILHO, Carlos Augusto; SALVADOR, João Pedro Favaretto. "Crypto wars e bloqueio de aplicativos: o debate sobre regulação jurídica da criptografia nos Estados Unidos e no Brasil". *Revista da Faculdade de Direito UFPR*, vol. 63, nº 3, 2018, p. 135-161. Disponível em: https://doi.org/10.5380/rfdufpr.v63i3.59422.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor*: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

NISSENBAUM, Helen. "Privacy as Contextual Integrity". *Washington Law Review*, vol. 79, pp. 119-158, 2004. Disponível em: https://digitalcommons.law.uw.edu/wlr/vol79/iss1/10.

OHM, Paul. "The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause". *In*: *The Cambridge Handbook of Surveillance Law*, organizado por David Gray e Stephen Henderson, p. 491-508. Cambridge: Cambridge University Press, 2017.

QUEIROZ, Rafael Mafei Rabelo. "Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de trocas de mensagens". *In*: *Caderno Especial* – A Regulação da Criptografia no Direito Brasileiro, organizado por Danilo Doneda, p. 13-26. São Paulo: Thomson Reuters Brasil, 2018.

RICHARDS, Neil; HARTZOG, Woodrow. "A Relational Turn for Data Protection?", *European* Data Protection *Law Review*, vol. 6, nº 4, 2020, p. 492-497.

RODOTÀ, Stefano. *A vida na sociedade da vigilância* – A privacidade hoje. Organizado por Maria Cecilia Bodin de Moraes. Traduzido por Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

ROZENSHTEIN, Alan Z. "Surveillance Intermediaries". *Stanford Law Review,* vol. 70, 2018, p. 102-189.

SANTARÉM, Paulo Renã da Silva. *O direito achado na rede*: a emergência do acesso à Internet como direito fundamental no Brasil. Dissertação de Mestrado, Faculdade de Direito da Universidade de Brasília, 2010. Disponível em: https://repositorio.unb.br/handle/10482/8828.

SCHNEIER, Bruce. *Data and Goliath*: The Hidden Battles to Collect Your Data and Control Your World. New York: W. W. Norton & Company, 2015.

SELBST, Andrew D. "Contextual Expectations of Privacy". *Cardozo Law Review,* vol. 35, 2013, p. 643-709.

STRANDBURG, Katherine J. "Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change". *Maryland Law Review*, vol. 70, 2011, p. 614-680.

SWIRE, Peter. "The FBI doesn't need more access: we are already in the golden age of surveillance". *Just Security,* 17 de novembro de 2014. Disponível em: https://www.justsecurity.org/17496/fbi-access-golden-age-surveillance/.

TICOM, Miguel Ângelo Duarte; PEREIRA NETO, Wanderson de Freitas; ALBUQUERQUE, Silde Monteiro de; CARVALHO, Israel Carbone de; SILVA JR., Arnaldo Rosa. "Histórico, implementação e uso do Sistema Guardião® de interceptação de dados de informática e telemática nas garantias do cidadão". *Cadernos de Segurança Pública*, 12 de setembro de 2020.

VILALTA, Luís Antônio; MACHADO, Talles Amaral. "Novos Paradigmas da Investigação Criminal". *Revista Brasileira de Ciências Policiais* 9, nº 1 (8 de novembro de 2018): 13-41. Disponível em: https://doi.org/10.31412/rbcp.v9i1.542.

Informação bibliográfica deste texto, conforme a NBR 6023:2018 da Associação Brasileira de Normas Técnicas (ABNT):

ABREU, Jacqueline de Souza. Intermediação da vigilância do Estado no Brasil e proteção de dados entre cooperação, litígios e constrição de agentes privados: histórico, fundamentos e regulação. *Direitos Fundamentais & Justiça*, Belo Horizonte, ano 17, p. 125-147, dez. 2023. Número especial.

Recebido em: 30.07.2023
Pareceres: 18.10.2023; 03.11.2023 e 09.12.2023
Aprovado em: 08.03.2024