JACQUELINE DE SOUZA ABREU

PRIVACIDADE, SEGURANÇA E TECNOLOGIA

Tese de Doutorado

Orientador: Professor Titular Ronaldo Porto Macedo Junior

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo - SP
2022

JACQUELINE DE SOUZA ABREU

PRIVACIDADE, SEGURANÇA E TECNOLOGIA

Tese apresentada à Banca Examinadora do Programa de Pós-Graduação em Direito, da Faculdade de Direito da Universidade de São Paulo, como exigência parcial para obtenção do título de Doutor em Direito, na área de concentração em Filosofia e Teoria Geral do Direito, sob a orientação do Professor Titular Dr. Ronaldo Porto Macedo Junior.

UNIVERSIDADE DE SÃO PAULO
FACULDADE DE DIREITO
São Paulo - SP
2022

Catalogação da Publicação
Serviço de Biblioteca e Documentação
Faculdade de Direito da Universidade de São Paulo

Abreu, Jacqueline de Souza
Privacidade, segurança e tecnologia ; Jacqueline de Souza Abreu ; orientador Ronaldo Porto Macedo Junior -- São Paulo, 2022.

368

Tese (Doutorado - Programa de Pós-Graduação em Filosofia do Direito e Teoria Geral do Direito) - Faculdade de Direito, Universidade de São Paulo, 2022.
1. Teoria do Direito. 2. Direito Constitucional - Brasil. 3. Direito à privacidade. 4. Segurança pública. 5. Direito e Tecnologia. I. Macedo Junior, Ronaldo Porto, orient. II. Título.

AGRADECIMENTOS

São muitos a agradecer pelas mais diversas razões. Meu orientador, Ronaldo Macedo, por ter acreditado no meu trabalho lá atrás no início da graduação, incentivado as experiências de pesquisa no exterior, acolhido este projeto e me dado lições muito mais do que sobre teoria do direito. Rafael Mafei e Clarissa Gross, pelos mais diversos diálogos – sobretudo os comentários em minha banca de qualificação, que foram de crucial importância para o desenvolvimento do trabalho. Virgilio Afonso da Silva, pelo suporte e encorajamento em momentos cruciais da construção da minha formação acadêmica. Dennys Antonialli, Mariana Valente e Francisco Brito Cruz, por terem me oferecido a primeira oportunidade de trabalho em "direitos digitais" – a experiência no InternetLab me deu uma agenda de pesquisa (e grandes amigos). Caio Gentil Ribeiro, Beatriz Kira, Artur Pericles, Maria Luciano, Roberta Sati Cassoli, Rafael Zancheta pelo maior e melhor apoio de sempre – que também não faltou na hora de efetivamente fazer essa tese acontecer. A fantástica equipe do Barroso Fontelles, Barcellos, Mendonça & Associados, sobretudo Eduardo Mendonça, Roberta Mundim e Felipe Terra, por nunca deixarem de incentivar esta pesquisa e com quem compartilhei mais sobre a realidade de direitos à privacidade em tribunais Brasil afora do que imaginava quando embarquei nessa jornada. Laura Schertel Mendes, pelas tantas conversas e pelo aprendizado no âmbito da Comissão de Juristas encarregada de elaborar um anteprojeto de lei para lidar com tratamento de dados pessoais na segurança pública e em investigações criminais. Danilo Doneda, Miriam Wimmer, Marcela Mattiuzzo, Natália Langenegger, Bruno Bioni, Renato Leite Monteiro, Rafael Zanatta, Taís Tesser, Giovanna Ventre, Carina Quito, Gianluca Smanio, Riana Pfefferkorn, Greg Nojeim, Victor Fernandes, Nathalie Fragoso, Veridiana Alimonti e tantos outros profissionais e colegas que admiro com quem já troquei tantas reflexões sobre privacidade ao longo dos últimos oito anos. Chris Hoofnagle, que marcou minha experiência na Universidade da Califórnia em Berkeley com seu curso de computer crime law – e como a Quarta Emenda vinha sendo invocada para lidar com o mundo tecnológico. Urs Gasser e a equipe do Berkman Klein Center, onde nasceu uma pesquisa sobre criptografia que virou artigo e antecipou reflexões que desembocaram aqui. Os colegas do Summer Doctorate Programme do Oxford Internet Institute, sobretudo Ido Sivan-Sevilla, que me apresentou ao trabalho de Lucia Zedner. Todos que representam minhas estadas na Ludwig-Maximilians-Universität, onde me despertei para a intersecção entre direito e tecnologia, descobri o que era direito administrativo policial e fiz grandes amizades. Meu pai e minha mãe, pelo amor incondicional e o apoio incessante. Deus, a quem devo tudo em minha vida.

Jacqueline de Souza Abreu. **Privacidade, segurança e tecnologia**. 368 p. Doutorado - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2022.

Resumo: Esta pesquisa examina os fundamentos e o sentido de direitos à privacidade em face do Estado – mais particularmente, de seus interesses na promoção da segurança da população, a propósito de reflexões e mudanças provocadas pelo avanço tecnológico. Tem como objetivo defender e demonstrar que o modo como enfrentamos questões sobre o escopo desses direitos e a existência ou não de violação deles tem muito a se beneficiar de uma abordagem interpretativa – atenta à nuance dada por contextos, que não planifica o sentido de *direitos* equivalendo-os a interesses nem pressupõe uma rivalidade entre privacidade e segurança antes de depurar o sentido desses valores. A partir disso, ofereço um modelo sobre como pensar direitos à privacidade em face do Estado nesse campo – como identifica-los e como compreender a que propósito servem – e resgato o sentido da noção de segurança e os limites do que consegue justificar em termos de medidas estatais. Essa leitura reafirma uma noção central para a justificação do uso da força estatal nos campos de interação entre segurança e privacidade: o respeito a regras e procedimentos assentados em decisões coletivas de uma comunidade política que acomodem direitos morais contra abusos, erros e excessos, inspirados em compromissos de princípio que só admitem interferências em prerrogativas de privacidade quando razões específicas concretas o justifiquem – notadamente suspeita individualizada ou perigo concreto e iminente. Essas noções se perdem quando simplesmente se pressupõe que interesses públicos superam interesses privados ou que um teste de proporcionalidade serviria para balizar condutas estatais nessa intersecção. A seguir, o trabalho apresenta um panorama histórico das proteções jurídicas constitucionais de privacidades no Brasil e reconstrói a jurisprudência do Supremo Tribunal Federal (STF) em casos sobre privacidade e como concebe os limites do Estado sobre as "inviolabilidades" da vida privada, da intimidade, do domicílio e do sigilo de comunicações. Mostra como entendimentos se firmaram e como paradigmas de privacidade da Constituição Federal e da jurisprudência constitucional se alinham e se distanciam da tese apresentada sobre o que significa preservar direitos à privacidade em face do Estado. O diagnóstico é que estão amplamente fragilizados e desorientados especialmente em novas áreas de atuação ligadas ao avanço tecnológico, como o "sigilo telemático". Diante disso, o trabalho mostra como a retórica alarmista contra privacidade no campo do combate ao crime é frágil, oferece um ferramental regulatório para lidar com questões de privacidade e propõe encaminhamentos para o enfrentamento de questões concretas do campo "digital", para a identificação de limites e para o redirecionamento da jurisprudência constitucional e do debate público.

Palavras-chave: privacidade; segurança; tecnologia; direitos; STF

Jacqueline de Souza Abreu. **Privacy, security and technology**. 368 p. Doctorate – Faculty of Law, University of São Paulo, São Paulo, 2022.

Abstract: This study examines the foundations and meaning of rights to privacy vis-a-vis the government – more particularly, its interests in promoting the security of the population, in terms of reflections and changes caused by technological advances. It aims to defend and demonstrate that the way we face questions about the scope of these rights and the existence or not of violation of them has much to benefit from an interpretive approach - attentive to the nuance given by contexts, which does not flatten the meaning of rights to become equivalente to interests, nor does it presuppose a conflict between privacy and security before deepening the meaning of these values. From there, I offer a model on how to think about privacy rights vis-a-vis the government in this field – how to identify them and how to understand what purpose they serve – and rescue the meaning of the notion of security and the limits of what it can justify in terms of state measures. This reading reaffirms a central notion for the justification of the use of state force within the interaction between security and privacy: respect for rules and procedures based on collective decisions of a political community that accommodate moral rights against abuses, errors and excesses. These are inspired by commitments of principle that only allow interference with privacy prerogatives when specific concrete reasons justify it – notably individualized suspicion or concrete and imminent danger. These notions are lost when it is simply assumed that public interests outweigh private interests or that a proportionality test would serve to guide state conduct at this intersection. Next, the work presents a historical overview of the constitutional legal protections of privacy in Brazil and reconstructs the case law of the Brazilian Supreme Court (STF) in cases of privacy and how it conceives the limits of the State on the "inviolabilities" of private life, intimacy, domicile and communications secrecy. It shows how understandings were established and how privacy paradigms of the Federal Constitution and constitutional case law align and distance themselves from the thesis presented on what it means to preserve rights to privacy vis-a-vis the government. The diagnosis is that they are largely weakened and disoriented, especially in new areas linked to technological advances, such as “telematics secrecy”. In view of this, the work shows how the alarmist rhetoric against privacy in the field of fighting crime is fragile, presents a regulatory toolbox to deal with privacy issues and proposes directions for facing concrete issues in the "digital" field, for the identification of limits and for the redirection of constitutional case law and public debate.

Keywords: privacy; security; technology; rights; STF

Jacqueline de Souza Abreu. **Privatsphäre, Sicherheit und Technologie**. 368 S. Doktorarbeit – Juristische Fakultät, Universität São Paulo, São Paulo, 2022.

Zusammenfassung: Diese Studie untersucht die Grundlagen und die Bedeutung von Rechte auf Privatsphäre gegenüber dem Staat – insbesondere seine Interessen zur Förderung der Sicherheit der Bevölkerung im Hinblick auf Veränderungen durch technologischen Fortschritt. Sie zielt darauf ab, zu verteidigen und zu zeigen, dass die Art und Weise, wie wir Fragen zum Umfang dieser Rechte und Verletzung oder Nicht-Verletzung dieser Rechte begegnen, viel von einem interpretativen Ansatz profitieren kann – aufmerksam auf die durch Kontexte gegebenen Nuancen, die weder die Bedeutung von Rechten abflachen, sodass sie Interessen gleichgestellt, noch setzt sie einen Konflikt zwischen Privatsphäre (Freiheit) und Sicherheit voraus, bevor die Bedeutung dieser Werte vertieft wird. Von dort aus biete ich ein Modell an, wie man über Rechte auf Privatsphäre gegenüber dem Staat in diesem Bereich nachdenken kann – wie man sie identifiziert und wie man versteht, welchem Zweck sie dienen – und wie man die Bedeutung des Begriffs Sicherheit und die Grenzen an der Rechtfertigung staatlicher Maßnahmen retten kann. Diese Lesart bekräftigt ein zentrales Element für die Rechtfertigung des Einsatzes staatlicher Gewalt im Zusammenspiel von Sicherheit und Privatsphäre: die Achtung von Regeln und Verfahren, die auf kollektiven Entscheidungen einer politischen Gemeinschaft beruhen und moralische Rechte gegen Missbrauch, Fehler und Exzesse berücksichtigen. Diese sind von Grundstazverpflichtung inspiriert, die Eingriffe in die Privatsphäre nur dann zulassen, wenn konkrete Gründe dies rechtfertigen – insbesondere ein individueller Verdacht oder eine konkrete und drohende Gefahr. Diese Vorstellungen gehen verloren, wenn einfach davon ausgegangen wird, dass öffentliche Interessen gegenüber privaten Interessen überwiegen oder eine Verhältnismäßigkeitsprüfung als Orientierungshilfe für das staatliche Verhalten an dieser Schnittstelle dienen würde. Als nächstes bietet die Arbeit einen historischen Überblick über den verfassungsrechtlichen Schutz der Privatsphäre in Brasilien und rekonstruiert die Rechtsprechung des brasilianischen Obersten Gerichtshofs (STF) in Fällen der Privatsphäre und wie sie die Schranken des Staates für die "Unverletzlichkeit" des Privaten Leben, Intimität, Wohnsitz und Kommunikationsgeheimnis begreift. Es wird hervorgehoben, wie sich bestimmte Verständigungen durchgesetzt haben und wie sich Paradigmen der Bundesverfassung und der Verfassungsrechtsprechung an der vorgestellten These zur Wahrung der Privatsphäre gegenüber dem Staat ausrichten und distanzieren. Die Diagnose lautet, dass sie weitgehend geschwächt und orientierungslos sind, insbesondere in neuen Bereichen, die mit technologischen Fortschritten verbunden sind, wie z.B. „Telematikgeheimnis“. Angesichts dessen zeigt die Arbeit, wie brüchig die alarmierende Rhetorik gegen die Privatsphäre im Bereich der Kriminalitätsbekämpfung ist, stellt eine regulatorische Toolbox dar, und schlägt Richtungen vor, um konkrete Probleme im „digitalen“ Bereich anzugehen und für die Neuausrichtung der verfassungsrechtlichen Rechtsprechung und der öffentlichen Debatte.

Schlüsselwörter: Privatsphäre; Sicherheit; Technologie; Rechte; STF

The point that can be made, however, is that no society with a reputation for providing liberty in its own time failed to provide limits on the surveillance power of authorities. In this sense, American society in the 1970's faces the task of keeping this tradition meaningful when technological change promises to give public and private authorities the physical power to do what a combination of physical and socio-legal restraints had denied to them as part of our basic social system.

Alan Westin. The origins of modern claims of privacy. In: Ferdinand David Schoeman, ed., *Philosophical Dimensions of Privacy: An Anthology* (Cambridge: Cambridge University Press, 1984), p. 70-71.

SUMÁRIO

INTRODUÇÃO

1 O objeto de pesquisa

Em 2012, Elize Matsunaga atirou no marido, esquartejou seu corpo e o descartou em uma mata em Cotia, no interior de São Paulo. Foi um dos crimes célebres da época, daqueles que recebem toda a atenção midiática sobre seus detalhes mais macabros. Eram exibidos vídeos de câmeras de segurança dos elevadores do prédio em que o casal morava, com o marido, Marcos, executivo de grande empresa brasileira, subindo com uma pizza e, dias depois, Elize descendo com malas. Viria à tona também como Elize havia contratado um detetive particular que capturou em fotos e vídeos a traição de Marcos – revelação que teria levado à briga que resultou em seu assassinato; que Elize trabalhou como garota de programa – meio pelo qual conheceu Marcos; que havia confessado a reverendo da igreja que frequentavam que estavam tendo dificuldades no casamento; que o marido supostamente teria enviado um email à família após seu "desaparecimento"; que a polícia foi capaz de identificar por sinais do celular de Elize que ela esteve no local em que o corpo foi encontrado; que a polícia rodoviária chegou a pará-la em uma rodovia com o corpo no carro e multá-la por atraso no licenciamento, mas não fez revista por não apresentar "atitude suspeita"; que perícias chegaram a encontrar DNA de uma terceira pessoa (além do de Marcos e Elize) nos sacos descartados com o corpo na mata, mas nunca foi possível estabelecer participação de mais ninguém no crime. Em 2021, esses detalhes foram recontados em documentário no Netflix.[1]

O caso é de homicídio, mas chama atenção para várias questões que implicam o conceito de privacidade e o tratamento extraordinário que recebe em um processo penal: a polícia e autoridades de persecução em geral podem ter acesso a informações e conhecer detalhes tidos por "íntimos" da vida de alguém quando é no interesse de responsabilizar criminalmente, e, de forma mais geral, "promover a segurança". Isto é, mesmo abstraindo do trabalho da imprensa na busca e divulgação de vários desses detalhes do caso (que não é meu

[1] *Elize Matsunaga: Era Uma Vez Um Crime*, Documentário (Netflix, 2021), https://www.netflix.com/br/title/81043160.

foco aqui) e até desconsiderando revelações em depoimentos (da Elize e de testemunhas e informantes, que também não serão meu foco aqui), há implicações da noção de privacidade do início ao fim da atividade policial: desenterrando o passado profissional da principal suspeita (e como conheceu a vítima), depurando seus motivos ao vasculhar cartas e emails da família, levantando imagens de câmeras do local em que moram, analisando sinais de celulares e DNA.

O caso revela um modo de funcionamento de direitos à privacidade especialmente característico nesse contexto: um direito que a princípio temos em várias perspectivas e em relação ao qual se considera que a "vida íntima" (como o relacionamento de um casal) está no cerne, mas que aparentamos poder "perder" no processo penal. Isso não é curioso para muita gente: a explicação mais simples desse funcionamento consiste em dizer que o interesse público inerente a uma investigação criminal supera qualquer interesse privado sobre privacidade, que não há direitos absolutos, que a polícia pode apurar o que lhe compete em nome da segurança, que a privacidade não pode acobertar ilícitos. Então, sim, "perderíamos" direitos de privacidade no processo penal ou, de forma mais geral, sempre que o Estado esteja atuando pela "segurança".

Um jeito bastante popular de explicar isso é também dizer que as restrições a direitos à privacidade nessas circunstâncias são "proporcionais": o interesse público em apurar crimes é um interesse legítimo para motivar ações do Estado, medidas de investigação que envolvem o acesso a informações pessoais sobre suspeitos e sobre a vítima e suas associações são adequadas para a apuração de crimes; são também (ou o foram em um caso como o de Elize) necessárias à apuração, se faltarem alternativas que alcancem a mesma finalidade com menos efeitos colaterais; e os interesses da segurança, na promoção geral desse bem e na responsabilização criminal do envolvido de forma específica são mais intensos – ou pelo menos é possível supor que em muitas circunstâncias sejam, como o teriam sido no caso, – que os interesses de privacidade que o criminoso e pessoas relacionadas ao evento criminoso possam ter.

Existe outra maneira de olhar para o exemplo. O alcance e os limites das prerrogativas do Estado de agir e obter informações frente a um evento criminoso não são dados pelo pertencimento de uma informação a uma categoria "íntima" (o que acontece no casamento, na vida sexual, no domicílio) ou não, nem simplesmente por um juízo comparativo de

intensidade de interesses de privacidade e segurança. São dados pelo contexto: não só se temos expectativas de privacidade em face de terceiros sobre as informações implicadas em certa situação, mas se há razões específicas para obtê-las naquelas circunstâncias.

Elize tinha um direito à privacidade, por exemplo, sobre as localizações de seu celular. Ela podia opor esse direito a qualquer curioso que tentasse invadir seu celular para obtê-las ou vazá-las de sua empresa de telefonia, porque preservar a possibilidade de não ter de revelar esses aspectos a pessoas a quem não queira faz parte de como respeitamos sua autonomia como pessoa com uma vida que é sua. O fato de que a polícia excepcionalmente em tese pode obtê-las está predicado a razões que a colocavam como suspeita do crime no contexto do trabalho de apuração policial – razões que sugeriam que a motivação da polícia para obter essa informação era coerente com a investigação (não distorcidas, abusivas para finalidades estranhas), atendiam um nível de probabilidade razoável de que poderiam levar a informações relevantes que associassem Elize ao crime grave (não eram fruto de arbitrariedades aleatórias); e limitavam-se ao conjunto de informações que era relevante e necessário à investigação (continham excessos gratuitos). A possibilidade de acesso a essas informações e sua fundamentação não se dá nem pode se dar simplesmente porque a localização era uma informação "estática" que Elize compartilhou com uma empresa que supostamente não compunha sua "intimidade" ou suas "comunicações privadas" nem porque a restrição pontual do sigilo sobre seus trajetos era "proporcional" a satisfazer os interesses mais "pesados" ou "preponderantes" de coloca-la na cena do crime para permitir sua responsabilização e reforçar interesses de prevenção criminal geral.

No caso de Elize é fácil perder de vista o funcionamento contextual da privacidade olhando retrospectivamente ao trabalho investigativo que formou provas contra uma suspeita que não demorou a confessar o crime; mas essa lógica estava lá – não fosse o crime implicando o casal, não haveria razões para que a polícia pudesse acessar os sinais do celular de Elize – nem imagens de câmeras do prédio que mostravam suas atividades, o teor de mensagens de e-mail trocada entre eles, o DNA do casal e aquele encontrado na cena do crime. Não haveria razão para conhecer intimidades da vida do casal, não fosse por serem protagonistas dos fatos investigados. Em contraste, sem razão aparente, e sob contexto completamente diverso de controle de licenciamento de carro, não havia por que a polícia

rodoviária querer averiguar o porta-malas de Elize – como não o fez. Direitos à privacidade valem – e devem respeitados – mesmo em face de interesses de segurança do Estado.

O respeito a direitos de privacidade impõe a observância de certos procedimentos e ônus de fundamentação voltados a garantir a existência dessas razões e demarcar os limites sobre o que permitem adentrar. Não os "perdemos" no processo penal; pelo contrário, todas as contrapartidas regulatórias a que seu "afastamento" está (e deve estar) sujeito nessa área é o que mostra seu pleno vigor. Direitos de privacidade não são só interesses que foram ponderados e perderam para os interesses em segurança (na responsabilização criminal), mas prerrogativas morais enraizadas em nossas práticas e convicções que colocam barreiras de contenção contra arbítrio, excesso e erro do Estado no exercício de sua força. Essas prerrogativas são indevidamente violadas sempre que certos procedimentos que calibrem o nível de risco de sofrer injustiça – um afastamento indevido de um direito à privacidade – não sejam observados, sempre que o respeito a direitos não seja concretamente fundamentado, sempre que esses procedimentos de proteção regulatória das privacidades não existem.

Este é um trabalho sobre como se dá e deve se dar essa articulação entre as preocupações de privacidade que socorrem ao indivíduo e as de segurança que movem o Estado no processo penal – e, cada vez mais, até antes de fatos criminosos concretos, para fins preventivos (como a que enseja abordagens como a que Elize vivenciou em rodovia e a instalação de câmeras de segurança no elevador do prédio – fenômeno que se espalha por ruas, avenidas, prédios e residências). Mais particularmente, este é um trabalho sobre como devemos abordar e justificar a necessidade de "habilitar justiça" e "preservar a segurança" frente a noções de privacidade: sobre o que não é explicado nem capturado quando simplesmente dizemos que nessa situação o interesse público prevalece e a restrição é "proporcional". É também um trabalho sobre como a jurisprudência constitucional brasileira abordou essas questões até aqui e como é possível e preciso aperfeiçoá-la.

2 Um fator de urgência

Embora a questão sobre limites do poder do Estado na defesa da segurança seja antiga e suas várias instâncias já tenham sido objeto de diversas obras jurídicas, considero a proposta de revisitação dessa articulação que motiva esse trabalho cada vez mais urgente. Grande parte

das questões contemporâneas que recolocam o problema dos limites das prerrogativas do Estado em nome da segurança têm um traço comum marcante: foram diretamente provocadas pelo rápido desenvolvimento tecnológico pós-1988. O direito brasileiro permite que a polícia apreenda e consulte dados armazenados em celulares? O direito brasileiro autoriza a instalação de câmeras de vigilância pela cidade, associados a programas de reconhecimento facial, com captura e coleta de dados sobre pessoas em ambientes públicos? Quando celulares não eram uma ferramenta tão relevante para a vida cotidiana e quando não existia a capacidade de rastrear pessoas a todo tempo, não eram feitas as referidas perguntas.

Frente a essas questões, podemos procurar o que nisso pertence ou não a uma "vida íntima" protegida, em contraposição a um domínio não protegido, e dizer que devemos aceitar que perdemos a privacidade para atender propósitos de segurança. Mas isso não vai ajudar a resolver essas questões. Ou melhor: até oferece respostas, mas, vou defender, são pobres e desconectadas das razões normativas que impactam. É o caso quando se diz que "dados estáticos" contidos em mídias eletrônicas não são protegidos por privacidade ou que o que se faz em público também não: essas soluções ignoram nossas expectativas sobre os registros de nossas atividades que celulares hoje carregam e nossas preocupações com a maneira como o Poder Público fará uso da força ao ganhar capacidades de vigilância nunca antes vistas. A teoria do que autoriza tantas "exceções" ao Estado de tomar conhecimento sobre a vida de alguém em um processo penal não deve, portanto, se resumir a respostas simples. De forma normativamente reveladora, o avanço tecnológico nos provoca a rever não só como explicamos e justificamos a articulação entre privacidade e segurança, mas também como compreendemos o que torna expectativas de privacidade *direitos* em certos contextos e a quais condições e freios regulatórios nossos esforços de segurança estão sujeitos.

A razão é simples: tecnologias trazem mudanças sociais e alteram condições e possibilidades práticas, desafiando normas, doutrinas e práticas jurídicas que foram estabelecidas em circunstâncias fáticas pretéritas e nos obrigam a articular os valores que buscávamos proteger, as teorias normativas subjacentes. Como notou Lawrence Lessig, constituições e leis estabelecem um conjunto de restrições jurídicas à ação do Estado.[2] A exigência de uma autorização judicial prévia à atuação do Estado – como para ingressar em um domicílio – talvez seja a mais comum delas. Mas existem outros tipos de limitações ao

[2] Lawrence Lessig, "Reading the Constitution in Cyberspace", *Emory Law Journal* 45, nº 3 (1996): 870.

Poder do Estado, como regras sociais e, principalmente, restrições tecnológicas: "O requisito da ordem judicial é uma restrição jurídica à ação da polícia; que a polícia, ao contrário do Superman, não tem visão de raio-x é uma restrição tecnológica."[3]

O rápido avanço da tecnologia coloca um desafio a operadores do direito porque altera (retira, reduz ou cria) "restrições tecnológicas", de modo que questionamentos sobre privacidade e segurança serão cada vez mais frequentes, como começam a ser no Brasil e já o são ao redor do mundo. Deixa a suficiência de nossas "restrições jurídicas" tradicionais para trás. Se é desenvolvido um binóculo que permite enxergar através de paredes, apenas exigir mandado judicial prévio para ingressar e fazer busca em domicílio não vai servir. Se não é mais necessário o ingresso físico, a relevância desse acontecimento se perde. E mais: se a existência dessa ferramenta em si cria riscos de mau uso por policiais que vão usá-la sem reportar, sem autorização, contra quem bem quiserem, precisamos muito mais do que só de uma ordem judicial prévia para controlar seu uso. Por outro lado, ainda que estejamos fora de casa (em "público"), se máquinas passam a incorporar mecanismos de notificações à polícia sobre "comportamentos suspeitos" de pessoas e objetos na rua, o que isso significa para nossos direitos e a pertinência de "restrições jurídicas" ganha necessidade de articulação.

A tecnologia também constantemente afeta a disponibilidade de informações pessoais que podem ser obtidas e como podem ser usadas por terceiros – entre eles, o próprio Estado – de diversas maneiras: o ponto de inflexão das suspeitas sobre Elize foram os vídeos das câmeras de elevadores, reforçados pelos sinais de seu celular. A partir do momento em que todas as nossas atividades ficam de algum modo registradas (diminuindo a necessidade de *ouvir* pessoas *deporem* sobre o que houve/ o que viram/ o que sabem), e diante da constatação de que demandas por segurança (sobretudo responsabilização criminal) podem afastar os mais fortes interesses de privacidade (sobre a vida íntima de um casal) em certos contextos, nossas lealdades com valores que mobilizam demandas de privacidade e os limites que elas impõem ao Estado são testados. Se quisermos estar aptos a responder a esses desafios, precisamos de clareza sobre o que valorizamos ao falar em privacidade, que limites isso coloca ao Estado e, sobretudo, o que importa considerar nessa articulação.

[3] Lessig, 870.

3 Pergunta, objetivo e limites

Nesse contexto, esta tese se coloca na intersecção entre teoria do direito, direito constitucional, direito da proteção de dados pessoais, direito administrativo policial, direito processual penal e direito e tecnologia. Examino se, quando e em que condições a "privacidade" – aqui ainda como conceito genericamente referido – de uma ou mais pessoas, pode ser afastada em nome da segurança de pessoas pertencentes à comunidade política em questão, com especial interesse em ser útil para análise de novos problemas trazidos por usos de recursos tecnológicos incidentes a essas restrições. De forma específica, olho para medidas de "vigilância" estatal – termo pelo qual quero me referir às mais diversas práticas ativas de obtenção de informações sobre pessoas por parte do Estado. Em informações pessoais, incluo o conhecimento que alguém ganha ao tocar ou analisar o corpo de alguém ou o local em que esteve/habita e suas coisas, documentos, escritos – seus vestígios de toda espécie. Por outro lado, não vou tratar de informações pessoais obtidas por interrogatórios ou depoimentos (testemunhos), o que coloca questões específicas sobre direitos dessas pessoas se expressarem.

O objetivo é oferecer uma interpretação que consiga dar sentido aos contornos da privacidade como direito no contexto de investigações criminais e segurança pública e apontar como devemos abordar essa articulação, sobretudo se quisermos dar conta de novas questões colocadas pelo avanço tecnológico. No âmbito desse esforço, na primeira parte desse trabalho, faço uma incursão teórico-metodológica sobre a maneira como concebemos os conceitos de privacidade e segurança, seguida da defesa de concepções específicas desses conceitos. A partir disso, ofereço um retrato da relação entre privacidade e segurança que ajude a trazer clareza para essa articulação e suas diferentes manifestações.

De forma específica, defenderei que quando discutimos o que as noções de privacidade e segurança exigem, autorizam e limitam, nós as utilizamos como conceitos que se reportam a um valor e em relação aos quais oferecemos interpretações (concepções) que articulam o que seria a melhor maneira de revelar esse valor. Não são, portanto, conceitos que podem ser definidos apenas pela indicação de um critério compartilhado convencional, nem pela generalização descritiva de que englobam os mais diversos tipos de interesses que alguém possa ter sobre esses valores. Diante dessa constatação, e ao mesmo tempo em que reconheço que disputas persistirão, proponho aquelas que entendo serem as concepções mais

atraentes desses valores: no contexto de que aqui me ocupo, esses conceitos referem-se a direitos políticos devidos pelo Estado às pessoas a uma proteção regulatória – de contenção de poder – contra medidas que ameaçam o exercício de sua autenticidade e de sua responsabilidade pessoal sobre o curso de suas próprias vidas.

Não me proponho a responder a todas as questões de "privacidade *versus* segurança" que se possa imaginar, mesmo porque olhar para contextos específicos exigiria a elaboração de teses específicas. Ainda assim, espero contribuir para a elaboração de respostas mais consistentes e fieis às complexidades dos próprios conceitos que envolvem, olhando para um conjunto relevante de cenários em que essa relação se coloca e identificando os propósitos e princípios que os orientam. Nesse sentido, busco pensar o que poderia autorizar a ou o que impede a polícia, de forma concreta, e o Estado em suas políticas públicas de segurança, de superar prerrogativas (de "privacidades") que teríamos sobre quem participa do nosso lar (quando a polícia pode ingressar em domicílio ou saber o que nele se passa/é dito/é guardado), quem conhece nosso corpo (quando a polícia pode fazer enquadros – buscas em nosso corpo), quem mexe em nossos bens (quando a polícia pode fazer buscas e apreensões), quem sabe quem somos, de onde viemos e para onde vamos, nossas atividades e "pegadas" digitais (quando a polícia pode reconstruir e obter essas informações).

Em síntese, vou propor um modelo pelo qual podemos pensar direitos a privacidades que temos em face de agentes policiais do Estado de forma semelhante à que pensamos (e devemos pensar) direitos que temos contra terceiros de forma geral: se pudermos defender de forma coerente com nossas práticas sociais que temos, em certo contexto, uma prerrogativa oponível a terceiros contra forçar entrada em nosso lar, tocar nosso corpo, descobrir sinais do nosso celular, mexer nos nossos bens, saber quem somos e para onde vamos quando estamos na rua, o que falamos em conversas privadas e mesmo a quem ligamos, com quem nos encontramos e o que pensamos (inclusive no mundo digital) e até quando usamos o elevador de um prédio e o que fizemos nele, temos também esse direito em face de agentes policiais em suas atividades de combate ao crime.

Podemos pensar assim não porque há um conjunto pré-definido de aspectos do mundo que podemos agrupar sob a etiqueta da "privacidade" (da "vida privada") em qualquer contexto, mas porque, para os cenários que me importam nesse trabalho, o valor que queremos preservar (a autonomia, vou dizer) é um que poderia também ser violado por

terceiros: um policial corrupto, descuidado, arbitrário, preconceituoso que quisesse obter informações de alguém viola direitos morais, porque o tratamento à privacidade em questão nesses termos é injustificável sob uma teoria moral minimamente consistente sobre como devemos tratar uns aos outros.

Em respeito às privacidades que temos direito de ter e fazer valer, o Estado deve a nós uma regulação contra abusos, erros e excessos de autoridades policiais: ações que não são capazes de se justificar segundo uma teoria de moralidade política sobre direitos que o Estado deve a nós e sobre quais os limites dos seus esforços de segurança. Interesses gerais em segurança não superam nossas prerrogativas morais: apenas razões concretas e específicas, coerentes com os valores de nossa comunidade jurídica – como, vou defender, a suspeita individualizada sobre a prática de um crime ou a iminência dele é que podem, em tese, ser capazes de justificar a atuação policial que implique realizações de condutas que, não fossem por tais razões, seriam protegidas por prerrogativas de privacidade.

Esse "modelo do terceiro malicioso" para se pensar a privacidade oponível ao Estado em seus propósitos de segurança tem um limite: existem certas condutas que nenhuma pessoa consegue praticar à outra individualmente – só o Estado consegue impor políticas gerais de coleta de informações, de instalação de câmeras, de controle de documentos e de análise de informações em escala. Ao mesmo tempo, esse limite tem também um potencial analítico: se estamos frente a esse tipo de medida estatal, temos um sinal de que estamos diante de uma situação de exercício de poder estatal suficiente para ensejar ao Estado deveres de justificação de que a política de segurança é coerente com direitos e valores que a comunidade tem e de cuidado contra abusos, excessos e erros – contra injustiças, que podem inclusive extrapolar a linguagem da privacidade. Se não for coerente, nem contiver injustiças, não pode prevalecer: é por isso que não temos e não podemos ter políticas de segurança que envolvem instalar câmeras em todos os lares do Brasil preventivamente nem fazer testes de personalidade anuais de cidadãos para ver se crises emocionais podem resultar em crimes bárbaros como o de Elize Matsunaga, por exemplo. Ainda que isso trouxesse ganhos abstratos para a segurança pública, poupando alguns homicídios, isso seria incompatível com o valor que damos à privacidade – e a vários outros valores a que essa ideia se associa.

Com esse pano de fundo teórico, na segunda parte desse trabalho, faço uma reconstrução da jurisprudência constitucional brasileira que se insere nessa área, mostro

como problemas das formas mais tradicionais como se pensa privacidade (e privacidade *e* segurança) aparecem sob diferentes temas e levo as minhas considerações teóricas ao atual estado da jurisprudência. Nesse levantamento, passo pelas mais diversas questões em que discussões sobre privacidade já surgiram e qual a racionalidade da proteção que receberam e do tratamento regulatório a que foram sujeitados, e qual a lógica dos "afastamentos" admitidos e inadmitidos. Aponto os principais problemas teórico-metodológicos, normativos e regulatórios que identifiquei. Falo mais disso adiante.

Nesse momento, cabe ainda destacar que a pesquisa supõe questões de privacidade e segurança colocadas pelo interesse em reprimir e impedir o cometimento de crimes. Falo em crimes supondo certo contexto de "normalidade" institucional e social, não em cenários de guerras e crises humanitárias. Não estou afirmando que as instituições democráticas brasileiras funcionam perfeitamente no combate ao crime nem que não utilizam recursos retóricos que apelem a cenários extremos e de crise para justificar suas ações que afetam a privacidade de pessoas. Trata-se apenas de uma observação de recorte contextual necessário para especificar os sentidos de privacidade e segurança que vou explorar. Neste trabalho também não trato de questões de privacidade de organizações do Estado (como as decretações de sigilo sobre documentos) nem foco em segurança do Estado (atividades voltadas a proteger as instituições estatais), apesar de saber que existem crimes que protegem esse bem e que existe atuação do Estado sobre a privacidade em nome dele (como as de entidades como a Agência Brasileira de Inteligência). A pesquisa não se dedicou a essa literatura, isto é, a argumentos específicos que possam existir sobre esse nicho da discussão aplicável a serviços de inteligência.

Essas ressalvas são importantes porque logo de início vou defender que o modo como enfrentamos questões sobre o escopo de direitos à privacidade e a existência ou não de violação a eles precisa se despertar para uma abordagem interpretativa – atenta à nuance dada por contextos, que não esvazie o sentido de *direitos* nem pressuponha uma rivalidade entre privacidade e segurança antes de depurar o sentido desses valores e como poderiam estar conectados entre si. É uma doença intelectual que juristas apelem genericamente à noção de "proporcionalidade" sem aplicar a teoria de forma tecnicamente correta a um caso,[4] mas nem

[4] Nesse sentido, falando sobre liberdade de expressão, Ronaldo Porto Macedo Júnior, "Liberdade de expressão: que lições devemos aprender da experiência americana?", *Revista Direito GV* 13, nº 1 (30 de maio de 2017): 282.

mesmo sua versão robusta me ajuda a meus propósitos nesse trabalho. Ciente da crescente adesão a essa teoria e mesmo dos seus apelos algo intuitivos, falo mais das abordagens preterida e preferida nesse trabalho a seguir.

4 Abordagem

4.1 *A saída corriqueira*

Uma saída comum para questionamentos jurídicos que aparentem suscitar colisão de valores de ordem constitucional (como privacidade e segurança) é invocar o teste da proporcionalidade.[5] Metodologicamente, o teste é compreendido por muitos comentadores como "padrão de determinação da constitucionalidade da restrição de um direito fundamental por uma norma sub-constitucional".[6] Quando lei infraconstitucional, ato administrativo ou decisão judicial que realizam interesse público ou mesmo direito fundamental concorrente afetam o "âmbito de proteção" de um direito fundamental, diz-se que houve "intervenção" nesse direito fundamental. Em tal cenário, sob o prisma da teoria da proporcionalidade, fala-se que a limitação do direito fundamental afetado só é constitucional se for *proporcional*. Este juízo importa averiguar se a "interferência" sobrevive aos sub-testes de adequação, necessidade e proporcionalidade em sentido estrito (ponderação).

Na versão de Robert Alexy, a exigibilidade da análise de proporcionalidade decorre da "estrutura dos direitos fundamentais".[7] A teoria de direitos fundamentais de Alexy repousa na distinção entre regras e princípios enquanto tipos de normas jurídicas. Regras são "normas que são sempre ou satisfeitas ou não satisfeitas"[8] e aplicadas através do mecanismo da subsunção.[9] Princípios, por outro lado, são "normas que ordenam que algo seja realizado na

[5] Não posso dizer que aplicam o teste corretamente no Brasil; na verdade, na maior parte das vezes mais parece um recurso retórico e adicional de apresentação de certos argumentos. Ver Virgilio Afonso da Silva, "O Proporcional e o Razoável", *Revista dos Tribunais*, nº 798 (2002): 23–50; Virgilio Afonso da Silva, *Direito Constitucional Brasileiro* (São Paulo: Edusp, 2021), 122–23. No entanto, por apelar a certa concepção de como direitos fundamentais operam, trato aqui da versão global mais famosa do modelo de proporcionalidade.

[6] Aharon Barak, "Proportionality (2)", in *The Oxford Handbook of Comparative Constitutional Law*, org. Michael Rosenfeld e András Sajo (Oxford: Oxford University Press, 2012), 739.

[7] Afonso da Silva, "O Proporcional e o Razoável", 43.

[8] Robert Alexy, *Teoria dos direitos fundamentais*, trad. Virgilio Afonso da Silva, Segunda Edição (São Paulo: Malheiros Editores, 2015), 91.

[9] Afonso da Silva, "O Proporcional e o Razoável", 25.

maior medida possível dentro das possibilidades jurídicas e fáticas existentes"[10]. São mandamentos de otimização, aplicados por meio da "máxima da proporcionalidade".[11] Neste sentido, se e quando se admite que direitos fundamentais são *princípios,* por necessidade lógica, há que se resolver casos que os envolvam aplicando-se a máxima da proporcionalidade.

Essa visão do raciocínio jurídico sobre direitos fundamentais pressupõe que, se o caso não pode ser resolvido por subsunção a regras, vez que envolve *princípio(-s),* a única saída disponível ao aplicador do direito seria a aplicação do teste (ou "máxima") da proporcionalidade. A controvérsia é então traduzida nos seguintes termos, por exemplo: a interferência na privacidade, caracterizada pela instalação de câmeras de monitoramento, é proporcional, diante dos ganhos na realização da segurança pública que a intervenção representa? Assumir que a proporcionalidade é a única ou a melhor alternativa metodológica disponível ao julgador frente a aparentes "limitações" de direitos fundamentais ou a "colisões" entre princípios constitucionais é atitude recorrente.

No cenário em que a tecnologia fica recolocando questões de privacidade e segurança a todo momento, o instrumental do teste da proporcionalidade pode parecer ideal: basta checar o que é "proporcional" para certas tecnologias e em cada caso específico, ponderando esses valores. Trata-se de um ferramental aparentemente poderoso, disponível e acessível a qualquer operador do direito e que permitiria a revisitação e atualização constante dos contornos do direito à privacidade e do interesse público em segurança pública, sobretudo se aplicada corretamente e segundo a estrutura proposta.

Não faço esse tipo de análise neste trabalho. Nem mesmo a versão sofisticada do teste que estaria disponível para estruturarmos o que em tese nos permitiria dizer que torna restrições à privacidade "proporcionais" em um caso como o de Elize Matsunaga captura as nuances que pretendo mostrar aqui. Primeiro, porque o modelo parte de definições abrangentes do "âmbito de proteção" de direitos fundamentais (e de privacidade e segurança) para, por meio de etapas (legitimidade, adequação, necessidade e proporcionalidade em sentido estrito – onde ocorre "ponderação"), impor ônus de justificação do Estado para restringir esses direitos e chegar ao resultado final de delimitação da proteção no caso

[10] Alexy, *Teoria dos direitos fundamentais*, 90.
[11] Alexy, 116.

concreto.[12] Enquanto estratégia de dar transparência e estrutura para o ônus de fundamentação que o Estado tem para agir, entendo e reconheço o que torna a proposta atraente.

Meu desconforto com essa abordagem vem da compreensão de que essa definição generosa inicial deixa de capturar e alocar a dimensão normativa político-moral do nosso engajamento com concepções de direitos. Ela deixa de incorporar e dar sentido a nossas defesas de direitos não como interesses gerais que devem entrar no cálculo de proporcionalidade frente a outras considerações e às vezes perdem, mas como prerrogativas a que temos direito mesmo quando a maioria pensa que é errado fazê-lo, e mesmo se a maioria seria posta em situação pior por isso.[13] Interessa-me explorar e mostrar quando podemos falar em privacidade como uma demanda forte nesses termos frente a interesses proclamados pela segurança da comunidade, o que considero crucial para dar sentido a como ocorre e deve ocorrer a acomodação desses direitos na nossa prática jurídica voltada a promover segurança.

Outra razão para preterir essa abordagem é haver *outros métodos* de raciocínio jurídico, aplicados e reconhecidos em outras tradições jurídicas, além de ponderação. Apesar de a teoria de Alexy pretender esgotar as formas como procede o raciocínio jurídico sobre direitos fundamentais, por subsunção ou pela máxima da proporcionalidade, ele não dá conta de discussões normativas conceituais sobre o valor de direitos e como se articula com outros valores no direito. [14] Na própria prática brasileira, como se verá na segunda parte do trabalho,

---

[12] "The decisive weakness here is that protection can be denied without openly giving the reasons for it. This, sixthly, promotes judicial arbitrariness. Broad definitions, however, lead to a broad prima facie protection. Once certain behaviour is protected prima facie, the state has to justify the infringement of the right by applying the right's limitations, inter alia the proportionality test. Within the proportionality test, balancing has to be done according to the law of balancing, that means openly and traceably. Therefore, the state faces a duty to give reasons for not protecting rights when certain behaviour is protected prima facie. This burdens the state with the duty to give reasons for limitations, instead of burdening the people with the duty to justify exercising their rights, and thus prevents judicial arbitrariness. Therefore, broad definitions of rights are preferable." Matthias Klatt e Moritz Meister, *The Constitutional Structure of Proportionality* (Oxford: Oxford University Press, 2012), 48. Também Kai Möller, "Proportionality and Rights Inflation", in *Proportionality and the Rule of Law: Rights, Justification, Reasoning*, org. Bradley W. Miller, Grant Huscroft, e Grégoire Webber (Cambridge: Cambridge University Press, 2014), 155–72, https://doi.org/10.1017/CBO9781107565272.010. No caso do direito brasileiro, também defendendo a atratividade de concepções amplas do âmbito de proteção de direitos para explicitar a necessidade de justificativa constitucional para restrições, ver Afonso da Silva, *Direito Constitucional Brasileiro*, 102-3;120.

[13] Ronald Dworkin, *Taking Rights Seriously* (Cambridge: Harvard University Press, 1977), 199.

[14] Estruturando tais críticas e ilustrando seus problemas a partir de casos de liberdade de expressão, ver Caio Gentil Ribeiro, "Para além da subsunção e do sopesamento: uma crítica à teoria da proporcionalidade a partir do caso da liberdade de expressão", *Revista Publicum* 5, nº 1 (5 de novembro de 2019): 221–37, https://doi.org/10.12957/publicum.2019.30353.O autor argumenta que, por mais que a teoria da proporcionalidade pretenda ser neutra sobre quais os pesos devem ser dados aos interesses a serem ponderados, apenas almejando estruturar argumentos substantivos que podem ser lançados no debate constitucional, essa

temos um esforço de análise do que compõem certos direitos específicos de privacidade – embora, como também mostrarei, a jurisprudência brasileira seja por vezes inconstante e inconsistente. Essas não são só falsas discussões que escodem ponderação prévia na própria definição de um direito, mas reflexões sobre o valor dele – qual a melhor teoria que justifica por que temos um direito à privacidade, qual a melhor apresentação do ideal de segurança e como se articulam entre si e com outros valores da nossa prática jurídica. Penso que esse tipo de análise interpretativa deve ser aprofundada, não trocada por discurso de ponderação.

Assim, o trabalho analisa os conceitos de privacidade e segurança sem adotar as premissas e aplicações de uma análise tradicional de proporcionalidade, de modo que não estou pressupondo de partida que os conceitos de privacidade e segurança estão em conflito. Dito isso, essas ressalvas não significam uma rejeição completa de qualquer papel para todos os elementos da noção de proporcionalidade. Há espaço para fatores que balizem a atuação do Estado contra medidas inadequadas e desnecessárias. Há ainda lugar para certo "sopesamento" – conquanto o termo se reporte a um exercício de reconstrução conceitual, que é diferente do que chamei de "ponderação" de interesses nesta subseção, dentro dos pressupostos da teoria da proporcionalidade. Falo mais desse aspecto e das demais premissas da abordagem desse trabalho a seguir.

4.2 *O método preferido*

A abordagem que este trabalho avança para explicar e justificar a relação entre privacidade e segurança é baseado em (i) análise conceitual, (ii) interpretação reconstrutiva e (iii) na teoria dos direitos de Ronald Dworkin. Esses três elementos correspondem a três pilares da tese construída na parte teórica desse trabalho.

A começar, a contribuição que pretendo levar adiante com esse trabalho passa pelo enfrentamento de questões conceituais: o que significa *privacidade* enquanto direito moral e direito jurídico e qual a melhor maneira de compreender e reconhecer "*violações da privacidade*"? O que significa *segurança* enquanto objetivo social no qual se baseiam políticas públicas estatais? Como esses conceitos se articulam entre si: buscar garantir a

neutralidade é afastada por ser incapaz de acomodar teorias dos direitos e da justiça influentes como as de Ronald Dworkin e John Rawls. Se não consegue acomodá-las, precisaria tomar uma posição sobre os problemas dessas teorias, deixando de ser neutra como pretende.

privacidade como valor é sempre contraditório com a segurança e vice-versa? Esses conceitos são compatíveis? Em que sentido?

Por trás dessa abordagem está uma lição fundamental encontrada na obra de Ronald Dworkin acerca da "gramática dos conceitos": "pessoas participam de práticas sociais em que elas tratam certos conceitos como identificando um valor ou desvalor mas discordam sobre como aquele valor deve ser caracterizado ou identificado"[15] (tradução livre). Isso é comum principalmente entre conceitos de cunho moral – como "justiça", "liberdade" e igualdade: as pessoas concordam que esses conceitos designam valores e compartilham "exemplos paradigmáticos" da aplicação deles (e de quando são observados ou desrespeitados) – mas discordam quanto ao que exigem, requerem e orientam, mais precisamente.[16]

O modo de funcionamento desse tipo de conceito (que Dworkin chama de *interpretativo*) é bastante diferente de outros conceitos – os de tipo "criterial" (como o conceito de 'triângulo equilátero') ou os de tipo "natural" (como o conceito de 'leão'). Os "jogos de linguagem" que explicam o funcionamento desses conceitos são diferentes: eles podem se dizer "compartilhados" entre as pessoas quando elas estão de acordo quanto ao teste decisivo (procedimento) que rege a aplicação desses conceitos: "ser um figura geométrica com três lados iguais" (ter uma definição que fixa um critério de aplicação) ou "ter DNA que pertença à espécie nomeada de leão" (designar objetos que tenham certa estrutura química ou biológica).

Em contraste, não há compartilhamento de um "teste decisivo" no caso de conceitos de tipo *interpretativo*: há compartilhamento de instâncias paradigmáticas de uso, mas esse compartilhamento convive com grandes diferenças de opiniões – "concepções" rivais acerca do que explica e justifica os juízos que fazemos ao considerar algum paradigma como paradigma do conceito (de "justiça" ou de "injustiça", por exemplo).

Tomo essa observação como importante para esse trabalho porque acredito e defenderei que discussões acerca da *privacidade* são melhor compreendidas dessa maneira: enquanto debates em torno de um conceito interpretativo – em que são lançadas interpretações rivais para um conceito sobre o qual são compartilhadas instâncias

[15] Ronald Dworkin, *Justice for Hedgehogs* (Cambridge, MA: Harvard University Press, 2011), 160.
[16] Ronald Dworkin, "Do Values Conflict? A hedgehog's approach", *Arizona Law Review* 43 (2001): 254–55.

paradigmáticas do que significa "respeitar a privacidade" e do que significa "violar a privacidade". Esse caráter interpretativo é especialmente saliente e mais frequentemente visto em disputas de direito civil que envolvem o elemento de *divulgação* de informações pessoais obtidas por alguém – como quando se discute se a publicação de biografias não-autorizadas viola direito à privacidade ou se publicar em rede social a captura de tela ou a mensagem de áudio enviada por alguém em conversa privada viola a privacidade do interlocutor[17]. Também aparece no direito penal – como quando se discute se o ingresso e a permanência de alguém em um fórum de justiça sem autorização viola a privacidade (enquanto inviolabilidade do domicílio)[18] ou se o acesso e divulgação de conversas privadas mantidas em telefone celular, mas relativas a temas de interesse público e das quais os participantes eram agentes públicos, viola a privacidade (enquanto sigilo de comunicações privadas)[19]. Ele está, entretanto, presente nos mais diversos contextos e áreas do direito em que surgem reivindicações de privacidade – incluindo naquelas em face do Estado no direito processual penal e no direito administrativo.

Como observa Dworkin, por trás dessas controvérsias disputa-se qual é a melhor *concepção* – interpretação acerca do conceito de privacidade – que melhor o interpreta de um modo específico: mostra qual o sentido valorativo ou intencionalidade que melhor descreve e justifica nossas práticas sociais de uso do conceito de privacidade e do valor que elas possuem (e que o conceito designa) naquele contexto. Explorar qual é o sentido e o alcance da privacidade como direito, portanto, envolve justamente se engajar nesse tipo de controvérsia e buscar oferecer e defender aquela que seria a melhor concepção no contexto específico estudado. Isso me leva ao próximo ponto – a interpretação reconstrutiva.

---

[17] Ver Superior Tribunal de Justiça, REsp 1903273, Rel. Min. Nancy Andrighi, j. 24.08.2021, DJE 30.08.2021. Também: "Divulgação de mensagens do WhatsApp pode gerar indenização", *Notícias STJ* (blog), 2 de setembro de 2021, https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/02092021-Divulgacao-de-mensagens-do-WhatsApp-sem-autorizacao-pode-gerar-obrigacao-de-indenizar-.aspx.

[18] O exemplo banal é inspirado em caso real: "Habeas-corpus Violação de domicílio Trancamento da ação penal Advogado que ingressa com seu veículo no estacionamento do Fórum e lá permanece, mesmo ante a determinação expressa de funcionário público para a retirada de seu veículo do local. Conduta que não tipifica o crime de violação de domicílio. Objeto jurídico tutelado pelo tipo penal que visa a tranqüilidade domestica, proteção da moradia, liberdade e privacidade "individual-familiar'. Estacionamento do Fórum que não se insere no conceito legal. Ordem concedida Salientando que a conduta do paciente, em que pese não caracterizar violação de domicílio, pode ser enquadrada em outro tipo penal, podendo o ilustre membro do Ministério Público dar nova tipificação jurídica e ingressar com nova ação. Trancamento da presente ação que se impõe Ordem concedida". Tribunal de Justiça de São Paulo, HC 0280822-12.2011.8.26.0000, Rel. Des. Sérgio Ribas, 5ª Câmara de Direito Criminal, j. 02.02.2012, DJE 09.02.2012.

[19] Refiro-me ao caso da "Vaza Jato", ao qual retornarei no último capítulo do trabalho.

A melhor concepção de um conceito será aquela que melhor se ajustar ao significado valorativo das práticas sociais (e jurídicas) a que se refere o conceito. Não se trata de uma completa criação: pelo contrário, essa abordagem está baseada na própria fenomenologia de práticas sociais normativas, como a prática jurídica, em que juízes e advogados constroem e defendem teses, principalmente em casos difíceis, fazendo referência a regras, materiais e precedentes paradigmáticos, tentando justificá-los à melhor luz com base em alguma hipótese interpretativa, e lançando mão de uma tese acerca da resposta/proposição a que conduziriam no respectivo caso concreto. Mesmo fora de tribunais, nos comportamos assim para criticar alguém por certos comportamentos que contradigam a privacidade, articulando razões por que alguém teria violado uma certa regra social – como a mãe que espia o celular da filha adolescente; ou articulando razões para afastar essa mesma crítica em circunstâncias que a descaracterizam a contradição ao valor que essa regra prestigia – como quando pais instalam câmeras no quarto de um bebê ou de idoso que precisa de cuidados especiais. Heuristicamente, Dworkin fala nas dimensões de "fit" (ajuste) e "justificação" para se referir ao teste por que deve passar uma hipótese interpretativa para que se avalie e encontre a melhor interpretação disponível. [20]

A análise do conceito de segurança leva a constatações semelhantes: é também interpretativo e aberto a uma disputa sobre a concepção que melhor revela seu valor. Assim, depois de mostrar o caráter interpretativo desses conceitos no início dos respectivos capítulos que tratam desses conceitos (1 e 2), defenderei, como adiantei, uma certa concepção deles que, para o contexto mais geral de medidas de vigilância do Estado, acredito que melhor revele o seu valor – e o da relação entre eles: um compromisso mútuo com a contenção do uso da força, por meio da observância a procedimentos e da satisfação a ônus de fundamentação por parte do Estado, extraído da própria dignidade das pessoas.

Embora essa compreensão possa não soar inovadora, não precisaria ser: essa familiariedade é uma vantagem da concepção, já que tem um potencial explicativo e justificador maior de nossas práticas. Ainda assim, ela é impactante para a maneira como concebemos a justificação do poder do Estado em contraste com outras versões: as pessoas não simplesmente "perdem" privacidade para dar lugar à segurança, nem há apenas um

[20] "[U]ma interpretação plausível da prática jurídica também deve, de modo semelhante [à interpretação literária], passar por um teste de duas dimensões: deve ajustar-se a essa prática e demonstrar sua finalidade ou valor". In: Ronald Dworkin, *Uma questão de princípio*, 2º ed (São Paulo: Martins Fontes, 2005), 239.

exercício de adequação, necessidade e proporcionalidade entre privacidade e segurança; a privacidade que lhes é devida é traduzida em certas exigências normativas embutidas em procedimentos e deveres de fundamentação ligados ao contexto toda vez que o Estado atua pela segurança.

Como veremos no capítulo 3, a segurança a ser promovida de forma geral pelo Estado não é capaz de autorizar interferências em direitos morais à privacidade. Apenas circunstâncias concretas como aquelas em que ocorreu um crime pelo qual alguém deve ser responsabilizado ou uma emergência que requer resposta podem autorizar ações do Estado na obtenção de informações a essas finalidades de repressão e prevenção específicas concretas e nos limites do que faça sentido ao que é apurado – situações em que não apenas interesses genéricos de pessoas estão em jogo, mas direitos específicos concretos das pessoas imediatamente implicadas. Assim, enxergamos a relevância de exigências de *suspeita individualizada* para investigar alguém seletivamente e obter informações que em geral reservaríamos à sua privacidade; ou de *perigo concreto e imediato* para que certas medidas sejam autorizadas. Tudo isso é contextual e o alcance dessas exceções e das razões também.

Nossos esforços dogmáticos engajam-se na tarefa de extrair e consolidar certas regras sobre as circunstâncias em que restrições legítimas podem ocorrer, mas vêm sendo desafiados pelo avanço tecnológico – que tanto leva ao esgotamento de certas compreensões quanto provoca a reflexão sobre novos cenários ainda não capturados pelo estudo dogmático. Nessa linha, mostro como medidas gerais adotadas de forma preventiva e precaucionária – sobretudo a partir da coleta, uso e mineração de dados pessoais – em nome da segurança tem desafiado noções pelas quais traduzimos nosso compromisso de contenção do poder do Estado na prática jurídica. Esses são sintomas, a meu ver, não só de que precisamos rever nossos estudos dogmáticos nos campos de intersecção entre privacidade e segurança como no direito processual penal e no direito administrativo, mas de que há limites para o estudo dogmático – para compreender os conceitos de privacidade e segurança e certas disputas entre eles, precisamos entende-los como conceitos valorativos, que se reportam a teorias da justiça e da moralidade política mais abrangentes. Esse trabalho chama atenção a essas nuances que ficam escanteadas quando, sobretudo frente a novos desafios tecnológicos, reduzimos a relevância da privacidade frente à segurança ou só falamos em proporcionalidade a partir de definições abrangentes desses conceitos.

Sob essa abordagem, espero também recuperar a própria noção de "direito" para designar uma prerrogativa pela qual "seria errado interferir com a realização daquela ação, ou ao menos que razões especiais são necessárias para justificar qualquer interferência"[21]. Isso envolverá defender certa concepção de *direitos morais* que baseia-se na noção de que uma pessoa tem um direito contra o Estado *se* esse direito for necessário para proteger a dignidade (contra tratamentos inconsistentes com o reconhecimento de uma pessoa como membro de uma comunidade humana) e sua igualdade ao cuidado e respeito (mesmo entre membros "fracos" e "fortes").[22]

Nesse sentido, sustentar e articular o que é um direito é sustentar e articular um "objetivo político" – um "estado" (*state of affairs*) que se pretende alcançado ou protegido.[23] Isso somente faz sentido sob o pano de fundo de uma teoria política e a função e lugar que esse objetivo político tenha nela.[24] Direitos podem ser distinguidos de metas sociais pelo "caráter distributivo"[25] de sua justificativa nessas teorias: são objetivos individualizados a cada pessoa, não apenas um objetivo sem destinação ou referência particular, almejado para a comunidade como um todo indistintamente, em que o fator de benefício para uma ou outra pessoa em específico pode ser apenas contingente.[26] Compreendido dessa maneira, é preservado o sentido de "direito" que melhor captura aquilo que o torna valioso: não é simplesmente um interesse importante que alguém pode ter, mas uma prerrogativa que não pode ser limitada por uma justificação apenas baseada no benefício geral; direitos são aquelas prerrogativas que devemos às pessoas individualmente mesmo que a maioria seja colocada em uma situação pior por conta disso – são "trunfos", direitos "fortes", na terminologia que Dworkin deixou famosa.

No máximo, admitem-se "razões especiais" para restrições – fundadas em direitos fortes alheios, o que também só pode ser compreendido sob o pano de fundo de uma teoria coerente sobre o que torna privacidade e segurança valiosos, sobre os valores que constituem

---

[21] Dworkin, *Taking Rights Seriously*, 188.
[22] Dworkin, 198–99.
[23] Dworkin, 91.
[24] Dworkin, 92.
[25] Dworkin, 90.
[26] A reconstrução da teoria de direitos de Ronald Dworkin feita do Leonardo Rosa me foi útil para essa apresentação. Cf. Leonardo G. P. Rosa, "O liberalismo igualitário de Ronald Dworkin: o caso da liberdade de expressão" (Dissertação de Mestrado, São Paulo, Faculdade de Direito da Universidade de São Paulo, 2014), 20–74.

nossa comunidade jurídica. Quando direitos à privacidade são ameaçados e postos em risco na e pela atuação do Estado, há necessidade de observância a certos procedimentos e atendimento a exigências de fundamentação que contenham esses riscos e reafirmem princípios com que estamos comprometidos, sob pena de prejudicar a própria legitimidade do Estado. A teoria da privacidade e da sua relação com segurança apresentada na primeira parte desse trabalho é uma demonstração de tudo que fica de fora quando perdemos de vista as engrenagens de valor que alimentam esses conceitos e as práticas a que se referem.

5 A relevância do debate para o direito brasileiro

Ao oferecer essa teoria sobre a relação entre privacidade e segurança no contexto de combate ao crime, o objetivo é fazer uma construção de como esses conceitos se imbricam e se relacionam no direito que também coloque o significado de certas proteções jurídicas paradigmáticas sob uma melhor luz e dê maior clareza sobre quais e como enfrentar as novidades e os desafios trazidos pelo avanço tecnológico. Tendo percorrido esses passos sob essa abordagem teórica na primeira parte, a segunda olhará para o pensamento jurídico sobre privacidade e segurança no âmbito do direito constitucional brasileiro e mostrará mais concretamente o que ela tem a iluminar e redirecionar.

Nesse sentido, a segunda grande parte deste trabalho abre com o capítulo 4, em que apresento o panorama histórico das proteções jurídicas constitucionais de privacidades no Brasil e uma reconstrução da jurisprudência do STF sobre os limites das prerrogativas do Estado sobre a privacidade de cidadãos, com foco em suas pretensões de repressão e prevenção criminal. O capítulo é dedicado a retratar quais os tipos de controvérsias que surgem nessa matéria e quais os princípios e argumentos que as mobilizam. Assim, passo por diversos "objetos" de privacidade que já foram discutidos pelo STF e casos emblemáticos das respectivas áreas, mapeando uma série de controvérsias e o raciocínio jurídico em torno delas. Como demonstro, nossa jurisprudência constitucional confirma compromissos com os princípios morais a serem vistos na primeira parte, mas é, em certos aspectos, inconsistente em si própria e incorre em problemas sobretudo por não fazer análises contextuais ou por replicar entendimentos a novos contextos mesmo que as circunstâncias sejam distintas.

Um exemplo desde logo ajuda a ilustrar a fragilidade de que estou falando. Um paradigma regulatório que consagra os valores da privacidade e da segurança está previsto em regras claras da Constituição Federal (art. 5º, XII), da Lei nº 9.296/96 e em precedentes do STF: o de que comunicações telefônicas realizadas de modo privado entre dois agentes só podem ser *interceptadas* por um terceiro agente mediante ordem judicial que ateste o atendimento de certos requisitos materiais e autorize formalmente a medida. Quando há indícios razoáveis de envolvimento do alvo das comunicações interceptadas em crime punido com pena de reclusão e não existe outro meio disponível para produção de prova, não se fala mais em "violação" ou "desrespeito" ao direito à privacidade. Nesses casos, entende-se que a "quebra do sigilo" – como se nota da própria linguagem sobre o tema – é legítima e que a "privacidade" pode ser afastada/mitigada, sem incorrer em uma violação indevida a um direito, porque certo procedimento foi observado. Cabe a uma autoridade judicial concretamente fundamentar o respeito à prerrogativa moral em jogo sob considerações concretas, sob o pano de fundo desses parâmetros.

Esse é um paradigma jurídico há muito consolidado sobre uma atividade (comunicações privadas) que valorizamos e sobre as condições em que alguém pode ter superada sua prerrogativa de privacidade. Uma maneira de conceber esse paradigma é dizer que, no âmbito das atividades de comunicação (i) só comunicações privadas em fluxo são protegidas; (ii) outros tipos de comunicações ou dados não foram nem merecem ser objeto da mesma preocupação regulatória; (iii) a ordem judicial é o principal mecanismo para autorizar e legitimar que alguém perca privacidade de forma proporcional. Assim, todo o resto das atividades de vigilância que não caem nesse paradigma estariam desprotegidas ou, quando muito, poderiam ser viabilizadas por autorização judicial que também ateste proporcionalidade. Essa solução, entretanto, e como será visto na segunda parte deste trabalho, (i) não seria fiel à história do reconhecimento da proteção jurídica que resultou nesse paradigma; (ii) aos valores subjacentes a essa proteção; e (iii) nem aos contextos para os quais foi concebido. Precisamos aprender com os princípios extraídos desse paradigma e traduzi-los em outros contextos em que perguntas sobre privacidade e segurança surjam; não relegar tudo que não cai nessa caixa a fórmulas genéricas ou ignorar preocupações específicas dos novos contextos.

Um debate relevante hoje é se o direito brasileiro autoriza que autoridades policiais acessem dispositivos celulares sem autorização judicial prévia, após prisões em flagrante[27] ou mediante apreensão de coisa deixada no local do crime[28]. Como essas informações não estariam em fluxo, seria possível dizer que não seriam protegidas – na linha do que muitos tribunais fazem – e já encerrar qualquer discussão por aí. Quanto às operações massivas de tratamento de dados que visam a detectar práticas criminosas (como as do COAF), a fazer prova por antecipação (como o monitoramento de ruas por câmeras), ou até a rastrear pessoas (pela adição de mecanismos de reconhecimento facial), seria também fácil descartar maiores preocupações se só olharmos para o padrão do paradigma de interceptações: não envolvem um "objeto" textualmente protegido pela privacidade na Constituição, por isso dispensariam "ordem judicial". Essa simplificação é uma repercussão do problema de reduzir a maneira como justificar o uso da força pelo Estado em nome da segurança à noção de que privacidade possui sentidos convencionais, perde para segurança, não pode acobertar ilícitos – detalhes, valores, especificidades e contextos deixam de importar. Quando muito, será dito que a restrição deve ser proporcional e será feito um teste aproximado a este fim.

Nesse contexto, no capítulo 5 e final, destaco alguns aspectos da jurisprudência do STF que considero particularmente problemáticos à luz da teoria apresentada na primeira parte do trabalho. Em especial, e fechando o ciclo, retorno a onde comecei: demonstro a urgência do abandono de referências puramente retóricas de que privacidade não serve a acobertar ilícitos – o que mais polui reflexões do que as aprofunda. A seguir, comento o papel protagonista do controle judicial no afastamento de prerrogativas de privacidade e localizo essa ferramenta sob a perspectiva de outros instrumentos regulatórios. Se quisermos reafirmar as exigências materiais que justificam esse crivo e dar conta de problemas que extrapolam aquele que a autorização judicial prévia busca tratar na relação entre privacidade e segurança, precisamos melhor nos conscientizar e armar. Por fim, examino criticamente particularmente o atual estado de certas discussões que implicam "sigilo telemático" e "dados pessoais". De forma específica, mostro como o quanto desenvolvido na tese é capaz de

[27] Dennys Antonialli et al., "Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes: Retrato e Análise Da Jurisprudência de Tribunais Estaduais", *Revista Brasileira de Ciências Criminais* 154 (2019): 177–214.
[28] Hipótese do Recurso Extraordinário com Agravo nº 1.042.075, com finalização do julgamento ainda pendente após pedido de vista.

delinear estratégias regulatórias e iluminar e direcionar discussões jurídicas contemporâneas sobre o acesso de policiais a celulares, o acesso a dados junto a empresas controladoras de dados e a realização de monitoramento de áreas públicas. Isso envolve abandonar aplicações criteriais de noções de privacidade, refletidos em testes binários sobre o que está dentro ou fora de certa proteção, desconectado das circunstâncias; olhar para contextos; e elaborar, construir e aprender a conviver com outros recursos regulatórios.

6 Referências

Antes de efetivamente começar, faço uma observação bibliográfica. Já ficou claro que utilizarei as teorias do direito e da moralidade política de Ronald Dworkin em diversos pontos desse trabalho como referência em discussões normativas. A escolha do autor se dá tanto pela envergadura de sua obra, que me permite navegar por questões éticas, morais, filosóficas e jurídicas com certa consistência, quanto pela questão prática da familiariedade da autora deste trabalho com sua obra. Em particular, acredito que ele deixou um legado[29] metodológico que aponta problemas sobre a forma como compreendemos conceitos e nossas divergências político-morais que, quando comecei a estudar privacidade, notei que estavam subjacentes a vários debates.

Nesse sentido, embora as concepções dos conceitos de privacidade e segurança que proponho aqui neste trabalho estejam também baseadas em uma teoria da dignidade elaborada por Dworkin, sei que essa visão será disputada e não espero que haja concordância com todas as soluções concretas que a articulação que aqui exponho sugere. Pelo contrário, discordâncias reforçarão a constatação de que esses são conceitos valorativos disputados – um argumento filosófico que Dworkin desenvolve e que demonstro aqui também estar subjacente a discussões sobre privacidade e segurança, mas que não exige que se acolha toda sua obra. Não vou, neste trabalho, expor todo o pensamento de Dworkin – não é minha proposta, embora use argumentos dele.

[29] Ver Ronaldo Porto Macedo Junior, *Do xadrez à cortesia: Dworkin e a teoria do direito contemporânea* (São Paulo: Saraiva, 2013).

Dworkin, ademais, não é um autor que se dedicou à análise conceitual da privacidade e da segurança, exceto muito lateralmente[30], de modo que há um limite em sua própria obra ao tanto que poderia me ajudar neste estudo. Nesse contexto, este trabalho faz revisão de bibliografia de autores proeminentes de estudos de privacidade e segurança e que se ocuparam e se preocuparam com esse tipo de análise conceitual – ao que se referem, com a respectiva fundamentação –, porque o objetivo do trabalho é compreender o significado desses conceitos e mostrar a articulação entre eles. Quando trato de direito brasileiro, sobretudo na segunda parte, os materiais de consulta passam a ser textos doutrinários quanto à interpretação da Constituição Federal, além de julgados do próprio STF.

O tema das liberdades públicas e o direito probatório recebem atenção no direito processual penal de longa data,[31] assim como o direito à privacidade é estudado no campo do direito constitucional (e no direito civil[32] e no direito penal[33]) desde que conceituado assim. Há, ainda, uma produção cada vez mais crescente sobre proteção de dados pessoais.[34] Há estudos recentes que começam a integrar as áreas e a analisar o impacto da tecnologia nela.[35] Eu mesma já escrevo nessa área desde 2015. Estudos sobre polícia e sobre vigilância são, por sua vez, densamente trabalhados por sociólogos no Brasil.[36] Esse trabalho transita por essa produção científica e busca contribuir com ela, esperando conseguir mostrar que um olhar

[30] Dworkin, *Taking Rights Seriously*, 14;119; Ronald Dworkin, *Freedom's Law: The Moral Reading of the American Constitution* (Oxford: Oxford University Press, 1996), 50–51; Ronald Dworkin, *Domínio da Vida* (São Paulo: Martins Fontes, 2009), 74–75.

[31] Por exemplo, Ada Pellegrini Grinover, *Liberdades públicas e processo penal: as interceptações telefônicas* (São Paulo: Saraiva, 1976).

[32] Por exemplo, Pontes de Miranda, *Tratado de Direito Privado: Parte Especial – Tomo VII: Direito de personalidade, Direito de Família*, atualizada (São Paulo: Revista dos Tribunais, 2012); Milton Fernandes, *Proteção civil da intimidade* (São Paulo: Saraiva, 1977).

[33] Por exemplo, Paulo José da Costa Júnior, *O direito de estar só: tutela penal da intimidade*, 4ª ed. rev. atual. (São Paulo: Revista dos Tribunais, 2007).

[34] Por exemplo, Danilo Doneda, *Da Privacidade à Proteção de Dados Pessoais* (Rio de Janeiro: Renovar, 2006); Laura Schertel Mendes, *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental* (São Paulo: Saraiva, 2014); Bruno R. Bioni, *Proteção de dados pessoais: a função e os limites do consentimento*, 1º ed (Rio de Janeiro: Forense, 2019).

[35] Por exemplo, Danilo Knijnik, "A trilogia Olmstead-Katz-Kyllo: o art. 5o da Constituição Federal do século XXI", *Revista da Escola da Magistratura do TRF da 4a Região* 4 (2016): 77–96; Jürgen Wolter, *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*, org. Luís Greco (São Paulo: Marcial Pons, 2018).

[36] Por exemplo, Renato Sérgio de Lima, Samira Bueno, e Guaracy Mingardi, "Estado, polícias e segurança pública no Brasil", *Revista Direito GV* 12, nº 1 (abril de 2016): 49–85, https://doi.org/10.1590/2317-6172201603; Bruno Cardoso, *Todos os olhos: videovigilâncias, voyeurismos e (re)produção imagética* (Rio de Janeiro: Editora UFRJ; Faperj, 2014).

teórico de elaboração de conceitos que estão à frente das discussões pode também avançar questões práticas que precisamos inevitavelmente enfrentar quando discutimos se o direito brasileiro admite certas medidas de vigilância.

PARTE 1 – A ARTICULAÇÃO TEÓRICA

A primeira parte deste trabalho se volta a apresentar uma teoria da privacidade – e, mais particularmente, uma teoria da privacidade em face do Estado em suas atividades de prevenção e repressão criminal. No capítulo 1, mostro problemas de abordagens tradicionais de privacidade que trabalham com esse conceito a partir de distinções genéricas entre público e privado e também da proposta cada vez mais popular de traduzi-la sob a linguagem abrangente da teoria da proporcionalidade. Defendo que privacidade é um conceito interpretativo, que pode ter sentidos diferentes em diferentes contextos e que, se quisermos ainda manter a relevância da noção de um *direito* à privacidade frente a desafios tecnológicos, não há outro caminho. Sob essas premissas, no contexto de atividades de vigilância do Estado, defendo que a intencionalidade das práticas que associamos à ideia de privacidade diz respeito à proteção da dignidade pela contenção de poder.

No capítulo 2, mostro que o exercício pelo caminho inverso de análise do conceito de segurança – também interpretativo – chega a essa mesma conclusão, de modo que as concepções se reforçam mutuamente. Segurança não é um super-princípio: nós queremos a segurança que convive com as liberdades que valorizamos. O direito penal, direito processual penal e direito administrativo estão enraizados em princípios que reforçam esse compromisso. Em particular, a proteção da dignidade pela contenção de poder se dá mediante a observância de regras e procedimentos que carregam um compromisso fundamental de evitar injustiças, impondo a articulação de razões concretas que excepcionalmente justificariam a interferência a direito sem deixar de lhe mostrar respeito. Nessa linha, no capítulo 3, esboço os contornos das hipóteses de interação entre privacidade e segurança no âmbito de medidas de vigilância.

Capítulo 1 – Privacidade

O que significa dizer que alguém tem um direito à privacidade? Quando se pode dizer que está sendo violado? Em especial, quando o Estado *desrespeita* a privacidade? A pergunta é importante porque busco neste trabalho uma concepção desse direito que vá me ajudar a iluminar nossas práticas jurídicas no contexto de atuação policial. Elize Matsunaga tinha um direito à privacidade sobre o que guarda em sua casa e no seu carro? Sobre os locais em que seu celular aponta que esteve? Sobre o que fez e carregou no elevador de seu prédio? Como definimos isso e como essas garantias se opõem ao Estado?

Para responder a essas perguntas, este capítulo começa apresentando duas abordagens influentes do modo de enfrentamento da definição do escopo do direito à privacidade. A primeira delas é a ideia de associar privacidade a uma divisão entre público e privado e vincular ao privado a noção de segredo. O direito à privacidade protegeria o que é privado. Como veremos, essa abordagem traz dificuldades: ela oferece critérios que são ao mesmo tempo amplos ou reducionistas demais. Alguns desses problemas têm vindo à tona principalmente por conta do avanço tecnológico, como atividades em público e a coleta massiva de dados que não são tradicionalmente entendidos como "privados" ou sigilosos.

A segunda abordagem consiste em tratar o direito à privacidade como uma prerrogativa de controle abrangente sobre informações pessoais. Essa tendência é alimentada em parte pelos problemas da concepção mais comum decorrente da dicotomia entre público e privado e do diagnóstico de que realmente está ultrapassada e mal equipada para lidar com problemas contemporâneos que surgem com tratamento de dados pessoais. O revés dessa abordagem é que ela equipara "direito à privacidade" a um interesse de privacidade, que deve e pode sempre ser balanceado com outros interesses. Deixa de capturar as instâncias em que

postulamos algo muito mais forte ao articular esse "direito": que temos uma prerrogativa moral em face da própria comunidade política a que pertencemos de que ele seja observado.

Diante dessas dificuldades, apresento uma abordagem para reflexão sobre direitos à privacidade que penso que poderia evitar esses dois problemas. Ela passa por recuperar a ideia de Helen Nissenbaum e Daniel Solove de que o contexto é importante para identificar as práticas de privacidade que o compõem, as razões que as suportam, e regras que a governam, combinada com a ideia de que, nas instâncias em que discutimos se há violações, privacidade é um conceito e uma prática interpretativa. Isto é, com relação ao qual as pessoas reconhecem um valor, uma intencionalidade, e oferecem concepções, hipóteses interpretativas, de tipo construtivo sobre qual é essa intencionalidade e o que ela requer. Para enxergar quando há violação dessa prerrogativa, entender as regras que governam, o valor a que se voltam e a intencionalidade do agente também importará.

Feito isso, penso que terei preparado o caminho para afastar essas duas dificuldades perenes que alcançam também o enfrentamento de questões de privacidade em face do Estado no contexto de práticas de segurança pública e investigações criminais. Essa abordagem não afasta, entretanto, uma outra dificuldade: um profundo ceticismo sobre barreiras que privacidade poderia por a atividades policiais. O chavão de que a privacidade não pode servir de escudo para práticas ilícitas é tão comum quanto efetivo para apelar a uma intuição de que criminosos não podem reivindicar privacidade para ocultar seus crimes. Se queremos uma concepção de privacidade que vá ser útil para esse contexto e questões que envolvem o Estado, precisamos de uma capaz de iluminar também esse campo e em que medida fronteiras nele se colocam.

Diante disso, defendo que uma concepção de privacidade baseada na dignidade, inspirada na teoria da justiça de Ronald Dworkin, estaria apta a dar sentido a preocupações com a maneira como identificamos danos à uma prerrogativa de privacidade e como o próprio Estado tem o dever de mitigar riscos de danos deliberados que sua atuação acarreta, que possam comprometer valores que apreciamos. Deve atuar contendo ônus excessivos e mostrando respeito e cuidado às pessoas e sua responsabilidade de definir os caminhos de suas próprias vidas. Ao fim do capítulo, retomo situações hipotéticas como as que mencionei acima postas no caso Elize Matsunaga para melhor visualização das diferentes maneiras em que se apresenta e o que isso significa frente ao Estado-penal.

1 Desafios da definição do escopo de um direito à privacidade

1.1 *A dicotomia entre o público e o privado*

As origens da formulação de privacidade como direito

A elaboração conceitual seminal e mais famosa de privacidade está no artigo *The Right to Privacy*[37] de Samuel Warren e Louis Brandeis, de 1890. Preocupados com a popularização de câmeras instantâneas e a crescente circulação de jornais "que invadiram os recintos sagrados da vida privada e doméstica"[38], os autores se propusenham a analisar se o direito então vigente nos Estados Unidos oferecia um princípio que poderia ser invocado para proteger a privacidade do indivíduo – para assegurar a ele um "direito a ser deixado só"[39].[40] Para tanto, usaram um método reconstrutivo para defender a existência desse direito como princípio que justificava uma série de casos paradigmáticos, apesar de nunca mencionarem um tal direito[41].

Era o caso, por exemplo, de situações em que se protegeram publicações autorais de qualquer tipo e independente do teor, quando sem consentimento. Um interesse na propriedade intelectual seria insuficiente para explicar tudo: não é só o ganho que o autor poderia ter que estava em questão, mas a própria capacidade de definir se a publicação seria conhecida por outras pessoas ou não – e assim proteger contra emoções e sentimentos de sofrimento que a exposição ao público pudesse causar. Ainda, o caso mais famoso de *common law* sobre confidencialidade proibia que fossem reproduzidos não só gravuras que o Príncipe Albert e a Rainha Victoria teriam feito para seu uso pessoal, mas também descrições sobre elas que alguém que, a princípio legitimamente, teve acesso a elas pudesse fazer.[42] O direito da propriedade intelectual (copyright, no caso) apenas proibia reproduções

[37] Samuel Warren e Louis Brandeis, "The Right to Privacy", *Harvard Law Review* 4, nº 5 (1890): 193–220.
[38] Warren e Brandeis, 195.
[39] A formulação original nesses termos é atribuída, inclusive por Warren & Brandeis, ao juiz Thomas Cooley.
[40] Warren e Brandeis, "The Right to Privacy", 195;197.
[41] Dworkin, *Taking Rights Seriously*, 119.
[42] Uma referência ao caso Prince Albert v Strange, de 1849. Os monarcas tinham como hobby a elaboração de gravuras e os imprimiam para compartilhar entre amigos e familiares. O responsável pela impressão em Windsor fez as cópias solicitadas e devolveu as originais, mas um assistente seu fez cópias extras e as vendeu para compor uma exibição e um catálogo descritivo de William Strange. Prince Albert obteve a tutela inibitória. Warren e Brandeis, "The Right to Privacy", 200–205; Daniel Solove e Neil Richards, "Privacy's Other Path: Recovering the Law of Confidentiality", *The Geogetown Law Journal* 96 (2007): 130–31.

de obras literárias e pinturas sem autorização, não oferecendo proteção até mesmo contra elaboração de descrições dessas obras, nem listas do que as compõem. Nem mesmo a ideia de quebra de confiança pelo funcionário contratado servia para explicar o caso: se um terceiro estranho ilegitimamente tivesse obtido o material, uma proteção ainda seria acionada.[43] Daí concluía:

> Essas considerações levam à conclusão de que a proteção conferida aos pensamentos, sentimentos e emoções, expressos por meio da escrita ou das artes, na medida em que consiste em impedir a publicação, é apenas uma instância da aplicação do direito mais geral do indivíduo para ser deixado só. É como o direito de não ser agredido ou espancado, o direito de não ser preso, o direito de não ser processado maliciosamente, o direito de não ser difamado. Em cada um desses direitos, como de fato em todos os outros direitos reconhecidos pela lei, é inerente a qualidade de ser possuído [*being owned and possessed*] – e (como esse é o atributo distintivo da propriedade) pode haver alguma propriedade em falar desses direitos como propriedade. Mas, obviamente, eles têm pouca semelhança com o que é normalmente compreendido sob esse termo. O princípio que protege os escritos pessoais e todas as outras produções pessoais, não contra roubo e apropriação física, mas contra publicação em qualquer forma, é na realidade não o princípio da propriedade privada, mas o de uma personalidade inviolável.[44]

Assim, para defender que temos um *direito* a essa *privacidade,* Warren & Brandeis recorreram à ideia da "personalidade inviolada", que não é mais aprofundadamente elaborada no artigo senão pelo contraste a uma noção de propriedade e a outra de confiança entre as pessoas que não justificariam plenamente este e outros casos, e que precisaria ser resguardada contra "invasões" – danos de sofrimento mental. Embora o exemplo fosse sobre *publicações* pessoais de alguém (como as gravuras), no mesmo texto destacavam que "se as decisões indicarem um direito geral à privacidade para pensamentos, emoções e sensações, estes devem receber a mesma proteção, seja expressa por escrito, ou por conduta, por conversa, por atitudes ou por expressão facial"[45].

---

[43] Warren e Brandeis, "The Right to Privacy", 208;211.

[44] Tradução livre. No original: "These considerations lead to the conclusion that the protection afforded to thoughts, sentiments, and emotions, expressed through the medium of writing or of the arts, so far as it consists in preventing publication, is merely an instance of the enforcement of the more general right of the individual to be let alone. It is like the right not to be assaulted or beaten, the right not to be imprisoned, the right not to be maliciously prosecuted, the right not to be defamed. In each of these rights, as indeed in all other rights recognized by the law, there inheres the quality of being owned and possessed – and (as that is the distinguishing attribute of property) there may be some propriety in speaking of those rights as property. But, obviously, they bear little resemblance to what is ordinarily comprehended under that term. The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality."Warren e Brandeis, 205.

[45] Tradução livre. No original: "if the decisions indicate a general right to privacy for thoughts, emotions, and sensations, these should receive the same protection, whether expressed in writing, or in conduct, in conversation, in attitudes, or in facial expression.". Warren e Brandeis, 206.

A invasão que os autores tinham em mente, por sua vez, consistia na *fixação*,[46] em qualquer meio, de (i) questões (*matters*) que se referem à "vida privada" ("vida, hábitos, atos e relações privadas")[47] que "todos os homens igualmente teriam direito de manter à distância da curiosidade pública"[48] ou mesmo de (ii) outras questões que também seriam "privadas" porque a pessoa em questão não tem "posição que torne suas condutas alvo legítimo de averiguações públicas"[49] (por exemplo, alguém que não concorre a cargo público e portanto não deve ter sua guaguez reportada em jornal)[50]. O direito à privacidade, por outro lado, não proibiria publicação de questões "que são de interesse público ou geral"[51].

A referência implícita nessa exploração de escopo e de limites é a uma divisão entre o que é da esfera pública e o que é da esfera privada – seja em razão da *matéria* (um assunto ou questão *privada*) seja em razão da relativa *ocultação* dada à questão ou assunto (por conta do modo de vida da pessoa – ser uma pessoa comum, não um político – ou até mesmo de uma demarcação territorial – como por compor o ambiente doméstico). Quando algum aspecto da vida "privada" de um cidadão é afetado sem o seu consentimento, os autores defendem que há *invasão* na esfera privada e, portanto, uma possível violação a esse direito digna de reparação. Assim, a ideia de direito à privacidade é associada à proteção de áreas ou aspectos da vida nas quais terceiros não podem intervir, já que o indivíduo teria a prerrogativa de mantê-las em segredo. Protege-se aquilo que é de "ocorrência doméstica"[52] do público em geral e assim garante-se ao indivíduo a prerrogativa de fixar os limites da publicidade à coisa, fato ou informação em questão.

Nesses termos, a concepção de privacidade articulada pelos autores está orientada a resguardar ao indivíduo um tipo de liberdade: o poder de controle sobre a publicidade conferida a aspectos da vida privada, enquanto respeito a seu direito individual de definir os contornos de sua personalidade e influenciar a forma como se é conhecido publicamente. A tutela jurídica da privacidade serviria ao desenvolvimento e gerenciamento da personalidade. Daí surgiriam na jurisprudência americana quatro tipos de atos ilícitos – que ficaram

[46] Warren e Brandeis, 217. (excluindo remédio para invasão da privacidade por 'publicação oral na ausência de dano especial').
[47] Warren e Brandeis, 215–16.
[48] Warren e Brandeis, 216.
[49] Warren e Brandeis, 216.
[50] Warren e Brandeis, 215.
[51] Warren e Brandeis, 214.
[52] Warren e Brandeis, 201.

conhecidos como *privacy torts*[53]: *intrusion upon seclusion*;[54] *public disclosure* of *private facts*;[55] *false light*;[56] *appropriation of name or likeness*[57].[58]

Os bastidores e um recorte

À vista do contexto particular em que a discussão do texto se punha, a preocupação dos autores estava muito relacionada ao papel da imprensa e em dar uma resposta jurídica àquilo que parecia ser uma nova ameaça às pessoas decorrente da *divulgação* de aspectos de sua vida a outras do público em geral. Em trabalhos que recontam os bastidores do artigo, diz-se que a esposa de um dos autores, Mabel Warren, vinda de uma família aristocrática cujos "engajamentos sociais" (participação em jantares, festas, casamentos, velórios) sempre foram de interesse da imprensa, teria encorajado o marido a escrever o artigo. Em particular, atribui-se a preocupação com a reputação de membros de uma classe de elite – pessoas de interesse de repórteres cada vez mais ousados em suas colunas de jornais –, o que Neil Richards chama de uma crescente ansiedade porque "sentiam seu status e controle social ser posto em dúvida na medida em que classes urbanas mais baixas de pessoas alfabetizadas desafiam sua autoridade"[59] (tradução livre).

---

[53] William Prosser, "Privacy", *California Law Review* 48, nº 3 (31 de agosto de 1960): 383, https://doi.org/10.15779/Z383J3C.

[54] Sujeita aquele que invade a "solidão" ou "isolamento" de alguém ou suas questões privadas à responsabilização quando a intrusão for "altamente ofensiva a uma pessoa razoável". Daniel J. Solove e Paul M. Schwartz, *Information Privacy Law*, 5º ed (New York: Wolters Kluwer, 2015), 83.

[55] Sujeita aquele que dá publicidade a alguma questão relativa à vida privada de alguém à responsabilização quando a questão publicizada é "altamente ofensiva a uma pessoa razoável" e "não é de interesse legítimo do público". Solove e Schwartz, 109.

[56] Sujeita à responsabilização aquele que dá publicidade a alguma questão relativa a outrem que o coloque sob uma falsa perspectiva perante o público quando é "altamente ofensiva a uma pessoa razoável" e agiu-se com conhecimento ou "descaso imprudente" quanto à falsidade da questão. Solove e Schwartz, 199.

[57] Sujeita à responsabilização aquele que se apropria do nome ou imagem de alguém para seu uso e exploração. Solove e Schwartz, 213.

[58] Apesar de conhecidos como "privacy torts", como se nota pelos *torts* de "false light" e "appropriation of name or likeness", o interesse protegido por esses institutos não é simplesmente o da proteção de um domínio privado – mas também a reputação e interesses econômicos na exploração comercial de uma personalidade. A observação serve para nos alertar ao fato de que – não em poucas ocasiões – a jurisprudência ou o debate público pode nomear de "privacidade" algum interesse que não necessariamente seja de privacidade. É também por isso que é necessário analisar o conceito e buscar a melhor concepção de seu valor.

[59] Neil Richards, *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*, 1st edition (Oxford, UK; New York, NY: Oxford University Press, 2015), 18. Nesse sentido, também Stefano Rodotà, *A vida na sociedade da vigilância – a privacidade hoje*, org. Maria Cecilia Bodin de Moraes, trad. Danilo Doneda e Luciana Cabral Doneda (Rio de Janeiro: Renovar, 2008), 28.

Motivações à parte, realmente o escopo do direito à privacidade proposto por Warren e Brandeis sempre representou um desafio para conviver com proteções de liberdade de expressão, de pensamento e de imprensa: a parte mais afetada pelo reconhecimento desse direito parecia ser o trabalho da imprensa, que assim passaria a encontrar obstáculo nas informações que pode divulgar – o que é *privado* está fora do seu alcance. Não bastasse, a delimitação de fronteiras entre o que é público e o que é privado na vida de alguém não é tarefa fácil e o direito articulado parecia se orientar a proteger contra certos tipos de danos à emoção, algo que pode ser muito variável de pessoa para pessoa.[60] Essa concepção de privacidade, portanto, não foi celebrada por quem viu e vê o valor da publicidade e da circulação de informações em perigo.[61]

Tentando salvar o que haveria de aproveitável nessa concepção, Neil Richards sustenta que ela sobrevive se focarmos no problema da *invasão* – da coleta de informação, ao invés da divulgação – em "zonas de solitude ou isolamento" (*zone of solitude or seclusion*). A questão seria, então, definir que zonas privadas são essas para saber quando o direito é violado. Primeiro exemplifica: "é uma invasão da privacidade grampear o telefone de alguém ou gravar secretamente som ou vídeo em seu quarto" [62] (tradução livre). O que acontece em um quarto ou é dito em comunicações privadas pertence ao âmbito privado, portanto. A seguir articula: uma "invasão de privacidade só se aplica quando estamos falando de um local ou relação privada"[63]. Focando nessa perspectiva, problemas com conflitos com liberdade de expressão e imprensa desapareceriam.

Há algo de relevante para este trabalho nessa aposta: considerando que quero propor uma formulação para os limites e as condições que a noção de privacidade pode colocar ao trabalho de instituições estatais para segurança pública e para investigações criminais, olharei particularmente para atividades que envolvem não a *divulgação* de informações pessoais de alguém a um público geral (como é típico no trabalho da imprensa), mas o *acesso* a elas por uma instituição pública – a tomada de conhecimento da polícia sobre informações pessoais de alguém, paradigmaticamente. Embora "acesso" também possa ocorrer interrogando-se

[60] Richards, *Intellectual Privacy*, 49.
[61] Por exemplo: Fred Cate, "Principles of Internet Privacy", *Connecticut Law Review* 32 (1º de janeiro de 2000): 877–96.
[62] Richards, *Intellectual Privacy*, 69.
[63] Tradução livre. No original: "invasion of privacy only applies when we are talking about a private place or relationship". Richards, 69.

pessoas ou obtendo depoimentos (uma forma também de divulgação, ainda que não ao público em geral), vou focar nas situações em que a obtenção da informação se dá por observação/ coleta não-testemunhal, como adiantei na introdução. Nesse contexto, a concepção de Warren e Brandeis aparenta ser candidata a formular um direito à privacidade que possa ser relevante aqui se, como propõe Richards, focarmos no que ela diz para problemas de *coleta/acesso*.

A sistematização da noção de privacidade sob uma dicotomia criterial

A formulação simples e influente dos contornos do direito à privacidade contida na concepção de Warren & Brandeis diz então que direitos à privacidade serão implicados quando uma ação interferir no que pertence ao "âmbito privado", naquilo de "ocorrência doméstica" que a pessoa deve poder manter em segredo. Fundamentalmente, como adiantei, é uma concepção que apela a uma separação entre esferas pública e privada, que faz parte de muitos debates filosóficos. No direito constitucional, espelha-se, como falarei mais na segunda parte do trabalho, na linguagem daquilo que diz respeito à "intimidade", à "vida privada", à "casa", ao "sigilo". Na dogmática jurídica, já foi incorporada ao direito civil, para fazer triagem de interesses de privacidade que seriam protegidos por direitos de personalidade pela chamada "teoria das esferas" do alemão Heinrich Hubmann: faz-se separação entre o que pertenceria aos âmbitos do segredo, da intimidade e da privacidade e o que pertenceria ao âmbito da vida pública, para proteger os primeiros.[64]

Apesar de Warren & Brandeis terem alertado que "nenhuma fórmula fixa pode ser usada para proibir publicações desagradáveis"[65], os autores não aprofundaram tanto quanto a complexidade do tema e de cenários demandaria o que compõe a "vida privada" que pode ser invadida e que autoriza a invocação de um direito. Apesar de o exercício reconstrutivo que dá forma ao texto mostrar a relevância de explorar o princípio, a razão, o propósito, o que melhor justifica conjuntos de casos que de algum modo tratem de 'privacidade' em certo contexto, essa dimensão valorativa que pode ser investigada para dar sentido a controvérsias

[64] Heinrich Hubmann, "Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion", *JuristenZeitung* 12, nº 17 (1957): 521–28; Danilo Doneda, *Da Privacidade à Proteção de Dados Pessoais*, 2º ed (São Paulo: Revista dos Tribunais, 2019), 103–5; Rosa Maria de Andrade Nery e Nelson Nery Junior, *Instituições de Direito Civil: volume I [livro eletrônico]: parte geral do Código Civil e direitos da personalidade*, 2º ed (São Paulo: Thomson Reuters, 2019), RB-17.8 e RB-17.9 (e-book).
[65] Samuel Warren and Louis Brandeis, "The Right to Privacy," *Harvard Law Review* 4, no. 5 (1890): 215.

e disputas sobre privacidade e para avaliar se faz sentido falar em direito em certo caso, facilmente se deixaria escapar nas sistematizações doutrinárias que daí viriam.

A abordagem que apela à dicotomia entre público e privado acabou alimentando testes binários para solução de casos de privacidade: distinções entre informações privadas (sensíveis) e informações não-privadas (não-sensíveis), pessoas públicas e pessoas privadas, espaços públicos e espaços privados, para dizer alguns.[66] Como veremos na segunda parte desse trabalho, o paradigma da distinção entre público e privado é muito comum na jurisprudência. Pressupõe que exista certo "segredo" e destacamento para que se possa falar em algo privado, protegido por um direito à privacidade. Abandonando o método reconstrutivo voltado a depurar razões e princípios de justificação subjacente ao trabalho de Warren e Brandeis, a generalização dessa dicotomia tem por premissa que seria possível daí extrair um teste criterial para saber se estamos falando de algo que recebe proteção ou não: se o critério do que compõe "vida privada" estiver presente, o aspecto em questão seria privado (e protegido).

Como essa dicotomia responde à pergunta de quando há um direito à privacidade e quando é violado? Comecei o trabalho mencionando o caso Elize Matsunaga, que pode ser didático aqui. Vejamos a situação anterior ao homicídio, do vídeo de Marcos com a amante à frente de um restaurante, feito por detetive particular a pedido de Elize, e analisemos se houve uma violação a direito à privacidade.[67] Alguém poderia dizer que há uma "questão privada" implicada porque é um registro de um relacionamento romântico "privado" que só interessa aos dois ("ocorrência doméstica"), sobretudo considerando-se que Marcos não era ninguém famoso que deveria esperar que sua presença em locais despertasse comoção e interesse (apesar de executivo de uma empresa bem-sucedida brasileira, não era uma "pessoa pública" conhecida por aqueles estranhos a ele fora do dia-a-dia da empresa). Outros poderiam dizer que não era mais uma "questão privada", porque os envolvidos não se esforçaram minimamente em ocultar a quem estava à sua volta o que estavam fazendo – estavam em uma calçada pública, afinal – ainda que esses estranhos que viam a cena provavelmente não os conhecessem.

---

[66] Helen Nissenbaum, "Privacy as Contextual Integrity", *Washington Law Review* 79 (2004): 136.

[67] "Vídeo mostra diretor da Yoki com amante, na véspera do assassinato", *Bom Dia Brasil* (Globo, 11 de junho de 2012), http://g1.globo.com/bom-dia-brasil/noticia/2012/06/video-mostra-diretor-da-yoki-com-amante-na-vespera-do-assassinato.html.

Como se vê (e a imprensa já reclamava), delimitar quando é questão privada não é preto no branco. Richards, em particular, penso que diria que a segunda avaliação é a correta. Ele considera que:

> Pode ser rude tirar uma foto de alguém em uma rua pública ou em um restaurante, mas provavelmente não é uma invasão ilegal da privacidade. O limite da reclusão é um lembrete de que você só pode invadir privacidade se você está invadindo algo privado que seria ofensivo a uma pessoa comum.[68]

Na solução de Richards, ao que parece, quando uma informação que poderia ser sensível (detalhes da vida sexual de alguém) é de algum modo externada em local público, esse fator pesa e prepondera. Por outro lado, um espaço privado como a casa/quarto de alguém é tão associado a um "âmbito privado", que é provável que mesmo as interferências que não revelem uma "informação sensível" da pessoa seriam consideradas violação da privacidade. O local como fator definidor seria extremamente relevante: os perímetros de uma casa, uma zona de "comunicações privadas" como telefone também.

Territórios hoje praticamente incontroversos de proteção a um direito à privacidade – como casas e linhas telefônicas – acentuam a ênfase *espacial* a que essa concepção de privacidade baseada na dicotomia entre público e privado tende a dar lugar. Não por outra razão, as proteções à "inviolabilidade do domicílio" e à "inviolabilidade das comunicações privadas" são bem consolidadas no direito. Tais proteções jurídicas consagram tipos de espaços e informações que servem de *proxy* (de generalização) criterial para a delimitação do escopo do conceito de privacidade e de suas consequências jurídicas: se está em certo território, é protegido pela privacidade; se é um tipo de comunicação confidencial transmitida por certo mecanismo, também; se há interferência sobre tais perímetros, haveria dano e violação a direito. Se não houve interferência nesses perímetros, deixando de passar pelo teste, não há violação.

Esses são proxies que funcionaram relativamente bem para essas proteções por um bom período de tempo e agora começam a ser desafiados por tecnologias que alteram nossa compreensão de limites territoriais e categorias de informação, como falarei mais à frente.[69]

---

[68] Tradução livre. No original: "It might be rude to capture someone's photograph on a public street or in a restaurant, but it's probably not an illegal invasion of privacy. The seclusion limitation is the reminder that you can only invade privacy if you are invading something private that would be offensive to an ordinary person." Richards, *Intellectual Privacy*, 69.

[69] Sinalizei a essas dificuldades ainda na introdução, quando me referi a uma ferramenta que permitisse ver *através de paredes,* sem precisar ingressar em domicílios: por um teste criterial definido pelas fronteiras do território do domicílio, há quem poderia dizer que não há *violação a direito* porque não houve ingresso.

Os sinais de que essa abordagem tem problemas, no entanto, já se apresentavam antes disso: boa parte das principais controvérsias acerca de direitos à privacidade gira em torno da discussão sobre o que faz parte do *âmbito privado* nesses sentidos, apesar de estar fora dessas fronteiras bem delimitadas: quais informações, quais coisas, quais relações são também "privadas". O que constitui a inviolabilidade da "vida privada" e da "intimidade", por exemplo? A concepção de Warren & Brandeis, para além de facilitar a simplificação a testes binários para identificação do que é público e do que é privado, vai dizer pouco sobre isso – sobre a "personalidade inviolada" que resguarda. Como visto, sua preocupação era mais direcionada a problemas de divulgação, não de coleta/acesso. Mesmo os testes propostos pela teoria das esferas não afastam essa dificuldade no seu manejo, pois pressupõe a possibilidade de distribuição e categorização de atos, informações, relações entre os círculos concêntricos: a situação de Marcos e da amante pertence a qual? Essa exploração precisaria continuar.

Novos caminhos

Mais recentemente alguns autores começaram a perceber que essa redução à distinção entre público e privado – e ao paradigma da privacidade como algo reservado ou que está em segredo – (e a consequente busca por testes criteriais binários) padece de um problema mais profundo e deixa considerações importantes de fora. Por isso tentam alterar a rota do empreendimento de exploração sobre o escopo do direito à privacidade. Observaram que essa abordagem deixa de reconhecer que pessoas podem querer manter coisas privadas em face de algumas pessoas mas não de todas, por exemplo. Assim, essas reduções tornam difícil falar em proteger privacidade depois que uma informação é compartilhada com alguém. Deixam também de captar que informações a princípio banais podem ser bastante reveladoras a depender de como forem conjugadas e como usadas. Apenas distingui-las entre o mundo das informações sensíveis e o das não-sensíveis pode ser simplificador demais. Nossa gestão de privacidade é mais complexa do que os testes binários querem simplificar. Diante disso, abriram-se as portas para diferentes estratégias para localizar "privacidades" que devem ser protegidas que ultrapassem a lógica públixo x privado.

Helen Nissenbaum, por exemplo, defende a pertinência de analisar violações de privacidade a partir de uma preocupação de que fluxos de informações pessoais devem atender a noções do que é apropriado coletar e usar em certo contexto, quais os papeis dos

atores envolvidos (de quem e para quem as informações podem ser distribuídas) e a título do quê existe o fluxo – uma abordagem chamada de "integridade contextual".[70] Ela faz o diagnóstico de que focar na delimitação do âmbito privado para fixar fronteiras do valor da privacidade a partir de dicotomias simplificadoras como "informação sensível ou não sensível" e "espaço público ou espaço privado" frustra nossa capacidade de lidar com problemas que tanto não são detectáveis por essas distinções como, ainda assim, parecem atingir o valor que associamos à ideia de privacidade.[71] É o caso de diversos desafios postos por tecnologias da informação, como a vigilância de áreas públicas que comprometem a capacidade de obscuridade das pessoas quando estão em público – uma repercussão que causaria desconforto a muitas pessoas, diz. Usa, portanto, um exemplo que a princípio parece paradoxal, de uma privacidade em público – a obscuridade –, para dizer que ela nos leva a rever como pensamos em privacidade e violações da privacidade a que moralmente temos direito em geral.

Vejamos um exemplo. O "anonimato" pode ser visto como "estado de privacidade" que pessoas, principalmente em grandes cidades, gozam em uma multidão mesmo em locais abertos. Talvez seja esse um "estado de privacidade" em que Marcos e a amante estivessem mesmo na calçada de uma rua perante estranhos. Os que estavam à sua volta podiam ver o que faziam e ouvir o que falavam, mas não sabiam quem eram nem se importavam com o que discutiam. Ainda que esperassem aparecer em fotos tomadas por turistas ou outras pessoas, como provavelmente estes não ligavam para o que estavam fazendo, tampouco se preocupariam. Quanto a um garçom que já tivesse visto Elize e Marcos no mesmo restaurante e em face de quem não havia "estado de privacidade", talvez esperassem dele que seria discreto, porque os funcionários do local usualmente o são. Ainda que tenham "tornado acessível" seu relacionamento romântico às pessoas na rua, pode ser que não pretendessem abrir mão da "privacidade" dessa "questão privada" em face de Elize. Essa obscuridade

[70] Nissenbaum, "Privacy as Contextual Integrity"; Helen Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life* (Stanford, CA: Stanford University Press, 2010); Andrew D. Selbst, "Contextual Expectations of Privacy", *Cardozo Law Review* 35 (2014 de 2013): 643–709.

[71] "The crucial point I am arguing here is not that the private/public dichotomy is problematic, per se, but that it is not useful as the foundation of a normative conception of privacy. Although, in the past, it might have served as a useful approximation for delineating the scope of a right to privacy, its limitations have come to light as digital information technologies radically alter the terms under which others—individuals and private organizations as well as government—have access to us and to information about us in what are traditionally understood as private and public domains." Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, 116–17.

deveria mudar a avaliação sobre a existência de uma violação de um direito à privacidade pela captura em vídeo do que faziam na calçada de uma rua por um detetive particular?

O detetive sabia quem eram (não eram anônimos a ele) e tinha um propósito ao tomar as fotos de suas atividades (no caso, também de um detalhe da vida sexual deles) para compartilhar com Elize, que suspeitava de traição. Usou de seu próprio anonimato para, a olho nu, não oferecer a Marcos e à amante qualquer indício de que não estavam mais apenas entre estranhos; e executou um trabalho delegado por Elize. Elize, através do detetive, violou uma privacidade que Marcos tinha direito de reivindicar perante ela, diante de sua obscuridade? Embora em um casamento seja típico que o casal compartilhe um com o outro diversas informações que não revelam a mais ninguém, também nele se acomodam espaços de confiança mútua, sobretudo sobre as coisas que se faz e se fala quando o parceiro não está por perto e que, em geral, não envolvem acompanhamento por um detetive particular no momento em que não estão fisicamente juntos.

Se Marcos quisesse reivindicar um direito à privacidade contra esse "acesso" e tivesse de desafiar a ideia de que "não existe privacidade em público", sua demanda teria de se reportar a expectativas de obscuridade e sua importância em face de quem não está fisicamente perto nem tem uma memória interessada nem infalível. Ainda, apelaria a valores de confiança, lealdade e respeito mútuo, que se estenderiam a experiências de Marcos mesmo quando Elize não está presente. Talvez Elize tenha violado uma prerrogativa moral que Marcos esperava ter perante ela, pelo menos.

Como as ações de Marcos também destroçam as expectativas de confiança mútua do casal e expectativas de lealdade em um casamento, sua reivindicação fica "manchada" e a inclinação é achar que ela está corrompida. Provavelmente seria mais fácil de enxergar a violação caso o detetive em ação o tivesse perseguido, não tivesse encontrado nada sobre traição, mas ainda assim tivesse montado um dossiê de todos os locais que frequentou e das pessoas com quem se encontrou. Estaríamos nesse caso prontos a dizer que houve violação de um direito à privacidade? Para as diferentes pessoas com quem nos encontramos ao longo de um dia cheio de atividades, ou mesmo a que nos veem nas ruas, há revelações pontuais do que fizemos. Um trabalho de reconstrução de tudo isso a ponto de conferir a alguém para além de Marcos uma visão sobre tudo o que fez e com quem se encontrou que de outro modo só ele teria, pode ser relevante à visão que ele tem de si e de como vive. Teríamos que

investigar então o que essa obscuridade tem de importante e se, por que e como deve ser protegida nesses contextos em que esse valor se coloca.

Tecnologia e o esgotamento de testes binários

Como se vê, era tudo mais simples quando se podia dizer que não há privacidade em público. Ao mesmo tempo em que o abandono pela fixação de um "âmbito privado" planificado e de soluções baseadas em testes binários torna análises mais complexas e mais difíceis, elas também acrescentam nuances que ficam perdidas em abordagens que não levam em conta contextos em que o uso da noção de privacidade se coloca e os sentidos – que podem ser diversos e se combinar e expressar por diferentes valores – em diferentes ocasiões. Isso é especialmente relevante diante do avanço tecnológico, que extrapola aquilo que é humanamente possível fazer e a disponibilidade de informações que pessoas têm, causando disrupção em expectativas e comportamentos que compõem práticas de privacidade.

As máquinas fotográficas que incomodaram Warren & Brandeis já eram uma dessas revoluções: a popularização dessa tecnologia de repente fez pessoas ganharem a capacidade de fixar eternamente um momento específico em uma imagem ou vídeo que poderiam ser guardados e compartilhados ilimitadamente. Quando essa capacidade não existia, pessoas não precisavam esperar que isso poderia acontecer nem imaginar o que poderia decorrer daí; também não precisavam de um remédio jurídico que preservasse uma capacidade que não podia ser ameaçada apenas com os recursos naturais que humanos têm. Essa privacidade era natural.

Hoje em dia a tecnologia desafia teste binários inclusive aplicáveis às "zonas" incontroversas de privacidade: obriga a rever mesmo quando "zonas" "clássicas" de privacidade (como a casa e a linha de telefone) são violadas – e a pensar sobre como devem se expandir ou são reduzidas por versões "digitais" desses ambientes. É o caso de tecnologias que permitem que as pessoas vejam através de paredes: que a casa é um local protegido, isso mesmo a concepção simples de privacidade capta, mas se não é necessário que a pessoa *penetre* nesse espaço fisicamente para ver o que nela ocorre, ainda há violação? E se a casa é uma 'smart home', cheia de câmeras e aparato com internet das coisas, com dados armazenados junto às respectivas empresas que prestam os serviços que amparam o uso dessas tecnologias: os dados da casa foram "compartilhados" já de uma maneira que se

tornaram menos sensíveis? Quando ocorreria uma violação se algum terceiro acessar tais dados? A dificuldade da separação criterial entre público e privado, e dos testes binários, retorna.

Privacidades e seus problemas

Nissenbaum não é a única a fazer o diagnóstico sobre o esgotamento dessa abordagem. Daniel Solove, por exemplo, defende a relevância de analisar a rede de "problemas de privacidade", para entender o que tutelamos e levar a outros contextos.[72] Ele sugere ser melhor abordar o conceito de privacidade a partir da premissa de que suas aplicações guardam "semelhanças de família" – observação inspirada na obra de Ludwig Wittgenstein: para ele, "Proteções de privacidade endereçam uma teia de problemas interconectados que causam disrupção a atividades específicas. O ato de conceptualizar privacidade deve consistir em mapear a topografia dessa teia"[73].

O autor usa essa referência para justificar sua preferência por olhar para a "rede de *problemas*" que direitos de privacidade endereçam e abandonar a fixação de um conceito que contemple tudo – podemos ter mais de um conceito de privacidade, que estão relacionados entre si de diferentes maneiras. Há, no entanto, algo mais a que essa opção aponta: para a constatação de que privacidade é um conceito essencialmente contestado e que supõe uma gramática distinta, que torna a busca por certos "critérios" que identifiquem o que é privacidade e o reduzam a um fator binário acontextual algo pouco proveitoso para iluminar e resolver debates sobre privacidade[74]. No fundo, uma ideia melhor é entender os contextos paradigmáticos em que usamos esse conceito e os problemas, as características e os valores

[72] Daniel Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy", *San Diego Law Review* 44, nº 4 (2007): 763. "Because privacy involves protecting against a plurality of different harms or problems, the value of privacy is different depending upon which particular problem or harm is being protected. Not all privacy problems are equal; some are more harmful than others. Therefore, we cannot ascribe an abstract value to privacy." Embora não acolha sua estratégia pragmática nem suas conclusões, acredito que sua abordagem aponta para problemas que realmente existem na forma como ainda muitos discutem privacidade.

[73] Tradução livre. No original: "Privacy protections address a web of interconnected problems that disrupt specific activities. The act of conceptualizing privacy should consist of mapping the topography of the web".Daniel J. Solove, *Understanding Privacy* (Cambridge, MA: Harvard University Press, 2008), Kindle Locations 979-980.

[74] Sobre conceitos contestados: W. B. Gallie, "Essentially Contested Concepts", *Proceedings of the Aristotelian Society* 56 (1955): 167–98. Fazendo também esse diagnóstico para privacidade: Deirdre K. Mulligan, Colin Koopman, e Nick Doty, "Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy", *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374: 20160118, nº 2083 (28 de dezembro de 2016): 1–15, https://doi.org/10.1098/rsta.2016.0118.

a que se refere, para ser capaz de usá-lo, interpretá-lo, identificá-lo e aplicá-lo e/ou distinguí-lo em outros e novos contextos. Há algo disso que já estava subjacente lá atrás ao esforço reconstrutivo de Warren & Brandeis, mas que foi esgarçado pela linguagem e pela sistematização convencional da dicotomia entre público e privado e que poderia ser resgatado.

Não é exatamente assim que a análise jurídica contemporânea tem respondido. Diante do avanço tecnológico, uma das maneiras como o direito respondeu ao que seriam novas ameaças à privacidade, é pelo desenvolvimento de um "direito à autodeterminação informacional", que deu lugar à prática jurídica do "direito da proteção de dados pessoais". Entre as razões propulsoras dessa concepção estaria justamente o fato de que a concepção de privacidade tradicional está muito próxima da proteção de "segredos", daquilo que é "privado", ao passo que o avanço tecnológico teria trazido à tona novas maneiras como mesmo informações "públicas" ou que já foram "compartilhadas", e inclusive aquelas que aparentam ser banais e não-sensíveis, e que não estão em "locais" privados, poderiam ser usadas de maneiras que causem danos ou riscos de danos a pessoas. Essa abordagem propõe ver toda operação de tratamento de dados pessoais como uma atividade que pode implicar um direito. O trabalho de Alan Westin é associado às origens dessa articulação. Em 1967, por exemplo, no livro *Privacy and Freedom,* o autor defendeu que privacidade é a "reivindicação de indivíduos, grupos e instituições de determinar por si mesmos quando, como e em que medida informações sobre eles são comunicadas a outros"[75] (tradução livre). Com uma concepção assim, talvez os problemas colocados pela tecnologia seriam melhor capturados. Esse cenário nos leva à discussão da segunda tendência nos debates sobre privacidade.

1.2 *Privacidade como interesses*

<u>As origens do direito à autodeterminação informacional</u>

A concepção de privacidade de Warren & Brandeis ficou marcada pela associação a um *direito a ser deixado só*.[76] Essa articulação da privacidade teria natureza individualista e

[75] Alan F. Westin, *Privacy and Freedom*, org. Daniel J. Solove (New York: Ig Publishing, 2015).
[76] Doneda, *Da Privacidade à Proteção de Dados Pessoais*, 2006, 7–30; Mendes, *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*, 27–29.

de liberdade *negativa*, voltada a aspectos ou espaços da vida nas quais o Estado e terceiros não podem intervir. Seria, portanto, fundamentalmente distinta da noção de direito à autodeterminação informativa sobre a qual nasce o "direito da proteção de dados pessoais" – dimensão positiva e social que pretende assegurar o controle do indivíduo sobre a circulação de informações sobre si de forma muito mais abrangente.[77]

A decisão da Corte Constitucional alemã sobre a Lei do Censo de 1983 é o marco mais famoso dessa fomulação.[78] Nela se deu a articulação emblemática das preocupações em torno da automação relativa ao processamento de dados e da necessária resposta do direito a elas. A lei do Censo em questão previa a coleta de 160 pontos de informação sobre profissão, trabalho e moradia de todos os cidadãos alemães e tinha como objetivo declarado fornecer ao governo dados sobre o estado da população, sua distribuição geográfica e sua composição em termos demográficos, sociais e econômicos. A ser realizada na forma de questionário obrigatório (sob pena de multa pecuniária), a lei tocou em medos ainda recentes de vigilância estatal, recordando a atuação da Stasi, justo no ano que antecedia 1984 – e as lembranças ao livro de George Orwell[79]: as possibilidades de formação de dossiês, utilização e disseminação dos dados coletados para outras e estranhas finalidades ao censo, bem como do cruzamento e enriquecimento de informações de outros bancos de dados gerenciados pelo Poder Público

[77] Rodotà, *A vida na sociedade da vigilância – a privacidade hoje*, 17;92-98.

[78] Vou focar na Europa, em que a linguagem de direitos logo chegou a essa área. Observo, no entanto, que a história do direito da proteção de dados não começa aí e que receios semelhantes com o avanço tecnológico também geraram movimentos regulatórios em outros locais. Nos Estados Unidos da América, ainda no ano 1973, o Departamento de Saúde, Educação e Bem-Estar produziu o relatório *Computers, Records, and The Rights of Citizens* chamando atenção para os perigos e ameaças latentes às então crescentes práticas de documentação baseada em computadores. Ver: Report of the Advisory Committee on Automated Data Systems, "Records, Computers, and The Rights of Citizens" (U.S. Department of Health, Education & Welfare, julho de 1973), https://www.justice.gov/opcl/docs/rec-com-rights.pdf. Tais consequências estariam relacionadas às potencialidades da "computerização", que (i) permite o armazenamento e o processamento de grandes volumes de informações; (ii) facilita acesso a dados interna e transversalmente a uma entidade ou organização; (iii) cria uma "nova classe" de entidades "documentadoras" de informações, cujas funções são técnicas e cujo relacionamento com os titulares das informações é em geral remoto. Segundo o relatório, por trás das promessas, se escondem diversos problemas. Os exemplos são característicos da indústria e da tecnologia da época: segundo o relatório, vão desde os incômodos mais simples com uma cobrança indevida ou uma assinatura duplicada de uma revista, ocasionadas pela má manutenção, operação ou design de sistemas automatizados de informações, passando pelo "incômodo ocasional e potencial injustiça" de ser erroneamente sinalizado como infrator, em razão do uso excessivo e de resultados incorretos de cruzamento de informações entre bancos de dados imprecisos, até chegar na criação de sistemas concentrados que guardam elevado *potencial* coercivo e manipulador se abusados ou de outra forma usados maliciosamente. Diante disso, o relatório tece uma série de recomendações que dariam origem aos *Fair Information Practices* – princípios que se tornaram referência em leis de proteção de dados ao redor do mundo.

[79] Wolfgang Hoffmann-Riem, "Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme", *JuristenZeitung* 21 (2008): 1009.

gerou tamanha insegurança que a controvérsia foi levada para a Corte Constitucional da Alemanha.

O Tribunal invocou e reconheceu – não de forma original, mas com linguagem semelhante à de Westin[80] – um *direito à autodeterminação informacional*, extraído das cláusulas constitucionais que protegem a dignidade e o direito geral de personalidade, para declarar a parcial inconstitucionalidade da lei em pauta.[81] Segundo o Tribunal, o processamento automatizado de informações possui uma dimensão ameaçadora decorrente das possibilidades de (i) agregar, armazenar e recuperar informações específicas sobre indivíduos em questão de segundos (sem as dificuldades manuais e de deslocamento que antes existiam); e também de (ii) combinar, mapear e influenciar o comportamento individual e a tomada de decisão de maneira sem precedentes. A fórmula da proteção de uma esfera privada não se apresentava como uma solução viável para tais problemas. Como explica Laura Schertel Mendes: "Afinal, não mais importava se as informações coletadas dos cidadãos eram íntimas, privadas ou públicas; tratava-se, antes, dos riscos para a personalidade que poderiam surgir do processamento eletrônico de dados"[82].

Diante dessas novas circunstâncias, o Tribunal assentou que a decisão de se e em que medida dados pessoais podem ser processados deve ser prioritariamente deixada ao indivíduo titular das informações, já que a possibilidade de se desenvolver segundo sua própria vontade dependeria dessa capacidade de controle. Para o Tribunal, como o poder de tomar decisões, fazer planos e associar-se em grupos pode ser afetado caso o indivíduo não tenha (i) informações sobre quem sabe o que sobre ele, (ii) poder de corrigir informações errôneas sobre si em repositórios, ou mesmo (iii) capacidade de impedir a coleta, o uso ou a divulgação de seus dados, o ordenamento jurídico deve resguardar tais proteções. Do contrário,

> isso não só restringiria as possibilidades de desenvolvimento pessoal do indivíduo, como também seria prejudicial ao bem público uma vez que a autodeterminação é um pré-requisito elementar para o funcionamento de uma sociedade democrática livre predicada na liberdade de ação e participação de seus membros.[83]

---

[80] Alan Westin, *Privacy and Freedom,* 1963, p. 7: "Privacy is the claim of individuals, groups, or institutions to determine for themselves when, how, and to what extent information about them is communicated to others."
[81] Volkszählung (BVerfGE 65, 1 15 de dezembro de 1983).
[82] Laura Schertel Mendes, "Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da Corte Constitucional alemã", in *Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD*, org. Danilo Doneda, Laura Schertel Mendes, e Ricardo Villas Bôas Cueva (São Paulo, 2020), 229.
[83] Tradução livre. No original: "Dies würde nicht nur die individuellen Entfaltungschancen des Einzelnen beeinträchtigen, sondern auch das Gemeinwohl, weil Selbstbestimmung eine elementare Funktionsbedingung

Apenas em situações excepcionais norteadas por interesse público "prevalecente" tratadas em lei de forma proporcional esse direito poderia ser superado – a ferramenta de avaliação seria o *balanceamento*.[84] Seria esse o caso, inclusive, da Lei do Censo de 1983, que acabou por ter apenas declarados inválidos certos dispositivos que previam a transmissão de dados para outros órgãos da administração e a checagem de outros bancos de dados de registros públicos. (A realização do Censo foi, entretanto, cancelada pelo Governo alemão, que não quis aplicar sequer uma versão modificada).[85]

Após e em razão da decisão do Tribunal Constitucional Alemão, o escopo do "direito à autodeterminação informacional" foi fixado de forma abrangente e *achatado* (aos moldes dogmática tradicional de direito constitucional alemão e da moldagem teórica da teoria da proporcionalidade): a definição generosa de autodeterminação informacional foi compreendida como controle sobre se, quando e em que medida pode haver coleta, uso e tratamento de dados pessoais do titular.[86] Um direito de decidir por si próprio sobre o uso de dados pessoais.[87] Nesse contexto, toda atividade ou operação que importa coleta ou uso de dados pessoais – "tratamento" é o termo genérico – passou a ser concebida como *intervenção* em direito fundamental, que precisa ser justificada, sob os ditames do princípio da legalidade, da legitimidade e, principalmente, da proporcionalidade. Hoje em dia, no modelo europeu, essa abordagem dá lugar a um ferramental analítico de verificação da juridicidade de operações de tratamento de dados pessoais, a partir do estabelecimento de bases jurídicas, princípios, direitos e deveres, e estrutura de fiscalização.[88]

---

eines auf Handlungsfähigkeit und Mitwirkungsfähigkeit seiner Bürger begründeten freiheitlichen demokratischen Gemeinwesens ist." Volkszählung em (C.a).

[84] Paul M. Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", *American Journal of Comparative Law* 37 (1989): 692; Spiros Simitis, Gerrit Hornung, e Indra Spiecker gen. Döhmann, orgs., *Datenschutzrecht* (Baden-Baden: Nomos, 2019), 171–72.

[85] Schwartz, "The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination", 700.

[86] Veja-se, por exemplo, a definição do âmbito de proteção desse direito em um dos manuais mais importantes de direito público alemão: Bodo Pieroth e Bernhard Schlink, *Grundrechte, Staatsrecht II*, 28. Auflage (Heidelberg: C.F. Müller, 2012), 93. Também o relato de Hoffmann-Riem, "Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme".

[87] Doneda, *Da Privacidade à Proteção de Dados Pessoais*, 2019, 168; Bioni, *Proteção de dados pessoais: a função e os limites do consentimento*, 101–3.

[88] Sobre as características gerais do modelo: Orla Lynskey, *The Foundations of EU Data Protection Law* (Oxford: Oxford University Press, 2015), 14–41. Para uma retrospectiva histórica mais detalhada, demarcando diferentes "gerações", ver Viktor Mayer-Schönberger, "Generational Development of Data Protection in Europe", in *Technology and Privacy: The New Landscape*, org. Philip E. Agre e Marc Rotenberg (Cambridge,

Privacidade neutra

Essa nova abordagem para lidar com a exaustão de paradigmas antigos diante do avanço tecnológico, revigorada como direito à autodeterminação informacional e definida de forma abrangente, guarda algumas semelhanças metodológicas com certas abordagens teóricas que foram formuladas sobre privacidade ao longo do tempo. De fato, as premissas metodológicas não eram novas, nem necessariamente precisaram da tecnologia para inspirarem a definição de conceitos. É o caso daquelas abordagens que destacam a distinção entre abordagens "descritivas" ou "normativas" desse conceito.[89]

Uma concepção descritiva de privacidade para Ruth Gavison, por exemplo, seria uma concepção "*neutra"* no sentido de que definiria privacidade sem ainda dizer qual é seu valor e quando há violação dessa privacidade.[90] Essa abordagem parte de relato daquela que seria a "situação" ou "condição" de privacidade: para Gavison, trata-se da situação em que não somos conhecidos por outras pessoas, não estamos sob atenção de outras pessoas, nem estamos próximos fisicamente de outras pessoas – é a situação de inacessibilidade. Haveria então "perda" de privacidade sempre que alguma informação sobre nós se torna conhecida, quando passamos a ganhar a atenção de outrem ou se alguém se aproxima fisicamente de nós[91].

A autora defende que essa abordagem serve para compreender apelos de que há "perdas" e "invasões" de privacidade. O conceito neutro identificaria todo tipo de questão sobre privacidade, das "perdas" indesejáveis ("invasões") àquelas desejadas (como as que decorreriam de escolhas do indivíduo). Posteriormente, e então de modo atento às "funções"

MA: The MIT Press, 1997), 219–41. Raphaël Gellert associa dispositivos sobre princípios e bases legítimas da Diretiva Europeia de proteção de dados, respectivamente, com a "eficiência" e a "legitimidade" de determinado processamento de dados pessoais, lidos como parte de um teste de proporcionalidade sobre a "aceitabilidade" da operação. A associação é feita a partir de obra de Herbert Burkert, que vê em legislações de proteção de dados um esforço de "legitimação" para difusão de tecnologia na sociedade e de garantia de "eficiência" do potencial dessa utilização. Ver Raphaël Gellert, "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative", *International Data Privacy Law* 5, nº 1 (1º de fevereiro de 2015): 8, https://doi.org/10.1093/idpl/ipu035; Herbert Burkert, "Privacy-Data Protection: a German/European Perspective" (1999), http://www.coll.mpg.de/sites/www/files/text/burkert.pdf.

[89] Ruth Gavison, "Privacy and the Limits of Law", *Yale Law Journal* 89, nº 3 (1980): 421–71; Adam D. Moore, *Privacy Rights: Moral and Legal Foundations* (University Park, PA: Penn State University Press, 2010), 14; Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, 68–69.

[90] Gavison, "Privacy and the Limits of Law".

[91] Pense em um elevador ou em um parque com diversos bancos vazios, mas em que alguém decide sentar justo ao seu lado.

que teria a privacidade para o indivíduo e para a sociedade (à luz de alguma teoria normativa), seria possível delinear que interesses mereceriam mesmo proteção jurídica e, portanto, quais invasões consistiriam em "violações". Entre essas funções estaria promover liberdade, autonomia, individualidade, relações humanas e a existência de uma sociedade livre, essencial para a democracia: são razões que apoiam por que as pessoas querem e precisam de privacidade.

Para Gavison, embora seja verdade que em contextos como o jurídico utilizemos a noção de privacidade para designar algo que valorizamos, se começassemos com um conceito de privacidade que já o formulasse como um valor, certas questões e aspectos do conceito poderiam ficar ocultas: pensa em elementos como a escolha do indivíduo, o caráter de uma informação e a fonte pela qual foi obtida – se esses aspectos já influenciassem o conceito do que compõe a privacidade, certas perguntas nem sequer seriam colocadas. Para ela, o valor da privacidade pode ser determinado na conclusão da discussão sobre o que privacidade é e quando e por que certas perdas de privacidade são indesejáveis.

O trabalho de Alan Westin também ilustra esse ponto. Em 1967, como adiantei, no livro *Privacy and Freedom,* o autor defendeu que privacidade é a "reivindicação de indivíduos, grupos e instituições de determinar por si mesmos quando, como e em que medida informações sobre eles são comunicadas a outros"[92] (tradução livre). Antecipando em parte a abordagem que Gavison iria elaborar, ele já identificava quatro "estados de privacidade": *solitude* (solidão ou isolamento), referente a estar separado de um grupo e livre de observação de outras pessoas; intimidade, relativo também a estar livre da observação alheia, mas inserto dentro de um pequeno grupo (família, amigos, colegas de trabalho); anonimato, que ocorreria mesmo quando se é observado por outras pessoas, mas se está livre de identificações; e reserva, que ocorre pela criação de uma barreira psicológica que preserva pessoas contra intrusões indesejadas – um distanciamento mental que limita comunicações e compartilhamento de informações entre pessoas, mesmo entre quem convive entre si.

Paralelamente, sustentou que a privacidade exerce diversas "funções" em uma sociedade democrática. Com respeito (i) à autonomia pessoal, a privacidade serve ao desenvolvimento da individualidade e, com ela, de pensamento crítico, diversidade de visões e comportamentos não-conformistas. Serve também (ii) ao alívio emocional, para que as

[92] Westin, *Privacy and Freedom*.

pessoas possam descansar da pressão de exercer certos papeis sociais e até cometer pequenas transgressões a normas sociais. Funciona também para (iii) a limitação da comunicação, de forma que as pessoas não tenham que ser a todo tempo completamente sinceras em relação a outras, com respeito ao que sentem e pensam, e possam manejar com quem compartilham confidências.[93] Nesse contexto, defendeu que

> cada indivíduo deve, dentro de um contexto mais amplo de sua cultura, de seu status, de sua situação pessoal, fazer um ajuste contínuo entre suas necessidades de isolamento e companhia; intimidade e interação social geral; anonimato e participação responsável na sociedade; reserva e abertura. Uma sociedade livre deixa essa escolha ao indivíduo, porque esse é o núcleo do "direito à privacidade individual" – o direito do indivíduo de decidir por si mesmo, com apenas exceções extraordinárias nos interesses da sociedade, quando e em que termos seus atos devem ser revelados ao público geral.[94]

Westin reconhece, portanto, que sua formulação do conceito de privacidade – sensível a reivindicações de controle que está em sintonia com os estados de privacidade que uma pessoa pode escolher para si (no seu balanceamento pessoal na vida) – é abrangente, conflitará com interesses rivais e precisará ser posto na balança social. Para lidar com esses interesses da sociedade que podem colocar exceções às reivindicações de privacidade, ou interesses conflitantes em geral, mais à frente em seu trabalho Westin propõe que seja feito "*balancing*". Diz que não pode ser de qualquer maneira: se só bastasse apontar para um problema social (como interesse da polícia de solucionar crimes), e dizer que vigilância ajudaria, "não haveria balanceamento nenhum, apenas um procedimento de qualificação de uma licença para invadir a privacidade"[95]. Nesse contexto, propõe que haja avaliação de certos critérios, como

> mensurar a seriedade da necessidade de realizar vigilância; decidir se há métodos alternativos que satisfazem a necessidade; decidir que grau de confiabilidade será exigido do instrumento de vigilância; determinar se foi dado consentimento verdadeiro para a vigilância; medir a capacidade de limitação e controle da vigilância se for permitida.[96]

---

[93] Westin. (e-book)

[94] Tradução livre. No original: "each individual must, within the larger context of his culture, his status, and his personal situation, make a continuous adjustment between his needs for solitude and companionship; for intimacy and general social intercourse; for anonymity and responsible participation in society; for reserve and disclosure. A free society leaves this choice to the individual, for this is the core of the "right of individual privacy"—the right of the individual to decide for himself, with only extraordinary exceptions in the interests of society, when and on what terms his acts should be revealed to the general public."Westin, 44-5 (e-book).

[95] Tradução livre. No original: "there is no balancing at all, but only a qualifying procedure for a license to invade privacy". Westin, 248 (e-book).

[96] Tradução livre. No original: "measuring the seriousness of the need to conduct surveillance; deciding whether there are alternative methods to meet the need; deciding what degree of reliability will be required of the

Concepções descritivas, interesses e o que lhes escapa

O método de Gavison e de Westin de lidar com conflitos de interesses lembra o teste de proporcionalidade ao lidar com conflito de princípios e a própria sistemática de legitimação de interferências que veio a ser consolidada na formulação europeia de autodeterminação informacional, em que toda operação que envolva dados pessoais deve ser justificada. De forma específica, a semelhança mora na etapa descritiva abrangente inicial e no apelo a algum teste posterior pelo qual se chegaria ao resultado do conflito concreto – ainda que não adentremos na questão aqui se estão falando exatamente do mesmo tipo de "*balancing*".

Essa abordagem que separa a etapa descritiva de definição de privacidade (e/ou autodeterminação informacional) da etapa de avaliação normativa tem uma clara vantagem de detectar toda e qualquer situação em que um *interesse* de privacidade/autodeterminação informacional pode estar implicado e que deva ser considerado/avaliado. Trata-se de uma ferramenta para rastrear todo o fluxo de informações pessoais e absolutamente qualquer interesse que se possa ter sobre ele. Por isso lembra a estratégia das concepções abrangentes e generosas de direitos que orientam a teoria da proporcionalidade e o ferramental que a torna tão atraente como mecanismo que identifica tudo que deve ser justificado, de que falei na introdução. Quando quiséssemos identificar quando medidas de segurança do Estado ameaçam a privacidade, por exemplo, este conceito neutro serviria para identificar todos os casos em que o Estado deve atender ao ônus de fundamentação sobre suas ações: das mais simples às mais complexas (e invasivas).

Como a própria Gavison reconhece, no entanto, o jogo de linguagem que é característico no direito nas situações em que o conceito de privacidade aparece gira em torno de reivindicações sobre práticas, situações e possibilidades que valorizamos. Por exemplo, quando Elize Matsunaga contratou um detetive particular para seguir os passos do marido, é certo que Marcos havia "perdido" a privacidade nessa concepção neutra e abrangente: Gavison não nos deixaria afastar a privacidade apenas pelo fato de que tudo ocorreu aos olhos

surveillance instrument; determining whether true consent to surveillance has been given; and measuring the capacity for limitation and control of the surveillance if it is allowed." Westin, 247 (e-book).

de qualquer transeunte (publicamente), mas insistiria que a captação do vídeo e a direção de atenção particularmente ao que Marcos fazia afetava sua "inacessibilidade" e constituiria uma "intrusão". Mas ela não pararia por aí: Marcos teria uma reivindicação legítima de que um direito moral seu foi desrespeitado pelo detetive/por Elize? E, além, teria uma reivindição jurídica postulável por isso? Gavison perguntaria se essa perda é indesejável, se há algo de valioso nela que mereça proteção, voltando-se às funções da privacidade que identificou.

Quando discutimos sobre esse cenário, no entanto, discutimos o próprio conceito – e o que ele requer, autoriza e proíbe enquanto direito – não nos limitamos a descrever interesses. As pessoas lançam mão de diversas concepções de privacidade nesses debates. Há quem poderia dizer que Marcos teria o direito de controlar tudo o que afeta sua acessibilidade, inclusive quem capta fotos dele, porque esse é o único jeito de respeitar sua personalidade. Sob outra (e a tradicional) concepção de privacidade, alguém rebateria para dizer que ninguém tem o direito de alegar privacidade sobre as coisas que faz em público, porque simplesmente não se pode impedir que pessoas vejam e se expressem sobre o que lhes é apresentado. Uma terceira pessoa poderia dizer que nem uma nem outra está correta, mas que há certos tipos de controles em circunstâncias específicas que se reportem a atividades especiais podem ser devidas à pessoa, inclusive em público, apesar de nunca genericamente. Mesmo sem ter ainda de nos comprometer com uma dessas concepções, o ponto é que a discussão relevante no debate moral e jurídico é, em partes muito centrais do debate sobre privacidade, de tipo normativo e engajado sobre a própria melhor maneira de expressar o valor da privacidade. É importante, portanto, que nossa concepção de privacidade participe deste debate e o ilumine, não que fuja[97] dele, estipulando definições abrangentes.

[97] Uma outra maneira de apresentar o problema é apontar que essas estratégias pressupõem que haveria um ponto de vista externo a partir do qual é possível descrever um objeto (no caso, o conceito de privacidade) de forma neutra, sem juízos normativos. Ocorre que, quando debatemos se a privacidade deve ser respeitada em certa situação – como no exemplo que dou no parágrafo ou, em outro, como quando discutimos se obter, ler e divulgar mensagens privadas trocadas entre autoridades públicas viola a privacidade–, esse ponto de vista externo não existe. Alguém vai dizer que privacidade é devida a todos, independente do conteúdo ou do emprego dos titulares; outro vai contradizer dizendo que privacidade não envolve informações de interesse público. As discussões em nível normativo são também conceituais. E, se quisermos articular porque temos ou não direitos à privacidade nesses casos, teremos de defender certa concepção do que os torna valiosos – o que envolve atribuir um valor ao conceito e explicá-lo e justifica-lo à luz dele. Em sua obra, em certas ocasiões, Ronald Dworkin chama esses esforços de separar etapas descritivas e normativas de análises de um conceito de *arquimedianismo*: arquimedianos pressupõem esse ponto de vista externo. Como explica, em certos exercícios, a dimensão normativa é inescapável à própria atividade de "descrição" em razão da própria natureza da prática ou do ideal que se "descreve" e que mesmo a discussão normativa é com frequência conceitual. Ver Ronald Dworkin, "Hart's Postscript and the Character of Political Philosophy", *Oxford Journal of Legal Studies* 24, nº

A abordagem de Gavison e também a definição de Westin, no final das contas, tratam a privacidade como um conceito criterial cujo papel é trazer à tona e definir os critérios daquilo que configura privacidade e, consequentemente, do que significa perder algum aspecto dela. O problema é que, nos contextos das reflexões que me preocupam aqui (questões sobre o que a noção de privacidade requer, autoriza ou proíbe em casos concretos em que reivindicamos a necessidade de uma proteção ou a existência de uma violação[98]), há com frequência disputa justamente sobre o *teste* do que significa violar a privacidade. Em ocasiões em que oferecem argumentos morais e jurídicos, quando as pessoas alegam que certa conduta ou prática acarreta perda de sua privacidade, elas estão imputando certa interpretação a esse conceito e com frequência a reclamação é baseada no fato de que elas perderam *algo de valor*. Críticos então discordam desse conceito proposto de privacidade – por não entenderem que afete o valor (da privacidade) e o que a faz importante, por exemplo.

Ainda, uma concepção de privacidade inspirada em seu sentido descritivo "neutro" – retomando: que designa a situação em que não somos conhecidos por outras pessoas, não estamos sob atenção de outras pessoas, nem estamos próximos fisicamente de outras pessoas, tornando qualquer restrição disso uma "perda" e possível "violação" – está sujeita à crítica

1 (1º de março de 2004): 1–37, https://doi.org/10.1093/ojls/24.1.1. Nesse contexto, o problema de concepções "neutras" de privacidade não é só "fugir" do debate, mas cometer um erro filosófico. De todo modo, o termo serve aos meus propósitos aqui de concluir que reduzir a concepção de privacidade a um sentido neutro, descritivo e abrangente é uma tendência que deixa escapar uma dimensão relevante das discussões sobre privacidade. Não encararmos isso é deixar de compreender a razão de ser desses debates.

[98] Falando da prática jurídica, Dworkin chama de "questões doutrinais" as questões sobre o que o direito requer, autoriza ou proíbe – ao que faço referência aqui. Essas são as questões do dia a dia da prática jurídica: como a de se o direito brasileiro autoriza a contratação de detetives particulares para a investigação de parceiros e, particularmente, se essa possibilidade alcançaria que o detetive possa instalar um GPS no carro do investigado, por exemplo. Alguém poderia dizer que não, porque viola um interesse de propriedade no carro e a privacidade cobre nossos bens privados; outro poderia concordar que não, mas porque é incompatível com o tratamento devido às pessoas que elas tenham seus trajetos, encontros e afazeres monitorados para fins escusos alheios; outro poderia dizer que é do jogo que ninguém tem privacidade em público e que o carro trafega em público. Nesse "estágio" da discussão jurídica, para nos reportar ao que tornaria uma proposição de que o uso do GPS é válido/não é válido é inescapavelmente "interpretativo", não criterial: as pessoas imputariam valor à noção de privacidade e ao que a faz valiosa ao construir seus argumentos. Não estou esquecendo que as pessoas fariam referências legislativas, mas apontando que essa dimensão valorativa da discussão também seria inescapável e ela influenciaria inclusive como interpretaríamos dispositivos que protegem a 'vida privada'. O exemplo é inspirado, além do próprio caso de Elize, em uma variável de outro caso real: "PRESTAÇÃO DE SERVIÇOS - Ação de ressarcimento - Contrato para investigação particular - Questões de caráter familiar - Alegado pagamento integral sem a devida contraprestação dos serviços - Contratação de detetive particular resulta lícita, respeitadas as prerrogativas individuais (monitoramento de pessoa em ambiente público) - Entretanto, parte do serviço oferecido e pactuado é ilícito (colocação de rastreador em veículo utilizado por outrem) – (…)." (Tribunal de Justiça de São Paulo, Apelação Cível 1103117-25.2016.8.26.0100, Rel. Des. José Wagner de Oliveira Melatto Peixoto, 15ª Câmara de Direito Privado, j.13.09.2017, DJE 18.09.2017.

de que não é capaz de explicar como as pessoas empregam o termo *direito.* De forma específica, no caso associado à privacidade, quando o reivindicam em um sentido forte: não simplesmente que desejam certa privacidade que foi "perdida", e que um interesse seu está sendo frustrado, mas que esse interesse particular à privacidade em questão é uma prerrogativa moral sua (*are entitled to it*) que deve ser respeitada pela comunidade, mesmo que os interesses desta sejam a longo prazo prejudicados e a maioria das pessoas talvez assim tenha menos controle sobre o ambiente em que convivem nessa comunidade. Isso não significa defender que privacidade é um direito 'absoluto', mas sim reconhecer que, nas circunstâncias em questão, argumenta-se que algo de valor devido à pessoa está sendo desrespeitado. As abordagens vistas, por outro lado, reduzem as noções de privacidade e autodeterminação informacional a uma designação de interesses – esses "direitos" não se referem mais a prerrogativas morais que possuem o sentido forte de que devem ser respeitadas e não podem ser banidos mesmo que a maioria seja colocada em situação pior.

Mais do que isso, se lançássemos essas concepções simples descritivas no jogo normativo, de forma a dizer, por exemplo, que a pessoa tem direito a não ser conhecida, a não receber atenção, não ser aproximado ou, de forma análoga, a controlar todas as hipóteses em que é conhecido, em que recebe atenção, em que se está próximo fisicamente a outra pessoa, também teríamos de ver "conflitos" com outros direitos e princípios para todos os lados. Uma concepção tão abrangente assim seria uma tragédia em si mesma: seria inevitável que a todo tempo afrontasse outros princípios. Ainda implicaria nos contentar com uma noção mais fraca do que significa ter um direito: uma prerrogativa frágil, sempre sujeita a ponderações com outros interesses.

Como antecipei na introdução, entendo que interpretações amplas, inspiradas em sentidos descritivos neutros, possam obscurecer disputas sobre o próprio conceito (sobre a melhor maneira de articular o valor a que se refere). Ademais, instâncias em que um direito moral – no sentido de direito forte, não de um simples interesse – está em jogo poderiam não ser detectadas. A ideia de "direito (geral) à privacidade" é em certa medida problemática tanto por pressupor e criar uma ideia aparente de conflito com outros valores (como segurança), quanto por sugerir um argumento simples demais de por que achamos certas restrições injustas, como se fosse só em razão do impacto em um interesse pessoal qualquer. Assim corre o risco de não mostrar o que realmente está em jogo. Não destacam liberdades

específicas (e especialmente valiosas) que possam estar em questão (e como essas liberdades específicas oneram a maneira como o próprio Estado pode se engajar em esforços de segurança).[99]

Uma ilustração

Concepções abrangentes não dão espaço, por exemplo, para a discussão sobre o valor da obscuridade no contexto dos debates sobre privacidade em público e a força que pode ter. Por exemplo, imaginemos a polícia no lugar do detetive particular, tomando fotos do Marcos com a amante. Podemos então pensar que a tarefa de promoção da segurança da polícia a permite capturar em imagens e vídeo tudo o que é feito publicamente. Marcos tem alguma demanda moral legítima de direito contra essa coleta? Alguma pretensão jurídica? Alguém poderia dizer, a partir de uma definição abrangente, que há interesses de privacidade de Marcos implicados pela coleta de sua imagem com a amante, mas dizer que ela ou não é legítima (porque não é desejável que pessoas possam impedir que outras vejam, tomem nota e registrem o que viram em público) ou que é proporcional ainda assim (por conta de interesses da sociedade no combate ao crime, mais intensos que os interesses de Marcos em não ser fotografado nem gravado). Mas outra pessoa poderia dizer que temos um direito à privacidade fundado na obscuridade quando estamos em público ou um 'direito a ser deixado só', de simplesmente não ser perturbado nem catalogado inclusive em público, e que mesmo a polícia deve respeitá-lo, sobretudo se não tiver boas razões (e inteligíveis como argumentos jurídicos válidos) para colocar alguém sob vigilância. A linguagem que foca em proporcionalidade e ponderação a partir de uma definição abrangente nos distrai do engajamento normativo sobre a existência ou não de um *direito,* de uma liberdade de algum tipo especial que seria comprometida e sobre como a própria polícia poderia estar obrigada a conviver com direitos morais. Mesmo se existe um direito, outro princípio prepondera.

Para que fique claro, não penso que essa estratégia de "inflação" das definições de direitos daria carta branca a atuações pela segurança: como Westin mostra, é possível pensar como o teste de proporcionalidade analisaria a legitimidade do interesse da polícia, se é adequado, necessário e proporcional. Mas ela não capta como os próprios conceitos de

[99] Ver como Dworkin contempla e rejeita uma concepção geral de direito à liberdade: Dworkin, *Taking Rights Seriously*, xiii; 266.

privacidade (e também de segurança, como veremos no capítulo seguinte) são disputados, inclusive de uma maneira apta a preservar o sentido de um direito forte que esses conceitos poderiam expressar – de que dizem respeito a uma prerrogativa moral e devem ser respeitados pelo seu valor, a não ser que razões especiais fundadas em direito forte alheio estejam presentes. E se, afinal, pudéssemos sim falar em um direito à privacidade mesmo sobre certas ações que realizamos em público – não apenas um interesse, mas um direito inclusive em face de interesses de segurança e que atividades policiais devem respeitar e acomodar?

1.3 *Privacidade, contextos e direitos*

Privacidade e interpretação

Uma possível maneira de contornar esses problemas de definições abrangentes, ao mesmo tempo em que não retrocedemos à solução binária público x privado, em que privacidade é só o que está em segredo e for privado, seja lá o que isso for, é recuperar a ideia de Nissenbaum e do Solove de que o contexto é importante, identificar as práticas de privacidade que o compõem e as razões que as suportam. Trata-se de trabalhar com a ideia de que privacidade é um conceito interpretativo – isto é, com relação ao qual as pessoas reconhecem um valor, um propósito, uma intencionalidade, e oferecem concepções, hipóteses interpretativas, de tipo construtivo sobre qual é essa intencionalidade e o que ela requer. Se quisermos descobrir quando há violação da privacidade, precisamos nos voltar às regras intersubjetivas compartilhadas que permitiriam essa avaliação.

Para enxergar quando há violação dessa prerrogativa, importará entender as regras que governam e o valor a que se orientam. Nessa linha, podemos pensar que privacidade é um conceito que usamos para nos referir a uma prática social normativa compartilhada[100] diante da qual as pessoas desenvolveram uma certa atitude: (i) as pessoas reconhecem que práticas de privacidade não só existem, mas que têm valor, servem a um propósito (*point*), têm uma intencionalidade; (ii) as exigências que essas práticas colocam não necessariamente ou exclusivamente constituem o que sempre foram, mas são sensíveis ao propósito (*point*),

[100] Sobre a teoria interpretativa do direito de Dworkin, v. MACEDO JR, Ronaldo Porto. Do xadrez à cortesia: Dworkin e a teoria do direito contemporânea. São Paulo: Saraiva, 2013.

de tal modo que regras sociais de privacidade devem ser entendidas, aplicadas, ampliadas ou qualificadas segundo seu *point.* [101]

Ronald Dworkin chama essa atitude de "interpretativa" porque nossas formulações sobre o que é a prática – no caso, o que seria privacidade, ao que esse conceito se refere no mundo em que vivemos e o que o tornaria importante – e que comportamentos ela exige ou condena poderiam ser explicadas por um exercício em três etapas: (i) na etapa pré-interpretativa, o intérprete identifica os materiais e padrões que incontestavelmente constituem a prática, ou seja, aqueles sobre os quais há alto grau de consenso de que são práticas de privacidade*,* e não alguma outra prática (por exemplo, e não uma prática de cortesia); (ii) na etapa interpretativa, ele se concentra em oferecer uma *justificativa* geral para os elementos identificados na etapa pré-interpretativa, que deve *ajustar-se* às práticas; (iii) na etapa pós-interpretativa, formula considerações sobre a prática, podendo recomendar que um comportamento seja aceito ou criticado, conforme o que seja mais coerente com a justificativa geral encontrada.[102]

Assim, uma interpretação plausível da prática ou objeto interpretado deve passar por um teste de duas dimensões, como adiantei na introdução: deve ajustar-se (*fit*) à prática e mostrar seu *point* ou valor.[103] É isto que permitirá dizer que uma interpretação é superior a outra, se uma proposição sobre privacidade é verdadeira ou falsa: uma será tanto melhor quanto melhor adequar-se às práticas ou ao objeto e melhor justificar o valor a que serve. Esse ajuste (*fit)* não consiste em mera convergência empírica, nem são essas duas dimensões separáveis: a melhor interpretação é aquela que melhor se ajusta ao significado valorativo da prática a que ela se refere.[104] As melhores concepções de privacidade serão aquelas, portanto,

---

[101] Falando sobre direito e cortesia, ver Ronald Dworkin, *Law's Empire* (Harvard University Press, 1986), 46. Um exemplo: pode ser que algum dia falar em privacidade tenha incluído reivindicar controle de um homem sobre o corpo de sua mulher e as atividades de seus escravos. Hoje em dia, pela própria reflexão da prática do que significa e deve significar a 'privacidade do lar', isso seria aberração porque não mostra o valor da 'privacidade', pelo contrário. As críticas feministas, por exemplo, tanto denunciaram como o 'direito a ser deixado só' em tribunais foi interpretado a ponto de significar que homens poderiam bater em esposas (ver Reva B. Siegel, "'The Rule of Love': Wife Beating as Prerogative and Privacy", *The Yale Law Journal* 105, nº 8 (1996): 2117–2207, https://doi.org/10.2307/797286; Catharine A. MacKinnon, *Toward a Feminist Theory of the State* (Harvard University Press, 1989)., quanto abraçaram o conceito, formulando-o de forma a destacar outros sentidos que deveria ter, como a de proteger a autonomia procriativa (ver Anita L. Allen, *Uneasy Access: Privacy for Women in a Free Society* (Rowman & Littlefield, 1988), 55..

[102] Dworkin, *Law's Empire*, 65–66.

[103] Dworkin, *Uma questão de princípio*, 239.

[104] Sobre o *fit* valorativo de Dworkin, alvo de muitas incompreensões sobre sua obra, cf. Macedo Junior, *Do xadrez à cortesia: Dworkin e a teoria do direito contemporânea*, 199–234.

que melhor reconstruírem o significado do valor a que se refere esse conceito.

Jeffrey Reiman propõe uma concepção que explicitamente supõe essas premissas: sustenta que oferece uma melhor *interpretação* para um "direito à privacidade" por oferecer uma melhor interpretação de nossas práticas sociais da privacidade e do seu propósito (*point*). Nessa proposta, sustenta que:

> Privacidade é um ritual social por meio do qual a prerrogativa moral de um indivíduo à sua existência é concedida. Privacidade é uma parte essencial da prática social complexa pela qual o grupo social reconhece – e comunica ao indivíduo – que sua existência lhe pertence. E isso é uma pré-condição da personalidade. Para ser uma pessoa, um indivíduo deve reconhecer não apenas sua capacidade real de moldar seu destino pelas suas escolhas. Ele deve também reconhecer que ele tem um direito moral exclusivo de moldar seu destino. E isso por sua vez pressupõe que ele acredita que a realidade concreta que ele é, e pela qual seu destino é realizado, pertence a ele em um sentido moral. [105]

Nesse sentido, privacidade seria uma prática social voltada à criação do "eu" e ao reconhecimento da existência pessoal. A relação entre personalidade e privacidade se daria de duas formas: de um lado, (i) práticas de privacidade seriam um "ingrediente" para a formação de pessoas como "pessoas" desde a infância e seu reconhecimento como tal; e (ii) práticas de privacidade – e de reverência à privacidade alheia (desde as mais corriqueiras como as de bater na porta antes de entrar no cômodo de alguém, de respeitar o corpo e tomar distância, de pedir permissão para ver um bem seu) – confirmariam e demonstrariam respeito por essa personalidade – pela pessoa com um "eu" próprio. A concepção de privacidade avançada pelo autor, portanto, está fundada na ideia de *personalidade.* Acaba se candidatando para encher de maior sentido a ideia de Warren & Brandeis de "personalidade inviolada", de que é essa a intencionalidade de práticas (e da proteção) de privacidade.

Naturalmente, é inerente à noção de que privacidade é um conceito interpretativo que uma concepção como a de Reiman seja disputada como a que melhor revela seu valor e inclusive como interpretação geral do conceito que valha em qualquer contexto. Dito isso, vale considerar a que outro tipo de abordagem ela leva.

---

[105] Tradução livre. No original: "Privacy is a social ritual by means of which an individual's moral title to his existence is conferred. Privacy is an essential part of the complex social practice by means of which the social group recognizes –and communicates to the individual– that his existence is his own. And this is a precondition of personhood. To be a person, an individual must recognize not just his actual capacity to shape his destiny by his choices. He must also recognize that he has an exclusive moral right to shape his destiny. And this in turn presupposes that he believes that the concrete reality which he is, and through which his destiny is realized, belongs to him in a moral sense." Jeffrey H. Reiman, "Privacy, Intimacy, and Personhood", *Philosophy & Public Affairs* 6, nº 1 (1976): 39.

Nessa formulação, teríamos direito ao respeito de certas práticas de privacidade que são valiosas à proteção da pessoa e ao reconhecimento de sua existência como uma que é "sua". Proteções jurídicas a esse direito moral poderiam ser vistas como garantias que possuem um compromisso com essa capacidade e reforçam a importância de que o exercício de certas práticas de privacidade especialmente valiosas seja respeitado. Assim, a análise de dispositivos jurídicos e de sua aplicação a um caso é e deve ser também interpretativa. Deve analisar os sentidos que certas práticas tenham em certo contexto, para rever o que o respeito à privacidade autoriza, exige ou dispensa. Para verificar se uma ação viola a privacidade, será necessário verificar se a conduta do agente deixa de observar regras e expectativas que podem ser extraídas das práticas sociais e que permitiriam dizer que alguém tinha a prerrogativa de ver a privacidade respeitada naquela situação e que a intencionalidade do agente é uma sobre a qual se pode dizer que está usurpando essa prerrogativa alheia.

Essa abordagem tem o potencial de driblar os problemas vistos. Não admitiria testes binários/criteriais para identificação de violações de privacidade automaticamente. Não é porque uma informação tem uma dimensão no espaço público ou porque foi compartilhada com alguma pessoa que imediatamente qualquer discussão sobre direito à privacidade foi descartada. [106] Tampouco abraçaria definições abrangentes: não é porque um interesse de privacidade foi afetado que imediatamente temos uma intervenção a direito a ser ponderada. Essa abordagem abraçaria fatores contextuais, o valor da privacidade (ou outros) nele e exploraria se há um direito à privacidade dentro do contexto específico a partir de sua justificativa.

Nesse sentido, a informação de que uma jovem mulher passou por um aborto é uma que pode ser compartilhada com médico, e por este com sua equipe médica sem que qualquer um veja violação. O cenário seria bastante distinto caso a mesma informação pretenda ser acessada pela família, pela imprensa, pela polícia. Um professor que pergunta o nome de um

[106] Falando sobre direito à reputação e liberdade de expressão, Clarissa Gross faz observações semelhantes: "Dessa forma, critérios tomados muitas vezes como definidores do próprio escopo do direito à reputação em algumas democracias liberais, por exemplo, o critério que distingue entre discurso relativo a pessoa pública X discurso relativo a pessoa privada, ou o critério que distingue entre proposição verdadeira de fato X proposição falsa de fato, passam a ser considerados não mais como critérios definitivos de determinação dos limites da liberdade de expressão, mas apenas úteis na busca pelas regras intersubjetivas vigentes em contextos discursivos distintos, necessárias para avaliação da intencionalidade de cada ato discursivo em questão." Clarissa Piterman Gross, "Pode dizer ou não? Discurso de ódio, liberdade de expressão e a democracia liberal igualitária" (Tese de Doutorado, São Paulo, Faculdade de Direito da Universidade de São Paulo, 2017), 203.

aluno em sala de aula antes que responda a uma pergunta está longe de ser acusado de violar da privacidade. Já a insistência de um estranho na rua em saber o nome daqueles que nela trafegam o pode ser; e a resposta do inquirido de que não lhe interessa, perfeitamente adequada, em respeito à privacidade. Aproximar-se de alguém e tocá-lo em luta romana não é violação de privacidade, mas fazer o mesmo em outras situações pode ser não só ser visto como violação da privacidade, mas muito mais. Pular o muro e/ou quebrar a porta da casa de alguém para responder a um barulho que sugira que alguém possa ter escorregado e precisando de ajuda também não aciona a mesma linguagem de violação, ao passo que fazer o mesmo por curiosidade pode ser uma das mais graves violações de privacidade.

Embora compartilhe do diagnóstico de Solove e Nissenbaum sobre o caráter interpretativo e contextual do conceito de privacidade, essa abordagem não se filia àquelas que os autores propõem. As considerações de Solove sobre as diversas manifestações de problemas de privacidade o levam a defender uma abordagem "pragmática" que, embora convide a analisar e teorizar sobre os problemas específicos em questão, vai ao fim e ao cabo ligar o valor da privacidade às suas contribuições para a sociedade no balanceamento com interesses rivais.[107] Com Nissenbaum ocorre algo semelhante: ao propor olhar para as normas de um fluxo de informação – sobre o que é adequado revelar em certo contexto e que transmissões de informações autoriza ou não –, sua ideia é a de identificar aquilo que causa desconfortos e reivindicações de privacidade. A sua teoria da integridade contextual vai então propor uma presunção em favor do status quo, suspeitando de tudo que quebra normas informacionais.[108] Quando novas práticas promoverem os valores internos ao contexto e também valores fundamentais sociais, políticos e morais, são admitidas.[109] Com esse último aspecto, quer preservar a capacidade de explicar reivindicações sobre a sociedade em que queremos viver.[110] Ocorre que, nos casos de intervenções na integridade contextual que sejam propostas em nome da segurança, Nissenbaum parece retornar à proposta de balanceamento.[111]

---

[107] Solove, *Understanding Privacy*.
[108] Nissenbaum, "Privacy as Contextual Integrity", 145.
[109] Nissenbaum, 146.
[110] Falando de um software ("Cassie") de monitoramento de leitores em uma biblioteca: "contextual integrity integrity suggests librarians ought to reject the monitoring capabilities of CASSIE, except if it is clear that monitoring can directly abet dire national security needs." Nissenbaum, *Privacy in Context: Technology, Policy, and the Integrity of Social Life*, 183.
[111] Nissenbaum, 215–16.

Nenhuma dessas abordagens, portanto, se propõe a considerar a articulação de *direitos* morais*,* nem a mergulhar em como é essa interação de questões de privacidade com polícia e seus próprios pressupostos contextuais, sem se render diretamente ao que parece já ser um balanceamento. Como já ressalvei na introdução, não estou dizendo que nunca há espaço para *balacing* (nem que estão falando do mesmo *balacing*), mas suspeito que há mais que esses conceitos podem contar sobre nossos valores e a relação entre eles, tornando esse "balanceamento" mais uma reconstrução conceitual do que ponderação de interesses. No empreendimento interpretativo proposto, portanto, prossigo nessa investigação. No que segue, mostro como essa abordagem dribla os problemas vistos (ao mesmo tempo que mostra tudo o que deixam escapar), bem como joga uma nova luz sobre como enfrentar questões de privacidade.

Um direito à privacidade que vale em público – e em face da polícia?

É possível ver mais concretamente como essa abordagem supera os problemas do paradigma "público vs privado", sem reduzir a noção de privacidade a um conceito que apenas identifica interesses, retomando questões de privacidade em público.

O que dizer, por exemplo, da hipótese referida em que uma autoridade policial capta a gravação em vídeo, por exemplo – um policial no lugar do detetive particular de Elize? Provavelmente a primeira providência que tomaríamos é dar maior atenção aos detalhes do contexto: a gravação é feita por uma câmera de vigilância já instalada no local previamente pela própria polícia, para fins de policiamento em geral, do local, de qualquer pessoa? Que tipos de uso está fazendo disso: está rastreando toda e qualquer pessoa a todo tempo, usando como registro visual caso ocorram eventos específicos, e a captura de Marcos com a amante é mais um desses? Ou está usando para procurar pessoas específicas e a polícia sabe quem é Marcos e estava interessada na captura de seu comportamento e de seus encontros de forma específica? Por quê?

Instituições policiais também geram expectativas sociais sobre sua própria conduta e sobre o que orienta e pode orientar suas ações tendo em vista seus papeis sociais em um regime constitucional democrático. Da perspectiva do transeunte, autoridades policiais são só mais um estranho frente ao qual achamos estar obscuros mesmo em locais públicos e, sem praticar crimes, que seríamos irrelevantes a elas. Dito isso, reivindicar andar na rua sem que

nenhuma outra pessoa andando na mesma rua o veja parece extravagante: estranhos se veem. Policiamento ostensivo é também algo típico de atividade policial: impedir que caminhem em ruas seria extraordinário. O monitoramento geral comum feito pela polícia na rua provavelmente não viola, portanto, um direito à privacidade de toda e qualquer pessoa vista. Mas estranhos também não tomam nota, não se importam, não possuem memória perfeita, nem sabem a identidade de outras pessoas – o que molda uma prática e expectativa de privacidade na forma de obscuridade. Ademais, diferente de um estranho comum, a polícia carrega poderes estatais que nenhuma outra pessoa tem – exercer força com suposição a priori de legitimidade, podendo inclusive levar pessoas presas; também por isso, espera-se que a polícia seja capaz de prestar contas sobre o que faz.

Retornamos assim à tarefa de ver o que a obscuridade tem de importante e o que isso significa em termos de limites para a atuação policial, mesmo quando fundada em interesses de segurança. Essa obscuridade pode ter importantes "funções" na linha que Gavison e Westin já sinalizavam – proteção contra escrutínio público, proteção a relações de intimidade (nas quais realmente queremos compartilhar informações), promoção a individualidades, fomento ao exercício de participação política. Para além de funções, podemos ver também em nossas práticas de não andar de crachá na rua nem expor quem somos e para onde vamos a qualquer estranho, nem de sair perguntando o mesmo aos demais na rua uma certa intencionalidade na linha do que Reiman apontava: um reconhecimento de que cada um tem existência própria, é responsável pelo seu destino, e não tem que, para qualquer um a qualquer momento, prestar contas de quem é e por onde esteve. Daí poderíamos extrair um direito a não ser rastreado de forma identificável por mecanismos que possuem capacidades sobre-humanas de estabelecer conexões e gerar arquivos. Nós temos aqui, portanto, um candidato a direito moral (forte) em jogo: um direito que trunfa interesses gerais de segurança, porque prestigiar esse valor nessas circunstâncias é parte necessária daquilo que manifesta respeito à pessoa– e que o Estado deve a cada uma. Para que alguém perca sua obscuridade, razões muito contundentes e concretas deveriam estar presentes.

Nesse sentido, o caso de usos de tecnologias que armazenam imagens desse trânsito de pessoas em rua, montando um repositório que pode ser consultado, e que permitem identificar as pessoas é mais complexo porque constituiria uma ameaça potencial a desgastar um valor relevante da obscuridade e expor pessoas a riscos de que uma violação concreta a

um direito à privacidade ocorra – a de que se tornem objeto do rastreamento.[112] Quando a polícia ganha a capacidade de fazer isso em escala, e o risco de fazer isso sem razões legítimas passa a existir, o receio se coloca porque os fluxos de informação mudam e a pergunta de que direito temos e podemos mobilizar contra isso também. De repente uma entidade passa a ter capacidades de reconstrução de nossas atividades sob uma perspectiva que até então era limitada à própria pessoa (e possivelmente mais perfeita que a memória pessoal): uma máquina do tempo do que fez, por onde esteve, com quem se encontrou na vida. No caso direcionado à identificação, procura e captura de registros de pessoas específicas, em que a polícia já sabe quem é e o procura e monitora de forma específica, as razões que a polícia teria para esse interesse seriam especialmente relevantes para que se pudessem avaliar como pertinentes à sua atuação no contexto. Há uma razão para o tratamento diferenciado dessa(-s) pessoa(-s)?

Essas observações, por sua vez, levam a nuances que concepções abrangentes de privacidade (e de autodeterminação informacional) não consideram. O valor da privacidade contido na noção de obscuridade, e sua possível articulação como *direito*, não como mero interesse, poderia passar despercebido pelo teste de proporcionalidade, que inclui uma legitimidade (que para assuntos de segurança é quase sempre pressuposta), adequação, necessidade e proporcionalidade. Não estou sugerindo que pelo teste de proporcionalidade o aplicador não chegaria à conclusão de que é desproporcional: penso que, provavelmente, poderiam considerar a vigilância desnecessária frente a alternativas e/ou, no exercício de ponderação entre os potenciais ganhos para segurança pública frente à "força" da invasão na privacidade e seus efeitos colaterais sobre outras liberdades, poderiam concluir que é despropocional. Mas daí escaparia uma discussão substantiva relevante sobre prerrogativas morais que nós temos que faz parte até do conceito de privacidade e aos valores com que se articula: de que seria incompatível com o respeito devido às pessoas e às premissas de um estado democrátido de direitos que fosse feito algo assim. Pelas razões que apresentei acima, entendo que há um direito forte à privacidade (nesse sentido de obscuridade) contra ser rastreado o tempo todo, mesmo que genericamente queiram defender que se a polícia tivesse esse tipo de arquivo de todas as pessoas haveria algum ganho para a segurança pública. Para além de desproporcional, isso seria errado, indigno, porque o respeito à obscuridade é um

[112] Nessa linha, ver Selbst, "Contextual Expectations of Privacy".

que devemos à pessoa enquanto pessoa moral e o Estado deve conviver com isso para sua própria legitimidade. Voltarei à fundamentação disso adiante.

Polícia na rede de valores – implicações de igualdade e reputação

Essa perspectiva contextual também aponta para outros direitos que são relevantes quando falamos de atuação policial e que inevitavelmente aparecem de forma imbricada com questões de privacidade – no exemplo e ao longo deste trabalho. Um deles é o direito a ser tratado como igual: esperamos que o Estado seja capaz de oferecer uma justificativa contundente para justificar o tratamento diferenciado entre pessoas em circunstâncias semelhantes. Por que o Marcos seria objeto do rastreamento específico e não a Jacqueline? Se não for capaz, por exemplo, de justificar porque uma medida de vigilância afeta uma pessoa ou um grupo de pessoas de forma destacada, esta não pode prevalecer. Além da privacidade, outras exigências normativas moldam o propósito das ações estatais inclusive no contexto policial. Se cria também um risco de afetar negativamente interesses de uma pessoa ou um grupo específico de pessoas, esperamos que o Estado adote medidas que contemplem mecanismos de contenção desses problemas e diminuição desse ônus. Não é nem deve ser só um interesse em igualdade que poderia ser relegado se o interesse rival em segurança "pesar mais".

Um outro exemplo é como o trabalho policial pode afetar um direito à reputação. Como visto no início do capítulo, existem certos problemas de divulgação de aspectos de nossa vida que acionam um interesse de reputação. Ser considerado suspeito, ser acusado, ser condenado afeta a percepção social sobre tema de relevância publica – envolvimento em crimes – e a própria maneira como nos vemos e somos vistos. Causa prejuízos materiais e morais que extrapolam a linguagem da privacidade. Em outras palavras, ser apontado como suspeito pode ser estigmatizante: atribui-se à pessoa uma característica indesejável, de ter quebrado uma norma básica da comunidade, de uma maneira que afeta como as pessoas a percebem e como ela percebe a si própria.[113] Esperamos que a polícia também observe determinadas regras intersubjetivas de tratamento que respeitem a pessoa como pessoa moral, como só dar o tratamento de suspeito quando há alguma razão apropriada a tanto. Se

[113] Katerina Hadjimatheou, "The Relative Moral Risks of Untargeted and Targeted Surveillance", *Ethical Theory and Moral Practice* 17, nº 2 (2014): 189; Elizabeth E. Joh, "The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing", *Harvard Law & Policy Review* 10 (2016): 31–32.

entendermos o direito à reputação como competição justa sobre a percepção social sobre si[114], por exemplo, o poder do Estado de submeter as pessoas a tratamentos criminalizantes exige esse correspondente cuidado. Isso inclui evitar que atividades policais que desafiem práticas sociais de privacidade não sejam deliberadamente amorfas a esse estigma. A polícia não pode fazer uma batida surpresa na casa de alguém surpreendendo o alvo e sua família e acordando a vizinhança de um prédio às 6h da manhã sem ter alguma boa razão para isso e com cuidado para não espetacularizar a diligência.

A concepção interpretativa de privacidade é mais rica porque se insere em uma teia de conexões de valores que se reforçam mutuamente. Se a polícia vai passar a monitorar os as atividades de alguém de forma particular, podemos dizer que ela precisa de boas razões que justifiquem a suspeita de que esse alguém está engajado em uma conduta criminosa. Isso seria necessário para se reconciliar com o respeito devido à privacidade (por exemplo, enquanto obscuridade). Mas não só: precisa disso também para se compatibilizar com uma exigência de respeito ao tratamento de igualdade entre as pessoas (que justifique a diferenciação no tratamento de alguém pela polícia, frente a outras pessoas) e até à reputação (porque seu tratamento de suspeito, sobretudo se for acompanhado de grandes operações e publicidade e até mesmo gerar um processo criminal que gere 'fichas' de antecedentes) pode acionar esses direitos.

Meu foco nesse trabalho é privacidade, e por isso vou falar mais dessa perspectiva. O ponto no momento é que reconhecer e abraçar a concepção interpretativa é também encontrar reforço em vários outros valores e compreender como interagem entre si em certos contextos – percepção que poderia escapar em outras abordagens. Isso tem o potencial de tornar a justificação do uso da força pelo Estado mais robusta, quando existente, reforçando a legitimidade do Estado. Ao mesmo tempo, dá melhor dimensão aos problemas que a ausência de uma tal justificação ou que a ausência de fundamentação por um esquema geral de valores imbricados, e limitada a resultados de ponderação caso a caso, pode representar.[115]

Proteção de dados pessoais

[114] Elaborando essa concepção de direito à reputação ver Gross, "Pode dizer ou não? Discurso de ódio, liberdade de expressão e a democracia liberal igualitária".
[115] Criticando a utilização disseminada da proporcionalidade como forma de justificação da coerção do Estado, ver Ribeiro, "Para além da subsunção e do sopesamento", 235.

Ao apontar problema das definições abrangentes de privacidade e tratar da versão mais reproduzida de "autodeterminação informacional", não quero sugerir que toda a prática jurídica que hoje constitui o "direito à proteção de dados pessoais" não tenha firme fundamento moral. O que a abordagem proposta até aqui sugere, na verdade, é a possibilidade de conceber de uma outra maneira o desenvolvimento da prática jurídica de proteção de dados pessoais que a concepção abrangente impulsionou e de inseri-la na rede de valores de que falei.

Criar riscos de dano é também um tipo de dano.[116] Como apresentarei adiante, a razão de ser do direito é também proteger contra riscos de danos: riscos de que, na relação política que temos com o Estado e a comunidade política como um todo, nossa dignidade seja atacada pelo poder coercitivo do Estado injustificadamente.[117] Diante desse risco, em nossas práticas em democracias liberais estabelecemos várias instituições que controlam como o Estado pode agir, como pode tratar as pessoas, e instituimos uma prática jurídica que permita avaliar quando há legitimidade nessa atuação e identificar e punir abusos. A submissão a um poder coercitivo que não é correspondida com esse tipo de cuidado seria um constrangimento das pessoas enquanto pessoas.

Essa preocupação é, naturalmente, muito mais abrangente do que lidar apenas com interesses de privacidade: trata de interesses de justiça, fundamentalmente, e é reforçado por outros valores que prezamos em uma comunidade política democrática. Entendo que a prática da proteção de dados pessoais constitui um despertar para os riscos específicos que relações informacionais assimétricas de poder colocam e constitui um esforço de levar nossos princípios de justiça a essa esfera. Nesse sentido, leis gerais de proteção de dados pessoais podem ser vistas sob essa luz: como políticas de contenção de riscos inerentes a relações informacionais e que atraem a elaboração de uma política regulatória de contenção desses problemas.[118] Na sociedade da informação, apresentam-se velhas disparidades: de assimetria

---

[116] Dworkin, *Justice for Hedgehogs*, 306.
[117] Dworkin, 319.
[118] Há uma crescente produção acadêmica no sentido de que a direito da proteção de dados pessoais seria, ao fim e ao cabo, um tipo de regime de regulação de riscos – uma interferência em processo econômico e social que pode produzir consequências adversas para indivíduos e sociedade. Ver Raphaël Gellert e Serge Gutwirth, "The legal construction of privacy and data protection", *Computer Law & Security Review* 29, nº 5 (1º de outubro de 2013): 522–30, https://doi.org/10.1016/j.clsr.2013.07.005; Gellert, "Data Protection"; Raphael Gellert, "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection", *European Data Protection Law Review (EDPL)* 2 (2016): 481. Nessa linha, o ramo é cada vez mais analisado à luz da teoria

de poder, de informações, de recursos entre titulares e controladores de dados – desde empresas ao Estado. Pessoas devem poder entrar nessas relações informacionais com confiança de que haverá um padrão mínimo de respeito, de honestidade, de segurança contra riscos razoavelmente previsíveis, para que se reequilibre a situação de vulnerabilidade.[119] Daí a política regulatória.

Sob essa perspectiva, esse exercício de contenção de riscos naturalmente não afasta e não poderia afastar a análise de uma potencial violação a um direito moral no contexto de uso de dados – e não só o que associamos à privacidade normalmente, mas a outras liberdades e exigências de dignidade. É possível trabalhar com a proteção a interesses na proteção de dados pessoais de forma geral sem termos de nos contentar com uma concepção de direito à autodeterminação informacional e outra de privacidade que se reduzam a uma formulação fraca de direito, abrangentemente definida e que funciona com considerações de proporcionalidade.

Assim, o direito da proteção de dados pessoais e sua técnica regulatória não deveriam tomar lugar de toda discussão sobre privacidade. Ele ainda deve conviver com o reconhecimento de que certa privacidade em público e certo respeito à igualdade de tratamento, por exemplo, são um limite duro a medidas propostas em nome do interesse público em geral, sem cair e se deixar apenas ponderar. Preserva-se assim a noção de direito. O teste de proporcionalidade e a ponderação, aliás, ainda que levasse a essa mesma

---

dos riscos, ganhando influência de estudos tradicionais da área de direito ambiental. Cf. Gellert, "Data Protection"; Dennis Hirsch e Jonathan King, "Big Data Sustainability: An Environmental Management Systems Analogy", *Washington and Lee Law Review Online* 72, nº 3 (31 de março de 2016): 406; Rafael Zanatta, "Proteção de dados pessoais como regulação do risco: uma nova moldura teórica?" (30 de janeiro de 2018), https://doi.org/10.13140/RG.2.2.16815.43684. Esse processo ajuda a explicar a inclusão do "princípio da precaução" e de "análises de avaliação de risco à privacidade" em legislações modernas de privacidade, como explica Luiz Costa, "Privacy and the Precautionary Principle", *Computer Law & Security Review* 28, nº 1 (1º de fevereiro de 2012): 14–24, https://doi.org/10.1016/j.clsr.2011.11.004. De forma geral, a abordagem da "risquificação" caminha de mãos dadas com a ideia de que o direito de proteção de dados serve de proteção contra riscos, que vão desde a coleta inesperada de dados, ao uso secundário de informações, até o vazamento de dados e os incômodos – falsidade ideológica e fraude daí decorrentes. No campo penal, tais riscos podem se concretizar em exposição a inquirições e prisões indevidas, a preconceito, a condenações injustas, a tratamento definido pelo grupo social a que se pertence, não pela vida que se conduz. Apesar dessa sintonia com o que o próprio campo vem discutindo, e como não me debruço mais que nesse trecho nessa literatura, ressalvo que meu sentido de risco aqui é de risco de causar/sofrer uma injustiça, no sentido moral. Não estou falando simplesmente de mapeamento de riscos para propósitos eficientistas – de levar fluxos de dados pessoais a um patamar mínimo aceitável de desvios, garantindo eficiência geral à sociedade.

[119] Nessa linha, tratando de direito do consumidor, ver Ronaldo Porto Macedo Junior, *Contratos Relacionais e Defesa do Consumidor*, 2º ed (São Paulo: Editora Revista dos Tribunais, 2007), 206–39. Sobre "desníveis de poder" em relações informacionais, ver Rodotà, *A vida na sociedade da vigilância – a privacidade hoje*, 37;101.

conclusão, não reafirmaria da mesma maneira princípios e valores morais com que estamos comprometidos em nossas práticas.

O direito da proteção de dados pessoais também não deveria ser tão associado ao modelo europeu a ponto de ofuscar o sentido que um direito à autodeterminação informacional como direito moral e jurídico forte poderia ter.[120] Para começar, esse entendimento não dá sentido a trabalhos acadêmicos em que se aponta deficiências no modelo e se defende a necessidade de que a autodeterminação informacional seja capaz de conter danos relevantes que estão deixando de ser endereçados: que contemple um direito a inferências razoáveis em processos de *big data*, por exemplo,[121] e que proteja contra oportunismo ou *self-dealing*[122] – exploração de vieses que nós humanos temos contra nós mesmos e manipulação. Também não dá sentido a críticas de que um *direito* (moral) à autodeterminação informacional na era tecnológica deve ser mais do que "*an exercise in managerial box-checking*"[123] – uma referência ao fenômeno de *compliance* gerado pelo modelo regulatório firmado numa concepção abrangente em que se faz um exercício voltado a legitimar[124] operações de tratamento de dados por vinculação de cada uma delas a bases jurídicas e observância de princípios e direitos pura e simplesmente. Está posta discussão regulatória que almeja alcançar uma concepção mais robusta de "justiça no tratamento de

[120] Não estou dizendo que o modelo regulatório europeu (da GDPR, que inspirou a LGPD) sobre tratamento de dados pessoais é um problema em si, nem que haja melhores alternativas – uma avaliação real disso extrapola o escopo desse trabalho. O ponto que estou tentando construir é que a noção de direito à autodeterminação informacional, na formulação abrangente que recebeu, não aparenta poder ser compreendida como nem reivindica ser um *trunfo*; é confessadamente uma formulação de direito *fraco,* que deu lugar a uma prática jurídica voltada a *legitimar* intervenções (as operações de tratamento de dados) e que ainda hoje patina para explicar quando há danos morais. Considero os debates sobre o regime de responsabilidade civil que a LGPD brasileira teria imposto um sintoma desse problema maior: para além da tutela *administrativa* da autoridade nacional contra agentes de tratamento que desrespeitem as normas da lei, há divergência sobre quando pessoas podem pleitear por indenização por violação a regras da lei (individualmente ou mesmo quando entidades representativas de direitos coletivos o podem), sem que danos sejam demonstrados. Ver um retrospecto desse debate, por exemplo, em Bruno Bioni e Daniel Dias, "Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor", *civilistica.com* 9, nº 3 (22 de dezembro de 2020): 1–23; Bárbara Pombo, "Consumidores buscam danos morais por vazamento de dados", *Valor Econômico* (blog), 18 de julho de 2021, https://valor.globo.com/legislacao/noticia/2021/07/18/consumidores-buscam-danos-morais-por-vazamento-de-dados.ghtml.

[121] Sandra Wachter e Brent Mittelstadt, "A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI", *Columbia Business Law Review* 2019 (2019): 494–620.

[122] Neil M. Richards e Woodrow Hartzog, "A Duty of Loyalty for Privacy Law", SSRN Scholarly Paper (Rochester, NY: Social Science Research Network, 3 de julho de 2020), https://doi.org/10.2139/ssrn.3642217.

[123] Julie E. Cohen, "How (Not) to Write a Privacy Law" (Knight First Amendment Institute, 23 de março de 2021), https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.

[124] Rodotà, *A vida na sociedade da vigilância – a privacidade hoje*, 50.

dados", sem que para isso seja necessário que um direito à autodeterminação informacional tenha um sentido *fraco*. Nesse sentido, e em linha com o que proponho de abordagem aqui, a problematização de definições abrangentes quer resgatar uma dimensão de valor que lhes escapa e que penso relevante para este trabalho.

Estados de privacidade, transformações sociais e o papel do direito

Por fim, vale explorar se resta um papel a uma noção como a de "estados de privacidade" sob a abordagem proposta em lugar de levar a uma concepção abrangente e neutra de privacidade desconectada de contextos. Lisa M. Austin sugere que as considerações de Alan Westin devem ser lidas no sentido de que "quando nós fazemos uma reivindicação de privacidade, o que reivindicamos é que cabe a nós escolher o equilíbrio entre privacidade e revelação. Mas o que escolhemos quando escolhemos privacidade é um estado de privacidade."[125] A ideia é que ter um direito à privacidade não significaria, portanto, ter de escolher exercê-la a todo tempo: as práticas sociais que suportam a proteção respaldariam a possibilidade e a capacidade disso, sob a observação de que faz parte do que significa respeitar a pessoa como pessoa moral. Nesse sentido, nos retrairmos à nossa casa, limitarmos a comunicação de nossos pensamentos a certas pessoas, e nos abstermos de contatos físicos com outras pessoas seriam exercícios de privacidade, que nossas práticas sociais em geral apoiam. Manter o anonimato em público (na rua ou na internet), também.

Alan Westin então vai dizer: é difícil escolher solidão quando não há espaços para o indivíduo exercer isso, por exemplo. "Se é importante que seja o indivíduo quem escolha entre um estado de privacidade ou de revelação social, então é importante que seja possível escolher um estado de privacidade. Mas a disponibilidade de um estado de privacidade requer a presença de múltiplos fatores ambientais e sociais para apoiá-lo"[126]. Com respeito à "disponibilidade" de estados de privacidade em geral, Austin destaca como da obra de Westin se extrai a observação de que normas sociais influenciam essas opções:

[125] Tradução livre. No original: "When we make a claim of privacy, what we claim is that it is up to us to choose the balance between privacy and disclosure. But what we choose when we choose privacy is a state of privacy". Lisa M. Austin, "Re-Reading Westin", *Theoretical Inquiries in Law* 20, nº 1 (1º de janeiro de 2019): 59, https://doi.org/10.1515/til-2019-0003.

[126] Tradução livre. No original: "If it is important that it is the individual who decides between a state of privacy or social disclosure, then it is important that it is possible to choose a state of privacy. But the availability of a state of privacy requires the presence of multiple environmental and social factors to support it." Austin, 63.

> A escolha do indivíduo é portanto afetada por normas relativas ao que é apropriado dentro daquele contexto. Entretanto, o indivíduo ainda tem uma escolha relativa a seguir ou não essas normas ou escolher mais ou menos privacidade do que essas normas sociais ditam. A facilidade de qualquer escolha individual particular depende em parte do nível em que os desejos do indivíduo relativos ao equilíbrio entre privacidade e revelação se conformam a normas sociais.[127]

A adoção e a normalização de mecanismos de vigilância do indivíduo colocam desafios porque "não só adiciona[m] pressão a um indivíduo que está tentando decidir sobre o equilíbrio certo entre privacidade e revelação, mas também fundamentalmente molda a disponibilidade de estados de privacidade em uma sociedade"[128].

Na linha do que foi visto, não seria possível dizer que a pessoa tem *direito* a todo estado de privacidade que queira ter; teríamos de retornar às nossas práticas para verificar, se nos contextos específicos em que essa reivindicação é feita, é uma noção que tem fundamento, de que aquela era uma privacidade valiosa. De todo modo, o ponto no momento a que as considerações de Westin chamam atenção é que transformações sociais causam processos de revisão do que nos referimos em nossa vida comum quando falamos em privacidade e podem levar à ampliação ou redução das experiências que ele chamou de "estados de privacidade". Por conta do avanço tecnológico, há quem diga, por exemplo, que "privacidade morreu" pela maneia como as pessoas agora se comportam na internet, exibindo aspectos de sua vida, usando dispositivos eletrônicos que coletam inúmeros dados de seus hábitos e do seu corpo, adotando jogos de realidade aumentada e acolhendo outros mecanismos de conveniência por troca de dados, como reconhecimento facial e coleta de biometria para proteção de sua casa e de seus bens.

Westin temia que esses constantes processos de mudança dificultassem reivindicações de privacidade. Para o que falei aqui, a dificuldade parece ser a mesma: se parece que há erosão ocorrendo, será mais difícil assentar que o valor de proteger certa expectativa de privacidade está firmado em nossas próprias práticas. Afinal, pelo que falei,

---

[127] Tradução livre. No original: "The individual's choice therefore is affected by norms regarding what is appropriate within that context. However, the individual still has a choice regarding whether to follow those norms or choose more or less privacy than those social norms dictate. The ease of any particular individual choice depends in part on the degree to which an individual's desires regarding the balance between privacy and disclosure conform to social norms." Austin, 64.

[128] Tradução livre. No original: "[Although Westin does not give a clear account of this, his descriptions of the different social balances in different societies show that surveillance] does not just add pressure to an individual who is trying to decide on the right individual balance between privacy and disclosure, but also fundamentally shapes the availability of states of privacy in a society" Austin, 65.

as práticas que associamos com o conceito de "privacidade" são substrato constante do teste para nossas interpretações sobre quando há em questão um direito à privacidade – uma liberdade valiosa ao nosso status como seres dotados de valor intrínseco e responsabilidade de definir nossos destinos. No entanto, pelas mesmas razões, percebe-se que o diagnóstico de que "privacidade morreu" é um exagero e que a privacidade se refere a fenômeno muito mais complexo: as pessoas vivenciam privacidade de outras maneiras – selecionam públicos que receberão suas fotos em redes sociais, deixam de postar/comentar aquilo que não pretendem que não vejam, possuem certas expectativas sobre como vão usar dados de seu app fitness e de desbloqueio de seu celular. Práticas e expectativas de privacidade ainda estão lá e o que esses comportamentos revistos nos fazem perceber é que tentativas de simplificar o valor dessas práticas para agora anunciarem que "morreram" são precipitadas.

Nesse contexto, as observações de Westin nos fazem perceber que proteções jurídicas podem ser mobilizadas para resguardar certas experiências de privacidade quando justamente nos parece que certas mudanças – novas variáveis tecnológicas – estão prejudicando práticas de privacidade que valorizamos. A busca pela consolidação jurídica de práticas de privacidade é parte da resistência a essa erosão a que Alan Westin já apontava e da qual a própria articulação de um direito por Warren e Brandeis lá atrás é manifestação. Como Nissenbaum observou para a obscuridade em público, algumas transformações nos levam a perceber e a formular valores que antes não precisavam dessa formulação, mas que podemos rever e perceber que tinham ou ganharam valor pela alteração das circunstâncias.

Há novos horizontes para essa percepção: hoje é um "estado de privacidade" o fato de que podemos controlar nossos pensamentos e quem os conhece. Se a tecnologia ganhar a capacidade de ler pensamentos,[129] poderemos ser obrigados a rever nossas práticas e sem muitas dificuldades poderemos concluir que é valioso a nós como pessoas com vida própria que seja reconhecido um direito à privacidade sobre quem conhece nossos pensamentos em

[129] Escrevendo isso em 2022, é certo que o exemplo é radical a ponto de supor uma máquina que permitisse visualizar todo o pensamento de alguém em tempo real, ou historicamente – e que pudesse a ser usada por policiais para *acessar* informações de pessoas, mesmo sem se darem conta. Dito isso, as discussões privacidade e "leitura de mentes" ou com o "interior" – uma preocupação com a psique – é de longa data e perpassa o desenvolvimento testes de personalidade feitos por psicólogos, a emergência de consultas sobre antecedentes e condições familiares feitas por potenciais empregadores e por escolas, a criação de detectores de mentira, e até a arquitetura de bairros como subúrbios que, ao mesmo tempo em que concediam certa privacidade espacial, também ampliavam a capacidade de membros de uma comunidade saberem sobre rotinas de outras pessoas. Ver Sarah E. Igo, *The Known Citizen* (Cambridge, MA: Harvard University Press, 2018), 99–143. Esses episódios e suas discussões fogem do meu contexto (policial) aqui – por isso não aprofundo essa dimensão.

inúmeros contextos e que o uso que seria feito dessa ferramenta deve ser obstacularizado em tudo que ameace nossa autonomia nos contextos relevantes. Se os riscos de desnaturarem nossa percepção do que é ser pessoa e de abuso forem tamanhos, a tecnologia não deveria ser desenvolvida.

Proteções jurídicas hoje bem estabelecidas – e das quais falarei mais na segunda parte desse trabalho – podem ser vistas como respostas a processos desse tipo. A "inviolabilidade da casa" pode ser vista (e aqui me limito a fazer aproximações), por exemplo, como a proteção de uma prática de privacidade. Reconhecimento de que a casa é um símbolo e em geral um catalisador de exercícios valiosos de privacidade, que regras sociais nos permitem dizer que pessoas valorizam e que já estiveram em xeque se qualquer terceiro – inclusive autoridades policiais – pudesse entrar e vasculhar quando lhe desse na telha. Há diversas "funções" que poderia exercer – exercício de isolamento, de intimidade, por exemplo –, mas sua intencionalidade é proteger a pessoa e, como falarei adiante, sua autonomia e por isso as violações a esse direito estarão relacionadas a ela. A existência e o reconhecimento desse tipo de proteção jurídica refletem um compromisso com a proteção e a reparação contra condutas que ameacem práticas de privacidade valiosas que relacionamos à casa; a correção de uma proposição concreta de que a inviolabilidade do domicílio e a privacidade está sendo violada depende do contexto e do valor que a orienta nele.

O mesmo se pode dizer da "inviolabilidade do sigilo das comunicações privadas": a viabilização de um canal para a pessoa compartilhar informações e pensamentos com pessoas específicas conforme o contexto de suas relações sociais mesmo que estejam à distância. Isto é, sem que a distância e o fato da intermediação de uma empresa tenham que significar abrir mão de uma prática de privacidade que valorizamos – conseguir expressar pensamentos e discursos a alguém sem que outras pessoas sempre participem ou fiquem sabendo. Reconhecimento de que isso serve ao exercício de intimidade, de reserva, que prestigia uma "privacidade intelectual"[130] com relação aos nossos pensamentos e sua observância fundamentalmente tem como propósito respeitar o indivíduo como pessoa. A proteção de um direito à privacidade no contexto de uso de ferramentas de comunicação privada à distância não significa que as pessoas não tenham direito à privacidade em outros contextos que ainda impliquem comunicações privadas, muito menos que não impliquem outros conteúdos

[130] Richards, *Intellectual Privacy*.

expressivos e informações pessoais. Isso depende do contexto; a proteção jurídica consagra um compromisso de que esse tipo de prática de comunicação à distância não seja de extremo risco à exercícios valiosos da privacidade; não implique erosão de uma prática valiosa.

O dever de sigilo profissional poderia ser visto, por sua vez, como uma proteção reforçada àquele que revela informações para pessoas específicas: diálogos ocorrem e documentos são transmitidos para finalidades específicas, equilibradas com um dever de cuidado de quem as recebe de usá-las para a estrita finalidade da relação. Por essa razão já se supõem expectativas de privacidade que vinculam o que poderá ser feito, como poderá ser usada e com quem (não) poderá ser compartilhada, mas cuja confiança poderia ser traída e gerar danos especialmente graves à pessoa e à sua autodeterminação sobre as relações em que gostaria de compartilhar tais aspectos de sua vida, caso pressupostos de confidencialidade não sejam observados. Daí também proteções jurídicas que criam deveres de confidencialidade mesmo na ausência de uma relação de confiança prévia e bem construída entre os envolvidos nessas relações profissionais.[131]

O que a "inviolabilidade do corpo" significaria? Proteção contra ações que, nos contextos específicos em questão, possa se dizer que atacam a prerrogativa de autonomia que a pessoa deve ter sobre o que é feito sobre seu próprio corpo e com sua própria vida. O escopo e o significado disso dependem, de novo, naturalmente, dos contextos específicos: o mesmo toque no corpo que pode ser admitido em um relacionamento romântico, em um jogo esportivo ou entre parceiros de dança pode constituir crime se feito por um passageiro desconhecido no metrô ou por um deputado em plena sessão de uma Assembleia Legislativa. Diante das muitas práticas nas quais damos centralidade a um controle básico sobre o que é feito com o próprio corpo, não é surpresa que haja uma resposta jurídica de reconhecimento de que há algo relevante a se proteger e a se reparar, em caso de violação.

Atualmente, como disse, se discute como o direito deve resguardar a obscuridade em público. O fato de que hoje há a percepção de que está "ameaçada" pelo avanço tecnológico não é fator para não o reconhecer, mas a razão para as amplas discussões sobre como o direito deve responder a essas transformações, acolher essas reivindicações morais que são coerentes com nossas práticas e o que esperamos que o direito faça nessas situações de ameaça à dignidade, e preservar o que valorizamos. Esse é só um exemplo: há muitas frentes de

[131] Solove e Richards, "Privacy's Other Path", 172.

discussão mobilizadas em torno da articulação de direitos morais à privacidade que também mereceriam reconhecimento no direito – há muito disso no campo "digital" e subjacente às discussões sobre estratégias regulatórias para lidar com o uso e fluxo massivo de dados.

***

Feitas essas ressalvas e observações sobre como pensar proposições que reivindiquem direitos à privacidade, cumpre passar a um outro problema que acomete o enfrentamento da delimitação do conceito de privacidade e do escopo desse direito – e à concepção que vou propor de referência para o trabalho. No que segue, vou retomar as justificativas apresentadas por diferentes teóricos para defender e amparar essas proteções jurídicas tradicionais – e como se transformam (ou não) em limites inclusive perante autoridades estatais policiais. Nesse exercício, tenho a oportunidade de expandir o argumento aqui apresentado sobre o propósito de proteções de privacidades e sua fundamentação em diferentes contextos, inclusive contra riscos de danos. Ao final, vai me levar a uma última observação sobre os contornos do conceito de privacidade que deve orientar esse trabalho e a interpretação devida quando estivermos falando de atuação do Estado para segurança.

2 Razões para proteger privacidades

2.1 *Privacidades que acobertam crimes? Um desafio remanescente*

Em contraste com a preocupação com o trabalho da imprensa, um dos autores do artigo seminal sobre o direito à privacidade, que se tornaria ministro (*justice*) na Suprema Corte dos Estados Unidos, Louis D. Brandeis curiosamente sempre pensou que havia uma segunda parte do artigo a escrever: um artigo que articularia o "duty of publicity" em contraste com o "right to privacy" por causa do problema de "proteger malfeitores e acobertá-los"[132]. Rememora que "se diz que a luz do sol é o melhor dos desinfetantes; a luz elétrica, o mais eficiente policial"[133]. Essa observação deixa dúvidas sobre como o direito à privacidade que articularam Warren & Brandeis poderia ser usado para justificar reivindicações, demandas e normas que façam frente ao trabalho policial. Como vimos, os trabalhos de Alan

[132] Tradução livre. No original: "shielding wrongdoers and passing them off". Richards, *Intellectual Privacy*, 31.
[133] Tradução livre. No original: "Sunlight is said to be the best of disinfectants; electric light the most efficient policeman". Richards, 32.

Westin e Helen Nissenbaum também deixam transparecer certa fragilidade de reivindicações da privacidade frente a um trabalho que se volte a buscar segurança pública – seja pela prevenção ou pela repressão ao crime: são interesses ponderáveis.

Há algo de intuitivo nessa aversão. Práticas de privacidade que servem para proteger ilícitos não são valiosas: Gavison está certa quando diz que um criminoso não tem um direito a que seja respeitada sua expectativa de manter em segredo seus planos de um mega assalto a uma cidade. Concordo com isso: não temos direito moral de esconder preparativos para o cometimento de crime, muito menos o de que ninguém descubra que cometemos crimes. Há *interesse* de ocultar essas atividades, sem haver direito. Proteger privacidade nessa situação não é o que a torna valiosa: do mesmo modo que não protegemos a liberdade de matar, a privacidade para cometer ilícitos e praticar crimes não é um exercício de privacidade importante. Nossas práticas não apoiariam esse direito à privacidade; pelo contrário.

Soma-se a isso o fato de que autoridades estatais policiais em geral possuem razões muito fortes e legítimas para agir nessas circunstâncias. Isso porque, ao combater crime, em geral não agem com finalidades éticas – no sentido de limitar certos estilos de vidas porque seriam piores segundo sua propria visão do que é uma vida boa. Embora ainda hoje exista criminalização de certas condutas que levam a essa discussão (porte de drogas leves para uso pessoal, aborto, por exemplo, como um dia deixou de ser crime o adultério), em geral nessa área o Estado atua para promover a segurança (*safety*) – um motivo moral (tratamento que devemos a outras pessoas), não ético (sobre como devemos viver nossas próprias vidas).[134] Como uma reivindicação de privacidade poderia fazer frente a isso? O Estado não pode nos forçar a a viver segundo decisões políticas coletivas de princípio moral?[135]

Frente a tudo isso, como é que justificamos limites de "privacidade" ao trabalho policial? Quando não aparece sob uma acusação de conveniência com que ilícitos fiquem acobertados, o desafio vem sob bordão contra os compromissos éticos de quem suscita argumentos de privacidade: "quem não deve não teme". Para rebater essas insinuações e reafirmar a importância da privacidade mesmo frente aos interesses de promover segurança, autores retrucam com uma observação descritiva e prática de que "todo mundo tem algo a

[134] Dworkin, *Justice for Hedgehogs*, 374.
[135] Ronald Dworkin, *Is democracy possible here?* (Princeton and Oxford: Princeton University Press, 2006), 20.

esconder", por vezes combinada de uma defesa mais elaborada de que "privacidade não é sobre ter algo a esconder".[136] Sobre o que é, então?

No que segue, e a partir da obra de diversos autores proeminentes que já se dedicaram a estudar privacidade, vou apresentar como (1) razões elencadas para proteger a privacidade reforçam que não é de proteger ilícitos que se trata, ao mesmo tempo em que (2) algumas delas parecem fracas para articular e justificar limites contra o trabalho policial. Vou propor então como uma teoria baseada na teoria da dignidade de Dworkin poderia oferecer essa base ao longo deste trabalho: ajudaria a dar sentido à intencionalidade de nossas práticas de privacidade em contextos paradigmáticos – e relevantes para a atuação policial, ao mesmo tempo em que também alcançaria explicar o que o respeito a esse valor significa em termos de limites para a atuação do Estado em nome da segurança. Essa abordagem aproveita os insights metodológicos vistos: não cair na armadilha de testes binários e não pressupor um conceito abrangente. Isso nos retiraria a chance de pensar como a polícia também é obrigada a respeitar direitos morais e como também deve observar expectativas contextuais de comportamento e de privacidade. Precisamos olhar para o contexto social em que o trabalho policial se insere, quais práticas sociais afeta e o que isso ocasiona em termos de deveres institucionais e de tratamento contra abusos, erros e excessos.

Como falei, o trabalho foca em medidas de *acesso* – obtenção ativa de informações por parte polícia sobre as pessoas – e por isso vale olhar instâncias paradigmáticas disso: acesso a casas, comunicações, bens, o corpo (tocar nele e/ou extrair informações dele). Esse universo de atividades é desafiador frente a nossas práticas sociais: a *soberania* para decidir quem pode ingressar em nossos lares, quem pode conhecer, ouvir e ler nossos pensamentos e expressões, mexer em nossa propriedade, saber quem somos e tocar no nosso corpo, se para alguns não parece tão fundamental quanto deliberar sobre autonomia procriativa ou política, é uma prerrogativa que prezamos em diversos contextos e que está por trás de muitas regras sociais e jurídicas que giram em torno da ideia de um direito à privacidade, ainda que não seja absoluta e válida em qualquer cenário.

Como mostro a seguir, em meio às inúmeras concepções de privacidade já propostas, há linhas comuns quanto a valores e razões com que são associadas, que dão pistas sobre o que valorizamos ao dar protagonismo ao indivíduo para definir quem *acessará* suas casas,

[136] Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy".

bens, corpo, comunicações privadas e que podem ser revistas para chegarmos a justificativas mais completas sobre por que tentamos e devemos tentar preservá-los contra ataques e ameaças de terceiros, inclusive do próprio Estado quando movido a propósitos de segurança. A retomada dessas razões é útil para avançar uma concepção que seja atraente para expressar o que de valioso há na noção de privacidade que invocamos em face de atividades de vigilância do Estado para investigações e segurança pública – e que deve ser preservada mesmo diante de avanços tecnológicos.

2.2 *Privacidade e escrutínio público*

Em *What is the right to privacy?* (2015)[137], Andrei Marmor defende que a habilidade de controlar como apresentamos aspectos de nós mesmos a outras pessoas é necessária, se queremos nos proteger de um contínuo escrutínio social. Assim, resguarda-se um espaço para tentar e falhar, para lidar com certas questões isoladamente ou simplesmente para se engajar em algo sem convidar crítica. O ponto não é novo: é destacado por diversos teóricos que frisam o "valor social da privacidade" como espaço de desenvolvimento humano – necessário ao crescimento, à criatividade, à saúde mental. Já vimos em Ruth Gavison, em Alan Westin e em Warren & Brandeis.

É o caso também de Edward Bloustein que já em 1964 sustentava que quem fosse obrigado a viver a todo instante entre outras pessoas ou a ter todos os seus pensamentos, desejos e alegrias sujeitos ao escrutínio público "se fundiria com a massa"[138]. Havendo e exigindo-se a completa publicidade de opiniões, aspirações e sentimentos, elas tenderiam a se tornar igual às de todos os homens, que perderiam sua individualidade. Nesse sentido, defendia que "uma invasão na nossa privacidade ameaça nossa liberdade como indivíduos de fazer o que quisermos, assim como agressões, lesões ou detenção de nossa pessoa ameaçam"[139]. Sua postulação é abrangente: haveria uma ameaça geral à individualidade, à liberdade de se fazer o que se quer fazer e ser quem se quer ser, se não existisse respeito à

[137] Andrei Marmor, "What Is the Right to Privacy?", *Philosophy and Public Affairs* 43, nº 1 (Winter de 2015): 3–26.
[138] Edward J. Bloustein, "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser", *New York University Law Review* 39 (1964): 1003.
[139] Bloustein, 1002. Tradução livre. No original: "An intrusion on our privacy threatens our liberty as individuals to do as we will, just as an assault, a battery or imprisonment of our person does."

"privacidade" contra pressões sociais.

Nessa linha de razões, intervenções alheias em lares, em bens, no corpo de alguém, violam a privacidade quando e porque consistem em forçar à exposição aspectos da vida de alguém que são de relevância pessoal, levando a um escrutínio público que é nocivo ao livre desenvolvimento da personalidade, uma liberdade que valorizamos e queremos fomentar. Falar em um direito à privacidade contra essas intervenções não-autorizadas de terceiros significaria preservar a capacidade de as pessoas viverem sem medo de praticarem e expressarem – em suas casas, em suas comunicações privadas, com seu corpo – o que lhes interessa porque outras pessoas poderiam ver e analisar quando bem quiserem. Isto é, protegeria a capacidade de pessoas viverem sem receio de que terão que se explicar sobre tudo o que fazem e de terem suas reputações julgadas por isso.

O foco no medo da crítica pública atribui um papel defensivo a reivindicações por privacidade, enquanto alguns veem nela um papel muito mais forte do que deter efeitos inibidores sobre o comportamento pessoal.[140] Como Thomas Nagel observa em *Concealment and Exposure* (1998)[141], há vezes em que nós não queremos nos expor completamente a estranhos mesmo quando não há medo de desaprovação ou hostilidade. Para ele, certo controle sobre o que expomos teria a ver com a capacidade de gerenciar aqueles aspectos da nossa personalidade que "convidam atenção e uma resposta coletiva e o que permanece individual e pode ser ignorado" e por isso seria um dos "atributos mais importantes da nossa humanidade". [142] Sua resposta ainda aponta a um papel de gerenciamento de nossas relações sociais e do que permitimos que outros conheçam, mas adiciona a ideia de que não é apenas se importar com o que o outro vá achar e com o impacto da observação alheia no comportamento que nos faz buscar e reivindicar privacidade.

A preservação contra o escrutínio público, como já sinalizavam as considerações sobre o trabalho da imprensa vistas na primeira seção deste capítulo, não parece ser a intencionalidade que melhor justifica práticas de privacidade e reivindicações sobre elas formuladas no contexto de intrusões ao lar, a comunicações privadas, ao corpo, ao ir e vir, por terceiros, que não possuam repercussões de *divulgação*. De certo modo, esse foco faz

[140] Nesse sentido, também Julie E. Cohen, "What privacy is for", *Harvard Law Review* 126 (2013): 1904–33.
[141] Thomas Nagel, "Concealment and Exposure", *Philosophy and Public Affairs* 27, nº 1 (janeiro de 1998): 3–30.
[142] Nagel, 8.

parecer, por exemplo, que se a intrusão ocorrer sem o conhecimento da pessoa afetada e sem divulgação a outros, inexistiriam problemas: as pessoas podem invadir a casa das outras, ouvir suas comunicações, tocar seu corpo, desde que não contem a mais ninguém ou o façam de modo despercebido, para que não existam efeitos inibidores. Há algo de perturbardor nessa possibilidade contra a qual seria estranho supor que nossos valores não protegem e que essa razão de preservação contra escrutínio público (e desenvolvimento de individualidades humanas sem inibições) não captura para o conjunto de questões sobre *acessos* decorrentes de medidas de vigilância que ora me ocupam. No contexto policial a que esse trabalho se destina, essa justificativa poderia ser destrutiva de qualquer postulação de privacidade: desde que a vigilância seja encoberta, não haveria implicação nem limite posto por direitos à privacidade.

Assim, concepções de privacidade que focam na detenção do escrutínio público parecem apontar a um propósito que, se não é irrelevante, conta apenas parte das razões por que certas privacidades são valiosas nos contextos de medidas de vigilância que envolvem *acesso* – em que a polícia obtém informações pessoais de alguém. Esse propósito dificilmente faz oposição ou impõe qualquer limite ao trabalho policial a não ser possivelmente uma obrigação de preservar sigilo sobre o que ficarem sabendo da vida da pessoa que não é diretamente relevante à investigação e à imputação do crime contra divulgações a um público mais amplo, bem como um cuidado para evitar criminalizações indevidas, tendo em vista a maneira como suas consequências afetam como a pessoa percebe a si e os outros a percebem, impactando a condução de sua vida.

2.3 *Privacidade e relações sociais: intimidade, confiança, responsabilidades e honestidade*

Andrei Marmor destaca outras razões que seriam distintivas da privacidade e que poderiam ser candidatas a fundar uma melhor concepção de privacidade. Na linha de Charles Fried[143], ele observa que amigos e amantes abrem mão de certas informações pessoais uns para os outros, o que é característico de sua intimidade. Nesse sentido, sem ter controle sobre o que revelamos a outros e sobre os modos como fazemos, diferentes tipos de relações com pessoas seriam muito mais difíceis de serem criadas e mantidas. O que contamos para um

[143] Charles Fried, "Privacy", *Yale Law Journal* 77, nº 3 (1968): 475–93.

amigo, para um amante, para um colega de trabalho é completamente diferente em cada relação – a quantidade e a natureza das informações que nós revelamos a outras pessoas definem o caráter de nossas relações com elas. Desse ponto de vista, privacidade é importante porque permite que relações valiosas de amizade, amor, companheirismo sejam realizadas.[144] O raciocínio se estenderia a relações de confiança, em que o compartilhamento de informações está também diretamente atrelado às expectativas sobre tratamento que lhes serão dadas segundo as premissas da própria relação e seus propósitos.

Marmor também sugere que ser capaz de controlar a distância que mantemos de certas pessoas, a partir das informações que compartilhamos, nos daria controle sobre as responsabilidades que assumimos em nossa vida. Em especial, a medida da responsabilidade que assumimos sobre cuidar ou ajudar o outro e as expectativas de responsabilidade que geramos em outras pessoas. Isso porque a intimidade gera expectativas de cuidado e consideração, decorrentes da própria proximidade. Exemplo disso é como tais expectativas operam entre familiares e amigos, por exemplo, e como sentimos um dever de ajudar quão mais próximos somos confrontados sobre certa situação pela qual estão passando (exemplo: doença na família), ao mesmo tempo em que também sentimos um dever de levar em conta o impacto de nossas decisões pessoais sobre eles e de participa-los sobre elas (exemplo: mudar de emprego). De fato, a intimidade é um valor que as pessoas podem querer realizar em suas vidas, nas suas relações sociais – mas não com qualquer pessoa, também por conta das responsabilidades daí decorrentes. O mesmo vale para a honestidade, por exemplo: este é um valor que prezamos em diversas relações, mas não desejamos ter uma relação de completa honestidade e transparência com toda e qualquer pessoa porque aquilo que comunicamos envolve e acarreta expectativas, reações e responsabilidades.

Essas considerações apontam para os valores que podemos entender ameaçados em situações em que alguém intervém em nossos lares, em nossas comunicações privadas, em nosso corpo sem autorização. Victor Tadros, por exemplo, entende que se um terceiro observa e/ou interfere em uma relação de intimidade, a realização desse valor é comprometida.[145] Tendo em vista que pessoas reivindicam um tipo de privacidade relacionado à intimidade, e nossos lares oferecem uma arquitetura que permite que pessoas

[144] Marmor, "What Is the Right to Privacy?", 8–9.
[145] Victor Tadros, "Power and the value of privacy", in *Privacy and the Criminal Law*, org. Erik Claes, Serge Gutwirth, e Antony Duff (Antwerp/Oxford: Intersentia, 2006), 105–20.

o realizem, parece que essas considerações realmente nos aproximam mais do que está em jogo quando um terceiro interefere no lar sem ser convidado/forçadamente. O mesmo raciocínio se estenderia para nossas comunicações privadas: nossas práticas sugerem que compartilhamos nossas expressões e pensamentos com pessoas específicas segundo a relação que temos e queremos ter com elas; se isso não é respeitado, também não conseguimos realizar e constituir relações de amizade, de confiança. Também o nosso corpo: em certas ocasiões, deixar que o outro nos toque é característico da relação de amor, de intimidade, de carinho que temos ou queremos ter com esse outro. Isso não é algo que queremos com qualquer um e por isso forçar um toque sem que essa relação exista seria invasivo e a razão pela qual reivindicamos privacidade também sobre como dispor do corpo.

Uma dificuldade com esse tipo de justificativa é que ela faz parecer que práticas de privacidade existem em função de relações sociais. O respeito à privacidade deve existir para que as pessoas se engajem de forma verdadeira em relação de intimidade com outra pessoa, por exemplo. Isso implicaria que nós só temos um direito a andar pelados em nossa casa sem bisbilhotice alheia, ou que só temos o direito a não ser tocado por quem não demos essa liberdade, porque senão isso não seria possível genuinamente nas instâncias em que queremos nos engajar numa relação de intimidade que envolva estar pelado ou ser tocado.[146] Faz também parecer que quem não quer se engajar nessas relações em sua própria vida ou não as pode realizar não teria reivindicações legítimas de privacidade. Essa concepção, portanto, também não parecer oferecer uma justificativa completa para proteções a privacidades nos contextos de interesse aqui, ou a só apoiar situações bastante específicas.

Outra objeção que se poderia fazer à relevância dessas considerações neste trabalho é que quando o Estado – e autoridades policiais – se engaja em atividades que envolvem ingresso no lar, ouvir comunicações privadas alheias, tocar o corpo, e de outro modo *acessar* informações pessoais, o propósito dessas condutas não é diretamente interferir nessas relações sociais: não é observar por curiosidade algo a que não foi chamado nem forçar um relacionamento íntimo para satisfação pessoal ou alguma outra obsessão, por exemplo.

De fato, em certas instâncias, nossas práticas jurídicas chegam a reconhecer um direito de ser dispensado de revelar a privacidade alheia que conhecemos para tutelar valores inerentes a relações sociais – e muito disso acontece perante autoridades policiais: quando

[146] Reiman, "Privacy, Intimacy, and Personhood", 36.

reduz a participação de familiares em processos criminais, no máximo, à figura de informantes (não obrigados a depor), não de testemunhas; quando dispensa padres e médicos de prestar depoimentos se não quiserem; e quando se discute se o advogado (ou mesmo padres e médicos) tem direito de deixar de depor ou se esse é um dever, não importa sua vontade. Direitos morais de privacidade que devemos uns aos outros cirandam todos esses arranjos e debates jurídicos e a relevância de relações sociais é aparente neles.

Ocorre que, embora essas associações da noção de privacidade com valores como a intimidade, e nosso gerenciamento de responsabilidades morais pareça mesmo relevante de algum modo para explicar o que valorizamos e refletidos de algum modo na prática jurídica, a atividade policial de *acesso* que propus analisar não diretamente se presta a atacar esses valores. Muito embora possa colateralmente causar disrupções a eles e por isso seja importante que não causem ônus excessivo a essas relações sociais e que tenham boas razões para agir diante dessa possibilidade, medidas de vigilância policial não obrigam diretamente as pessoas envolvidas a agirem contra valores que dão a relações sociais.

Temos uma concepção que seria capaz de articular o valor da privacidade tanto de forma mais atraente e completa a como nos reportamos a esse valor quanto de modo que mantenha relevância frente a propósitos de segurança do Estado?

2.4 *Privacidade, identidade e autonomia*

Charles Fried defende em "Privacy" (1968) que o controle sobre a exposição de aspectos de nossa vida a outras pessoas passa pela liberdade de nos definir a nós mesmos: "pensamentos, antes de serem expressados, são meras possibilidades de ação não-ratificadas. Somente expressando-os é que nós os adotamos, os escolhemos como parte de nós e os atraímos para nossas relações com os outros"[147]. Mireille Hildebrandt, sem dar tanta ênfase na noção de 'controle', entende que privacidade se reporta a uma liberdade de não sofrer restrições irrazoáveis na construção da própria identidade. Nós estamos continuamente nos reconstruindo à luz de novos eventos que moldam como vemos nós mesmos, o mundo e os

[147] Tradução livre. No original: "*thoughts, prior to being given expression, are mere unratified possibilities for action. Only by expressing them do we adopt them, choose them as part of ourselves, and draw them into our relations with others".* Fried, "Privacy", 485.

outros; privacidade daria condições e espaços imanentes a esse processo.[148]

Nesse sentido, a ideia de privacidade é apresentada como um "*breathing room*" necessário à própria construção da identidade. O termo é usado por Julie Cohen que, em *What Privacy Is For* (2013), convida a reconhecer "processos de auto-diferenciação" pelos quais passamos desde a infância, enquanto pessoas que nascem situadas em certas redes de relacionamentos, crenças e práticas e que vão com o tempo tendo novos encontros e experimentos com outras. Privacidade "permite sujeitos situados a navegarem por matrizes culturais e sociais pré-existentes, criando espaços para o jogo e o trabalho da auto-produção"[149]. A ideia, portanto, é que práticas de privacidade ajudam a moldar como nos apresentamos e gerenciamos os traços e os limites de nossa identidade segundo o estilo de vida que escolhemos levar e frente às diferentes situações sociais em que estamos inseridos ao longo do tempo. Não é só um instrumento para isso, mas uma necessidade a essa capacidade.

Essas considerações apontam para uma relação muito próxima entre proteção de práticas de privacidade e proteção da autenticidade, um termo que tomo emprestado dos trabalhos de Ronald Dworkin. O autor sugere, fazendo o mesmo exercício interpretativo que usei acima, que podemos extrair de nossas práticas mais fundamentais de respeito à vida humana um compromisso com a independência ética e com a responsabilidade pessoal – "princípios da dignidade", ao lado do autorrespeito (do reconhecimento de que importar-se com a própria vida e com como é conduzida é algo relevante).[150] Independência ética não significa não poder ser influenciado pela cultura em que estamos inseridos, mas não ser dominado nem usurpado de opções éticas – sobre como viver a própria vida – por ser quem somos. Significa, ainda, tomar decisões sobre como viver não por medo nem preguiça, mas por convicção. Assim se permite que as pessoas assumam responsabilidade sobre a vida que estão vivendo.

Não é preciso ser excêntrico nem inovador, mas é crucial que busquemos a nossa própria resposta ao desafio da vida na situação em que estamos e aos valores que

[148] Mireille Hildebrandt, "Privacy and Identity", in *Privacy and the criminal law*, org. Erik Claes, Antony Duff, e Serge Gutwirth (Oxford: Intersentia, 2006), 43–57.
[149] Cohen, "What privacy is for", 1911.
[150] Dworkin, *Is democracy possible here?*, 9; Dworkin, *Justice for Hedgehogs*, 196–212.

consideramos apropriados.[151] Para nossa responsabilidade sobre nossas vidas ser efetiva, precisamos de uma imunidade moral – que incluiria um "poder de controle": "algum poder para selecionar quais atos serão praticados no exercício da tarefa pretendida"[152]. Se o que fazemos em nossas vidas está sob controle alheio, não temos como ter responsabilidade. Nessa mesma linha, esse princípio da dignidade autoriza que pessoas sejam responsabilizadas pelos seus atos e escolhas sempre que essa atribuição causal de responsabilidade for apropriada – o que dependerá de outras considerações morais e políticas para se determinar.[153]

É possível buscar a fundamentação de direitos concretos de privacidade em certos contextos na proteção do direito mais abstrato de definir o destino e a "pintura" de nossas vidas – muitas vezes chamado de direito à "autonomia".[154] Esse direito incluiria a habilidade de não estar sob controle de outras pessoas, de ter certa imunidade básica sobre o que é feito ao nosso corpo e aos nossos bens,[155] e o que mais fizer parte dos nossos recursos por direito,[156] e de exigir respeito a certas práticas de privacidade. Isso, conquanto regras de comportamento intersubjetivamente compartilhadas permitam sustentar que devemos ter tais prerrogativas como parte das nossas práticas que preservam e prestigiam a autenticidade e que o desrespeito a elas causa um tipo de *dano moral* – um dano decorrente de injustiça no tratamento.

Essa perspectiva é também capaz de colocar sob uma nova luz o papel dos valores vistos na subseção anterior. Certos valores éticos que muitos gostariam de exibir como forma de responder ao seu próprio desafio da vida – uma vida com amigos, cheia de amor, mantida com relações de confiança – supõem autonomia quanto ao nosso engajamento nessas

---

[151] Dworkin, *Justice for Hedgehogs*, 209–10.
[152] Tradução livre. No original: "some power to select which acts are performed in the exercise of the purported assignment". Dworkin, 288.
[153] Dworkin, 209–10.
[154] Nesse sentido, ver também Mark Bennett e Petra Butler, "A Dworkinian Right to Privacy in New Zealand", in *Dignity in the Legal and Political Philosophy of Ronald Dworkin*, org. Salman Khurshid, Lokendra Malik, e Veronica Rodriguez-Blanco (Oxford: Oxford University Press, 2018), 442–43.
[155] Dworkin, *Justice for Hedgehogs*, 288.
[156] "if we accept the two principles of human dignity, we must work out the implications of each in the light of the other. If I accept both that everyone's life is of equal intrinsic value and that everyone has the same personal responsibility for his life as I do, then these assumptions must shape my definition of my own responsibility. I must define that responsibility so that it is compatible with a like responsibility among other people because their lives are of equal importance to mine. So I cannot regard proper distributional constraints, which allocate resources among these different lives, as compromising my personal responsibility for my own life. I must regard them as helping to define what my personal responsibility is." Dworkin, *Is democracy possible here?*, 70.

relações. Na medida em que envolvem práticas de privacidade, reportam-se ao próprio exercício e respeito mútuo da autenticidade nessas relações. Resguardar a disposição sobre a identidade que apresentamos e que expressamos nessas relações é também aspecto condicionante da gestão de responsabilidades que assumimos na vida. Assim, o "cardápio" de escolhas éticas pressupõe a existência de arranjos e práticas de privacidade que viabilizam as próprias escolhas e dão sentido e significado a elas.

Intervenções na casa, em bens, no corpo que desrespeitem a dignidade (independência ética e responsabilidade pessoal) nesses sentidos violam direito. Para essa conclusão, a intencionalidade do agente deve ser uma que ataca o modo como a pessoa escolheu viver sua vida e suas escolhas de gestão de privacidade (de só compartilhar espaços, bens e seu corpo com quem quiser ou com certas pessoas em certos contextos). A violação existe em contextos em que era devido respeito a esse poder de controle àquela pessoa enquanto pessoa única com responsabilidade sobre aquele aspecto de sua própria vida. Concluir que houve violação é um esforço interpretativo – e não estou sugerindo que seja sempre tarefa fácil.

Há, certamente, outras frentes que podem resultar em reconhecimento a outros direitos específicos de privacidade (e de violações) também derivados da proteção devida à autenticidade, mas não mais sobre o que o indivíduo reserva apenas à sua responsabilidade – a autenticidade em sua dimensão de engajamento em discurso público e mobilização sobre a organização da comunidade política: como a proteção de manifestações políticas anônimas[157] e a proteção sobre membros e atividades de associações políticas, por exemplo.[158] Essas são liberdades de cunho fundamental para a participação democrática e para nossas noções de auto-governo – tendo a privacidade um papel fundamental para seu exercício e promoção.[159]

---

[157] Ver Artur Pericles Lima Monteiro, "Online anonymity in Brazil: identification and the dignity in wearing a mask" (Dissertação de Mestrado, São Paulo, Faculdade de Direito da Universidade de São Paulo, 2017).

[158] Como referência para essas discussões, ver o capítulo 2 de Westin, *Privacy and Freedom*, 25–56., em que discute as "funções da privacidade organizacional", sob a premissa de que "grupos" possuem um papel central em sociedades democráticas, promovendo a experiência de auto-governo. Privacidade fomenta autonomia, protege contra hostilidades sociais que poderiam desencorajar mobilização e provê sentimento de aceitação e coesão do grupo. Também Annabelle Lever, "Privacy rights and democracy: a contradiction in terms?", *Contemporary Political Theory* 5 (2006): 142–62.

[159] Nesse sentido, ver Hildebrandt, "Privacy and Identity".: "In a constitutional democracy, the government should be sensitive to unreasonable constraints on identity-building. This is a matter of the *public good* because democracy needs citizens who will form publics to make an issue of what affects their lives, every time representative politics fails to take their interest serious." Também Julie Cohen: "To put the point a different way, the liberal self and the liberal democratic society are symbiotic ideals. Their inevitably partial, imperfect

Direitos à privacidade podem ser importantes para o exercício de outras liberdades de importância fundamental para a democracia, como a liberdade de expressão e a liberdade de associação.[160]

O que essa justificativa para proteção da privacidade baseada na autenticidade seria capaz de dizer sobre intervenções praticadas pela polícia? A princípio, a mesma dificuldade vista para a justificativa anterior retorna: quando a polícia se engaja em certas práticas que interferem em lares, corpo e bens de alguém, normalmente não há a intencionalidade de usurpar uma soberania sobre como aquela pessoa deve viver sua vida. O objetivo é prevenir e/ou combater crimes. Como se poderia falar então em um direito à autonomia opondo-se a essas atividades?

Neste ponto, as considerações sobre as nossas expectativas e práticas sociais sobre o trabalho policial a que sinalizei precisam retornar: a polícia tem o dever de compatibilizar seu poder com a autonomia/autenticidade de cidadãos mostrando cuidado com ela e instituindo mecanismos que controlem o seu próprio poder e contenha riscos de erros, abusos e excesso que causem disrupção sobre o nosso modo de vida indevidamente mesmo que a finalidade não seja impedir um modo de vida nem usurpar uma escolha que deveríamos ter. A polícia pode em tese não agir com o propósito de suprimir prerrogativa moral a que tenhamos direito, mas deve agir de modo a que seu poder não reverbere nelas indevidamente e sem razão contundente, causando dano sério ao seu exercício. Também não deve acumular recursos que lhe conferem poder injustificadamente. Na próxima seção finalmente expando essa relação entre privacidade e (controle do) poder estatal.

2.5 *Privacidade, poder e democracia*

Kevin Macnish desenvolve um argumento que é útil para ilustrar como o receio do abuso se aproxima e se distancia de concepções de privacidade e, assim, oferece uma boa

realization requires habits of mind, of discourse, and of self- restraint that must be learned. Those are the very same habits that support a mature, critical subjectivity, and they require privacy to form. The institutions of modulated democracy, which systematically eradicate breathing space for dynamic privacy, deny both critical subjectivity and critical citizenship the opportunity to flourish. The liberal democratic society will cease to be a realistic aspiration unless serious attention is given to the conditions that produce (aspiring) liberal selves". Cohen, "What privacy is for", 1918. Ver também Richards, *Intellectual Privacy*, 100.

[160] Para uma associação com liberdade de expressão, ver Richards, *Intellectual Privacy*.

janela de entrada para a apresentação da relação entre privacidade e contenção de poder.[161] Ele toma um objeto fortemente relacionado a noções de privacidade pessoal – um diário – e imagina a situação em que alguém esquece o seu diário em um estabelecimento (uma cafeteria, por exemplo) por certo tempo e depois retorna para busca-lo – apenas para encontra-lo na posse de outra pessoa e em outra mesa. Uma violação à privacidade inequivocamente teria ocorrido caso alguém – digamos, um funcionário da loja ou outro cliente – pegasse o diário e o lesse. Isto é: por essa tese, há violação da privacidade quando ocorre um acesso de terceiro, não autorizado pelo dono do diário, às informações que este contém; a soberania da disposição do dono que expressou aquelas ideias naquele papel de forma privada foi desrespeitada. Caso o funcionário não lesse o diário, por outro lado, dizer que ainda assim houve invasão de privacidade implicaria associá-la simplesmente à perda de *controle* sobre o bem em si, não ao acesso ao que o diário contém.

Macnish utiliza o exemplo para defender uma concepção de privacidade que vincula a noção de "perda" de privacidade a "acessos" a certas informações e espaços, em detrimento de uma que centre na noção de controle. Invasões de privacidade ocorreriam quando há acessos a certos espaços e informações, não simplesmente perda de controle. Na linha do que já expus acima, sua tese sobre invasões aparenta adotar e discutir a rivalidade entre conceitos puramente descritivos de privacidade, mas sem almejar oferecer uma concepção interpretativa das hipóteses em que se argumenta em sentido forte que houve/há violação a um *direito* de privacidade. Sua concepção descritiva é incapaz de distinguir o acesso a um diário permitido pelo dono, daquele não-autorizado por ele: nos dois haveria perda, assim como a concepção plana do controle seria indistinta a como a "perda" de controle existiu: se por mero esquecimento (passivamente), por livre vontade do dono, ou por coleta ativa de um terceiro. Já falei da pobreza dessas noções.

Dito isso, seu argumento sinaliza algo relevante: ainda que não se fale diretamente em violação da privacidade, o fato de que o diário está/esteve na posse de outra pessoa suscita interesses que, ainda assim, não são desprezíveis: a perda de controle sobre o diário enceta uma situação de vulnerabilidade – um risco aumentado de que a privacidade, mesmo que ainda não tenha sido, poderá ser violada pelo novo controlador do diário (de que um dano

[161] Kevin Macnish, "Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World", *Journal of Applied Philosophy* 35, nº 2 (2018): 417–32, https://doi.org/10.1111/japp.12219.

poderá ocorrer); para o dono do diário, o cenário de incerteza pode levar ao caso de ter de se comportar como se sua privacidade tenha sido sim violada. Pode ainda expor o dono a outros tipos de danos: mesmo que o novo controlador não leia o material, poderia utilizar o diário para extorquir o dono por exemplo ou para adotar comportamentos que de qualquer outro modo o beneficiem. Assim:

> Diante dessa situação, é provável que me sinta extremamente vulnerável. NC [Novo Controlador] agora é capaz de acessar minhas informações (ou seja, violar minha privacidade) e, tudo o mais constante, provavelmente usará minhas informações em seu benefício. Seja qual for a intenção real do NC, temo que ele viole minha privacidade, pois ele tem os meios e o incentivo. Se eu não sei se ele realmente acessou minhas informações e não tenho meios de intervir em suas ações, irei, como os cidadãos da RDA [República Democrática Alemã] ou presidiários do Panóptico de Bentham, supor que ela já o fez.
> Se NC não for um indivíduo, mas o estado, então as consequências de minha preocupação de que minhas informações foram acessadas, ou serão acessadas se eu perturbar o estado, são graves. Posso sentir efeitos assustadores que me impedem de me engajar em manifestações contra o governo democraticamente legítimas, mas impopulares (para aqueles que estão no poder, pelo menos); posso tentar me conformar com o resto da sociedade um pouco mais de perto; e posso recusar-me a falar contra as políticas das quais discordo. Isso tem consequências tanto para o indivíduo, cuja autonomia é suprimida e cujo senso de segurança é desafiado, quanto para a sociedade, que, como resultado, terá menos debate livre e experimentará mais frustração reprimida.[162]

O que essa observação sugere é que muitas reivindicações e reclamações – por vezes até veiculadas como argumentos pelo direito à privacidade – estão baseados em uma preocupação com abusos de poder.[163] Fora da dimensão teórica sobre a justificação da privacidade, temos inúmeros motivos para desconfiar de certos agentes que obtém

[162] Tradução livre. No original: "Given this situation, I am likely to feel extremely vulnerable. NC [New Controller] is now both able to access my information (i.e. violate my privacy) and, all other things being equal, is likely to use my information for her benefit. Whatever the actual intention of NC, I fear that she will violate my privacy as she has both the means and the incentive. If I do not know whether she has actually accessed my information and I have no means of intervening in her actions, I will, like the citizens of the GDR [German Democratic Republic] or inmates of Bentham's Panopticon, act under the assumption that she already has.
If NC is not an individual but the state then the consequences of my worrying that my information has been accessed, or will be accessed if I upset the state, are severe. I may feel chilling effects that deter me from engaging in democratically legitimate but unpopular (to those in power, at least) demonstrations against the government; I may seek to conform to the rest of society a little more closely; and I may decline to speak out against policies with which I disagree. These have consequences both for the individual, whose autonomy is suppressed and whose sense of security challenged, and for society, which will as a result enjoy less free debate and experience more pent-up frustration." Macnish, 12.

[163] Cf. Marmor, "What Is the Right to Privacy?", 15. No tema específico em que aqui me debruço, ver Paul de Hert e Serge Gutwirth, "Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power", in *Privacy and the Criminal law*, org. Erik Claes, Antony Duff, e Serge Gutwirth (Antwep/Oxford: Intersentia, 2006), 61–104. (apresentando privacidade e proteção de dados pessoais como, respectivamente, uma ferramenta de opacidade e outra de transparência – ambas como controle do poder).

informações sobre nós – ainda que a princípio de forma genuína ao contexto, sem dano ou de forma fundamentada – e recear daqueles que acumulam prerrogativas e ferramentas capazes de serem mobilizadas para interferir em nossas vidas (fazer grampos, instalar câmeras escondidas, aliciar informantes, entrar em casas), isto é, na nossa autonomia. Daí surge uma reivindicação por proteção decorrente unicamente da exposição a riscos imanentes a essas capacidades e na imposição de regras que balizem medidas que interferem em expectativas, práticas e prerrogativas de privacidade. Uma reivindicação de direito a uma proteção regulatória.

Não se trata de constatação nada muito diferente das que levaram às instituições e princípios que norteiam e consubstanciam o tipo de associação política subjacente a uma comunidade política em que há um Estado que exerce poder coercitivo. Com efeito, preocupação com poder não é uma preocupação exclusiva de questões de privacidade nem de proteção de dados, como já pontuei. Participar de uma sociedade civil é participar de uma relação de risco: tornamos uma parte de nossas vidas vulnerável ao que for decidido coletivamente, abrindo mão de soberania, e admitimos que certas pessoas devem acumular um poder maior para fazer valer essas decisões coletivas, pelo uso da força, se preciso. A única maneira de manter a dignidade nesse tipo de relação é se essa vulnerabilidade for equilibrada com senso maior de cuidado para conosco.[164]

Para o Estado, isso se traduz, como defende Dworkin, em uma obrigação de agir com legitimidade: de tratar cidadãos com igual consideração e respeito – de respeitar os princípios da dignidade.[165] Cidadãos devem ter participação nas decisões coletivas sobre justiça e moralidade[166] e devem ter sua autenticidade respeitada, nos termos que já antecipei. Além de não poder proibir e banir completamente o exercício de um direito incidente à dignidade, qualquer acomodação de interesses alheios mediante *regulação* não pode desqualificar o próprio direito e sua razão de ser, não pode impor um dano sério ou ônus excessivo para seu exercício nem ser incongruente com a concepção mais atraente dos direitos específicos à privacidade que pudermos articular. Dizer se há "ônus excessivo" ou se a regulação mostra respeito ao direito ou causa "dano sério" passará por um esforço interpretativo, que depende das circunstâncias e detalhes concretos da regulação, e que está comprometido com um

[164] Dworkin, *Justice for Hedgehogs*, 306.
[165] Dworkin, 2; 319.
[166] Dworkin, 379.

parâmetro de avaliação que é sua coerência com os valores dessa comunidade jurídica. Esse é um tipo de reconstrução conceitual, não uma ponderação ad hoc.[167] Qualquer regulação deve mostrar respeito a direitos e às repercussões da conduta estatal em caso de injustiça no tratamento. Viver em uma democracia é acomodar essas preocupações e garantias a cidadãos como exigências morais que devemos um ao outro e a nós mesmos.

A associação da proteção de direitos à privacidade com uma noção de democracia comprometida com o tratamento com igual consideração e respeito põe ênfase na ideia de controle do exercício do poder pelo Estado. Tira o foco de medir interesses do indivíduo e põe no Estado o dever de fundamentação sobre suas ações. O Estado deve conter riscos de que o seu poder seja *abusado* de forma geral, incluindo riscos de que use o poder que lhe cedemos, sob uma promessa de respeito e consideração, para interferir em prerrogativas de privacidade indevidamente, de que cause danos sérios ao exercício de práticas de privacidade. Seria o caso, por exemplo, em que a polícia mobiliza suas estruturas de vigilância para fazer perseguição política, por exemplo – uma violação à independência ética. Sua atividade deve ser regulamentada para acomodar essas preocupações, detectar esses abusos, remediar esses riscos e responsabilizar os envolvidos.

À polícia também não deve ser dado poder indiscriminado; isso é incompatível com a dignidade. Por exemplo: a configuração default não é nem pode ser que autoridades policiais podem entrar na casa de qualquer pessoa a qualquer tempo. Pelo contrário, exigimos que razões contundentes devem estar presentes para permitir que o Estado se engaje em uma ação que, em qualquer outra circunstância, pressuporíamos ser valiosa à pessoa e referente à sua "privacidade", como é o caso de definir quem ingressa sobre sua casa, quem participa de

[167] Essas observações se inspiram em dois trabalhos de Dworkin. Em um, discute um direito ao aborto e o valor da autonomia procriativa, admitindo 'regulamentação' para acomodar interesses do feto (no que se refere a limites temporais para realização de procedimentos) que vão crescendo conforme a gravidez avança e para admitir aconselhamentos psicológicos sobre essa tomada de decisão da mulher, por sua relevância (e exercício da responsabilidade pessoal). Ao mesmo tempo, argumenta que submeter a mulher a obter a autorização do pai do feto descaracterizaria o direito e representaria uma coerção travestida ao exercício do direito – tornando esse tipo de exigência em regulamentação um "ônus excessível", pois incompatível com o direito e seu valor, por exemplo. Cf. Dworkin, *Domínio da Vida*, 236–37.Em outro trabalho, Dworkin questiona se temos um direito à pornografia. Nele, defende que proibições do consumo de pornografia violam um direito à independência ética. Por outro lado, regulamentações sobre exibição pública, que implicam interesses alheios, podem não violar esse direito – desde que não causem "danos sérios" ao seu exercício (trata de inconveniência, despesas e embaraço aos consumidores de pornografia e discute quando a distância, o valor adicional e a exposição poderiam ser incompatíveis com o direito). Cf. Dworkin, *Uma questão de princípio*, 528–33. Nos dois casos, vemos o engajamento reconstrutivo de que falo aqui que – ainda que se quisesse chamar de 'balanceamento', não é uma ponderação de intensidade de interesses, muito menos com pesos arbitrários.

suas comunicações privadas, quem revista seu corpo e até quem sabe quem é e de onde vem e para onde vai quando anda na rua, em nossos paradigmas tradicionais.

Por essa razão, estabelecemos procedimentos regulatórios e impomos um ônus de fundamentação para que isso possa ocorrer legitimamente, de maneira que ainda mostre respeito à nossa autenticidade. Esses procedimentos visam mitigar tanto instâncias de *abuso* (motivações distorcidas, arbitrárias e/ou discriminatórias, que divergem daquelas possíveis a atividades policiais no combate à criminalidade), quanto as de *erro* – em que o afastamento da privacidade de alguém não traz quaisquer informações relevantes às apurações de crime nem mostram qualquer envolvimento da pessoa em crime; e de *excesso* – em que instituições e agentes do Estado acessam mais do que lhes cabe e do que há necessidade. Essas não são simplesmente instâncias em que, na verdade, restringir a privacidade em nome da segurança seria "desproporcional" – mas injustiças que o Estado tem o dever de evitar. (Vou me reportar a elas ao longo desse trabalho.)

Quando decisões morais da comunidade sobre a convivência coletiva foram violadas e os envolvidos precisam ser responsabilizados; entender o que houve, quem agiu e como o fez é parte dessa tarefa. Por outro lado, instituições do Estado não poderiam se engajar nessas práticas para satisfazer apenas algum interesse geral em melhorar o trabalho policial na promoção da segurança da comunidade: se a polícia pudesse entrar na casa de quem quisesse quando quisesse, averiguar qualquer um a qualquer momento ou, em um clique, verificar os rastros de todos os lugares que alguém esteve segundo sua própria vontade, isso poderia até ser bom para a segurança coletiva, mas não seria compatível com a dignidade das pessoas. É por isso que colocamos e devemos colocar limites e possuímos e devemos possuir mecanismos de controle.

Nesse contexto, a justificativa de proteção da autonomia que vimos na seção anterior tem potencial de sustentar proteções a direitos a privacidades também em face do próprio Estado quando atua na prevenção e repressão de crimes. Em síntese, entendo que podemos dizer que essas preocupações com a autonomia de alguém que a atividade policial pode causar, da perspectiva da noção de privacidade como direito e da necessidade de proteção regulatória, são acionadas sempre que, fosse a autoridade policial qualquer outra pessoa praticando o *acesso* em questão, diríamos que houve *violação*. O exercício de identificação de direitos à privacidade que a polícia pode implicar e deve respeitar envolveria imaginar um

terceiro do povo comum que, para satisfazer interesse próprio, causasse dano deliberado a uma prerrogativa de privacidade que nossas práticas sustentariam e reservassem para aquela pessoa afetada. Isso não significa ignorar que o propósito da atuação policial é, em geral, e deve ser, bastante distinto, mas uma constatação de que esse é um recurso que ajuda a detectar quando pode ocorrer danos na forma de abuso, erro ou excesso que podem implicar prerrogativas morais relevantes. Chamo isso de um "modelo do terceiro malicioso" para pensar a privacidade oponível ao Estado em atividades policiais.[168]

Paralelamente, é certo que há ameaças a privacidades que extrapolam o que uma pessoa comum pode fazer a outra. Assim, embora seja possível pensar que um terceiro curioso que ingressa num lar sem autorização viola direito, de modo que o ingresso de agentes policiais também deve se preocupar com a possibilidade de causar violação, o teste já não funciona tão bem se o que autoridades estatais estão fazendo é implementar uma política pública de instalação de câmeras em todas as ruas e até casas. Nesse contexto, se o recurso heurístico de pensar o terceiro malicioso também sugerir que a comparação contextual não é possível, é um sinal de que a medida de vigilância em questão envolve acúmulo de poder e possível dano sem equiparação nas nossas práticas sociais e, portanto, senão as mesmas, também preocupações com abuso, erro ou excesso.

Nessas linha, essa perspectiva também mostra como "privacidade" pode ser um conceito acionado para se referir a uma preocupação global com as implicações que a extensão de prerrogativas do Estado tem para liberdades – uma preocupação, de novo, com o exercício do poder.[169] É o caso do uso desse conceito para questionar medidas de vigilância estatal direcionadas a toda a coletividade indistintamente, por exemplo – algo que foge do que está ao alcance de qualquer outra pessoa comum praticar: não só quando instala câmeras

[168] Se houve uma leitura importante para que enxergasse essa maneira de introduzir e articular o ponto, retirando momentaneamente a discussão adicional sobre prerrogativas do Estado, foi Malcolm Thorburn, "Justifications, Power, and Authority", *Yale Law Journal* 117, nº 6 (2008): 1170–1130. Não é um texto sobre privacidade, mas sim sobre teoria do direito penal – mais particularmente, sobre exclusões de ilicitude, como são justificadas, e o que daí se extrai de lição para a teoria do direito penal como um todo. O texto abre com a observação de que às vezes podemos fazer o que em geral o direito penal proíbe. Serviu-me para ver que, embora a polícia às vezes possa fazer o que não autorizamos a mais ninguém, é justamente por isso que carrega um risco de causar danos morais – se, no final das contas, abandonar ou se afastar dos propósitos que legitimam sua conduta.

[169] Solove, "'I've Got Nothing to Hide' and Other Misunderstandings of Privacy"; Rodotà, *A vida na sociedade da vigilância – a privacidade hoje*, 31; Neil M. Richards, "The Dangers of Surveillance", *Harvard Law Review* 126 (2013): 1934–65; Lisa M. Austin, "Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)", in *A World without Privacy: What Law Can and Should Do?*, org. Austin Sarat (Cambridge: Cambridge University Press, 2014), 131–89.

em toda cidade e monta centrais de monitoramento, mas quando determina a guarda obrigatória de dados de telecomunicações, de transações, de viagens, ou contrata novas tecnologias de vigilância e hacking supostamente apenas disponíveis a clientes governamentais, por exemplo.

Como já diziam Westin e Nissenbaum, esse uso reporta-se a questões fundamentais sobre a sociedade que queremos construir e ocorre diante de movimentações políticas e jurídicas que parecem ir na contramão do resguardo a estados e atmosferas de privacidade que valorizamos em nossas práticas sociais e a ampliar nossas situações de vulnerabilidade: de que danos morais individuais venham a se concretizar, para além de poder gerar efeitos inibidores sobre o exercício de liberdades à sociedade em geral[170]. Os trabalhos de Neil Richards colocam bem essa preocupação:

> Vigilância não é perigosa porque é assustadora. É perigosa porque dá ao observador poder sobre o que está sendo observado e é perigosa porque ameaça nossa privacidade intelectual. Em uma sociedade livre, devemos nos importar com os processos pelos quais todos nós aprendemos e desenvolvemos nossas crenças em relação ao mundo. Se soubermos que estamos sendo observados, provavelmente pensaremos, leremos e nos comunicaremos de maneira diferente - é menos provável que nos envolvamos com ideias perigosas ou desviantes.[171]

Diante disso, é dever do Estado instituir mecanismos de contenção de risco a exercícios de direitos em geral, incluindo aí os de privacidade. Pensando em tratamento de dados pessoais, Chirs Berg observa que

> Confiar o Estado a usar informações coletadas para fins liberais é não só confiar no sistema democrático com seus freios e contrapesos de forma geral, mas também confiar em processos governamentais (como as regras que controlam a coleta e o armazenamento de informações) e na virtude de servidores públicos,[172]

Na realidade, sabemos dos riscos: alguns não aceitamos correr e combatemos por serem contrários aos valores da comunidade; para outros, exigimos salvaguardas. Privacidade frente a interesses de segurança do Estado carrega essas preocupações. Nesse sentido, há uma sinergia entre a articulação desse sentido de privacidade frente a propósitos

---

[170] A esse respeito, ver Richards, "The Dangers of Surveillance".

[171] Tradução livre. No original: "Surveillance isn't dangerous because it's creepy. It's dangerous because it gives the watcher power over the watched, and it's dangerous because it menaces our intellectual privacy. In a free society, we have to care about the processes by which we all learn about and develop our beliefs regarding the world. If we know we are being watched, we are likely to think, read, and communicate differently—we are less likely to engage with dangerous or deviant ideas." Richards, *Intellectual Privacy*, 185.

[172] Tradução livre. Chris Berg, *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change* (London: Palgrave Macmillan, 2018), 140, https://www.palgrave.com/gp/book/9783319965826.

de segurança e o direito da proteção de dados pessoais: tratar potenciais abusos e riscos de danos morais a que pessoas são expostas.[173] Para a proteção de dados, isso representa a chegada de preocupações antigas com a existência de relações assimétricas de poder para o ambiente das relações informacionais agora colocadas pela tecnologia e pelo seu uso pelo Estado (e empresas). Já fazemos isso há muito tempo e nas mais diversas áreas. Não há nada que justifique que o Estado não seja vinculado a elas no âmbito do processo penal e de segurança pública; pelo contrário, nossos esforços regulatórios tradicionais nessas áreas, como veremos, reforçam esse compromisso – os futuros também o devem.

Nesse contexto, a fundamentação baseada na autonomia é promissora e atraente, quando estivermos pensando no que a privacidade obriga o Estado mesmo frente à sua atuação para repressão e prevenção criminal. Não se trata de proteger criminosos, mas de obrigar o Estado a conter riscos e ter boas razões para se engajar no que está fazendo e em todas as liberdades que está implicando: nos preocupamos com o poder do Estado porque nos importamos com a autonomia.

3 Hipóteses em análise

Para finalizar este capítulo, vou retomar alguns exemplos inspirados no caso Elize Matsunaga e revê-los a partir das discussões metodológicas e substantivas feitas aqui.

Casa

Elize tinha um direito à privacidade sobre o que mantém em sua casa? Essa deve ser a pergunta mais fácil entre as que são colocadas. Em geral, dizemos que ela e seu marido têm soberania mesmo para definir o que acontece e quem entra e vê o que ocorre no seu lar. Resulta do próprio símbolo que o território 'casa' hoje representa em nossas práticas sociais:

[173] Paul de Hert e Serge Gutwirth associam proteção de dados ao processo penal: "For us privacy is an example of a 'tool of opacity' (stopping power, setting normative limits to power), while data protection and criminal procedure can be mainly -not exclusively- seen as 'tools of transparency' (regulating and channelling necessary/reasonable/legitimate power). Much can thus be learned from making and ascertaining the differences in scope, rationale and logic between privacy on the one hand, and data protection on the other." de Hert e Gutwirth, "Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power". Tendo em vista que privacidade é contextual, sugiro aqui que nossas proteções regulatórias em área como a do processo penal é uma manifestação do compromisso com um direito à privacidade que vale perante o Estado nessa área. Privacidade não é só ferramenta de opacidade – no processo penal, onde é mais afastada (e menos serve para opacidade), ela é quem informa diversas regras processuais e materiais.

como representação máxima da autonomia e separação individual enquanto local em que se pode *estar só,* se nutre as relações de intimidade com quem se quer nutrir tais relações, em que se expressa com liberdade livre de escrutínio, em que se constrói a personalidade.

Já as instituições do Estado desrespeitariam essa importância se tratasse a casa de modo indiferente com a sua relevância em nossas práticas sociais. Se pudesse entrar na casa a qualquer momento, quando bem entendessem, sem razões específicas contundentes, não só o impacto na soberania seria sentido, como o valor que se associa à casa pareceria estar sendo posto em xeque. Não é surpresa, portanto, que nossas práticas jurídicas amadureceram para estabelecer condições mais claras sobre as hipóteses em que o Estado teria razões hábeis a justificar esse ingresso – no caso da polícia, como a situação em que há indícios de que no local haja provas de ocorrência de crime, em situações de emergência para fazer cessar dano a alguém (um "estado de necessidade", como traduzimos na dogmática), ou quando a própria pessoa autoriza o ingresso policial. Falarei mais desse arranjo regulatório em outros capítulos.

O valor da privacidade do lar a que um direito constitucional como a "inviolabilidade do domicílio" se refere não é da casa pela casa, sem mais: é pelo que representa para a concepção das pessoas como seres que podem ter um espaço que é seu e pelo que se pode fazer nela de valor ético sem prestar contas a mais ninguém. Ninguém é obrigado a dar essa mesma concepção de algo sagrado à sua própria casa, mas a proteção jurídica a ela contém o reconhecimento de que temos práticas sociais consolidadas que dão valor a tanto. Por essa razão, sim, há um direito à privacidade do lar e a polícia deve mostrar respeito a tanto, não podendo entrar sem fundadas razões. Cabe ao Estado o estabelecimento e a observância de procedimentos que superem esses ônus de fundamentação – que evitem abusos, erros, excessos.

Nessa abordagem, seria completamente inconcebível que fosse negada a existência de um direito à privacidade porque inventaram uma máquina que é capaz de ver através de paredes sem que o terceiro que a manipula tenha que fisicamente ingressar no lar. Um teste binário que vinculasse uma violação a um ingresso físico ("*penetrar*" na casa) pura e simplesmente seria completamente desconexo com as razões normativas que constituem o direito, ainda que por muito tempo tenha sobrevivido como um *proxy* que, em muitos contextos, servia para identificar uma violação. Mesmo uma concepção que detectasse e

reconhecesse que essa máquina causaria "perda" da privacidade porque dados pessoais seriam coletados também deixaria de capturar dinâmicas de valor atinentes ao contexto e ao conceito de privacidade relevante nele – não é só um interesse pessoal que está em jogo.

De modo semelhante, seria um erro reduzir a privacidade ao "espaço privado" e físico "casa". Se passa a fazer parte das nossas práticas de privacidade aquilo que salvamos na nuvem ou em uma comunidade virtual (um "domicílio virtual"), por exemplo, não a protegeríamos simplesmente porque não se encaixa no teste binário tradicional do que é espaço privado e de quais informações são sensíveis? Se nossos valores contemplam o reconhecimento de outros direitos de privacidade, a reivindicação não para na "casa" – o fato de que o paradigma de proteção da casa existe não significa que se limita ao que até aqui convencionalmente se chamou de casa, muito menos que é o único direito que temos. Privacidade não é só o que uma convergência semântica em algum momento definiu que seria parte de um âmbito privado nem a violação dela se reduz a um teste criterial.

Carro na rua

O que dizer das proteções de Elize sobre seu próprio carro e enquanto trafegava na rua? Como visto, com seu marido esquartejado no porta-malas, chegou a ser parada pela polícia rodoviária ao ser detectada com veículo que estava com documentação irregular. Em linha com tudo o que foi visto nesse capítulo e também se observa em nossas práticas, nós esperamos ter certo nível de controle sobre nossos bens, inclusive quando transitamos com ele nas ruas. Nossas práticas de não sair tomando o que é dos outros e vasculhando o que carregam se reportam a um respeito básico à autonomia, da pessoa como pessoa: cada um cuida da sua vida e do que é seu.

Para a polícia, esse mesmo nível de respeito é devido: seu tratamento perante as pessoas deve observar essa intencionalidade de nossas práticas, de modo que o que quer que fizer que se desvie disso precisa ter uma razão clara, e não pode causar ônus excessivo à pessoa. Se as pessoas tem direito de transitar pelas ruas sem terem seus bens vasculhados por terceiros, a polícia precisa de razões para se desviar disso – e de uma regulação pertinente para evitar abusos, erros e excessos. Se não há nada no comportamento da pessoa que cause suspeita de que a pessoa está envolvida em crime, não há razão para interferência na vida dela em específico, muito menos em aspectos que usualmente consideramos de relevância

pessoal e reservamos para controle daquela pessoa. (Mais adiante nesse trabalho veremos como níveis de *suspeita* contra alguém tem papel fundamental na modulação do tratamento pela polícia e na responsabilização criminal – na vedação de abusos, erros e excessos). Não havia qualquer razão aparente à polícia para suspeitar que ela carregava alguém assassinado no porta-mala.

Agora vamos supor que, sem essa razão, a polícia tivesse ainda assim feito a busca. Teria violado um direito à privacidade? Uma alternativa seria dizer que Elize estava em público e trafegava em via pública, devendo responder a tudo quanto a polícia quiser. Nesse sentido, não haveria o que impedisse a polícia de tal conduta. Também se poderia dizer que não se pode alegar privacidade para proteger ilícitos e que o "flagrante" validaria a ação. Afinal, no caso tanto seria verdadeiro que a privacidade estava acobertando ilícito que levou ao descobrimento de que Elize carregava um corpo em seu carro. Nos dois casos, a discussão sobre privacidade seria encerrada antes mesmo de começar.

Outra possibilidade seria dizer que vistoriar o carro representaria uma perda de seu direito à privacidade (ou, se não há qualquer privacidade em público, a algum "direito geral de liberdade", cujo âmbito de proteção seria genericamente definido como liberdade de se fazer o que se quer fazer), mas que seria "proporcional". A polícia exerceria a função legítima de preservação de segurança pública e essa medida seria adequada (apta), necessária (não haveria alternativas menos gravosas se se quer fazer 'flagrantes' na rua) e proporcional para reprimir crimes, porque a intensidade do interesse em segurança é maior que a invasão na privacidade.

Pela abordagem que proponho aqui, essas conclusões estariam erradas: nós temos um direito à privacidade sobre bens que carregamos mesmo em vias públicas, que extraímos de nossas práticas de respeito um ao outro e da responsabilidade que temos sobre nossas próprias vidas – mesmo na rua, não achamos que podemos fuçar bens alheios. Não havendo qualquer suspeita de que ela praticava crime, não há razão para tratamento invasivo ao que a polícia em geral deve à população e para desvio com relação a direitos que devemos uns aos outros. A finalidade da parada de Elize pela polícia (controle de documento e aplicação de multa) vincula o trabalho policial. Ir *além* do que a sua "justa causa" permite, vasculhando sua vida e realizando qualquer outro tratamento extraordinário sem razão, fere um compromisso fundamental do Estado com a autenticidade: não comprometer a vida de cidadãos de forma

extraordinária ao contexto sem que tenham dado qualquer motivo aparente para tanto em meio às pessoas em situações semelhantes. Nessa linha, quando e se a polícia se engaja nessas condutas sem um pano de fundo regulatório – que vede abusos, erros e excessos – ameaça direitos e amplifica riscos de causar danos morais injustificadamente.

Alguém poderia dizer que pela teoria da proporcionalidade também seria possível concluir que a conduta teria sido excessiva. De fato, não descarto essa hipótese. A teoria da proporcionalidade só planeja ser "estruturante" da análise – a partir da definição abrangente, não se propondo a oferecer um critério para a atribuição final de pesos na "ponderação".[174] Ela não oferece uma teoria substantiva sobre valores. No meu exemplo, o intérprete concluiu que é proporcional, mas poderia ter concluído que não era se, aguém pode dizer, tivesse melhor calculado o interesse de propriedade das pessoas sobre seus bens e as repercussões que uma autorização para que a polícia pudesse averiguar todos os carros que quisesse para o temor público.

Ainda assim, penso que a abordagem que propus é mais atraente e esse ponto valerá também para meus próximos exemplos: ela reafirmaria princípios e valores que fundam certa comunidade voltando-se à interpretação do melhor sentido deles; não se tornaria a um discurso genérico de ponderação de interesses.[175] A teoria da proporcionalidade não acomoda a possibilidade de que podemos estar lidando com direitos morais que não podem ser genericamente balanceados com o interesse público.[176] Se temos um direito à privacidade sobre o que carregamos em nosso carro mesmo em público, ele não é simplesmente ponderável – a regulação e a fundamentação da conduta estatal deve ser uma que mostre respeito a ele e se comprometa a não causar danos sérios a seu exercício e que busque não causar injustiças. Isso exige uma reconstrução conceitual a partir de uma teoria moral. As

---

[174] "Now it is true that the Weight Formula does not tell us what an interference with a constitutional right (I_i, I_j) comes to, when the scale light (l), moderate (m), and serious (s) is used. It also does not tell us what the abstract weights (W_i, W_j) of the colliding principles are. Finally, it says nothing about the reliability (R_i, R_j) of the relevant empirical assumptions." Robert Alexy, "Constitutional Rights and Proportionality", *Revus - Journal for Constitutional Theory and Philosophy of Law* 22 (2014): 11. Também: "Ainda que o sopesamento em si não estabeleça um parâmetro com o auxílio do qual os casos possam ser decididos de forma definitiva, o modelo do soperamento como um todo oferece um critério, ao associar a lei de colisão à teoria da argumentação jurídica racional." Alexy, *Teoria dos direitos fundamentais*, 173.

[175] Nesse sentido, ver Alexander Aleinikoff, "Constitutional Law in the Age of Balancing", *Yale Law Journal* 96, nº 5 (1987): 987;991.

[176] Stavros Tsakyrakis, "Proportionality: An assault on human rights?", *International Journal of Constitutional Law* 7 (2009): 489; Ribeiro, "Para além da subsunção e do sopesamento".

razões por que algo seria "proporcional", por outro lado, não necessariamente envolvem um compromisso de integridade com os valores da comunidade jurídica e a melhor concepção deles. Ao fim e ao cabo, a falta desse compromisso compromete a própria legitimidade do exercício da coerção pelo Estado.

Localização

Revistas essas situações mais 'tradicionais' sem tecnologia, passemos às que têm essa variável. Elize tinha um direito à privacidade sobre as informações de geolocalização de seu celular? Uma primeira possibilidade é dizer: esses dados não são privados, porque dizem respeito a movimentações sobretudo públicas de Elize (e não existe privacidade em público), além de terem sido compartilhados com empresas de telefonia, que possivelmente utilizam essas informações para fins de marketing. Então: não, Elize não tem direito à privacidade sobre esses dados em face da polícia (e, segundo a lógica, em face de ninguém, aliás).

A outra alternativa seria dizer: ela tem um direito à privacidade, retraduzido na forma de autodeterminação informacional, porque qualquer atividade de coleta e uso dessas informações seria um tratamento de dado pessoal que interfere em seu direito de controlar tais informações sobre si. Porém, para saber se esse direito lhe serve de qualquer modo frente ao trabalho policial, precisa passar no teste de proporcionalidade. No contexto em que seu marido está desaparecido, por conta dos propósitos legítimos, e do fato de que os dados são adequados como meio de prova, seriam supostamente necessários, e haveria proporcionalidade em sentido estrito (os interesses na solução do crime pesariam mais que qualquer interesse que Elize tenha em que não seja acessados), alguém poderia dizer que a restrição ao seu direito é proporcional.

No modelo que propus aqui, essa análise não teria essa estrutura. Elize utiliza seu telefone celular para fazer ligações, mandar mensagens, se conectar à internet – uma atividade extremamente comum e expressiva na vida cotidiana e da qual as pessoas são cada vez mais dependentes. A coleta de dados de localização é parte imprescindível desse serviço: sem sinal, não é possível utilizar as funcionalidades do celular. A geração de informações de um catálogo de informações de geolocalização de Elize é, então, um subproduto do seu uso do celular: provavelmente ninguém mais em sua vida, a não ser a si própria, tem essa capacidade de ter uma visão sobre todos os seus trajetos. Provavelmente por isso Elize tem

uma expectativa de privacidade sobre essas informações. Por conta de seu relacionamento contratual com a empresa de telefonia, provavelmente espera que as informações serão usadas dentro de suas expectativas e do que faz sentido no contrato, e que isso não envolveria repasses a terceiros inadvertidamente – muito menos à polícia. Algumas empresas engajam-se em parcerias comerciais que envolvem usos a uma finalidade diferente do motivo da coleta inicial e também compartilhamentos, mas em geral dessa relação espera-se confidencialidade ou ao menos algum outro lastro que atenda a interesses de Elize e não envolvem exposição a outras pessoas, só destinação de publicidade para ela.

Provavelmente se um *stalker* quisesse ter acesso aos dados de geolocalização dela junto à empresa, seria negado pela sua privacidade. A um jornalista, provavelmente também. Se forçassem esse acesso, provavelmente veríamos uma violação de expectativas de Elize de manter e dispor dessas informações sobre o mosaico de sua vida reconstruído pelos seus trajetos como parte de sua autonomia e autodeterminação, de modo que a princípio há razões para falar em direito à privacidade, tanto como falávamos na sua soberania sobre o que mantém em sua casa e em seu veículo. O ponto de vista relevante para vermos se há uma reivindicação coerente de privacidade é a de participantes de uma prática de privacidade – apesar de celulares serem populares, de captarem informações inclusive de quando estamos em vias públicas e de empresas de telefonia se engajarem em outras utilizações dessas informações, se nós não possuímos acesso às localizações de todas as outras pessoas, não há porque desconsiderarmos que ainda há privacidade entre as pessoas com relação a essa informação e que ela pode ser *valiosa* para como nos enxergamos enquanto pessoas, isto é, para nossa autonomia. Se é esse o caso, a polícia pode muito bem violar um direito se lhe for concedido acesso a localizações de alguém informadas por seu celular sem um pano de fundo regulatório que vede abusos, erros e excessos.

Nossas práticas sugerem a importância da obscuridade na condução de nossas vidas e é justamente isso que seria posto a prova forçadamente. Da polícia, por sua vez, espera-se que não se engaje em condutas que ameacem esse valor despropositadamente e que tenham boas razões: faz sentido buscar esses dados de Elize, dentro do contexto de sua atuação? Por que ela estaria sendo selecionada para esse tipo de averiguação? A polícia age dentro de procedimentos que limitam hipóteses de abuso, excesso e erro? Naturalmente, quando essa se torna uma controvérsia jurídica, existem diversos materiais legislativos e paradigmas

jurisprudenciais que passam a ter de ser considerados, mas já se percebe que as considerações seriam distintas do que as abordagens mais comuns, sobretudo para interpretação de quais direitos Elize têm e quando há violação deles. A disputa relevante é sobre o valor da obscuridade sobre nossas localizações e como evitamos injustiças – tratamentos incompatíveis com esse valor – inclusive por parte da polícia.

Elevadores

A Elize e o Marcos tinham direito à privacidade sobre o que fizeram e quando estiveram em elevadores do prédio em que moravam? Essa sequer parece uma pergunta que nos colocamos no dia a dia atualmente ou que tenha sido posta na investigação: o mais provável é que os vídeos tenham sido entregues pela administração do condomínio assim que solicitados pela polícia, que deu sorte que ainda estavam disponíveis.

As áreas comuns de um prédio podem ser consideradas áreas "semi-públicas": já constituem propriedade privada, mas não o núcleo do domicílio familiar. Entre os habitantes do prédio, as áreas comuns são o que o nome diz – comuns aos moradores e portanto de livre acesso e visualização a todos. No interesse de garantir a segurança da propriedade e de seus moradores, bem como para facilitar a resposta a emergências que possam envolver ocorrências em elevadores, a instalação de câmeras é um fenômeno de máxima adoção em prédios e residências de grandes cidades. Daí surge a possibilidade de dizer que: não, moradores não tem direito à privacidade sobre o que fazem em elevadores, porque isso é matéria que já mais se aproxima de nossa vida pública.

A alternativa é dizer, a partir do que pressupõe a teoria da proporcionalidade e a concepção abrangente de autodeterminação informativa, que a captura de imagem de pessoas em vídeo é uma coleta de dado pessoal – e portanto há uma interferência em direito que precisa ser fundamentada. Nessa linha, a administração do condomínio tanto teria de demonstrar ter interesses legítimos nessa atividade de segurança privada, quanto que a disponibilização a autoridades policiais está contemplada também por esses interesses e era adequada, necessária e proporcional aos propósitos de repressão criminal que os orientavam.

A abordagem proposta aqui talvez não altere conclusões, mas para chegar nelas acentuaria outras engrenagens da justificação. Moradores podem ter expectativa de privacidade sobre o que fazem em elevadores no seguinte sentido: podem aceitar e deliberar

que a portaria pode ter acesso em tempo real e que apenas a gerência terá acesso aos vídeos gravados, em casos de ocorrências relevantes que mereçam essa gravação, ao mesmo tempo em que não esperam nem admitem que será disponibilizado ao público em geral na internet ou mediante simples solicitação de quem quer que seja nem que quem tem acesso fará uso das gravações para catalogar passos de moradores e tudo o que fazem e explorar essa informação contra eles. Esse é um arranjo de privacidade, que deixaríamos de notar se só olhássemos para o fato de que há câmera e que as pessoas estão fora de casa.

Já a disponibilização de acesso de recortes específicos que possam estar relacionados a crime à polícia faz parte daquilo que compõe o próprio objetivo da instalação da câmera que, mediante deliberação dos condôminos, a administração implementou: garantir segurança e existência de prova para ajudar investigações. Assim, a existência das câmeras não obriga compartilhamento com a polícia de qualquer maneira, muito menos em qualquer extensão. A depender do apetite de privacidade dos moradores e se um acusado quisesse questionar o uso dessas imagens, não seria impossível articular um direito à privacidade de moradores contra terceiros em que a polícia é mais um deles. Em particular, em razão desse direito, para dizer que da polícia teria sido exigível previamente que provasse a necessidade de obter os vídeos não só da vítima Marcos, mas da suspeita/ré Elize, e a relevância para sua investigação – e que a justificação disso deve também passar por um pano de fundo regulatório que busque evitar abusos, erros e excessos.

O argumento é mais difícil porque em geral não associamos a andar no elevador sem ser visto por mais ninguém que não é morador atividades valiosas nem uma capacidade única de controle de um aspecto relevante de nossa vida. Essas nuances são relevantes à maneira como justificamos direitos e parâmetros regulatórios sobre os potenciais danos morais em jogo. Talvez por isso, portanto (e volto a dizer que tudo o que fiz aqui foi elaborar aproximações), ao final tivéssemos de concluir que não há tantos riscos de injustiças no acesso policial ocasional e específico a essas imagens. Sendo este o caso, estaríamos do mesmo lado de quem imediatamente descartou privacidade porque o ambiente era semi-público e porque os interesses de segurança eram mais intensos. Mas não o fizemos do mesmo modo – não concluiríamos isso sem revisitar nossos direitos, o sentido e o valor deles, nem as maneiras como a facilitação desse acesso à polícia possa causar injustiças.

4 Conclusão parcial

Neste capítulo, procurei rever três abordagens comuns sobre privacidade, apontar seus problemas e propor uma maneira de evita-los. Penso que esse ajuste de contas é importante para a jornada deste trabalho. Primeiro, falei da concepção de privacidade a partir da dicotomia público-privado e suas inclinações a testes "binários" criteriais para identificação de direitos, que são simplificadores demais e, sobretudo por conta do avanço tecnológico, cuja aplicação tem levado a distorções entre o resultado do teste e expectativas normativas. Fatores expressados nessas dicotomias entre público e privado podem ser relevantes para constatarmos violações e danos em alguns contextos e relações de fluxo de informações, mas não é possível dizer que é assim sempre, sem nos voltarmos aos valores que estamos protegendo quando protegemos a privacidade e as ameaças de usurpação da nossa autodeterminação sobre aspectos de relevância pessoal que ainda podem estar em pauta no contexto em questão. Embora pudéssemos desejar que a possibilidade existisse e sonhar com o quão útil isso seria para resolver disputas judiciais, não há um teste de papel de tornassol disponível para identificar universalmente todo e qualquer dano moral à privacidade com essa lógica binária e criterial.

A segunda abordagem de que falei é a da concepção abrangente de privacidade a partir do mesmo enfoque neutro e abrangente da "autodeterminação informacional", que passou a ser elaborada conceitualmente e ganhou proeminência por conta dos problemas que abordagens dicotômicas já levavam para estabelecer proteção jurídica da privacidade. O problema dessa abordagem é sua propensão a diluir o sentido de ter um direito e a pressupor conflitos trágicos entre princípios. Igualar direito à privacidade a uma concepção de "ser capaz de ocultar o que se quiser ocultar" ou de "controlar todo fluxo de informação sobre si", bastante semelhante a um sentido genérico de liberdade como simplesmente "poder fazer o que se quer fazer", deixa de servir para a identificação de reivindições de um direito *moral* forte à privacidade que esteja sendo violado por certos tipos ou finalidades de tratamentos de dados pessoais e que possa se opor inclusive ao desejo da maioria de uma comunidade política. Isto é: a direitos no sentido de que, ainda que se concluísse que uma sociedade sem essas proteções a certas práticas de 'privacidade' fosse melhor para todos a longo prazo, seria errado privar as pessoas dessas liberdades.

A seguir defendi que devemos abraçar o fato de que quais *privacidades* são um *direito* é com frequência objeto de divergência e só são determináveis pelo contexto em que a prática de privacidade em questão se coloca. Nossa capacidade de defender uma tese bem-sucedida de violação à uma privacidade e a seu sentido como direito moral e político passa por nossas práticas sociais e jurídicas e a intencionalidade delas – e que a disputa sobre a necessidade de proteção ou não é interpretativa, girando em torno de valores. Dito isso, apesar de nossas proteções jurídicas nascerem de um caldo de práticas, convenções e convicções, o teste para proteção não é a existência de um acordo social sobre o que caracteriza a quebra dessas regras. Entender assim deixaria justamente de dar sentido a diversos desacordos jurídicos interpretativos sobre privacidade e a demandas por proteção – que inclusive originaram paradigmas jurídicos que serão vistos no capítulo 4. Alimentada sobre nossas práticas, a interpretação de direitos de privacidade procura o melhor significado desse conceito tendo em vista os valores a que está orientada a prestigiar no contexto específico (a melhor concepção do conceito de privacidade nele).[177] Assim, é importante olhar para a relevância de considerações de privacidade no contexto do e frente ao trabalho policial.

Daí surgiu uma terceira frente de discussão que precisaria ser enfrentada: uma profunda aversão em falar de privacidade como oposição a ações estatais promovidas em nome da segurança. Que sentido poderiam ter direitos à privacidade frente a essas atividades? Revi algumas justificativas comuns para proteção da privacidade e busquei mostrar como a concepção que enxerga em nossas práticas paradigmáticas de privacidade uma intencionalidade de proteção da pessoa como pessoa dotada de dignidade – e de seu processo de criação de uma vida que possa ver como *sua* carrega seu significado e valor inclusive frente ao trabalho policial. Nesse contexto, argumentei que grande parte dos esquemas jurídicos regulatórios que emergiram em torno desse conceito estão relacionados à exigência de que o Estado preserve a independência ética e a responsabilidade pessoal de seus cidadãos diante da constatação de que estão vulneráveis a riscos e excessos nas mais diversas direções – isso vale para privacidades frente às atuações do Estado, ao uso de dados pessoais em geral, e mais genericamente como exigência de igual consideração e respeito em uma democracia

[177] Para uma primeira versão das objeções de Dworkin ao convencionalismo e sua incapacidade de explicar o apelo a juízos morais sustentar regras sociais, ver Dworkin, *Taking Rights Seriously*, 46–80. Para referência completa sobre esse debate, ver Macedo Junior, *Do xadrez à cortesia: Dworkin e a teoria do direito contemporânea*.

comprometida com a dignidade em que cidadãos convivem com o poder do Estado e se submetem ao seu uso da força.

Assim, no contexto policial, direitos à privacidade que nos resguardam contra terceiros podem conviver com *regulações* para acomodar interesses legítimos – como razões de ordem moral para prevenção e repressão do crime. Na verdade, como retomo adiante, essa pode ser inclusive a forma como, nesse contexto, o Estado mostra respeito a tais "inviolabilidades", como é o termo comum que qualifica proteções jurídicas no direito brasileiro – ao que retornaremos no capítulo 4. É importante, entretanto, que essa regulamentação não desqualifique o próprio direito e sua razão de ser; nem que imponha um ônus excessivo para seu exercício (cause danos sérios) nem seja incongruente com a concepção mais atraente dos direitos específicos à privacidade que pudermos articular. Lidar com privacidade no contexto penal é complexo porque a discussão é, já se antecipa aqui, em grande parte regulatória nesse sentido e, às vezes, até de sintonia fina sobre aspectos específicos dessa regulação que já não são exigências de princípio, mas escolhas políticas.

Mas nada disso autoriza que tratemos de privacidade nesse contexto de modo simplista, como se não houvessem compromissos de princípio que vinculem a atuação do Estado nessa área. Nessa linha, mostrei o que essa abordagem adiciona para a análise de algumas situações hipotéticas baseadas no caso Elize Matsunaga ao longo do capítulo: a impossibilidade de descartar a existência de direitos relevantes em jogo simplesmente com base em noções binárias, ou de aplicar genericamente noções de proporcionalidade. Práticas de privacidade variam contextualmente e os valores que as orientam vinculam inclusive a atuação do Estado.

No próximo capítulo, analiso o conceito de segurança e seus reflexos na prática jurídica que governa atividades de segurança pública e investigações criminais.

Capítulo 2 - Segurança

No artigo *Safety and Security* (2006)[1], Jeremy Waldron destaca como existe pouca elaboração conceitual sobre o significado do termo "segurança", apesar de muito se falar dele – inclusive sobre como por vezes precisamos "trocar" certas liberdades por segurança. Chama essa negligência de chocante, pois é um conceito profundamente importante na filosofia política. De fato, a noção de segurança aparece nas teorias clássicas sobre origem e fundamentação do poder do Estado: Thomas Hobbes defendeu que é por uma questão de segurança – uns contra os outros e nossa contra terceiros – que estabelecemos um soberano e abrimos mão da liberdade natural; Locke via na segurança à propriedade conferida pelo Estado – limitado pelo direito, sob pena de se tornar ameaça à segurança dos indivíduos – a razão pela qual homens constituíam uma comunidade política; Jeremy Bentham entendia que "o cuidado pela segurança" é o principal objeto do direito.[2] Apesar da centralidade discursiva da segurança como ideal que é uma meta primária ou função do estado, muito mais se diz sobre o que precisamos fazer para promover ou melhorar a segurança do que sobre o que ela significa.[3]

Como já falei, a "garantia da segurança" é possivelmente o principal argumento lançado para justificar restrições à privacidade justamente nesse contexto (enquanto direito oponível ao Estado em atividades policiais). Por vezes é apresentado ainda como uma espécie de "superprincípio"[4], já que aparece como trunfo em debates políticos para fundamentar iniciativas e

[1] Jeremy Waldron, "Safety and Security", *Nebraska Law Review* 85, nº 2 (2011): 454–507.
[2] Para análises do conceito de segurança nas obras clássicas de filosofia política, e do direito ver Lucia Zedner, *Security*, 1 edition (London; New York: Routledge, 2009), 26–33; Liora Lazarus, "The Right to Security", in *Philosophical Foundations of Human Rights*, org. Rowan Cruft, S. Matthew Liao, e Massimo Renzo (Oxford: Oxford University Press, 2015), 424–27; Rhonda Powell, *Rights as Security: The Theoretical Basis of Security of Person* (Oxford, New York: Oxford University Press, 2019), 45–50.
[3] Nesse sentido, também Powell, *Rights as Security*, 54.
[4] Cf. Gustavo A. Paolinelli Castro, "Direito à segurança pública no Estado Democrático de Direito: uma releitura à luz da teoria discursiva", *Revista Direito, Estado e Sociedade* 33 (2008): 70–84, https://doi.org/10.17808/des.33.239.

projetos de lei que implementam tecnologias de monitoramento e ampliam prerrogativas de investigação, bem como ordens judiciais que afastam a privacidade de alguém. Já mostrei no capítulo anterior como é um erro o tratamento que deixa a noção de privacidade completamente intimidada e enfraquecida frente a postulações em nome da segurança. Agora cabe o reverso: em um trabalho que pretende explorar quais os limites que a privacidade coloca no contexto de segurança pública e investigações criminais, é importante que seja dada também atenção ao que significa garantir a segurança.

Aqui, nós podemos revisitar o caso Elize Matsunaga da seguinte perspectiva: nós temos naturalmente um interesse de não sermos assassinados; e mais, nós temos um direito moral forte a não sermos assassinados. Tirar a vida de alguém deliberadamente como Elize fez é causar um dano que nega a dignidade daquela pessoa. É de se esperar, portanto, que o Estado tenha instituições que impeçam e desencoragem as pessoas de cometer esse tipo de crime uns contra os outros e, como já adiantavam filósofos politicos antigos, essa é uma das maiores expectativas que colocamos sobre o Estado. Onde é que isso para? Queremos que o Estado responsabilize quem mate pessoas, e que possa ter instituições para impedir que isso ocorra. Mas qual o limite? Temos um direito à segurança que envolva o Estado dispensar esforços para vigiar lares, exigir que pessoas prestem contas de suas intenções sobre seus esposos, para evitar que isso ocorra? Ou até mesmo a por câmeras dentro de lares para que haja prova documental caso algum crime venha a ocorrer? Se o direito à segurança é tão abrangente, por que não? A privacidade sobre o lar então interfere em um direito à segurança quando dizemos que é errado obrigar a instalação dessas câmeras em lares?

Naturalmente, o exemplo do caso Elize Matsunaga é limitado porque o direito de não ser assassinado não é o único que nós temos. Também temos o direito de não ser furtados ou roubados – eventos que, inclusive, mais alimentam o ânimo de colocar câmeras em casas e cidades. E outros tantos valores também são protegidos, como a moralidade política e a integridade do sistema financeiro, dando lugar ao reconhecimento de outras condutas criminosas em decisões políticas coletivas. Mesmo direitos à privacidade são parte daquilo que o Estado nos garante contra os outros e alimenta esforços e atividades policiais. O que é que esses direitos autorizam em nome da segurança? Até que ponto a vigilância do Estado para que esses crimes não ocorram ou para que sejam eficientemente punidos é justificada? Impedir que o Estado conduza testes em pessoas e agrupe aqueles que têm tendências a cometer homicídio para prestarem contas rotineiramente

sobre o que fazem a policiais e para receberem educação especial é violar um direito à segurança? Talvez isso tivesse impedido Elize de agir. Mas é mesmo exigência do nosso direito a não sermos assassinados?

Como passo a mostrar, semelhantemente ao conceito de privacidade, segurança é também um conceito contestado e essa é uma constatação que existe na literatura sobre o tema. O debate, portanto, é sobre qual a concepção que melhor revela o valor da segurança. Concepções abrangentes são criticadas porque contribuem justamente para o problema do "superprincípio": fomentam uma ideia de que segurança vence (quase) tudo. Tendo isso em vista, ofereço uma concepção de segurança também fundada na dignidade que não só é mais atraente como concepção sobre o que valorizamos quando prezamos "segurança" como também é mais apta se reconciliar com o quanto visto sobre privacidade no capítulo anterior.

Feito isso, analiso como essas noções aparecem e se relacionam às nossas práticas de Direito Penal, Direito Processual Penal e Direito Administrativo policial e à maneira como o estudo dogmático dessas áreas do direito traduziu compromissos de princípio nessas áreas de atuação. A tecnologia está também desafiando conceitos que já há muito tempo nos auxiliam a verificar se atuações do Estado em nome da segurança estão de acordo com fundamentos básicos do que conhecemos por *rule of law*; avanços tecnológicos, justamente por avançarem capacidades que humanos não possuem, caem como luva a uma concepção de segurança que quer ser abrangente – que quer ter vista de tudo para conter todo risco à vida e à propriedade, toda interferência em interesse de alguém. Esse fenômeno tanto reforça a necessidade de perceber a natureza interpretativa de conceitos no tratamento jurídico da matéria, como alerta para a necessidade de lançar mão de instrumentos regulatórios novos e de reafirmar compromissos de princípio para uma nova era.

1 Desafios conceituais: o caráter relacional e disputado do conceito de segurança

Lucia Zedner chama o conceito de segurança de "promíscuo"[5]. Pode ser utilizado para se referir a diferentes níveis de sujeitos: a uma pessoa (segurança individual), a um grupo de pessoas, a uma comunidade política como um todo (segurança pública), ao Estado (segurança nacional), a um conjunto de nações (segurança coletiva) – e a bens materiais (segurança patrimonial) ou

[5] Zedner, *Security*, 9.

imateriais (segurança da informação, segurança de dados). Sua utilização é também frequentemente flexionada com base no tipo de ameaça contra o que se quer proteger ou na sua origem: ameaças externas/estrangeiras (segurança nacional) ou ameaças internas (segurança pública, segurança interna) que envolvam uso de violência, mas também contra desastres naturais, acidentes, prejuízos financeiros. Também pode ser usada para qualificar quem oferece um serviço de segurança: empresas (segurança privada), a comunidade (segurança comunitária) ou o Estado (segurança pública). As variações também se aplicam a ambientes: segurança do trabalho, segurança do trânsito, segurança do lar (doméstica), segurança hospitalar, segurança cibernética, segurança aeronáutica, etc. Em qualquer caso, a ideia é proteger ou preservar algo que se valoriza – ninguém fala em "segurança da doença"[6], muito embora existam esforços para segurança em e da saúde.

Nenhuma das denominações listadas acima pretendeu ser inequívoca; quis apenas indicar utilizações comuns que mostram a multiplicidade de aplicações do termo. Essa característica levou Rhonda Powell a categorizar o conceito de segurança como um conceito eminentemente *relacional*: para explorar seu sentido, é preciso questionar (i) segurança para quem (qual agente); (ii) segurança do quê (qual valor ou interesse a ser protegido); (iii) segurança contra o quê (quais riscos e ameaças); (iv) segurança por quem (que provedor da proteção). Essa estrutura seria preenchida conforme o contexto e permitiria delimitar e compreender a natureza da discussão: "O conceito de segurança é silente sobre o nível em que é aplicado (internacional, nacional, de grupo, individual); silente sobre o interesse ou valor que é para ser assegurado; silente sobre o tipo de ameaças e riscos que são relevantes; e silente sobre quem deveria prover a proteção e como eles deveriam fazê-lo. É portanto sensível ao contexto"[7].

Nesse trabalho, o foco é a segurança que é devida pelo Estado às pessoas como membros de uma comunidade política contra atividade criminosa interna – por ser essa uma das principais motivações para restrição de direitos de privacidade. Interessa-me, portanto, principalmente a noção de "segurança pública" – tanto no sentido de uma atividade prestada pelo Estado quanto de atividade relativa à comunidade como um todo e voltada a ameaças presentes e originadas dentro

[6] Encontrei esse exemplo no livro de Rhonda Powell, atribuída a PE Digeser em artigo não publicado. Cf. Powell, *Rights as Security*, 57.

[7] Tradução livre. No original: "The concept of security is silent about the level at which it is applied (international, national, group, individual); silent about the interest or value which is to be secured; silent about the type of threats and risks which are relevant; and silent about who should provide the protection and how they should do so. It is therefore context-sensitive." Powell, 62.

do território nacional – nesse trabalho, as ameaças em foco são os *crimes*. Por outro lado, é também relevante saber em que medida falar em "segurança pública" se difere ou se aproxima da referência a uma "segurança pessoal" – um objetivo político que também valeria contra crimes, mas que da própria linguagem parece reivindicar ser devido às pessoas individualmente, não mais apenas à comunidade como um todo, sem destinação particular.

Nesse sentido, a natureza ambivalente e referencial de segurança a que Powell sinaliza não deixa de ser semelhante ao que vimos para o conceito de privacidade – das diferentes maneiras como pode se referir a diferentes objetos e ganhar significados variáveis conforme o contexto. É bom, portanto, termos clareza sobre a que estamos nos referindo. Ocorre que, mesmo mais ou menos delimitadas as práticas sobre as quais queremos nos referir ao tratar de "segurança", o conceito é também ainda profundamente disputado.[8]

Uma discussão conceitual frequente é da diferença entre segurança como situação factual (segurança objetiva) e segurança como sentimento (segurança subjetiva).[9] Ao tratar da segurança, dizem, podemos nos referir tanto à realidade como à percepção subjetiva dela. Essa distinção descritiva aponta para a existência de um debate normativo mais interessante: devemos considerar não só as condições objetivas, mas também a percepção subjetiva como parte do ideal de segurança? A segurança que devemos buscar deve também contemplar o sentimento das pessoas? Waldron, por exemplo, no texto já mencionado, defende que nossa concepção de segurança deve ser capaz de ser complexa o suficiente para acomodar o medo psicologicamente debilitante sobre nossa vida, saúde, posses e modo de vida.[10] Apenas dessa perspectiva, portanto, já existe debate.

Para além do papel que a experiência subjetiva do medo deve ter nessa concepção, Waldron tece outras considerações que mostram o caráter contestado do conceito de segurança em operação – a disputa sobre como melhor revelar o valor a que se reporta. Uma "concepção de pura segurança (*pure safety conception*)[11]" seria aquela pela qual uma pessoa está segura na medida em que está

---

[8] Nesse sentido, ver também Zedner, *Security*, 10; Giovanni Manunta, "What Is Security?", *Security Journal* 12, nº 3 (1º de julho de 1999): 59, https://doi.org/10.1057/palgrave.sj.8340030.

[9] Além de Waldron, (Waldron, "Safety and Security", 466–67.), ver por exemplo Humberto Barrionuevo Fabretti, *Segurança pública: fundamentos jurídicos para uma abordagem constitucional* (São Paulo: Atlas, 2013), 17–18; Conrado Hubner Mendes, "Direito à segurança e a sensação de segurança", Época, 25 de janeiro de 2019, https://oglobo.globo.com/epoca/direito-seguranca-a-sensacao-de-seguranca-23397881.

[10] Waldron, "Safety and Security".

[11] Waldron, 461.O inglês contém uma variação linguística entre *safety* e *security* que não possui equivalência no português. Isso torna a distinção mais difícil de ser capturada pelo leitor. O próprio Waldron não propõe uma distinção para os dois termos diretamente, quase que apelando a uma distinção intuitiva que o leitor, conhecedor da língua, já fosse capaz de captar. Grosseiramente, e a partir de definições de dicionário que apenas servem para dar algum

viva e livre de danos físicos – para ela, o valor de nossas práticas de segurança seria proteger contra esse tipo de dano. Nessa concepção, segurança está, figurativamente, associada à probabilidade de alguém ser explodido por uma bomba em um atentado terrorista: quanto menor essa chance, mais segurança existe. Waldron vai dizer que essa é uma concepção pobre de segurança: apesar de ele mesmo não ter se proposto a defender uma concepção por completo, defende que essa concepção simples deixa de contemplar a importância de outros elementos.

Entre eles, defende que a concepção pura deixa de contemplar que as pessoas esperam poder ter segurança também sobre o modo de vida que levam (escolhas e aspirações) e o papel que seus bens têm nela – sobre aquilo que conquistaram ao por em ação o seu plano de vida[12]. Nesse sentido, de nada valeria ter bens seguros de ataques, se modos de vida não estão – se, mesmo com família, trabalho, casa e carro, tivéssemos que ficar a maior parte do tempo enclausurados, por exemplo. Um outro elemento que a concepção pura deixaria de fora é o da *garantia* sobre o futuro – uma concepção atraente de segurança deveria contemplar o conjunto de práticas de segurança que se projeta ao futuro e permite que a pessoa faça planos e usufrua de seus bens sem ter de se ocupar apenas com precauções paralisantes. Outro é a relevância do "padrão de impacto" – das ações do Estado em nome da segurança àqueles que estão sob seu poder e às limitações existentes para desnivelamentos nesse impacto. Seria irracional que as pessoas concordassem em se submeter ao Estado se não pudessem esperar que sua situação melhoria assim. Esse ponto sugeriria, ao menos, um argumento contra a posição de que Estados possam negligenciar ou impactar negativamente a segurança de alguns para aumentar a segurança de outros.[13] O conceito de segurança deveria acomodar esse fator, portanto.

Nossas disputas interpretativas sobre esse conceito, experimentadas em debates morais, políticos e jurídicos, é *engajada* dessa maneira – se propõe a articular e defender a melhor maneira de apresentar o que faz da segurança algo valioso. Waldron quer defender e mostrar que a concepção simples seria pobre tendo em vista intuições, convicções e expectativas muito básicas que temos sobre segurança e, portanto, seria incorreta. Se há um valor na segurança, ele não seria

---

contexto linguístico, pode-se dizer que o termo *safety* é mais frequentemente utilizado para se referir à condição de alguém estar seguro de riscos que pudesse sofrer ou causar. *Security,* por sua vez, se refere com mais frequência ao estado de estar seguro contra danos e perigos, principalmente deliberados de terceiros. Ao longo do texto, entretanto, Waldron associa *safety* à proteção da integridade física, em detrimento de uma concepção mais rica de *security* que reportaria a uma concepção mais rica que ele pretende começar a elaborar no trabalho. Para ele, é *security* está ancorada em *safety,* mas não se reduz a ela. Cf. Waldron, 505.

[12] Waldron, "Safety and Security", 466.

[13] Waldron, 493.

só o que a concepção simples reporta. Por essa discussão, vemos como segurança é também um conceito contestado e, na linguagem de Dworkin, interpretativo: disputamos a melhor maneira de formular o valor a que se refere.

Rhonda Powell, que chama atenção ao caráter "relacional" do conceito de segurança, disputa a caracterização de que o conceito seja contestado: para ela, as diferentes *políticas* de segurança o são.[14] De fato, são e, como tratarei adiante, nós realmente debatemos imensamente sobre qual meta social de promoção da segurança nós devemos avançar em uma comunidade e como isso deve ser feito. A permanente discussão brasileira sobre a redução da maioridade penal é um exemplo disso: seus maiores propositores defendem a medida como algo que vai trazer melhoria para a segurança da população. Por outro lado, críticos contestam que essa medida seria efetivamente positiva para promover a segurança. De um lado ou de outro, nesse contexto se vê e se discute a políticas de segurança pública: como melhor promover o objetivo político da segurança pública à comunidade como um todo.

Ainda assim, as considerações vistas no capítulo anterior se aplicam aqui: podemos tentar separar um esforço descritivo do esforço normativo sobre o conceito de valor da segurança, mas o faremos ao custo de nos enganar sobre o tipo de gramática conceitual que está em jogo em postulações político-morais sobre o que o conceito de segurança exige, requer e autoriza. Powell está certa de que precisamos ter mais ou menos clareza sobre a que conjunto de práticas estamos nos referindo (sobre o conceito) e que o significado pode variar em diferentes contextos. Entretanto, nada disso significa que, reportando-se ao mesmo conjunto de práticas e a um mesmo contexto, haverá um critério compartilhado para determinar se a proposição acerca do que a segurança requer naquela situação está correta, que pessoas não disputarão qual a melhor maneira de expressar o valor da segurança (a melhor concepção) ou que apenas se limitarão a dizer o que elas pessoalmente preferem promover, como se, não sendo possível a solução de dicionário, seria só questão de opinião pessoal.

Em particular, tendo em vista as maneiras como se associa hoje à noção de segurança o próprio qualificador de "direito" e a ideia de que está sendo "violado", essa saída que separa os engajamentos descritivos e normativos não está disponível para nosso empreendimento nesse trabalho. Se é verdade que em um debate como o da maioridade penal seria incomum que se alegasse que as pessoas têm um direito a que ela seja reduzida a 16 anos, nas discussões sobre

[14] Powell, *Rights as Security*, 58.

privacidade e segurança, apelações a um direito já não são tão incomuns. Se temos um direito a não sermos assassinados, por exemplo, alguém poderia dizer que o Estado deveria ter feito muito mais para prevenir homicídios como o que Marcos sofreu – providenciado instalação de câmaras em casas, submetido pessoas a testes de inclinação à violência – e, ainda, que crimes do tipo são tão graves que as instituições responsáveis por reprimí-lo não deveriam ter de passar por tantos obstáculos investigativos para encontrar e punir o responsável. Se Marcos tinha esse direito, por que não poderíamos falar em um direito à segurança que restringe privacidades para prevenir esses crimes ou para melhorar a repressão deles? Outro poderia responder que o caso é excepcional, que o Estado não tem o dever nem a prerrogativa de intervir na vida das pessoas em geral para eliminar completamente a possibilidade de ser assassinado, que a eficiência na responsabilização criminal é importante, mas não o único elemento que valorizamos – também queremos evitar acumular poder gratuitamente com o Estado e usar o orçamento público para outras atividades e políticas.

Nessas discussões, o conceito de segurança e a melhor maneira de concebê-lo é disputado: são postuladas diferentes maneiras de apresentar o valor da segurança e seu escopo. Por isso, penso que devemos tratar concepções genéricas ou abrangentes de segurança com a mesma suspeita com que tratamento a concepção "neutra" de privacidade. Por que estaria qualquer interesse que a pessoa possa ter contra sua vida, propriedade e integridade física, ou mesmo até outros objetos e bens, dentro do escopo de um direito à segurança? É essa concepção a que melhor revela seu valor? Quando dizemos que interesses em segurança trunfam interesses da população em privacidade, que sentido é esse que estamos dando a segurança e por que ele seria o correto? Na próxima seção, passo à crítica de concepções abrangentes e prioritárias de segurança, para a seguir apresentar aquela que entendo mais atraente do ponto de vista de nossas práticas e do seu potencial explicativo da articulação entre privacidade e segurança.

2 Segurança: desconstruindo um superprincípio

2.1 *O direito à segurança de Liora Lazarus*

Liora Lazarus chama o fenômeno da retórica política de dar à segurança um status de "superprincípio", especialmente impulsionado pelo atentado do 11 de setembro de 2001, de

"endireitamento" ou "direitização" da segurança ("*righting security*").[15] A autora alerta que "A narrativa do direito à segurança permite que políticos apresentem suas ações coercitivas como o correlativo necessário de um direito. Em outras palavras, buscar segurança não é meramente uma escolha política em busca de um bem público, é o cumprimento de um dever imposto ao Estado pelo direito básico de cada indivíduo à segurança"[16]. Em outras palavras, a noção de direito aí retiraria a suposição de que determinado curso de ação é uma escolha política da comunidade; passa a ser a execução de um "dever de princípio". Para Lazarus, a incorporação dessa linguagem é um recurso de "sanitização" de certas medidas estatais "menos palatáveis"[17] – buscando justificá-las pela execução de um dever jurídico correlativo a direito.

Nesse contexto, Lazarus vem discutindo o que poderia efetivamente ser o significado de um *direito à segurança.*[18] Grande parte de sua discussão é motivada por dispositivos legais que falam e reconhecem um tal direito em documentos internacionais de elevada importância para a proteção de direitos humanos: o art. 5º da Convenção Europeia de Direitos Humanos dispõe que "Toda pessoa tem direito à liberdade e segurança", por exemplo. Apesar disso, como também nos dizia Waldron, é pouco discutido. Por isso, faz questão de registrar que está particularmente preocupada em explorar um sentido de segurança não simplesmente como um ideal político, mas como um direito jurídico – do qual decorrem prerrogativas acionáveis na Justiça e obrigações de agir do próprio Estado.[19]

Em *The Right to Security* (2015), Lazarus atribui a transição das articulações de "segurança" do campo da filosofia política (como as de Hobbes e Locke) para o direito a William Blackstone na metade do sec. XVIII – em um tratado que pretendeu sistematizar a *common law*

---

[15] Liora Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", in *Examining Critical Perspectives on Human Rights*, org. Rob Dickinson (Cambridge: Cambridge University Press, 2012), 97.

[16] Tradução livre. No original: "The framing of the right to security allows politicians to present their coercive actions as the necessary correlative of a right. In other words, pursuing security is not merely a political choice in pursuance of a public good, it is the fulfilment of a duty imposed upon the state by each individual's basic right to security". Lazarus, 97.

[17] Lazarus, 106.

[18] Liora Lazarus, "Mapping The Right to Security", in *Security and Human Rights*, org. Liora Lazarus e Benjamin Goold (Oxford; Portland: Hart Publishing, 2007), 325–46; Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?"; Lazarus, "The Right to Security".

[19] O conceito de Lazarus de direito jurídico é semelhante ao de Dworkin, para quem os direitos jurídicos são aqueles que as pessoas têm de fazer valer em instituições adjudicatórias (que dão última palavra sobre direitos e deveres, como os tribunais), sem mais intervenções legislativas. Cf. Dworkin, *Justice for Hedgehogs*, 405. A autora não aparenta compartilhar, entretanto, a compreensão de que o direito é um departamento da moralidade política, nem estar claramente disposta a reconhecer que direitos jurídicos, se forem direitos fortes baseados em argumentos de princípio, exigem justificação moral, como faz Dworkin. De todo modo, como esse ponto não impede a discussão de sua concepção de um "direito à segurança" como uma concepção que pretende ser verdadeira, cabe prosseguir.

daquele período, identificando direitos e princípios nela existentes.[20] Blackstone defendeu que um "direito à segurança pessoal" se encontra entre os direitos naturais do homem e engloba um direito de proteção contra o Estado e direitos a recursos. Trata-se de um direito que protege primariamente a vida (doação do Criador) e, por consequência, proíbe que o Estado possa lançar mão de execuções capitais como meio de punição, oferece base para criminalização de homicídios e abortos, e resguarda um direito de auto-defesa. Essa proteção se estenderia a membros do corpo, aos recursos necessários à subsistência e abrange riscos à saúde e até danos à reputação.

Lazarus entende que nessa formulação de Blackstone está as raízes do debate que perdura até hoje sobre o escopo do direito à segurança. Nos nossos materiais jurídicos autoritativos de referência – leis, constituições, decisões judiciais, convenções, tratados – existiria um caráter multi-facetado da segurança – que por vezes aparece ligado à proteção contra violência física e em outras como um direito ligado à própria liberdade contra o Estado. Afinal, então, qual o conteúdo desse direito? Trata-se de um direito básico como a própria liberdade e que é muito mais do que resguardo à integridade física, como Blackstone sinalizou há séculos (e que baseava também a crítica de Waldron à concepção simples)? Lazarus discute algumas visões centrais contemporâneas – dentre as quais destaco duas.[21] Primeiro, a de Henry Shue, segundo o qual a segurança – que abrangeria segurança física contra homicídio, tortura, mutilação, estupro e agressão – é um direito básico uma vez que o gozo (*enjoyment*) dele é "essencial para todos os outros direitos". Segundo, as de Susan Fredman e Rhonda Powell, diferentes entre si, mas ambas alimentando-se de uma "abordagem das capacidades" (de Martha Nussbaum e Amartya Sen) para justificar um direito à segurança que se estenderia a uma dimensão positiva de proteção também a direitos socioeconômicos (subsistência, alimentação, saúde, moradia).

Lazarus defende que ambas as visões são enganosas e perigosas. Nos dois casos, haveria problemas[22] de vagueza sobre o escopo de direito e "duplicidade" – repetição com outros direitos

[20] Cf. Lazarus, "The Right to Security", 427–29.
[21] Lazarus, 429–33.
[22] Nas articulações abrangentes, qual seria o dever correspondente do Estado? Lazarus argumenta que assim o direito à segurança "gives rise to correlative duties for states to create the conditions in which objective risks of future threats which might reasonably cause subjective feelings of apprehension or insecurity, are minimized to a degree that allows the enjoyment of other rights". Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 100; Lazarus, "The Right to Security", 438. O problema é que (i) "A right conceived of this way is simply too broad to be legally workable": esse conceito é muito ligado a riscos futuros que não conhecemos e cujo nível aceitável para o exercício de outros direitos também não conseguimos determinar. Ademais, (ii) não parece adicionar nada ao que já precisava ser assegurado – o exercício dos demais direitos. No máximo, seria como um holograma pelo qual você

já reconhecidos. Para além disso, o erro estaria em ver a segurança como um "meta-direito" (direito que assegura direitos).[23] Na abordagem de Shue, Lazarus vê uma confusão entre um direito condicionante de fato para outros direitos e direitos que são fundantes de uma perspectiva baseada em valor.[24] Para ela, de fato, só é possível usufruir de liberdades se houver vida – sentido em que o direito à vida é condicionante de fato para outros direitos; do direito à vida em si, entretanto, não nasceria nenhuma outra noção de valor sem que se faça referência a noções como dignidade, liberdade e igualdade. Esses três direitos são, defende Lazarus, "fundantes" de uma "plataforma baseada em valor" de onde se extraem diversos outros – como o direito a não ser objeto de tortura e o direito a um julgamento justo. A segurança, por sua vez, no máximo teria um papel semelhante à vida – se só houvesse segurança no mundo e nenhum outro valor, nada dela decorreria e, se o seu papel é só ser condicionante de fato, não haveria porque falar em outro direito quando já se fala assim da vida.

O problema principal dessas abordagens, entretanto, segundo Lazarus, seria avançar a "securitização de direitos"[25]. A confusão entre fato e valor na tese de Shue e as proposições expansivas de Fredman e Powell alimentariam um tipo de visão (e de retórica política) segundo a qual a base de todos os direitos está na segurança – não na dignidade, na igualdade, nem na liberdade. Para a autora, que aqui repousa em crítica que Waldron também fez, o problema disso está no caráter "voraz" da segurança – que nos afastaria do gozo de outros direitos.[26] Se a segurança é posta na base, há uma mudança de prioridades. Além de não ser verdade que a segurança seja condicionante a tal ponto que não é possível usufruir de outros direitos (dá o exemplo de que posso votar pela manhã e ser assaltado a tarde), isso traria uma perspectiva uni-dimensional para valores. Sob o manto de que estão sendo servidos, não perceberíamos distorções quando direitos estão na

deixa sua mão passar. Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 101; Lazarus, "The Right to Security", 438.

[23] Waldron, aliás, sinalizou a existência desse debate ao lançar a "concepção pura de segurança" (*pure safety protection*) e o que entendia como a necessidade de aprofundá-la conceitualmente – como vimos, para dar conta da maneira como parece ter várias conexões internas com outros valores, para além da proteção da integridade física. Entretanto, entendo que não há coincidência entre as visões: é possível admitir que segurança é um valor conectado a diversos outros valores sem que se suponha que é um meta-direito em qualquer dos sentidos aqui. Retomo o ponto mais à frente.

[24] Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 101–3.

[25] Securitização se refere ao fenômeno discursivo de articular questões e ideias em termos de segurança. Segurança se torna a lente pela qual questões sociais, econômicas e políticas são vistas. Cf. Zedner, *Security*, 13; Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 103.

[26] Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 101; Lazarus, "The Right to Security", 439.

verdade sendo ameaçados pela segurança.[27] Essas abordagens não se dão conta do potencial (perigoso) de utilização de um "direito à segurança" com essa abrangência e centralidade para legitimar extrapolações coercitivas do estado.[28]

Não entendo que tais críticas à securitização de direitos prevaleçam: para usar uma imagem que o próprio Waldron utiliza, nosso modo de vida é um "reservatório comum de valores"[29], sendo muito provável portanto que existam conexões entre valores em dimensões muito mais próximas e profundas do que se possa querer imaginar. Esse argumento de Lazarus, portanto, não me parece em si suficiente para enxergar um problema teórico na "securitização de direitos", ainda que realmente exista; seu argumento mais parece um registro sobre um perigo político que enxerga. Há mesmo então um problema em colocar a noção de segurança na base de uma compreensão de direitos, a ponto de sugerir que o propósito da proteção deles é conferir segurança? Se essas versões que enxergam um direito básico e fundamental à segurança em uma posição central oferecerem uma boa e melhor interpretação das nossas convicções e práticas, por que não a acolher?

Entendo que as críticas de Lazarus servem de termômetro apontando que há algo de errado nessas concepções de segurança que passa por uma observação fundamental: elas não mostram qual o valor do que, nas nossas práticas, associamos ao conceito de segurança. Nós não valorizamos segurança com tamanha prioridade a ponto de transformar qualquer ameaça às nossas vidas e de outras pessoas em razão para limitar liberdades, nem aceitamos que instituições que promovem segurança o façam a todo e qualquer custo. Não valorizamos certas liberdades apenas nem ultimamente por segurança. Há indícios fortes de que um projeto que coloque segurança no centro falharia, inclusive a partir de um exemplo dado por Lazarus[30]: essa concepção do valor que associamos ao conceito de segurança não conseguiria explicar uma diversidade de práticas em que nos expomos a riscos de falhar e de comprometer não só a nossa integridade física, mas nossa subsistência, saúde e bens.

Responder ao desafio da vida de forma autêntica e responsável pode envolver profundos riscos de derrota. Pergunte isso a qualquer um que largou a universidade para se dedicar a uma start-up ou a uma banda que nunca vingou; pelo contrário, que só trouxe dívidas e prejuízo a

[27] Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 99–100; Lazarus, "The Right to Security", 439; Zedner, *Security*, 45.
[28] Também nesse sentido Zedner, *Security*, 11.
[29] Waldron, "Safety and Security", 506.
[30] Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 104.

relações pessoais. Ou a alguém que se engajou a práticas esportivas arriscadas e sofreu acidentes; ou que levou uma vida boêmia e acabou se tornando viciado em bebida. Ou mesmo a quem se voluntaria a lutar em uma guerra. Ainda, ser capaz de exercer certas liberdades com frequência está atrelado a certos níveis de riscos – ainda que busquemos mitiga-los e leva-los a níveis razoáveis: dirigir, voar de avião, fazer trilhas na selva, submeter-se a tratamentos médicos experimentais. "Segurança" não parece justificar nossas práticas a nível fundante porque é incapaz de explicar como somos capazes de acomodar liberdades que ameaçam nossa integridade física e nossa subsistência.

De igual modo, essas concepções de segurança não mostram como dirigimos nossas expectativas em torno da atuação do Estado para a segurança com essas mesmas nuances: a de que comportamos certos níveis de risco a nossa vida e ao gozo de direitos desde que sejam necessários para o exercício e a preservação de liberdades fundamentais que valorizamos, e que a razão que apoia ações de uso da força do Estado, inclusive pela segurança, pressupõe um compromisso com as pessoas enquanto pessoas que merecem consideração e respeito. É claro que queremos exercer direitos de forma segura, mas o que dá intencionalidade à segurança que buscamos sobre o exercício desses direitos é o valor deles; não o contrário.

A liberdade pessoal – e particularmente os diversos direitos especiais de liberdade que prezamos – seria bem diferente (e possivelmente bastante limitada) se tivesse como fundamento uma concepção de segurança física ou de subsistência com essa prioridade. Se o Estado nos mantivesse presos dentro de quartos em centros residenciais e apenas nos alimentasse e checasse nossa saúde diariamente, provavelmente eliminaria riscos à nossa integridade física e subsistência com enorme eficiência, mas ao custo de eliminar todo sentido do que é ter uma vida que é própria e bem vivida. Como, ao contrário do exemplo radical, nos importamos com outros valores e, para gozar de certas liberdades, comportamos certos riscos à nossa integridade física e até à subsistência, não faria sentido que exigíssemos, muito menos que o Estado pudesse se reportar para basear suas ações, a um sentido de direito à segurança tão abrangente.

Isso vale também para iniciativas de combate ao crime. Se rotineiramente estivéssemos sujeitos a testes e avaliações da polícia para prevenção de crimes, e se o Estado controlasse tudo o que fizéssemos dentro e fora de casa, para garantir que terá provas para punir toda conduta criminosa, isso talvez diminuísse índices de criminalidade e diminuiria a impunidade. Mas valorizamos segurança a esse ponto? Medidas dessa escala fazem mesmo parte do nosso direito à

segurança? Nosso modo de vida seria diferente: a começar porque o significado disso não é só desencorajar e garantir responsabilização por condutas que pessoas não tem o direito de praticar (crimes), mas implementar uma medida de controle e desconfiança generalizada. Mesmo que o Estado não tenha razões para confiar que pessoas não estão tramando crimes ou queira garantir eficiência na apuração de condutas criminosas, tampouco tem desde logo razões para desconfiar de pessoas nem razões para acumular esse nível de controle sobre todos os cidadãos desnecessariamente, de sujeita-los a riscos de abuso, erro e excesso, ou exigir que pessoas prestem conta de tudo o que fazem, sem que haja motivos concretos razoáveis ou se tenha dado razão para desconfiança. Nesse sentido, se há um espaço para a segurança entre nossos valores, ele não parece ser fundante e prioritário nesse sentido.

Essas considerações servem também para afastar compreensões de um "direito à segurança" ou "princípio da segurança" que seja trazido a exercícios de "proporcionalidade" e "ponderação" com outros direitos vinculado a noções abrangentes de segurança ligado a todo tipo de "interesse" em segurança que possa existir, desconectado de um empreendimento voltado a compreender se e de que modo a segurança em questão é valiosa. Nessa concepção, proteger direitos como a privacidade em face do Estado é, em geral e por definição, "perder" segurança. Uma restrição a um direito à segurança que passa por ponderação. Mas se não valorizamos a segurança per se e com essa prioridade, por que essa deveria ser nossa concepção? Como já se via no capítulo 1, mesmo nossas expectativas quanto à polícia e práticas voltadas à segurança que esperamos do Estado não são acontextuais: queremos que o Estado ajude em emergências, diante de riscos concretos, esperamos que investigue e de algum modo puna corretamente quem cometeu crime, mas não que mobilize suas forças contra a vida de certas pessoas sem que os afetados tenham dado alguma causa, sem prestar contas e observar qualquer salvaguarda.

Se há um direito à segurança, seu sentido não é abrangente a ponto de absorver qualquer interesse abstrato e hipotético de alguém sobre sua vida; não são essas articulações que melhor revelam seu valor. Que espaço ocupa então a segurança entre nossos valores? Qual formulação então poderia ser a desse conceito que melhor capturasse seu valor?

As objeções e receios de Lazarus sobre segurança como um superprincípio a levam a defender que um direito à segurança e, por correlação, o dever do estado de dar segurança esteja sempre bem claramente delimitado – no final das contas, como ensinou Locke, deve conter ainda

uma proteção contra o próprio Estado.[31] Nesse sentido, sugere que o direito à segurança e o dever estatal correlativo deva significar apenas "o desenvolvimento de estruturas e instituições capazes de responder e minimizar 'ameaças críticas e generalizadas' à segurança humana, nomeadamente ausência de dano no sentido físico mais central de dano à pessoa. É importante ressaltar que o direito à segurança deve estar alicerçado na dignidade, igualdade e liberdade, e não o contrário."[32].

Como se vê, Lazarus parece sugerir uma espécie de "direito jurídico a uma regulação pública", à estruturação de instituições e adoção de políticas voltadas ao resguardo da segurança física das pessoas. Esse modo de conceber um "direito à segurança" – e que ainda seria baseado em concepções de dignidade, liberdade e igualdade, segundo aponta – me parece atraente de ser melhor explorado: nós esperamos que o Estado implemente certas políticas para promover a segurança das pessoas, ao mesmo tempo em que isso não significa ter e poder impor regime de proteção absoluta à vida. Esse uso da força tampouco pode representar uma ameaça à dignidade das pessoas; a intencionalidade do uso da força e dos freios que a contém é garantir dignidade das pessoas. Como Lazarus não desenvolve essa conexão, de algum modo sua ênfase remanescente em segurança física ainda lembra a "concepção pura" de segurança. Para destrinchar mais a segurança que nasce de um compromisso com a dignidade, faço isso na próxima seção, a partir da teoria da justiça de Ronald Dworkin.

2.2 *Segurança e dignidade*

Ainda no capítulo 1 tratei de como o Estado deve atuar com igual consideração e respeito aos cidadãos como contrapartida necessária ao seu uso da força, para a legitimidade do Estado. Lá já apontava como isso coloca deveres de cuidado com relação a direitos à privacidade. Agora chegamos a esse ponto a partir da análise do conceito de segurança: o Estado deve dedicar esforços para garantir certa segurança sobre o gozo de direitos morais. Acredito que não demoraríamos a dizer que o Estado que permitisse o crime avançar a ponto de que se tornasse quase impossível sair de casa sem ser vítima de violência está falhando em resguardar um direito à segurança. Nessa

[31] Lazarus, "The Right to Security", 434.
[32] Tradução livre. No original: "the development of structures and institutions capable of responding to and minimising 'critical and pervasive threats' to human safety, namely absence from harm in the most central, physical sense of harm to person. Importantly, the right to security must be grounded in dignity, equality and liberty, and not the other way round". Lazarus, "The Right to Security: Securing Rights or Securitizing Rights?", 106.

mesma linha, o Estado que obrigasse pessoas a ficar em casa em nome da segurança também estaria indo muito além do valor que efetivamente damos a esse direito.

Nesse contexto, a regulação nessa matéria deve ser adequada no sentido de que leis e políticas que a compõem deverão ser compatíveis –"pessoa por pessoa"[33]– com os dois direitos políticos mais abstratos de que somos titulares enquanto membros de uma comunidade política: devem tratar os destinos de cada um como igualmente importantes e respeitar as responsabilidades de cada um sobre suas próprias vidas – o princípio do valor intrínseco (ou autorrespeito), pelo qual cada vida é objetivamente importante, e o princípio da responsabilidade pessoal, que vimos no capítulo anterior. Um Estado deve, portanto, mobilizar suas instituições – notadamente o Poder Legislativo – para que atenda a essa exigência básica: aprove leis e implemente políticas que ofereçam uma interpretação razoável desse esforço de atender à dignidade nessa dimensão da segurança. Ter um programa de segurança pública e instituições voltadas a promovê-lo.

Uma característica imprescindível dessa regulação é que ela reconheça direitos morais que devemos uns aos outros no seguinte sentido: estabeleça normas como as de direito penal e de direito civil que reconheçam a incorreção moral de práticas que violem a "imunidade moral contra dano deliberado de outros"[34] – tipo de conduta que fere a responsabilidade pessoal de cada um sobre o curso de suas vidas e, portanto, viola a dignidade devida a toda pessoa.[35] A responsabilidade pessoal requer e justifica uma decisão política do Estado de exercer coerção sobre quem fira tal imunidade.[36] O nível de imunidade relativo a liberdades sobre *o que se faz* com o corpo e bens encontra limite na responsabilidade de outras pessoas e deve em si ser objeto de ajuste regulatório.[37] O nível mais básico de controle sobre a vida e integridade física, por sua vez, não precisa passar por esse mesmo tipo de acomodação regulatória – deve ser respeitado como condição necessária da dignidade.

Nesse sentido, o direito moral e político à segurança está fundado na dignidade e consiste

[33] Dworkin, *Justice for Hedgehogs*, 330–31.
[34] Dworkin, 288.
[35] Dworkin, 288.
[36] Nesse sentido, ver também Dworkin, *Taking Rights Seriously*, 94.
[37] Dworkin, *Justice for Hedgehogs*, 469. "Indeed, our assignment responsibility requires more than this minimum. You must have substantial control over what your body does – where you can take it and what you can use it to do – as well. That further control responsibility must be limited, however, to protect the control responsibility of others over their lives: you must not have control responsibility that would include damaging me or my property, for instance. So the criminal and tort law of any morally sensitive community will require fine adjustments. But the most basic level of control responsibility, over what happens to your body, does not need to be limited and has therefore been treated as a necessary condition of dignity."

em um direito à uma regulação pública nessa matéria. Ela deve conter proteções especiais à vida, à integridade física e à propriedade e algum sistema de responsabilização civil, administrativa e penal por danos que qualquer um venha a infligir sobre esses bens – inclusive autoridades estatais. Por essa perspectiva inclusive se vê como o poder coercitivo estatal é irremediável e necessário: "O governo coercitivo coletivo é essencial para nossa dignidade. Precisamos da ordem e das eficiências que somente um governo coercitivo pode fornecer para que possamos criar uma vida boa e viver bem."[38]

Esse direito à segurança, por outro lado, não poderia incluir nem significar um direito absoluto a ser garantido a qualquer custo – mas um esforço do Estado de manter ameaças à vida, à integridade, à propriedade e a outros dos nossos "recursos" por direito em níveis razoáveis. Esse nível não é preto no branco, não é universal, nem é resultado de "ponderação" de interesses – é, de novo, contextualmente definido em face dos riscos, resultado de um esforço de reconstrução conceitual, de interpretação de nossas práticas e do que valorizamos, do nosso modo de vida presente (e dos níveis de risco que nossa comunidade tolera). Nesse sentido, a regulação pública de segurança contempla e deve respeitar a proteção a liberdades que valorizamos – algo que já vimos ao tratar de privacidade; a regulação da segurança deve mostrar respeito a elas, evitando riscos e abusos, incorporando mecanismos regulatórios que atendam a lógica de contenção desses vícios e de fundamentação do exercício da força.

Muito embora as pessoas tenham um direito político a essa regulação, de modo que a mobilização por um arranjo possa ser sustentado por um argumento de princípio (de um direito moral básico), os moldes concretos dessa regulação é uma questão de política: o objetivo geral que ela recomenda é o que vimos – tratar cada cidadão e permitir que viva com dignidade; cada dispositivo de lei e políticas sociais voltadas a realizar esses compromissos básicos de segurança das pessoas sobre sua vida, integridade física e propriedade deve ser testado sobre o seu mérito quanto à promoção desse objetivo. Na frente de ameaças a esses bens que é foco nesse trabalho,[39] a criminalidade, discute-se vivamente como melhor fazer isso: que segurança pública não envolve

[38] Tradução livre. No original: "Collective coercive government is essential to our dignity. We need the order and efficiencies that only coercive government can provide to make it possible for us to create good lives and to live well." Dworkin, 320.

[39] Fosse o meu tema mais abrangente, poderia estar discutindo as possibilidades de ação do estado em nome de *segurança em saúde* para vigilância epidemiológica – e como conciliar tais pretensões com o direito à privacidade e à proteção de dados pessoais. Suspeito que a estrutura da discussão fosse em grande parte semelhante, como cheguei a explorar em outro trabalho.Jacqueline de Souza Abreu, "Privacidade, proteção de dados pessoais e crises epidemiológicas: racionalidades e lições da pandemia", *Internet & Sociedade* 3 (1º de julho de 2021): 5–26.

necessariamente ampliação de *policiamento* (engajamento policial) e encarceramento, mas também estratégias estatais de auxílio social (em educação, moradia, saúde, trabalho) que reduzam desigualdades, por exemplo.[40]

Ninguém tem o *direito político* (um direito moral em face do Estado) *de exigir* que uma ou outra medida seja adotada desse ou daquele jeito porque assim será mais beneficiado em termos de sua segurança pessoal e da sua propriedade, por exemplo. Não há argumento de princípio que funde essa exigência; a regulação é uma questão política.[41] No exemplo mais geral que comecei: as pessoas podem ter um interesse em ver a maioridade penal reduzida, mas isso não significa que possuem um direito de exigir e ver resguardadas essas providências como parte de seu direito moral à segurança. Para aproximar mais o exemplo: as pessoas podem ter *interesses* de segurança que incluam haver um posto da polícia em sua rua ou a instalação de câmeras em seu bairro, mas elas não possuem um *direito* moral a tanto a ponto de poder exigir isso do Estado.

Assim, parece-me que, inserido na Constituição Federal, um "direito social à segurança" é, no que tem de direito jurídico, algo muito próximo ao que Liora Lazarus defendeu: o que se pode exigir judicialmente é que uma regulação exista (não haver completa omissão estatal) – da forma que a comunidade no Legislativo vier a aprovar e que se revele um esforço compatível com a dignidade.

2.3 *Características necessárias da regulação em matéria de segurança*

O conteúdo e o modelo dessa regulação não é nem será aqui todo especificado, mas há características que deve observar de novo em respeito à dignidade e ao princípio igualitário. Nessa regulação, como visto, deve haver espaço para a proteção da imunidade moral básica – proteção do direito à vida, do direito à integridade física, do direito à propriedade – contra danos deliberados[42]. Mas não de qualquer jeito: é importante que a regulação dê conta da importância das conexões internas da segurança com outros valores. Como Waldron alertou, nós não queremos

[40] Para usar um exemplo recente: Adilson Paes de Souza, "PM aposentado conta assalto e sequestro que sofreu e critica políticas de segurança", *Folha de S.Paulo*, 22 de janeiro de 2022, https://www1.folha.uol.com.br/ilustrissima/2022/01/pm-aposentado-conta-assalto-e-sequestro-que-sofreu-e-critica-politicas-de-seguranca.shtml.
[41] Dworkin, *Law's Empire*, 310–11.
[42] Dworkin, *Justice for Hedgehogs*, 288.

apenas sobreviver, mas viver. Precisamos do Estado com poder coercitivo para poder viver – e bem. E por isso faz parte de uma concepção atraente de segurança aquela que inclua leis e políticas que busquem resguardar e que sejam conciliadas com liberdades – nosso modo de vida: o ajuste fino (e disputado) é o quanto da regulação para guardar liberdades não passa a tolher liberdades. Os ajustes estão profundamente relacionados com o tipo de Estado que queremos, que comunidade somos e que valores queremos exibir. Mais a frente, olho para o caso brasileiro no que se refere a essa acomodação da regulação de segurança com a privacidade.

O direito responde e mostra reconhecimento a esses direitos e valores com institutos como os de responsabilização criminal, administrativa e civil, muitos baseados em argumentos de princípio – proteção do direito à vida, do direito à integridade física, do direito à propriedade, etc, mas não exclusivamente. A decisão sobre como essa proteção é feita é, cabe notar, uma decisão política sobre como melhor proteger esses direitos e valores. Nesse contexto, é possível imaginar situações em que o Estado falha miseravelmente em seu dever de proteger até a imunidade básica: sem instituições policiais básicas, talvez alguém dissesse que haveria violação a um direito de ser tratado com igual consideração e respeito por uma regulação pública na área de segurança e que é fundamental à própria legitimidade do poder pelo Estado. Esse seria um marco negativo comprometedor.

Nesse contexto podemos inserir o "direito social" à segurança no art. 6º e a arquitetura institucional prevista no art. 144 sobre "segurança pública" na Constituição Federal. Tais dispositivos supõem a implementação de políticas públicas voltadas à segurança. Leis e as políticas de segurança de um país devem ser instituídas e revisadas para refletir interpretativamente uma tentativa real, mesmo que falha no final das contas, de respeitar a dignidade daqueles que estão em seu poder. Isso inclui promover a segurança contra o dano grave e deliberado de terceiros – atividades criminosas. Faz parte de um "direito a uma atitude" que deve ser observado minimamente para a legitimidade política: "um direito a ser tratado como um ser humano cuja dignidade fundamentalmente importa".[43] O "mínimo existencial" do qual se poderia falar nessa área se volta às noções mais básicas de proteção ao direito moral, de proteção da imunidade básica.[44] Estado não precisa nem deve parar no básico; pelo contrário, como já se viu. A

[43] Dworkin, 335.

[44] Nessa linha, no que já admitiu de pleitos que envolvam "direito à segurança", o STF trata apenas de casos de completa inadimplência de políticas públicas previstas e de "violação generalizada". Ver, por exemplo, Supremo Tribunal Federal, RE 559646 AgR, Rel. Min. Ellen Gracie, Segunda Turma, j. 07.06.2011, DJE 24.06.2011:

concretização deles, no entanto, depende de nova decisão política no Legislativo.

E o que freia até onde essa política de segurança pode chegar? Uma interpretação dos valores da nossa própria comunidade. Se valorizamos a autenticidade e o autorrespeito (enquanto aspectos da dignidade), a regulação pública deve proteger com essa dignidade, deve promover condições de uma vida bem vivida, mas – ao fazer isso – não pode violar esses mesmos princípios. Nesse sentido, a regulação em si deverá ser compatível com o princípio igualitário também em outros aspectos. Ela importa uma vedação a prejuízos deliberados a certos grupos de pessoas, ainda que variações nos modos como as pessoas se beneficiam da política de segurança sejam de início possíveis por questão de política – como melhor promover segurança sobre vida, integridade física e propriedade como um todo.

A começar, vale uma observação sobre exigências de um tratamento como igual. Na linha de Waldron, o modo como essa política deve ser implementada com relação à população como um todo, sua distribuição, deve estar sensível ao "fator de impacto": uma regulação/política social que afetasse *negativamente* especialmente um grupo de pessoas não poderia ser compatível com a igual consideração e respeito. Nesse sentido, há violação a um *direito* quando o Estado não faz uma distribuição igualitária dos seus esforços de segurança – deixa de contemplar regiões pobres em estratégias de segurança ou direciona incursões apenas para elas, por exemplo. Pessoas que são indevidamente tratadas de forma distinta por políticas de segurança e que comportam os ônus delas por uma caraterística inerente à sua identidade podem questioná-las, e devem ser capazes de derrubá-las, por questão de princípio. Mais fundamentalmente, quando *uma* pessoa se vê alvo de mobilização das estruturas do Estado-penal, é importante que haja uma razão para que o dano causado à sua responsabilidade pessoal sobre sua vida possa ser justificado como legítimo – possa

---

"DIREITO CONSTITUCIONAL. SEGURANÇA PÚBLICA AGRAVO REGIMENTAL EM RECURSO EXTRAORDINÁRIO. IMPLEMENTAÇÃO DE POLÍTICAS PÚBLICAS. AÇÃO CIVIL PÚBLICA. PROSSEGUIMENTO DE JULGAMENTO. AUSÊNCIA DE INGERÊNCIA NO PODER DISCRICIONÁRIO DO PODER EXECUTIVO. ARTIGOS 2º, 6º E 144 DA CONSTITUIÇÃO FEDERAL. 1. O direito a segurança é prerrogativa constitucional indisponível, garantido mediante a implementação de políticas públicas, impondo ao Estado a obrigação de criar condições objetivas que possibilitem o efetivo acesso a tal serviço. 2. É possível ao Poder Judiciário determinar a implementação pelo Estado, quando inadimplente, de políticas públicas constitucionalmente previstas, sem que haja ingerência em questão que envolve o poder discricionário do Poder Executivo. Precedentes. 3. Agravo regimental improvido." Mais recentemente, Supremo Tribunal Federal, ADPF 635 MC RJ, rel. Min. Edson Fachin, Tribunal Pleno, j. 18.08.2020: "A violação generalizada é a consequência da omissão estrutural do cumprimento de deveres constitucionais por parte de todos os poderes e corresponde, no âmbito constitucional, à expressão "grave violação de direitos humanos", constante do art. 109, § 5o, da CRFB. (…) Não cabe ao Judiciário o exame minudente de todas as situações em que o uso de um helicóptero ou a prática de tiro embarcado possa ser justificada, mas é dever do Executivo justificar à luz da estrita necessidade, caso a caso, a razão para fazer uso do equipamento, não apenas quando houver letalidade, mas também sempre que um disparo seja efetuado."

ser interpetrado como punição a uma conduta sua ou, ao menos, e antes disso, como uma investigação que minimamente faça sentido de ser conduzida contra si, à luz de nossas práticas e expectativas sociais. Trata-se, no final das contas, de aplicação do princípio do autorrespeito.

Como adiantei, a regulação pública em matéria de segurança deve ser também compatível com outros direitos políticos derivados da dignidade. Embora seja verdade que gostaríamos que alguém interviesse para impedir que um plano concreto de assassinato contra nós seja levado a cabo e que um direito à segurança sobre nossa vida parece ser acionado nessas circunstâncias, isso não poderia significar que temos direito a que um policial ande ao nosso lado a todo tempo, nem que todos os ambientes em que transitamos e tudo o que fazemos precise e deva ser vigiado. Se o risco desse assassinato é concreto e imediato contra pessoas específicas e chega à atenção da polícia, esperamos que tome providências possíveis para o interromper pois nessas circunstâncias passa a ser um risco *concreto*. Mas a possibilidade abstrata que isso ocorra a qualquer um não chega a tanto. Nós temos um direito à proteção regulatória que promova medidas que mantenham os riscos à vida e à integridade física dentro do razoável, mas não a uma proteção absoluta.

O risco em que incorremos por não ter essa vigilância total é parte daquilo que abrimos mão para dizer que vivemos com liberdade, que o Estado não é um que tem controle sobre tudo, que há outras políticas a serem promovidas, com o orçamento que seria gasto, em áreas que também consideramos importantes. Assim, em uma situação de normalidade social (sendo "normal"[45] um cenário que inclui a ocorrência de crimes, e que contrastaria com um cenário de guerra), uma lei que condicionasse o exercício de privacidade sobre o lar ao uso de câmeras pelo seu potencial puramente especulativo ou marginal de ser utilizado para cometer crimes não poderia compor a realização de um "direito à segurança" – na verdade, no máximo promoveria interesses genéricos em ganhos em segurança, que o nosso *direito* à privacidade do lar trunfa.

Se possível, gostaríamos que episódios como o de Elize Matsunaga fossem evitados; mas não a ponto de admitir que toda casa seja vigiada nem que as pessoas sejam perfiladas para supostamente descobrir se possuem tendências biológicas ou sociais de se envolverem em atividades criminosas. Ainda que a finalidade seja moral e a princípio legítima, isso causaria um

[45] Eu me reporto aqui a noções de "normalidade" discutidas em Macedo Junior, *Contratos Relacionais e Defesa do Consumidor*, 60–66. A partir da obra de Émile Durkheim, o autor exemplifica que o comportamento criminoso não é anormal – não existe sociedade em que não exista por completo. Seria "anormal" uma sociedade assim. Aquilo que constitui a "normalidade" é criado pela sociedade, não imposto de cima para baixo (p. 66). Nessa linha, "o normal, assim, define-se sempre relacionalmente, isto é, em comparação com outras médias históricas ou locais" (p. 61).

dano sério ao exercício do direito, porque basicamente anularia a possibilidade de exercício de uma prerrogativa de privacidade sobre o lar que valorizamos; haveria acúmulo de poder com o Estado – suscetível de riscos, abusos e erros – quando uma razão concreta para esse tratamento sequer tenha se apresentado e a implementação seria sobremaneiramente excessiva às necessidades, além de ser perturbador e causar efeitos inibidores ao exercício mesmo de outras liberdades protegidas. Há algo semelhante a isso no exercício da liberdade de expressão: uma lei que criminalizasse discursos políticos pelo seu potencial meramente especulativo de causar violência não seria compatível com a liberdade de expressão.[46] Muito embora o Estado tenha o dever de resguardar pessoas contra a violência, o risco deve ser presente e iminente para justificar restrição a outro direito forte.[47] Essa noção de "nível de risco à segurança" que desencadeia e justifica ação do Estado é objeto de diversos esforços de tradução em estudos dogmáticos no direito e, com o avanço da tecnologia, de desafios regulatórios. Voltarei a isso mais à frente.

Essas noções também terminam por aprofundar o capítulo 1 sobre privacidade e a mostrar como a concepção de segurança apresentada aqui se reconcilia com o visto lá. Em sua dimensão positiva, direitos à privacidade impõem ao Estado uma regulação de segurança que também resguarde esses direitos: proíba violações a eles, prevendo responsabilização a quem deixar de respeitá-los – como fazemos no direito penal e no direito civil; da concepção de segurança não faz parte qualquer prerrogativa que impeça o exercício dessas privacidades valiosas. Em sua dimensão negativa, por outro lado, direitos à privacidade oferecem um argumento de princípio contra certas regulações públicas de segurança que interfiram indevidamente neles – o que impõe a construção e implementação de arranjos regulatórios que deem *segurança* ao exercício desses direitos contra

[46] Dworkin, *Taking Rights Seriously*, 93;195;202. Diante dessa analogia, ressalvo que Jeremy Waldron, recuperando suas noções de *assurance* de que falei ainda no início do capítulo, defenderá que ela comporta a possibilidade de proteção contra certos tipos de discurso de ódio que negam um tratamento com dignidade a seus alvos e que contibuem para um ambiente de tratamento discriminatório em interações sociais. As pessoas teriam direito a se asseguradas contra esse tipo de discurso. Ver Jeremy Waldron, *The Harm in Hate Speech*, Reprint edição (Cambridge: Harvard University Press, 2014). A posição a que me refiro aqui é mais contida: só proibe/barra discurso diante de *clear and present danger.* Os problemas da visão de Waldron foram tratados por Clarissa Gross em Gross, "Pode dizer ou não? Discurso de ódio, liberdade de expressão e a democracia liberal igualitária". Em síntese que não faz jus à profundidade de seu trabalho, uma defesa de *assurance* nesses termos e magnitude importaria termos de banir diversos elementos da cultura popular e até política que leva a esses efeitos de injustiça social no ambiente social. Embora não vá expandir o ponto aqui para contemplar sua argumentação nesse livro e no que seria relacionável, suspeito que defender uma concepção de direito à segurança que inclua os sentimentos de medo das pessoas e perigos abstratos em igual medida também levaria a termos de encerrar e descaracterizar diversas interações e atividades sociais para anular o risco de dano que alguém pode causar ao outro. Isso impediria o exercício de diversas prerrogativas de privacidade, como no exemplo hipotético usado no parágrafo.

[47] Dworkin, *Taking Rights Seriously*, 202–4.

abusos e arbitrariedades, sem danos sérios ao seu exercício e de forma congruente com a relevância de um direito moral; da concepção de privacidade não faz parte um direito que impeça o Estado de promover a segurança nesses termos.[48] Se o arranjo regulatório de segurança pública confere prerrogativas ao estado de se imiscuir em liberdades, entre elas em práticas de privacidade, deve fazer de modo a não lhe conferir poder excessivo e de modo a conter riscos e ameaças indevidas – como intrusões arbitrárias ou motivadas por razões éticas (sobre quem a pessoa é ou no que acredita) – a direitos, riscos e ameaças de causar dano moral. A regulação, como já dizia no capítulo anterior, deve conter o poder do Estado e mostrar respeito ao cidadão.

Antes de fazer a transição mais concreta a como embutimos limites de princípio na atuação do estado pela segurança que envolve medidas de vigilância, vou primeiro revisitar fundamentos do Direito Penal, do Direito Processual Penal e do Direito Administrativo e como essas práticas jurídicas incorporaram e manifestam noções do valor de segurança e como ele próprio se adapta a diferentes contextos. Entendo que a compreensão de segurança imbricada com a dignidade aqui oferecida é capaz de trazer luz à fundamentação teórica dessas áreas do direito, ao mesmo tempo em que servirá de norte para enfrentar problemas novos que categorias dogmáticas já não conseguem alcançar.

3 Segurança no direito

3.1 *Segurança, polícia e justificação da coerção estatal pelo direito*

Na última seção, vimos que o Estado deve às pessoas o desenvolvimento de uma regulação pública que se dedique a promover a segurança das pessoas. Disse então que o direito à segurança é antes de tudo um direito político a uma regulação pública – adoção de leis e políticas – nessa matéria. Ao mínimo, essa regulação deve resguardar direitos básicos de imunidade moral de indivíduos (à vida, integridade física e propriedade). Como isso será feito é, friso, uma decisão política de *policy* sobre qual a melhor maneira de se proteger direitos de cidadãos. Não é diretamente claro como o dever de proteção de direitos pelo Estado por meio de uma regulação pública em matéria de segurança exija necessariamente algo como o direito penal que conhecemos hoje, senão a partir de uma noção de que em algum momento se entendeu que essa é uma boa

[48] Cf. também Barry Friedman, *Unwarranted: policing without permission* (New York: Farrar, Straus, Giroux, 2017), 407.

política para a prevenção de ofensas que sejam reconhecidas como crimes.

Nessa parte, vou relacionar as noções que exploramos até aqui – particularmente de "direito à segurança" enquanto direito a uma regulação – propriamente com o direito e nossas práticas jurídicas que envolvem esse conceito. Tendo em vista que esse trabalho se ocupa principalmente com uma parte específica e possivelmente a mais focal da regulação estatal em matéria de segurança pública – as razões que podem justificar a atuação estatal (principalmente *policial)* no combate ao crime, isto é, suas prerrogativas no exercício dessa atividade –, vou concentrar meus comentários sobre a atuação policial que orbita em torno do que chamamos de "direito penal". Como veremos, ela está comprometida por princípio com a contenção do poder estatal.

Uma parte significativa da atuação policial, e densamente regulada pelo "direito processual penal", é aquela *ex post facto* voltada à responsabilização criminal: trazer aqueles que praticaram um crime à Justiça – "restabelecendo-se" a ordem. Para tanto, no cenário brasileiro e à luz do art. 144 da Constituição Federal, temos toda uma estrutura de polícia judiciária (principalmente as Polícias Civil e Federal) para investigação de atividades criminosas com vistas a instruir inquéritos policiais e processos penais e apoiar a Administração da Justiça na execução de mandados de busca, mandados de prisão, conduções coercitivas, por exemplo.

Há também, por outro lado, o esforço policial voltado a resistir à conduta criminosa *ex ante,* isto é, evitar que ela ocorra. Atividade de "poder de polícia" no sentido mais clássico que o termo poderia ter no direito administrativo, essa área de atuação dos órgãos policiais (e de outras estruturas da Administração Pública) é bem menos regulada por lei. No cenário brasileiro e à luz do art. 144 da Constituição Federal, essa atividade está simplesmente inserida na noção abrangente de "preservação da ordem pública", de onde se extraem diversas prerrogativas do Poder Público de atuar em nome da segurança. Ao lado delas, e de forma mais concreta, Polícias Militares estaduais e a Polícia Rodoviária Federal devem se dedicar ao "policiamento" e "patrulhamento" ostensivo, respectivamente – em que "o seu agente identificado de plano, na sua autoridade pública, simbolizada na farda, equipamento, armamento ou viatura"[49] apresenta-se à vista para a população com propósito primordialmente preventivo, sem prejuízo da repressão imediata a infrações. Também contempla a atuação da Polícia Federal na prevenção ao tráfico de drogas, contrabando e descaminho, nos termos da Constituição.

[49] Álvaro Lazzarini, "A ordem constitucional de 1988 e a ordem pública", *Revista de Informação Legislativa* 115 (1992): 291.

A separação que é comumente feita para diferenciar as duas atividades é entre *polícia judiciária ou repressiva* e *polícia administrativa ou preventiva.*[50] De fato, a nomenclatura dá ênfase para as características preponderantes e mais marcantes de tais atuações. Há que se observar desde logo o que essa distinção não significa, por outro lado. A diferença não é institucional: polícias militares podem ter atuações pós-delitivas e polícias civis podem ter atuações pré-delitivas, de inteligência, por exemplo, de modo que um mesmo órgão pode se engajar em ambas as atividades.[51] Tampouco se poderia dizer que a atuação da polícia judiciária não tenha finalidade ou impacto preventivo; ou que a polícia administrativa não colabore na repressão a condutas criminosas – fazem, aliás, a atuação imediata. Ademais, volto a registrar que não quero reduzir toda a regulação pública em matéria de segurança à atuação da polícia: entre as medidas de polícia administrativa podem se inserir diversas outras políticas estatais que independem da instituição *polícia* propriamente dita para o tratamento da ocorrência de crimes.

Mas "nem por isso, no plano da natureza intrínseca da função, deixa de se estabelecer uma sensível diversidade entre a ação policial repressiva e o poder de polícia do Estado."[52] "Cada uma dessas espécies intervém em determinados momentos e tem os respectivos raios de ação."[53] Mesmo abstraindo de qual polícia, qual órgão faz, essas discussões e distinções se reportam ao fato de que há diferenças relevantes nesses modos de atuação e em como o Estado é autorizado a agir neles, porque os contextos são diferentes. Já vimos pelos exemplos que usei até aqui: o que a polícia rodoviária que parou Elize podia fazer é diferente do que a polícia civil pode a partir do momento em que se tornou suspeita de crime. Vale aprofundar mais o ponto para identificar as nuances dessas justificativas em cada contexto.

Nossa doutrina jurídica, ao longo do tempo, traduziu expectativas, pressupostos e questões normativas de contextos diferentes da atuação do Estado pela "segurança" em diferentes saberes jurídicos dogmáticos que ganharam autonomia: para além do próprio "Direito Penal", e de como se diferencia do Direito Privado, por exemplo, diferenciamos também o "Direito Processual Penal" e o "Direito Administrativo". Há também, embora não trate aqui, o Direito Militar ou o Direito da

[50] Caio Tácito, "O poder de polícia e seus limites", *Revista de Direito Administrativo* 27 (1952): 10; José Cretella Júnior, "Polícia e poder de polícia", *Revista de Direito Administrativo* 162 (1985): 14; Lazzarini, "A ordem constitucional de 1988 e a ordem pública", 280.
[51] Cf. Lincoln D'Aquino Filocre, *Direito Policial Moderno* (São Paulo: Almedina, 2017).
[52] Tácito, "O poder de polícia e seus limites", 10.
[53] Cretella Júnior, "Polícia e poder de polícia", 14.

Inteligência[54]. Esses destacamentos são indícios de que o conjunto de ações que governam possuem uma lógica e intencionalidade que permite alguma distinção.

Sob certa perspectiva, o mais natural seria contrapor Direito Penal e Direito Administrativo, enquanto duas áreas de direito material do Direito Público que compartilham a associação ao dever/tarefa de "preservação da ordem pública", mas que passaram por diferenciação entre si e possuem natureza distinta de um direito "auxiliar" ou "adjetivo" como o Processual Penal. De fato, entendo que institutos de Direito Penal e Direito Administrativo identificam princípios e regras jurídicas que são mobilizados pelo Poder Público para promover a regulação pública em matéria de segurança de que tenho falado – enquanto conjunto de medidas que compõem a estratégia de um Estado para lidar com os problemas – comportamentos – mais graves que a sociedade quer combater.

Quero, entretanto, chamar atenção a uma outra diferenciação que acaba caracterizando o destacamento desses diferentes ramos da prática jurídica – entre (i) intervenções estatais policiais de ênfase *repressiva, ex post facto*, concretas e individualizadas em processos penais, (ii) intervenções estatais policiais de ênfase *preventiva e repressiva* em reação a situações de perigo concreto e imediato com vistas a evitar ou controlar o alcance do dano; e (iii) medidas estatais gerais, de impacto coletivo, antecedentes a e independentes de processos criminais no combate à criminalidade contra perigos abstratos. A situação (i) se insere no que conhecemos por Direito Processual Penal, ao passo que (ii) está já na fronteira com o Direito Administrativo e (iii) inserto nele.

As divisões entre ramos do direito promovem certa previsibilidade sobre a aplicação de um princípio dentro de um conjunto de casos e também estimulam uma atitude de protesto quando casos se afastam desses princípios que seriam aplicáveis a tais limites práticos.[55] Quando as linhas entre o que é atuação repressiva e o que é atuação preventiva se borram ou as atividades preventivas se expandem – um fenômeno que está muito associado ao avanço tecnológico, como veremos –, o esforço de estabilização da dogmática nessas áreas sofre abalos. Isso afeta a justificação da atuação estatal e convida à avaliação de se estamos pondo a perder valiosos

[54] Chamo de Direito da Inteligência o direito aplicado a atividades de inteligência. Por exemplo, a Revista Brasileira de Inteligência, publicada pela Agência Brasileira de Inteligência (ABIN), é repleta de discussões jurídicas sobre o que o direito brasileiro admite ou não nesse campo. Quando o STF decide sobre o que agentes de inteligência podem ou não fazer, também produz um precedente que compõe esse universo.
[55] Nesse sentido, ver Dworkin, *Law's Empire*, 252–53.

compromissos com o controle do poder estatal que esses saberes consolidaram ou se na verdade é possível acomodar o que há de novo.

Assim, cabe olhar quais princípios, fundamentos e questões a construção dogmática consolidou e simplificou, bem como as razões normativas que captura para a seguir oferecer um retrato mais rico de como segurança interage com questões de privacidade em nosso tempo. Precisaremos estar abertos à complementação regulatória entre as áreas para o que ficou de fora porque não precisou ser endereçado antes e o que estamos pondo a perder se deixarmos de tratar, simplesmente porque regras centrais foram consolidadas em um outro período, sob circunstâncias distintas. A concepção de "segurança" que melhor revela porque a valorizamos é o que melhor servirá de norte para esses momentos. Passo a analisar essas áreas para desenvolver o argumento.

3.2 *Direito Penal*

O Direito Penal exerce o papel balizador das práticas consideradas ilícitos penais – identifica as condutas que ensejam responsabilização criminal, como também aquelas cuja ocorrência o Estado quer (e a polícia deve) prevenir. Faço essa observação elementar para frisar que o menciono aqui como balizador das condutas que ensejam atuação coercitiva estatal – e, particularmente, policial – tanto na esfera repressiva quando na esfera preventiva.

Uma parte importante desse ramo do direito como o conhecemos hoje gira em torno da teoria do delito – daquilo que constitui um "crime". Como adiantei, parece-me que o "direito à segurança" tem um papel notório na fundamentação de uma parcela expressiva da legislação penal. Não presumo, por outro lado, que todas as ofensas criminalizadas digam respeito à proteção da imunidade básica: podem apelar a uma noção de segurança que extrapola direitos que as pessoas têm pessoalmente e refletir, simplesmente, *políticas* para proteção de bens e valores da comunidade. Por exemplo, parece-me ser esse o caso para o regramento de responsabilização penal afeto à proteção do sistema financeiro e ao meio-ambiente. Na leitura de muitos penalistas, muitos tipos penais "mais recentes" (contra sistema financeiro, ordem econômica, meio ambiente) se inserem em um movimento no qual existiu a expansão dos objetos regulados pelo direito penal: de um direito penal 'clássico' destacado à proteção de interesses individuais como a vida, a integridade física e a liberdade, para interesses coletivos e difusos ("supra-individuais") da

comunidade – referidos a problemas que afetam (colocam em risco) a sociedade como um todo.[56] O Direito Penal contemporâneo é, portanto e em diferentes partes, apoiado tanto por argumentos que articulam muito mais do que apenas a segurança pessoal, avançando para a proteção de diversos "bens jurídicos" que importem à comunidade. Ele é, em regra, erguido sobre *motivos morais e impessoais* para regulação de violações contra liberdades. Um aspecto distintivo, mas necessariamente comum, delas é a identificação – por lei – como *crimes* (princípio da legalidade): uma decisão política da comunidade, o que enseja uma obrigação jurídica de seus membros de respeitá-la (e que é também desrespeitada quando crime ocorre); ao mesmo tempo, coloca uma garantia contra o arbítrio do Estado no exercício da coerção.[57]

As escolhas políticas-legislativas que resultam na legislação penal e seus arranjos concretos aplicados nas três frentes do Poder Público refletem escolhas que a área chama de "política criminal"[58]. Esta é objeto de disputa interpretativa fervorosa sobre seus compromissos e finalidades e com frequência gera e impulsiona críticas e revisões das próprias escolhas legislativas.[59] A meu ver, essas controvérsias podem ser interpretadas como disputas sobre o que significa e o que deve significar o "direito à segurança" enquanto regulação pública: qual deve ser a "cara" da proteção à segurança que o Estado deve a nós? Como ela deve ser feita? Quais devem ser os seus enfoques? Parte dessa discussão envolve a questão de o quão *preventiva* (e não apenas repressiva) a atuação do Estado deve ser e a quais ameaças deve responder com prioridade – voltarei a elas adiante.[60]

---

[56] Cf. Yuri Corrêa da Luz, "O combate à corrupção entre direito penal e direito administrativo sancionador", *Revista Brasileira de Ciências Criminais* 89 (2011): 429–70; Marta Rodriguez de Assis Machado, *Sociedade do risco e direito penal: uma avaliação de novas tendências político-criminais* (São Paulo: IBCCRIM, 2005), 99–112.

[57] Sobre características marcantes da dogmática do direito penal moderno, ver, com destaque para a noção de legalidade: Rafael Mafei Rabelo Queiroz, *O Direito a Ações Imorais: Paul Johann Anselm von Feuerbach e a construção do moderno direito penal* (São Paulo: Almedina, 2012), 204–14.

[58] "A política criminal é uma disciplina que oferece aos poderes públicos as opções científicas concretais mais adequadas para controle do crime, de tal forma a server de ponte eficaz entre o direito penal e a criminologia, facilitando a recepção das investigações empíricas e sua eventual transformação em preceitos normativos. Assim, a criminologia fornece o substrato empírico do sistema, seu fundamento científico. A política criminal, por seu turno, incumbe-se de transformar a experiência criminológica em opções e estratégias concretas assumíveis pelo legislador e pelos poderes públicos. O direito penal deve se encarregar de converter em proposições jurídicas gerais e obrigatórias o saber criminológico esgrimido pela política criminal". Sérgio Salomão Shecaira, *Criminologia*, 4º ed (São Paulo: Editora Revista dos Tribunais, 2012), 42.

[59] Miriam Guindani, "Sistemas de Política Criminal no Brasil: retórica garantista, intervenções simbólicas e controle social punitivo", in *Series Cadernos CEDES/IUPERJ n. 2* (Rio de Janeiro, 2005), 1–20; Maurício Stegemann Dieter, "O programa de política criminal brasileiro: funções declaradas e reais contribuições de Claus Offe para fundamentação da crítica criminológica à teoria jurídica das penas", *Revista Eletrônica do CEJUR* 1, nº 2 (2007), https://doi.org/10.5380/cejur.v1i2.16744.

[60] Sinalizei a essas questões acima. De forma específica, ver Andrew Ashworth e Lucia Zedner, "Prevention and Criminalization: Justifications and Limits", *New Criminal Law Review: An International and Interdisciplinary Journal* 15, nº 4 (1º de outubro de 2012): 542–71, https://doi.org/10.1525/nclr.2012.15.4.542; Victor Tadros, "Crimes

No Brasil, é bastante presente também a discussão sobre o quanto o combate a certos tipos de crime – como a corrupção – poderia autorizar flexibilização de garantias processuais; ou mesmo o quanto deve envolver o aparato do direito penal, em detrimento do direito administrativo sancionador, por exemplo[61]. Mais fundamentalmente, também envolve a própria discussão sobre a utilização do aparato repressivo do Estado como estratégia de combate à criminalidade, em detrimento de políticas sociais de redução da pobreza, promoção da escolarização, assistência social e emprego, como já falei.

A parte "principiológica" dessa discussão – as discussões sobre os limites das opções de política criminal frente a *direitos morais* – com frequência passa por controle de constitucionalidade em que se sustentam violações a liberdades: o respeito à dignidade de que já tanto falei e que já levou à descriminalização de condutas como o adultério e alimenta discussões sobre descriminalização do uso pessoal de drogas e do aborto, por exemplo. O resto, entretanto, envolve profundas escolhas de priorização política: como e o quê criminalizar, como ajustar a pena, que ameaças devem receber especial atenção, como prevenir a criminalidade (câmeras nas ruas ou projetos sociais?). É uma discussão eminentemente sobre o escopo e o conteúdo de uma meta social – promover "segurança" da população – que se quer alcançar e como fazê-lo.

Reconhecendo a existência dessas discussões de política criminal, que influenciam inclusive os traços do direito processual penal e do direito administrativo que analisarei adiante, o fato é que, tipificada a conduta como crime em lei penal, caso haja infração, as instituições do sistema de justiça criminal podem ser acionadas e são mobilizadas para punir o responsável. Por essa razão e tendo em vista o objeto desse trabalho, parece-me inevitável olhar para a intencionalidade desse ramo do direito e suas principais características, considerando a centralidade da noção de *pena* para a justificação da coerção estatal levada a cabo pelo Direito Penal: como preservamos a noção de tratamento com dignidade nessa área do direito?

Punir alguém é uma atividade que inflige dano: trancar alguém em uma cela por longos anos é algo que a princípio soaria completamente contraditório com a responsabilidade pessoal que todos têm sobre sua própria vida e que temos visto até aqui. Representa também diversas suspensões de direitos políticos – como o direito ao voto. Em muitos aspectos, a prisão representa

---

and Security", *The Modern Law Review* 71, nº 6 (1º de novembro de 2008): 940–70, https://doi.org/10.1111/j.1468-2230.2008.00730.x. Também Fabretti, *Segurança pública: fundamentos jurídicos para uma abordagem constitucional*.

[61] Luz, "O combate à corrupção entre direito penal e direito administrativo sancionador".

uma "violação dramática da dignidade"[62], como colocou Dworkin. Por outro lado, aceitar e reconhecer a responsabilidade pelos atos – inclusive e talvez especialmente os criminosos – é uma exigência ética (como devo viver minha vida). É curioso, portanto, que, assumindo que as exigências morais (como devo tratar os outros) e políticas (como o Estado deve tratar cidadãos) estão integradas com as exigências éticas, Dworkin se refira assim à necessidade de aplicar penas restritivas de liberdade aqui. A meu ver, a melhor maneira de entender o ponto é que prisões suprimem de pessoas uma dimensão importante daquilo que seria devido a elas, não fosse pelo ato criminoso pelo qual é responsável.

Nesse contexto, a existência desse tipo de mecanismo de atribuição de responsabilidade penal em um Estado, com certas características, não é incoerente se for ele mesmo pautado do início ao fim na noção de dignidade e concretizar valores que também entendemos importantes: o respeito devido às vítimas de atos criminosos (de modo que a interferência indevida no curso de suas vidas não pode ser ignorada pelo Estado sem destratar o valor intrínseco e a autenticidade dessas vidas) e a consideração à responsabilidade pessoal de pessoas que praticaram condutas criminosas (e a necessidade de que reconheça e se responsabilize pelos seus atos). Isto é, não é incoerente se for um dano que pode ser interpretado como *punição*.[63]

Para além dessa primeira aproximação teórica, o tema é objeto de enorme discussão no direito penal, de modo que meus comentários aqui são confessadamente sintéticos – medidos conforme o necessário para avançarmos na discussão sobre a justificação da atuação do Estado dentro do contexto de nossas práticas jurídicas pela "segurança".

Há diversas teorias que planejam justificar a imposição de penas e explicar o direito penal. Uma delas consiste na ideia que antecipei: "fazer justiça"; castigar alguém por ter praticado algo que é moralmente errado; punir porque assim se merece. São as visões 'retributivas', 'absolutas' ou 'moralistas' da pena. Outra se baseia na ideia de que a pena tem efeito inibitório: sua existência em si seria fator de prevenção, por desencorajar a prática delitiva na sociedade; também retiraria de circulação criminosos, impedindo que voltem a delinquir; contribui (em tese) à ressocialização de criminosos, também assim reduzindo crimes. São as visões 'preventivas', 'relativas' ou

[62] Dworkin, *Justice for Hedgehogs*, 299.
[63] Ronald Dworkin, "Terror & the Attack on Civil Liberties", *The New York Review of Books*, 6 de novembro de 2003, http://www.nybooks.com/articles/2003/11/06/terror-the-attack-on-civil-liberties/.

'consequencialistas' da pena.[64] Para alguns, a pena se justifica por uma combinação de ambos os conjuntos de razão. H. L. A. Hart, por exemplo, defendeu que o objetivo geral do direito penal é maximizar o bem-estar pelo efeito preventivo, mas que o critério de distribuição de penas é necessariamente retributivo, baseado no merecimento do ofensor.[65] Parece uma fundamentação que se reflete nos nossos materiais jurídicos: o Código Penal brasileiro fala em "reprovação e prevenção do crime" (art. 59) como fatores para fixação da pena, ao mesmo tempo em que a Constituição Federal limita a pena à pessoa do condenado (art. 5º, XLV). A dogmática penal contemporânea, segundo desenvolve Rafael Mafei, teria reunido as duas correntes.[66]

Longos debates sobre teoria da pena à parte, fato é que uma teoria que suportasse a sugestão de que penas pudessem por alguma razão ser distribuídas de forma aleatória não teria qualquer respaldo em nossas práticas e valores. Esse é um "teto moral" embutido em nossas leis penais.[67] Nesse sentido, para além da materialidade delitiva, deve haver prova suficiente da autoria ao imputado (arts. 386 e 413, CPP). O fato típico e ilícito e culpável deve estar vinculado ao responsável por sua autoria para que a pena possa ser aplicada. Ademais, o princípio da culpabilidade (*nullum crimen sine culpa*) é um dos mais basilares do direito penal e é reforçado por exigências ainda mais específicas: capacidade de culpabilidade, consciência da ilicitude e exigibilidade da conduta.[68]. Não é nada surpreendente que seja assim: a ideia de punir quem é inocente é uma das que mais nos causa aversão; lamentamos profundamente quando erros assim ocorrem.

Quem recebe a pena precisa ter se "auto-selecionado"[69]: deve ser operado e verificado

---

[64] Larry Alexander, "The Philosophy of Criminal Law", in *The Oxford Handbook of Jurisprudence & Philosophy of Law*, org. Jules Coleman e Scott Shapiro (Oxford: Oxford University Press, 2002), 815–67; Cezar Roberto Bitencourt, *Tratado de Direito Penal – Parte Geral 1*, 14ª Edição (São Paulo: Saraiva, 2009), 83–105.

[65] H. L. A. Hart, *Punishment and Responsibility: Essays in the Philosophy of Law*, 2º ed (Oxford: Oxford University Press, 2008); Malcolm Thorburn, "Criminal Law as Public Law", in *Philosophical Foundations of Criminal Law*, org. RA Duff e Stuart P. Green (Oxford: Oxford University Press, 2011), 25; Carla Henriete Bevilacqua Piccolo, "A moral e o conceito de direito em H.L.A. Hart" (Mestrado, São Paulo, Faculdade de Direito da Universidade de São Paulo, 2011), 88–100, https://www.teses.usp.br/teses/disponiveis/2/2139/tde-06062012-091850/publico/Carla_Henriete_Bevilacqua_Piccolo_ME.pdf.

[66] Queiroz, *O Direito a Ações Imorais: Paul Johann Anselm von Feuerbach e a construção do moderno direito penal*, 238.

[67] Queiroz, 232.

[68] Bitencourt, *Tratado de Direito Penal – Parte Geral 1*, 16.

[69] Uso termo que encontrei em Dworkin, "Terror & the Attack on Civil Liberties". A ideia de que o agente precisa ter desejado livremente cometer um delito, a partir de seu livre-arbítrio, e com isso "aceitado" a pena que poderia receber também se encontra na obra de expoentes da construção da dogmática do direito penal contemporâneo, como Paul Johann Feuerbach: Queiroz, *O Direito a Ações Imorais: Paul Johann Anselm von Feuerbach e a construção do moderno direito penal*, 233. Isso não se confunde com o problema da "seletividade do direito penal", o que designa um problema de desigualdade na aplicação de penas – uma discrepância nos grupos sociais que as recebem.

algum juízo de responsabilização causal que relacione quem é punido com a conduta – por ação, omissão, negligência que importou em violação a lei que se tinha o dever jurídico de respeitar. Não poderia ser diferente para poder justificar a conduta estatal: temos um direito moral a não sermos punidos se somos inocentes – o contrário, como apontei, desrespeitaria a nossa dignidade da forma mais visível e visceral possível. Retirar a soberania sobre o plano da vida de alguém, infligindo tamanho dano sem que as próprias condutas dessa pessoa assim tenham dado causa a essa suspensão de direitos e ainda que a maioria fosse se beneficiar disso desrespeita o valor intrínseco dessa vida e a responsabilidade pessoal sobre ela.[70] Há um limite da própria dignidade traçado pelo direito penal[71]: pessoas não podem ser punidas pelo que pensaram, cogitaram, desejaram abstratamente, por terem certa identidade ou opinião – apenas uma ação exteriormente reconhecida como criminosa e/ou da qual é possível antecipar lesão a um direito autoriza que o Estado mobilize suas instituições penais contra o agente.

Nesse contexto, pode-se dizer que o traço mais fundamental do Direito Penal, enquanto a frente mais clara da regulação pública movida pelo "direito à segurança", é anunciar as condutas que não devem ser praticadas, limitando sua aplicação a agentes que seriam *autores* do delito, *culpados* (art. 5º, LVII, CF/88), a que se engajou em conduta da qual resultou ou já se poderia antecipar lesão. Trata-se de um compromisso com a própria dignidade embutido na regulação pública do direito à segurança: não submeter à coerção estatal quem não deu qualquer razão para tanto. Como passo a mostrar, essa lógica perpassa todo o direito processual penal, enquanto estrutura institucional que leva à aplicação da pena. É nessa área que fazemos diversas outras escolhas de política criminal relativas à concepção de "direito à segurança" como regulação pública.

3.3 *Direito Processual Penal*

Se tamanho dano à dignidade só pode ser infligido àquele que se "auto-seleciona", é importante que o Estado disponha de um mecanismo para verificar que é este o caso. Se admitimos tamanho uso da força do Estado contra a dignidade de alguém, é importante que a esse poder seja correspondido um dever de cuidado que se traduza em certas salvaguardas institucionais para que

[70] Ver Dworkin, *Justice for Hedgehogs*, 299.
[71] Ver, dentro de um esforço de construção dogmática na obra de Feuerbach, Queiroz, *O Direito a Ações Imorais: Paul Johann Anselm von Feuerbach e a construção do moderno direito penal*, 183; 214–17.

esse sistema se mantenha compatível com a dignidade. Nesse sentido, o direito processual penal consiste em um sistema de adjudicação de direitos entre o indivíduo e o Estado voltado à verificação da presença ou ausência dos requisitos que ensejam e justificam a aplicação da lei penal. Trata-se, dizemos, de exigência do direito ao *devido processo legal* (art. 5º, LIV, CF/88).

O conjunto de regras e princípios que o compõem entram em cena mediante apresentação de indícios do delito – *repressivamente,* para esclarecer algo que já ocorreu.[72] É preciso, portanto, que exista um impulso externo – um fato – que acione a atuação do Estado. Na linha do que vimos e do que tenho elaborado, esse procedimento deve ser ele mesmo compatível com o respeito à dignidade que o Estado deve às pessoas – sem surpresa, a presunção de inocência é um princípio basilar aqui: entendemos que pressupor de início o contrário é um insulto à dignidade. Não deixa de ser uma questão de autorrespeito: conceber um tratamento contrário é menosprezar o valor de nossas próprias vidas, se postos em situação semelhante. O compromisso com o igual respeito que se revela por essa garantia impacta várias frentes do processo: (i) requer que fiquemos abertos à possibilidade de que imputados sejam inocentes; (ii) constrange os meios que usamos para determinar quem é culpado ou inocente; e (iii) constrange o modo como nós lidamos com aqueles que punimos, inclusive aqueles que temos plena convicção de serem culpados.[73]

Considerando a centralidade do critério retributivo para distribuição de penas no Direito Penal, não é surpresa que as etapas da imputação de uma conduta criminosa a alguém pelo Direito Processual Penal envolva tradicionalmente a progressão nas figuras de *suspeito, indiciado, imputado, acusado, condenado.* Desde as etapas pré-processuais de investigação do fato delituoso, a atuação do Estado passa pela ideia de atribuição do fato investigado a alguém: o trabalho policial prévio em investigação preliminar envolve obtenção de informações para identificar suspeitos e indicar aqueles cujos elementos de informação apontam para culpa (*indiciamento*[74]). O art. 6º do Código Processual Penal brasileiro envolve uma série de diligências a esse fim. Indícios suficientes de autoria podem ensejar uma diversidade de medidas cautelares contra um indiciado (art. 282).

---

[72] Cf. Luís Greco, "Introdução – 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 *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*, por Jürgen Wolter, org. Luís Greco (São Paulo: Marcial Pons, 2018), 51.

[73] Waldron, "Safety and Security", 476–77.

[74] "Indiciar é, com base nos elementos de informação colhidos no inquérito policial, indicar alguém como uma pessoa sendo o provável autor do crime que se investiga".Gustavo Henrique Badaró, *Direito Processual Penal*, 2º ed, vol. Tomo I (Rio de Janeiro: Elsevier, 2008), 56.

Os elementos reunidos por sua vez servirão para oferecimento da denúncia e propositura de ação penal (art. 41, CPP), baseada em *justa causa* (art. 395, CPP) e em que *provas* podem ser produzidas em contraditório.[75] O réu deve ser absolvido em caso de insuficiência de provas (art. 386, IV).[76]

Nesse sentido, a atividade probatória é prática focal do processo penal. Para tanto, a legislação prevê diversos *meios de prova* – instrumentos pelos quais se levará elementos de prova a juízo para revelação da verdade dos fatos. A começar pela compreensão do "corpo de delito": "o conjunto de elementos materiais deixados pelo crime", formado sobretudo pela pessoa ou coisa sobre a qual o crime foi praticado, os instrumentos utilizados na prática do crime, e a "constatação de todas as circunstâncias hábeis à reconstrução do crime investigado".[77] Isso envolve, portanto, a análise de vestígios deixados na cena do crime, como pegadas, impressões digitais e material genético (DNA), extraído de fios de cabelo, sangue, esperma, ao lado de outras de análises periciais (análises balísticas, por exemplo), sempre que pertinente. Há ainda as provas testemunhais, os reconhecimentos de pessoa ou coisa e provas documentais. Para além disso, há medidas *cautelares* das quais se pode lançar mão para assegurar meios, elementos e fontes de prova, como buscas domiciliares, buscas pessoais, apreensões e quebras de sigilo. Vem agora também se admitindo colaboração premiada. A depender do tipo de crime, a relevância de um meio de prova (e de um meio de obtenção de prova) pode ser maior ou menor. Diante do avanço tecnológico hoje experimentado, as inovações nesses meios de prova são gigantescas.

Eu retornarei a essas particularidades e ao modo como levantam questões de privacidade e proteção de dados adiante. Por ora, o ponto a ser observado é como lidamos com a incerteza entre alguém ser culpado e ser inocente. Como lidamos com o risco de punir alguém indevidamente? Com salvaguardas procedimentais:

> Nossos procedimentos insistem em salvaguardas, ademais, para garantir que aqueles que punimos sejam realmente culpados, isto é, que eles de fato se tenham responsabilizado por essa punição, pois correr qualquer risco substancial de que um réu seja punido embora inocente, apenas para melhorar a eficiência do processo de dissuasão, seria tratar a vida do réu como descartável.[78]

As salvaguardas têm papel fundamental de evitar a causação indevida de um dano moral –

[75] Badaró, Tomo I:205.
[76] Há outras situações que levam à sentença absolutória. Cf. o art. 386, CPP e Badaró, Tomo I:305–6.
[77] Badaró, Tomo I:227.
[78] Tradução livre. No original: "Our procedures insist on safeguards, moreover, to ensure that those we punish are indeed guilty, that is, that they have indeed made themselves liable to that punishment, because running any substantial risk that a criminal defendant may be punished though innocent, just to improve the efficiency of the process of deterrence, would be treating the defendant's life as expendable". Dworkin, "Terror & the Attack on Civil Liberties".

dano decorrente de injustiça – a inocentes durante a verificação dos fatos ("busca da verdade"). São um mecanismo de contenção de arbitrariedades por parte do Estado.

Para desenvolver a relação entre os sentidos de segurança que vimos e o direito processual penal, apresentarei uma discussão de Dworkin que me parece esclarecedora. Em *Principle, Policy and Procedure,* capítulo do livro "*A Matter of Principle*" (1985), Dworkin explora a seguinte pergunta: do fato de que temos um direito moral forte a não sermos punidos se somos inocentes deriva o direito de termos o processo mais acurado possível para se testar culpa ou inocência? O único procedimento compatível com a dignidade seria aquele mais preciso o possível? Se não, a que nível de acurácia temos direito? Hamish Stewart contextualiza a questão: em muitas ocasiões no processo de adjudicação, o desacordo não é teórico sobre o que direito exige, requer ou autoriza naquele caso (aspecto em que Dworkin mais esteve interessado em seus escritos), mas um desacordo sobre os próprios fatos do caso.[79] Como deve ser o procedimento atinente à determinação dos fatos de um caso e o nível de acurácia a que deve almejar?

Dworkin sustenta que temos direito ao nível de acurácia com que concordamos no momento em que fixamos as regras do processo, que devem distribuir igualmente o risco de dano moral (de ser vítima de injustiça). Assim propõe reconciliar sua noção de direito forte a não ser condenado se inocente com o fato de que nossos procedimentos penais amoldam-se a interesses gerais – como a otimização de recursos.[80] Para ele, na definição das "regras do jogo" do processo penal, cidadãos decidem sobre os pesos relativos que querem dar aos "riscos de dano moral" a que estão sujeitos na futura aplicação desse procedimento: os riscos de sofrerem injustiças – serem sujeitados a decisões incorretas (ser condenado sem ser culpado, sobretudo).

Dworkin usa o exemplo da definição de uma norma sobre o tipo de provas que podem ser produzidas em um processo – extremamente relevante quando estamos falando de direitos à privacidade, como já antecipei e que explorarei mais adiante –, mas podemos pensar em diversas outras: as condições que uma denúncia deverá atender para ser acolhida, as circunstâncias em que a acusação deve compartilhar provas exculpatórias, os requisitos materiais/standard probatório para condenação[81], a quantidade de jurados, as instâncias de recurso sobre questões de fato, etc.

---

[79] Hamish Stewart, "Concern and Respect in Procedural Law", in *The Legacy of Ronald Dworkin*, org. Will Waluchow e Stefan Sciaraffa (Oxford: Oxford University Press, 2016), 375–76.
[80] Stewart, "Concern and Respect in Procedural Law".
[81] "A formulação do [standard] BARD [*beyond any reasonable doubt*] teria em sua origem a pretensão de dificultar a condenação de inocentes. Como? Dificultando condenações de como geral. Se o sistema criminal passa a exigir robustamente mais da hipótese de condenação para que seja considerada verdadeira (95%), então, dificulta-se mais as

Defende então que as pessoas são tratadas como iguais na definição dessas disposições porque, antecipadamente, é igualmente provável que qualquer um seja levado ao processo penal, apesar de inocente, e igualmente provável que alguém se beneficie de uma norma menos onerosa que tenha sido por ventura escolhida.[82] Quando a regra fixada for aplicada no caso concreto, não há "decisão política nova", de modo que a negação ao processo perfeitamente acurado não viola direito. [83] Caso, por outro lado, um juiz afaste-se da regra procedimental antes fixada por alguma razão como o "bem-estar geral" ou qualquer outra, há decisão política nova que violaria direito. Não se pode mudar as regras sobre riscos casuisticamente.

As regras processuais que citei acima, bem como todas as demais do CPP e de legislação especial, podem ser vistas como reflexo dessas decisões políticas de primeira ordem que fixam a importância relativa do risco de dano moral com relação a outras prioridades sociais que possam existir. Podemos considerar "o desenho de procedimentos criminais e civis como um tecido tecido a partir das convicções da comunidade sobre o peso relativo das diferentes formas de danos morais, comparados entre si, e contra sacrifícios e lesões comuns."[84] De forma específica, as regras de processo penal que regulam as informações a que autoridades policiais podem ter acesso e sob qual padrão de justificação, desde a etapa inicial de investigação, para a reconstrução dos fatos do caso e imputação de conduta a indivíduos, podem ser compreendidas como decisões sobre pesos relativos do risco de ser penalizado se inocente frente a outras prioridades políticas que prejudicam a acurácia quanto à avaliação de inocência. Podem também ser compreendidas, a meu ver, como decisões sobre peso relativo do risco de ter uma prerrogativa de privacidade afastada abusivamente, excessivamente, erroneamente, frente a outras prioridades (afinal, o direito à não ser condenados se inocentes não é o único que temos).

Retomarei esse ponto mais à frente, pois consiste na principal interação de autoridades

---

condenações e, com isso, também as condenações de inocentes.(…) A lógica, como se vê, é de exigir mais das hipóteses fáticas quanto mais gravosas sejam as consequências delas extraídas". Janaína Matida e Antonio Vieira, "Para além do BARD: uma crítica à crescente adoção do standard de prova 'para além de toda a dúvida razoável' no processo penal brasileiro", *Revista Brasileira de Ciências Criminais* 156 (2019): 230–31.

[82] Ronald Dworkin, *A Matter of Principle* (Clarendon Press, 1985), 85.

[83] Nesse sentido, Dworkin sustenta que uma decisão que acidentalmente condena inocente é profundamente distinta de um caso em que a pessoa é deliberadamente condenada mesmo sendo inocente. No segundo caso, não se trata mais da mera incorrência no risco que se assumiu; nessas circunstâncias, a decisão política que impõe a pena é nova: impõe-se um dano moral sobre um risco que não se assumiu quando as regras do jogo foram fixadas. Também essas noções serão recuperadas mais a frente

[84] Tradução livre. No original: "the design of criminal and civil procedures as a fabric woven from the community's convictions about the relative weight of different forms of moral harms, compared with each other, and against ordinary sacrifices and injuries". Dworkin, *A Matter of Principle*, 86.

policiais com direitos de privacidade no processo penal: a questão do risco de injustiça no afastamento de direitos de privacidade para apuração de fatos. Em linha com o que já foi visto, exatamente porque a polícia exerce a força sobre alguém de forma específica no processo penal (em contraste com todas as pessoas em geral), e pode causar dano moral sério ao exercício de seus direitos, sobretudo se o fizer de forma abusiva ou por erro, é que é necessário estabelecer parâmetros que controlem o modo como a interação se dará e a partir de quais condições.

No momento, valem três observações. A primeira é como o "direito político à uma regulação pública em segurança" é e pode ser mobilizado – nas mais disputadas concepções do que esse ideal deve consistir – para avançar regras processuais que admitam mais erros de injustiça/danos morais: a comunidade pode achar que cometer injustiças durante investigações e até aumentar o nível de falsos positivos (condenações de inocentes) possa promover certa concepção de segurança. Podem disputar que isso compõe uma boa política criminal. Concessões que fazemos nesse sentido, como também argumentou o Dworkin, envolvem não propriamente o balanceamento com a liberdade, mas com a própria honra[85]: o autorrespeito que damos ao valor intrínseco da nossa vida, se nos acomodarmos com regras que permitem mais erros.

A segunda é sobre a conciliação das regras processuais a serem fixadas por um órgão como o Legislativo com uma concepção de direito à segurança imbricada com a dignidade. Pesos relativos atribuídos no exercício legislativo não serão objetivamente justos e corretos per se; esse é só um modelo prático de ajustes de prioridades que é adequado deixar a instituições democráticas como o Poder Legislativo. Mas não se supõe que a decisão fixada pela maioria ao aprovar regras processuais não possa ser contestada ou que haja carta branca. Se discriminar minorias/um grupo particular de pessoas, fazendo com que um grupo seja mais criminalizado ao custo da segurança de outros, poderá ser, por exemplo.[86] A decisão não pode impor um risco de dano moral muito maior a um cidadão do que impõe a outro. Não pode também, por outro lado, esvaziar o instituto

[85] Dworkin, *Is democracy possible here?*, 45.

[86] Assim como Dworkin já alertava sobre preferências impessoais (sobre como os outros devem levar suas vidas) na adoção e justificação de decisões políticas, Waldron também chama atenção a "tradeoffs intrapessoais entre liberdade e segurança": a situação em que aceitamos uma redução de liberdade que não será percebida por nós, mas por outras pessoas por serem quem são. Seu exemplo estava ligado a ameaças terroristas, e a como determinadas medidas restritivas de direitos expõe mais pessoas com determinado perfil étnico e religioso a coerções. De todo modo, a análise (e o alerta) pode ser levado para outras situações. Há sempre perdedores e vencedores na política, diz; mas outros são os limites quando a redução é a um direito que se assumia ter. Cf. Jeremy Waldron, *Torture, Terror, and Trade-Offs: Philosophy for the White House* (Oxford: Oxford University Press, 2010), 12–13.

da responsabilidade penal, a ponto de gerar impunidade de forma sistemática.[87]

Há duas características importantes que compõem esse quadro de compromisso com a dignidade – e, particularmente, com a integridade de nossos esforços legislativos que compõem o direito processual penal. Dworkin fala em dois tipos de direitos que as pessoas têm em processos criminais: (i) o direito à atribuição da importância correta ao risco de dano moral; e (ii) direito à consistência na avaliação da importância do dano moral, com respeito a nossas práticas históricas.[88] Nesse sentido, o órgão legislativo não está autorizado a ignorar uma possibilidade de injustiça ao fixar regras sobre acurácia na determinação de fatos; nem pode, por exemplo, alterar regras para aumentar o nível de risco a que sejam vítimas de injustiça, de uma forma incompatível com as práticas de processo penal. Regras procedimentais não podem ser simplesmente fixadas de forma utilitária nem acatando cegamente a definição da maioria se não refletirem uma versão plausível do que seria tratamento com igual consideração e respeito na hipótese, tampouco podem representar um retrocesso e se mostrar incoerente com outras avaliações sobre o peso de dano moral.[89] Como sustenta Waldron,

> sem dúvida, tais sistemas requerem ajustes de tempos em tempos, para refletir os maiores perigos que enfrentamos. Mas o ajuste nunca deve perder o contato com o princípio subjacente de respeito em relação a suspeitos e condenados. Não temos o direito de reajustar o sistema de liberdades civis simplesmente para nos tornarmos mais seguros. Se estamos preocupados em nos tornar mais seguros, qualquer reajuste deve ser filtrado por meio deste princípio.[90]

Nesse contexto, e em terceiro lugar, chamo atenção para a importância da legalidade também no processo penal, isto é, do estabelecimento de regras prévias que fixem os pesos relativos dos riscos de uma condenação injusta – uma questão de política conforme as diversas

---

[87] Defendendo essa posição, ver, por exemplo: Ronaldo Porto Macedo Junior, "Temos direito a uma justiça penal que não seja completamente ineficaz?", *Fumus boni iuris - O Globo*, 19 de março de 2021, https://blogs.oglobo.globo.com/fumus-boni-iuris/post/ronaldo-porto-macedo-junior-temos-direito-uma-justica-penal-que-nao-seja-completamente-ineficaz.html.

[88] Dworkin, *A Matter of Principle*, 89.

[89] Nesse ponto, discordo da crítica que Hamish Stewart vem dirigir ao Dworkin no artigo que citei (Stewart, "Concern and Respect in Procedural Law".). O autor parece supor que Dworkin entende que o direito processual é só uma questão de acurácia e que não acharia errado caso o legislativo praticamente suprimisse regras contra não-autoincriminação, por exemplo. O Estado deve às pessoas um procedimento justo, que leve a sério o risco de dano moral por erros na determinação de fatos e que seja compatível com a melhor interpretação nossas práticas e demais direitos políticos. Ver, por exemplo, Dworkin, *Justice for Hedgehogs*, 371–72.

[90] Tradução livre. No original: "no doubt such systems require adjustment from time to time, to reflect the greater dangers that we face. But the adjustment must never lose touch with the underlying principle of respect in regard to suspects and convicts. We are not entitled to readjust the system of civil liberties simply to make ourselves safer. If we are concerned to make ourselves safer, any readjustment must be filtered through the medium of this principle". Waldron, "Safety and Security", 477.

prioridades que possam existir e a que os cidadãos da comunidade forem sensíveis: por exemplo, se a comunidade comportaria provas ilicitamente obtidas em investigações de crimes graves, ou que autoridade judiciária indicasse fontes de prova à acusação, quando isso pudesse facilitar a condenação em certos tipos de casos graves e reduzisse a sensação de impunidade. Se a definição da regra não existiu, ou se desrespeita uma que foi fixada, o ajuste de pesos dos riscos que uma regra carrega é casuístico – desrespeita a responsabilidade pessoal e pode levar ao tratamento desigual; impõe-se um dano moral sobre um risco que não se assumiu quando as regras do jogo foram fixadas. É essa a lógica de contenção de arbítrio e reflexo do compromisso de princípio com a dignidade, que nessa área estebelece altos níveis de importância e rigidez a procedimentos.

Voltarei a essas ideias no próximo capítulo. Cumpre ainda aqui tratar de outro tipo de atuação policial – o braço de ênfase preventiva de políticas de segurança.

3.4 *Direito Administrativo*

Se o processo penal se especializou como prática e campo de saber jurídico que se preocupa em regular o que pode acontecer com pessoas que cometeram crime e como normas penais são aplicadas sobre alguém a partir do momento em que se constata a ocorrência de um fato criminoso, deixa de fora (ou ao menos na fronteira) as situações em que há uma lesão iminente a ser contida, mas ainda não foi concretizada, e outros esforços mais gerais de promoção da segurança pública, independente de atos criminosos concretos. Em tese, podemos associar esses contextos ao âmbito do direito administrativo, mas isso não torna o cenário menos complexo: como visto, faz parte do nosso compromisso com a dignidade – já embutida no direito penal e no direito processual penal – não punir pessoas que sejam inocentes. Somos capazes de reconciliar a causação do dano de prender alguém a uma pessoa apenas quando ela escolheu e deu causa à conduta criminosa. Até que ponto o valor da segurança (e o direito político a uma regulação pública em matéria de segurança) permite agir para *prevenir* e conter atividades criminosas e em que condições? Como justificamos isso? Já sinalizei a alguns desses limites, mas agora revejo a discussão de forma contextualizada a esforços dogmáticos e à realidade tecnológica atual e policial brasileira.

A área de direito administrativo viu e vê o crescimento da dimensão de atuação do Estado pelo "poder de polícia": tradicionalmente relacionado no Brasil à atuação do Estado na "garantia

da segurança, da tranquilidade e da salubridade públicas"[91] e à ideia de "fazer cumprir a todos os indivíduos o *dever de não perturbar*"[92], hoje se refere a todo tipo de atividade reguladora e disciplinadora da Administração Pública em nome do interesse público. É com base em uma noção abrangente de segurança, que extrapola o núcleo de proteção da segurança individual contra *violência* à vida, integridade física e propriedade, que se regula a "segurança" de diversas outras matérias – como na área sanitária, de trânsito ou de edificações, por exemplo. Vemos aí a mobilização de um direito administrativo *sancionador,* por vezes até mesmo no lugar do direito penal: para aumentar a segurança no trânsito, impondo multa a quem for pego em blitz e se recusar a fazer o teste do bafômetro; para aumentar a segurança contra problema sistêmico que afeta não só a Administração Pública, mas a vida em sociedade, impondo normas de *compliance* de combate à corrupção em empresas, cujo descumprimento gera responsabilização administrativa.

De forma específica quando se fala na atuação policial não coberta pelo direito processual penal, pode-se dizer que a área de segurança pública contra criminalidade é profundamente "desregulada" na esfera administrativa. O art. 144, *caput,* da Constituição Federal dá o tom geral: segurança pública é dever do Estado a ser "exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio", criando e dividindo atribuições institucionais. Fora isso, há pouca concretização normativa de como a "segurança pública" deve ser feita fora das estruturas de direito penal e direito processual que vimos acima. Nos textos clássicos do direito administrativo brasileiro, "ordem pública" é tida como conceito que abrange não só a preservação da segurança, mas todas as atividades que seriam necessárias para que o Estado possa garantir a convivência social – de forma nada elucidativa ou completamente expansiva, seria a "situação de fato oposta à desordem"[93]. Por conseguinte, o Estado estaria autorizado a disciplinar e intervir em todas as "atividades capazes de fazer perigar interesses gerais, importantes à vida pública".[94] De forma específica, a atividade policial então se prestaria à "prevenção e [ao] controle das condutas dos indivíduos, potencialmente capazes de impor ameaça aos bens sociais ou públicos referidos"[95]. Se na dimensão repressiva a atuação gira em torno de *suspeitos,* na dimensão preventiva a atuação seria contra *perturbadores.*

[91] Tácito, "O poder de polícia e seus limites", 3.
[92] Caio Tácito, "Poder de polícia e polícia do poder", *Revista de Direito Administrativo* 162 (1985): 2.
[93] Lazzarini, "A ordem constitucional de 1988 e a ordem pública", 279.
[94] Filocre, *Direito Policial Moderno*, 15.
[95] Filocre, 15.

A noção que tem pouco a pouco ganhado atenção pela doutrina dessa área do direito – bastante influenciada pelo direito alemão[96] nesse ponto – é a de perigo. Sendo a conduta perigosa aquela que tem o "potencial de causar dano à ordem pública", a *polícia de segurança pública* seria aquela que se dedica ao "controle de perigos decorrentes da criminalidade"[97]. As práticas definidas por lei como crime definem um conjunto específico de perigos que devem ser combatidos e controlados. Como esse trabalho se volta à atuação para criminalidade, não esbarramos diretamente na questão sobre a atuação que não é contra crime, mas ainda seria contra a "ordem pública" – um termo não surpreendentemente criticado[98]. Ainda assim, a definição de *como* esse combate de ênfase preventiva à criminalidade será e pode ser feito é pouco ou nada delimitada em lei e depende também de justificação.

Perigos concretos

Quando há um perigo de dano claro e imediato à vida de alguém ou de seus direitos, a justificativa para o Estado agir, em linha com o visto até aqui, já pode estar disponível: uma ação exteriorizada a partir da qual se pode antecipar lesão já autoriza que se aja para impedir dano a direito e conter o perturbador. Embora essa avaliação sempre dependa do contexto concreto (e por isso o "pode estar"), a hipótese teórica existe, pode ser fundamentada e está na fronteira já com os propósitos repressivos do processo penal. Não é de qualquer jeito: as mesmas contrapartidas de proteção da liberdade e da igualdade e de contenção do arbítrio devem se estender a essa área, para que seja compatível com a dignidade.

Há um desafio particular: apesar de tratarmos aqui de um núcleo mais facilmente identificável de "perigos" (aquilo que for também "crime"), sustenta-se que "as múltiplas formas das atividades individuais ditas perigosas, decorrentes da criminalidade, impedem que as leis prevejam todas as ocasiões que exigem a atuação policial de segurança pública, assim como todos os modos de atuação"[99]. Por essa razão, diz-se que há "discricionariedade" para a atuação policial dentro de sua competência legal de preservação da segurança pública, sem prejuízo da necessidade

[96] Cf. Greco, "Introdução – 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)", 51–54.
[97] Filocre, *Direito Policial Moderno*, 47.
[98] Fabretti, *Segurança pública: fundamentos jurídicos para uma abordagem constitucional*. (propondo um modelo de "segurança cidadã" para a segurança pública na CF/88 e defendendo que "manutenção da ordem pública" deve ser compreendido como preservação de direitos fundamentais e da cidadania (p. 107).
[99] Filocre, *Direito Policial Moderno*, 68.

de respeitar direitos fundamentais nessa atuação.[100] Qual o sentido possível dessa discricionariedade no âmbito de atividades de segurança comprometidas com a dignidade?

Essa questão é importante para essa seção porque nos leva às particularidades da justificação da coerção estatal nesse ramo do direito, no contexto a que se aplica. Ao princípio da legalidade estrita (art. 37, *caput,* CF/88) também foi dado papel norteador no desenvolvimento do direito administrativo brasileiro: ao administrador público só é permitido fazer o que a lei autoriza.[101] Trata-se de um princípio que se reporta diretamente ao valor do *rule of law,* enquanto um elemento básico para que o poder que o Estado exerce sobre cidadãos possa ser justificado – legitimado: como temos visto, a ideia é que aceitamos ser governados sob o compromisso de que pessoas em posições de autoridade encarregadas de executar as tarefas que permitem a existência e o funcionamento do Estado exercerão seu poder nos limites do seu mandato democrático, sob compromisso com a dignidade. Nessa linha, uma outra noção importante nessa área é de *accountability* – prestação de contas ou responsabilização: agentes estatais devem estar sujeitos a estruturas de controle administrativo e a avaliações em eleições. O Poder Legislativo deve instituir as regras que norteiam a o Poder Executivo, por sua vez supervisionado internamente e pelo Poder Judiciário.[102]

Já dentro de sua esfera de competência e atribuições e da margem de atuação que lhe conferir a lei, entende-se que órgãos da Administração Pública têm "discricionariedade", com base em juízos de conveniência e oportunidade, para definir como cumprir suas tarefas institucionais. De forma específica à atuação policial propriamente dita, na distribuição de competências feita pelo art. 144 da CF/88, os poderes executivos a nível estadual – com a Polícia Militar – e municipal – com a Guardas Civis, têm papel relevante na definição de estratégias de policiamento e regulamentação de protocolos de atuação. Os "comandos" dessas polícias, por sua vez, devem definir estratégias e protocolos ainda mais concretos de atuação – como será feito o acompanhamento de um protesto, como o resgate de reféns deve ser feito, em que circunstância pode haver engajamento, quando se pode parar e revistar alguém na rua, quando se pode forçar o

[100] Luís Antônio Francisco Souza, "Polícia, direito e poder de polícia. A polícia brasileira entre a ordem pública e a lei.", *Revista Brasileira de Ciências Criminais* 43 (2003): 295–321; Arthur Trindade Costa, "Como as democracias controlam as polícias: os mecanismos institucionais de controle da atividade policial", *Novos Estudos CEBRAP* 70, nº 3 (2004): 65–78.
[101] Hely Lopes Meirelles, *Direito Administrativo Brasileiro*, 22º ed (São Paulo: Malheiros, 1997), 82.
[102] Cass R. Sunstein e Adrian Vermeule, "The Morality of Administrative Law", *Harvard Law Review* 131, nº 7 (2018): 1933.

ingresso na casa de alguém, etc. – que devem ser observadas e executadas por agentes de campo. Estes, nessas e em outras situações, devem ainda ter de tomar decisões ainda mais concretas sobre uso da força – prender ou atirar em alguém, por exemplo.

De cima a baixo, a justificação da atuação policial preventiva deve ser corroborada pela existência de legitimidade para se agir. Parte disso e principalmente em estruturas policiais em que há clara "divisão de trabalho"[103] como o que expus acima, isso passa pela noção de *autoridade* – de discricionariedade para agir debaixo de uma ordem, de um protocolo, de uma norma autorizadora. Em um Estado comprometido com a dignidade, é imprescindível que toda essa cadeia manifeste um tratamento com igual consideração e respeito em todos os tipos de contatos da polícia com cidadãos em geral e, ainda mais, a todos abrangidos por uma situação em que se identifique *perigo* concreto e imediato a um direito forte de alguém (ameaça concreta à segurança do direito). Não faria sentido supor que haveria "discricionariedade" fora dessas premissas. O sentido de discricionariedade consiste em ser o agente que toma as decisões concretas e exerce capacidade de julgar, não que não deva responder ao que o direito – e uma concepção de segurança pública imbricada com a dignidade – exige.

Para usar categorias de *accountability* propostas por Jeremy Waldron, e em linha com o que coloca Arthur Trindade, essa discricionariedade não escapa da *forensic accountability*: as estruturas de controle interno e externo, administrativo e judicial, que devem complementar a legislação, os códigos de conduta e treinamentos, e as estratégias de policiamento enquanto mecanismos institucionais de controle democrático de atuação policial.[104] Ao lado dela, coloca-se também a *agent accountability*. Servidores públicos devem prestar contas porque atuam a mandato do povo; é próprio da relação política em uma democracia que o façam. Isso pode acontecer de forma mediada, entre várias camadas de uma hierarquia até chegar no povo (de um servidor para um secretário, do secretário para um governador). Mas existe – deve ser prestada conta sobre todos os atos praticados por agentes públicos no exercício de sua função. Deve haver transparência. "Em uma democracia, os agentes responsabilizáveis do povo devem ao povo uma explicação do que eles têm feito, e a recusa em fornecer isso é simples insolência."[105] A discricionariedade ainda deve

[103] O termo é emprestado de Thorburn, "Justifications, Power, and Authority".
[104] Costa, "Como as democracias controlam as polícias: os mecanismos institucionais de controle da atividade policial".
[105] Tradução livre. No original: "In a democracy, the accountable agents of the people owe the people an account of what they have been doing, and a refusal to provide this is simple insolence."Jeremy Waldron, "Accountability and

estar acompanhada de responsabilização e prestação de contas.

Não quero assim sugerir que a determinação do que seja uso legítimo da força e o que passa a ser abuso seja uma determinação fácil na prática. O abuso da discricionariedade – que passa a ferir direitos, extrapolar a legalidade e configurar resposta ilegítima – nem sempre é evidente. Em casos concretos, principalmente na tomada de decisão por policiais que estão na linha de frente da implementação do policiamento – o "burocrata do nível de rua"[106] – talvez seja ainda mais. Ainda assim, o argumento aqui é que, apesar dessas dificuldades, a referência de atuação de princípios de um direito administrativo comprometido com a dignidade é que existam políticas, protocolos e atuação prática em sintonia com a proteção a direitos – e que mecanismos de controle funcionem na manutenção e sustentação desses princípios.

Dito isso, reconheço desde logo que, no cenário brasileiro, casos de abuso policial principalmente a nível de rua são comuns e que os "perturbadores" são pessoas em situação de vulnerabilidade social, negligenciados pela política criminal que prefere a criminalização seletiva a outras políticas sociais[107]. Do ponto de vista sociológico, atribui-se o cenário à herança histórica de doutrinas que ligam a atuação da polícia a interesses do Estado (e não como mecanismo protetor de direitos), à existência de um "currículo oculto" ou "programa de rua" que incentiva a brutalidade, e a mecanismos frágeis e sistematicamente falhos de controle interno e externo.[108] Sob a perspectiva que tenho construído aqui, parte disso pode sinalizar problemas graves nessa estrutura de legitimação da atuação policial no Brasil – e, portanto, na forma como o Estado brasileiro está resguardando o "direito à segurança" enquanto regulação pública – que devem ser objeto de análise e reforma. A polícia que "mira na cabecinha"[109] ou que responde a protestos com

---

Insolence", in *Political Political Theory: Essays on Institutions* (Cambridge, MA: Harvard University Press, 2016), 190.

[106] Samira Bueno, Renato Sérgio de Lima, e Teixeira, Marco Antonio C., "Limites do uso da força policial no Estado de São Paulo", *Cadernos EBAPE.BR* 17, nº Edição Especial (2019): 796. Uma referência ao trabalho Michael Lipsky, *Street-Level Bureaucracy: The Dilemmas of the Individual in Public Service* (Russell Sage Foundation, 1983).

[107] Júlia Barbon e João Pedro Pitombo, "Casos de abusos de policiais em abordagem são rotina no Brasil", *Folha de S. Paulo*, 18 de julho de 2020, https://www1.folha.uol.com.br/cotidiano/2020/07/casos-de-abusos-de-policiais-em-abordagem-sao-rotina-no-brasil.shtml.

[108] Lima, Bueno, e Mingardi, "Estado, polícias e segurança pública no Brasil"; Bueno, Lima, e Teixeira, Marco Antonio C., "Limites do uso da força policial no Estado de São Paulo"; Rafael Mafei Rabelo Queiroz e Natalia Neris, "Revoar - Servir a quem, proteger o quê?", Temporada 1, acessado 6 de agosto de 2020, https://open.spotify.com/episode/6UnkIg44OkZdwifCB5uULL?si=oaHHYracRrOow1ZpkcrxQA; Gisela Aguiar Wanderley, "Entre a lei processual e a praxe policial: Características e consequências da desconcentração e do descontrole da busca pessoal", *Revista Brasileira de Ciências Criminais*, nº 128 (2017): 115–49.

[109] "Wilson Witzel: 'A polícia vai mirar na cabecinha e… fogo'", *VEJA*, 1º de novembro de 2018, https://veja.abril.com.br/politica/wilson-witzel-a-policia-vai-mirar-na-cabecinha-e-fogo/.

balas de borracha[110] não é uma polícia que se reconcilia com nossos compromissos de tratar as pessoas com dignidade – uma concepção de segurança que convive com a noção de igual respeito não poderia acomodar esse tipo de atuações. Nesse sentido, valendo de um diagnóstico de especialistas em segurança pública que também serve aqui: "falta-nos um projeto de governança das polícias brasileiras e de alinhamento das políticas de segurança pública aos requisitos da democracia e à garantia de direitos humanos"[111].

Os desafios vão além disso: as atividades comuns e básicas de preservação da segurança interna a um país vêm sendo confundidas com outras lógicas de atuação que, se possuem justificativa no seu contexto próprio, em tese não poderiam justificar como a polícia lida com seus próprios cidadãos. No Brasil, a criminalidade urbana é com frequência vista como "inimigo" (interno) a ser combatido – não só por polícias, mas até pelas Forças Armadas. Com efeito, a atuação das Forças Armadas brasileiras, uma instituição militar voltada à "defesa da Pátria" – do território brasileiro e de suas instituições constitucionais sobretudo – e a ser empregada principalmente em situações de conflito armado sobretudo (no papel) decorrentes de "ameaças externas", é também convocada em questões domésticas, e policiais, como nas atuações de "Garantia da Lei e da Ordem"[112] – atribuição que compartilha com as polícias, muito embora de forma subsidiária. Outro exemplo dessa confusão é a atribuição explícita de atividades tipicamente policiais – de patrulhamento, revistas e prisões em flagrante delito – aos órgãos militares em áreas de fronteira[113]. Os terrenos e as lógicas vão se confundindo.

---

[110] "Justiça de SP autoriza uso de bala de borracha pela PM em manifestações", *Folha de S.Paulo*, 8 de novembro de 2016, http://www1.folha.uol.com.br/cotidiano/2016/11/1830368-justica-de-sp-libera-uso-de-bala-de-borracha-pela-pm-em-manifestacoes.shtml.

[111] Lima, Bueno, e Mingardi, "Estado, polícias e segurança pública no Brasil", 50.

[112] Lei Complementar nº 97/1999, Art. 15, §2º: "A atuação das Forças Armadas, na garantia da lei e da ordem, por iniciativa de quaisquer dos poderes constitucionais, ocorrerá de acordo com as diretrizes baixadas em ato do Presidente da República, após esgotados os instrumentos destinados à preservação da ordem pública e da incolumidade das pessoas e do patrimônio, relacionados no art. 144 da Constituição Federal."Cf. Diego Nunes, "As iniciativas de reforma à Lei de Segurança Nacional na consolidação da atual democracia brasileira: da inércia legislativa na defesa do Estado Democrático de Direito à ascensão do terrorismo", *Revista Brasileira de Ciências Criminais* 107 (2014): 265–305; Diego Nunes, "'Garantia da Lei e da Ordem', 'comoção intestina' e outras vaguezas constitucionais na história dos regimes jurídicos da exceção", in *Estudos de direito público: aspectos penais e processuais*, org. Leonardo Schmitt de Bem, D'Plácido (Belo Horizonte, 2018), 633–38.

[113] Lei Complementar nº 97/1999, Art. 16-A (incluído pela LC nº 136/2010): "Cabe às Forças Armadas, além de outras ações pertinentes, também como atribuições subsidiárias, preservadas as competências exclusivas das polícias judiciárias, atuar, por meio de ações preventivas e repressivas, na faixa de fronteira terrestre, no mar e nas águas interiores, independentemente da posse, da propriedade, da finalidade ou de qualquer gravame que sobre ela recaia, contra delitos transfronteiriços e ambientais, isoladamente ou em coordenação com outros órgãos do Poder Executivo, executando, dentre outras, as ações de I - patrulhamento; II - revista de pessoas, de veículos terrestres, de embarcações e de aeronaves; e III - prisões em flagrante delito".

Essa confluência preocupa não só por invocar parâmetros de exceção de atuação das Forças Armadas a práticas de segurança cotidianas, como também da perspectiva da desnaturação de atividades policiais pela lógica do inimigo. Como explica Arthur Trindade Costa,

> Num regime democrático, a diferença fundamental entre polícia e exército reside no controle da força: se este não constitui uma questão central no caso das forças armadas, é justamente tal controle que torna as polícias compatíveis com um regime democrático. (...) Estruturalmente, ambos estão sempre de prontidão para usar a força, mas a polícia deve considerar a possibilidade de não usá-la ou de usá-la de forma limitada, mesmo quando isso implique o emprego de maiores recursos humanos e materiais.[114]

Como explica o autor, o que diferencia policiais de soldados é – em tese – a ausência da figura do "inimigo": soldados possuem inimigos bem-definidos e estão autorizados a usar a força para abatê-los; policiais lidam, por sua vez, com cidadãos – entendidos assim inclusive os que cometem infrações. Borrar fronteiras entre diferentes atividades de segurança traz esses prejuízos: "Essa analogia permite que as polícias elejam seus inimigos, normalmente entre os segmentos política e economicamente desprivilegiados, bem como incentiva o uso da violência".[115] Sintomaticamente, Humberto Fabretti aponta que, nos debates da constituinte de 1988, esteve em pauta um confronto entre um ideal de segurança pública de herança militar como um tipo de combate a inimigo – transmutado do 'comunista' para o 'traficante' (e outras categorias análogas) e uma visão de serviço público voltada a proteger cidadãos, comprometida com liberdades fundamentais e com a participação da sociedade civil na gestão do tipo de segurança a ser promovido.[116] Nenhum deles teria prevalecido no texto, mantendo-se espaços para disputas sobre seu sentido (e para o legado autoritário permanecer).

Nada disso contribui com qualquer clareza aos limites da atuação policial no Brasil, tornando ainda mais relevante retornar aos fundamentos da justificação teórica dessa atuação e a qual o valor da segurança que apreciamos e até onde o compromisso com a dignidade permite ir no contexto de combate a crimes internos. Sei que a "situação de normalidade" social que recortei para tratar de crimes em contraste a cenários de guerra é desafiada pela retórica política e por episódios graves que ficam na memória – como ataques coordenados, ordenados por facções, que param cidades –, além de atropelada por iniciativas práticas que querem lidar com o problema da

[114] Costa, "Como as democracias controlam as polícias: os mecanismos institucionais de controle da atividade policial", 69.
[115] Costa, 73.
[116] Fabretti, *Segurança pública: fundamentos jurídicos para uma abordagem constitucional*, 86–88.

ocorrência de crimes com táticas de guerra. Ao mesmo tempo, o que honra nossas pretensões de viver em condições que não se confundem com a de um estado de exceção é a constatação de que não estamos de fato em guerra, de que não devemos equivaler situações que não se equivalem e de que a segurança que valorizamos em uma democracia convive com liberdades e por isso exige políticas de segurança que não pressupõem guerra onde os problemas sociais que enfrentamos são de outra ordem.[117]

Perigos abstratos

O que dizer da situação em que não há um perigo concreto e imediato? Esse é justamente o campo em que a mobilização de estruturas do direito penal não está de modo algum justificada, porque se reserva às pessoas autonomia (ainda que cogitem, desejem e sonhem com o mal, enquanto isso não passar do plano intelectual, não se pune). Isso coloca um impedimento de princípio na forma como se faz policiamento e sobre quais políticas de segurança se implementa: a polícia não pode ter as mesmas prerrogativas que têm no processo penal e em situações de emergência, sob pena de equivaler circunstâncias que não se equivalem, de anular razões específicas que justificam sua atuação naqueles campos. Isso a princípio não obstaculiza, contudo, políticas públicas que busquem reduzir a prática de crimes, mas também não significa que

[117] Como disse ainda na introdução e retomo aqui, estou ciente de que o cenário da criminalidade no Brasil é com frequência associado a um de "guerra". Isso ocorre na retórica política para justificar políticas de segurança pública e é estudado por acadêmicos. Ver Bruno Paes Manso e Camila Nunes Dias, *A guerra: a ascensão do PCC e o mundo do crime no Brasil* (São Paulo: Todavia, 2018). Não acredito que o "mundo do crime" no Brasil coloca uma situação de "anormalidade" para efeitos do que estou falando aqui – por "normalidade", refiro-me a um contexto, a um modo de vida, que convive com ocorrências de crimes, mas que possivelmente seria abalado se houvesse uma guerra que tomasse o país. Embora despontemos em rankings internacionais sobre índices de homicídios, roubous/furtos, tráfico de drogas, corrupção, o que mostra que o brasileiro provavelmente vive sob uma probabilidade maior de ser vítima de crime do que cidadãos de outros países, os crimes que se pratica no Brasil não são específicos do Brasil nem permitem analogia com a vivência de países em guerra. Além disso, para o contexto das discussões de privacidade que faço nesse trabalho, a associação com um cenário de guerra para imprimir medidas invasivas mais agressivas pela "segurança" seria um erro. Como sugerem as próprias obras que estudam a "guerra" que o crime organizado provoca no Brasil, as origens dessa "guerra" são políticas de segurança pública falhas que (i) não mitigam problemas de desigualdade; (ii) focam em patrulhamento de rua e não equipam a polícia com aparato de investigação capaz de pegar responsáveis pelo "atacado"do tráfico de drogas (não o varejo); (iii) não oferem melhores condições de sobrevivência e ressocialização de condenados no sistema penitenciário; (iv) alimentam a nacionalização de facções criminosas e, ao deixa-las crescer, as brigas (e violência) entre membros delas. Nada disso é um problema provocado pela existência de práticas de privacidade, a ponto de sugerir que devemos considerar as consequências dessa política de segurança pública fracassada uma "situação de anormalidade" que deveria justificar restrições ao direito à privacidade e ao sentido que deve ter em um Estado democrático comprometido com a igual consideração e respeito. A causa dessas "guerras" e episódios internos é outra e, se quisermos tratá-la, não são direitos de privacidade que devem pagar – não só porque não trataria das raízes do problema, mas porque seria um erro achar que o preço de buscar um direito à segurança a que temos direito moral segundo a melhor leitura da dignidade (tal como propus aqui) é um em que não temos direitos à privacidade que se extraem desse mesmo compromisso com a dignidade.

iniciativas nesse campo não devam estar sujeitas, como toda atuação do Estado em nome da segurança, a mecanismos de controle.

A dimensão geral preventiva da atuação estatal para segurança envolve uma série de escolhas de política criminal sobre a definição de "perigos" – mais abstratamente tratados mas ainda dentro do conjunto de crimes tipificados – que se vai priorizar combater e como isso será feito. Isso é anterior à atuação policial, por vezes independente dela e pode alcançar um número indeterminado e generalizado de pessoas – muito além dos "perturbadores". Como ilustra Shecaira:

> "(...) [Q]uando a Prefeitura, diante da ocorrência de sucessivos crimes de estupro, em um lugar mal iluminado da cidade, resolve prevenir a ocorrência de novos delitos, com a instalação de novos postes de luz, está fazendo política criminal preventiva. Também o faz quando elege a segurança dos munícipes como uma de suas prioridades ao criar a *Secretaria de Segurança Urbana.* Da mesma forma, ao implementar políticas públicas mitigadoras de contrastes sociais, estará implantando uma política com repercussão na esfera criminal. Também o Poder Executivo na esfera do Estado faz política criminal. A Secretaria de Segurança Pública de São Paulo, ao adotar o sistema informatizado de mapeamento da criminalidade, rua a rua, denominado Infocrim, agiu conforme uma política criminal."[118]

Como se vê, há uma ampla variação de atuações possíveis do Poder Público em nome da "segurança" nessa dimensão preventiva geral, anterior a e até independente de atuações policiais e/ou, mais particularmente, anterior a investigações concretas sobre fatos específicos. Muitas delas não envolvem qualquer questão de privacidade; outras já começam a despertar discussões sobre o tema e suscitam a questão de sua compatibilidade. A política de policiamento amparada em "enquadros" nas ruas (abordagens policiais para identificação e busca pessoal) é um exemplo – alcança-se uma enorme quantidade de pessoas sob a justificativa de prevenção criminal, mesmo sem situações claras de perigo.[119] As políticas de prevenção à lavagem de dinheiro e ao financiamento ao terrorismo pelo monitoramento de todas as transações do sistema financeiro, outro. No próximo capítulo, quando voltar a falar mais particularmente de privacidade, voltarei a esses exemplos.

O último exemplo do excerto citado já acena ao leitor a nova fronteira impulsionada pela tecnologia – policiamento por *big data* e outros sistemas de monitoramento "inteligente". A ideia que tem ganhado popularidade é utilizar as capacidades atuais de coleta, estruturação e análise de

[118] Shecaira, *Criminologia*, 42–43.
[119] Jéssica da Mata, *A política do enquadro* (São Paulo: Revista dos Tribunais, 2021).

grandes volumes e variedades de dados para produzir inteligência que sirva à atuação policial. Para que não haja dúvidas: é fato que a polícia sempre coletou informações e trabalhou com elas – inclusive alcançando pessoas de forma geral. Com o tempo, foram criando bases de dados de boletins de ocorrência, de identificação criminal, de abordagens, de mandados de prisão em aberto, e afins.

A tecnologia, no entanto, amplia essas capacidades de forma sem precedentes. Além de avançar para superar o caráter fragmentado dessas informações e bases de dados, há cada vez mais coleta de dados e formação e disponibilização de bancos de dados – públicos e até privados.[120] A polícia sempre monitorou vias públicas; mas agora consegue coletar informações sobre placas de carros que trafegam nas principais ruas e avenidas da cidade, guardar essas informações, analisa-las em escala, utilizá-las para localizar pessoas e como arcabouço de provas pré-constituídas, por exemplo. Essas possibilidades permitem o delineamento de novas estratégias de policiamento e de prevenção e detecção de atividades criminosas[121] – não sem preocupações sobre o impacto em pessoas de forma geral e sem *suspeita* sobre qualquer um deles.

Na obra de Lucia Zedner, suas observações sobre o tema fazem parte de um diagnóstico maior sobre como os paradigmas do sistema de justiça criminal vêm sendo desafiados pelo "ideal de segurança": o crime é menos visto como um ato moralmente errado cujas raízes estão em problemas sociais e econômicos e passa a ser visto principalmente como resultado de uma "oportunidade" gerada por alterações demográficas e processos de socialização.[122] O crime é

[120] Nesse sentido Sarah Brayne, *Predict and Surveil: Data, Discretion, and the Future of Policing* (Oxford: Oxford University Press, 2020), 78-101 (e-book).

[121] Andrew Guthrie Ferguson, *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement* (New York: New York Univeristy Press, 2017).Exemplo no Brasil é o "Projeto Tentáculos" da Polícia Federal, que repousou sobre a análise de notícias-crime envolvendo internet banking e clonagem de cartões da Caixa Econômica Federal. A análise agregada das informações serviu para identificar correlações, abrindo novas linhas de investigação e estratégias de repressão, antes da instauração de inquérito policial. Luís Antônio Vilalta e Talles Amaral Machado, "Novos Paradigmas da Investigação Criminal", *Revista Brasileira de Ciências Policiais* 9, nº 1 (8 de novembro de 2018): 13–41, https://doi.org/10.31412/rbcp.v9i1.542.

[122] "In a striking development, in the security society, crime is seen less as a moral wrong, a threat to shared values, or a culpable act in need of punishment than as a bundle of physical, psychological, and material losses or as a potential hazard whose cost can be calculated, minimized, and insured against (Williams 2005a). Gone is the understanding of deviance as inseparable from the wider sources of misery in modern society. Crime is no longer ineradicably linked with the big social and economic problems of poverty, inequality, poor education, housing, and health care. Personal life histories, the influence of family, social class, race, gender, and economic deprivation are excluded from consideration. Characteristic is Felson's claim that 'it is a mistake to assume that crime is part of a larger set of social evils, such as unemployment, poverty, social injustice, or human suffering' (Felson 2002: 12). Instead, crime is said to result more from the multiplication of opportunity than changes in demography, social structure, or socialization processes. Wide availability of small, light, portable and high-value consumer goods (like mobile phones), mass car ownership, and increased leisure activity (in particular, the night-time economy of clubs and bars) create new

reconceptualizado como um "risco de segurança"[123]. Decorrência disso é uma mudança de enfoques: para combater crimes, é preciso reduzir as oportunidades para praticá-lo. Nesse fenômeno se enxerga o avanço de uma lógica "pré-cime", "situacional", atuarial e precaucionária – e que traz mudanças nas orientações, modelos e formas de atuação policial – inclusive o avanço de estruturas de monitoramento (CCTV) e de retenção obrigatória de dados.[124]

Nesse cenário, a distinção entre esforços *repressivos* típicos do processo penal e esforços *preventivos* fica borrada. Se o Estado passa a acumular e analisar registros de atividades humanas por precaução, para não só prevenir crimes, mas garantir detecção de crimes e eficiência na punição, a linha de separação de ambos os campos de atuação que foram objeto de autonomização dogmática fica apagada. Pior: reprimir o crime enquanto uma violação moral a uma decisão polítca coletiva da comunidade vai pouco a pouco se tornando uma preocupação secundária àquela de estimar, conter e minimizar "riscos de segurança".[125] Isso contribui, conclui Lucia Zedner, para um "senso crescente de que 'presunção de inocência', 'prova além da dúvida razoável' e a exigência de proporcionalidade na punição são luxos jurídicos inadequados para os perigos atuais".[126] A submissão de pessoas a certas punições ou medidas coercitivas (como medidas de vigilância) não porque cometemerem e merecem certa pena, mas porque pertencem a certo grupo social que estatisticamente estaria mais associado a riscos de segurança passa a ganhar espaço nessa lógica atuarial. Nessa conjuntura, os valores que historicamente nortearam nossas avaliações morais no sistema de justiça criminal passam a ser ameaçados.

Essas novas tendências precisam ser submetidas a uma avaliação crítica – de sua compatibilidade com o tratamento com igual consideração e respeito que o Estado deve a nós e com uma concepção de segurança comprometida com a dignidade. Em termos de tutela de direitos e contenção de arbítrio, se nos questionarmos qual o controle sobre isso, sobre o que é possível ou não e principalmente sobre o *como,* não encontraremos resposta nas regras vigentes de direito processual penal, nem na construção dogmática atual do direito administrativo. A partir de tudo

temptations and new opportunities for crime as well as increased occasions for drunkenness, disorder, and interpersonal violence (Hobbs *et al.* 2003, Hadfield 2006). These opportunities are said to be more important in explaining crime rates than moral or social breakdown." Zedner, *Security*, 69.

[123] Zedner, 71. Para um exemplo de estudo que aplica essa lógica no Brasil, ver Tiago Ivo Odon, "Segurança pública e análise econômica do crime: o desenho de uma estratégia para a redução da criminalidade no Brasil", *Revista de Informação Legislativa* 55, nº 218 (2018): 33–61.

[124] Zedner, *Security*, 72–88.

[125] Zedner, 77.

[126] Zedner, 80.

visto, podemos certamente ver como essas iniciativas destoam de nossas práticas até aqui e dos pressupostos morais que as alimentam, já que se tornam secundários: o caráter retributivo da *pena* – elemento que coloca o "teto moral" sobre quem pode suportá-la vai pouco a pouco sendo apagado por uma associação do uso da pena a quem coloca "risco".[127] A ideia de que o aparato policial do Estado para segurança só será acionado contra alguém diante de lesão concreta (ou ao menos ameaça imediata) a direito alheio, também.

Nesse contexto, a concepção de segurança imbricada com a dignidade e que apoia esforços regulatórios de justificação distributiva no direito penal e no direito administrativo policial contra perigos concretos e imediatos encontra seu limite. Diante das novas tendências, e no que afetam direitos, ou as rejeitamos/abandonamos reafirmando compromissos contra uma política criminal atuarial e o arrastamento generalizado de pessoas inocentes ao sistema de justiça criminal (se não necessariamente correm risco irrazoável de serem condenados, certamente passam a ficar sujeitas a inúmeras microagressões e microinjustiças por violações indevidas à sua privacidade e outros direitos, além de a um tratamento que pressupõe desconfiança, por conta do projeto geral de diminuição de riscos de segurança) ou, no que reconciliável, traduzimos nossos compromissos frente a essas novas formas de atuação.

Algumas considerações tecidas por Lucia Zedner reforçam a necessidade dessa avaliação. Ela alerta que é comum se falar nessa "segurança" em discursos políticos como um bem público ou uma *commodity* desejável, como se atuações e escolhas políticas dessa envergadura não precisassem de justificação – o discurso do "superprincípio", como já vimos. Sustenta que isso é um erro, porque a adoção de medidas de segurança nessa linha atuarial carregam custos na forma de paradoxos: (i) buscam reduzir o crime, mas supõem que ele persistirá, com ameaças mudando constantemente;[128] (ii) supõem que podem ser capazes de reduzir repressão por direito penal, mas na verdade não parecem fazer isso e podem aumentar criminalização e encarceramento; (iii) buscam falar às necessidades de garantia (*assurance*) da população sobre sua segurança, mas podem aumentar a ansiedade ao lembrar constantemente da existência e ameaça de crime; (iv)

[127] Maurício Stegemann Dieter, "Política Criminal Atuarial: A Criminologia do fim da história" (Tese de Doutorado, Curitiba, Universidade Federal do Paraná, 2012); Maiquel Ângelo Dezordi Wermuth, "Política criminal atuarial: contornos biopolíticos da exclusão penal", *Revista Direito e Práxis* 8 (setembro de 2017): 2043–73, https://doi.org/10.1590/2179-8966/2017/22314.

[128] Bruno Cardoso, que fez pesquisa etnográfica em central de comando e controle da Polícia Militar do Rio de Janeiro, chama de "paradoxo do flagrante" o fenômeno ambíguo que observou entre policiais de querer que as câmeras de monitoramento reduzam crime ao mesmo tempo em que flagrantes continuem existindo como 'evidência' de que funcionam. Cardoso, *Todos os olhos: videovigilâncias, voyeurismos e (re)produção imagética*, 199–204.

supõem ser um bem de caráter universal, mas podem promover exclusão social segundo o que e quem considera, identifica e direciona como ameaça; (v) prometem garantir liberdades, mas têm igual potencial de reduzir níveis de liberdade; e (vi) buscam promover um bem que seria público, mas essa adoção é predicada em uma falta de confiança nos cidadãos e entre cidadãos, o que pode levar a uma erosão da solidariedade social.[129] Por essas razões, precisaríamos de um modelo que justifique tais medidas (ou denuncie e coíba o que não se justifique) tanto quanto precisamos de uma teoria para justificar a justiça criminal.

Em outras palavras, a dimensão mais abstrata da realização do valor da segurança pelo direito administrativo também precisa ser justificável e controlar o poder do Estado – na linha desenvolvida até aqui, precisa estar comprometida com a dignidade. Como fazer isso? A sugestão inicial de Zedner consiste em resgatar (i) o "princípio do minimalismo", que barraria a tendência de medidas de segurança por pequenas coisas (incômodos menores ou comportamentos ofensivos triviais) e (ii) o princípio da proporcionalidade: "essa precaução é proporcional ao risco colocado?".[130] Essas sugestões encontram eco no que a doutrina de direito administrativo já supõe ao falar no princípio da proporcionalidade para a atuação do poder público: medida deve ser adequada, necessária e proporcional em sentido estrito.[131] O princípio da proporcionalidade, sintomaticamente, nasceu no âmbito do *Polizeirecht* (direito de polícia) alemão.[132]

Há espaço para e necessidade de elaboração e afirmação de mais princípios que esses – e para o reconhecimento da discussão sobre o próprio valor da segurança (e de sua relação com outros direitos) que essas iniciativas colocam (e que escapam da pergunta de proporcionalidade em sentido estrito e das definições abrangentes de direitos com que testes desse tipo começam). Como vimos, uma concepção de segurança em que vale tudo e que não se reconcilia com as

---

[129] Lucia Zedner, "Too much security?", *International Journal of the Sociology of Law* 31, nº 3 (1º de setembro de 2003): 157–73, https://doi.org/10.1016/j.ijsl.2003.09.002.
[130] Zedner, 176.
[131] Cf. Marçal Justen Filho, *Curso de direito administrativo [livro eletrônico]*, 5º ed (São Paulo: Thomson Reuters Brasil, 2018). Também: "É a lei que deve pautar a atuação dos órgãos e é em cumprimento a ela que as polícias devem agir. Os direitos e liberdades só podem ser restringidos por lei, a mesma lei que autoriza a atuação dos agentes de segurança pública. Essa atuação, por sua vez, deve ainda ser adequada, necessária e proporcional. O registro, a justificação e a publicidade dos argumentos que atestam a presença de tais requisitos são indispensáveis não apenas para o controle interno e externo da atividade policial, como também para validar a legalidade da atuação dos órgãos de polícia." Maria Pia Guerra e Roberto Dalledone Machado Filho, "O regime constitucional da segurança pública: dos silêncios da Constituinte às deliberações do Supremo Tribunal Federal", *Revista de Informação Legislativa* 55, nº 219 (2018): 173–74.
[132] Jud Mathews e Alec Sweet, "Proportionality Balancing and Global Constitutionalism", *Columbia Journal of Transnational Law* 47 (1º de janeiro de 2009): 96–104.

liberdades valorizamos não é atraente. Há certos "riscos de segurança" que incorremos – como o de que nosso parceiro vá nos assassinar e não haverá um policial ao lado para contê-lo – simplesmente porque valorizamos outras coisas também, como a confiança e a cumplicidade. Embora seja mais que adequado e necessário que o Estado implemente políticas públicas contra violência doméstica, dificilmente essa meta de prevenção poderia justificar que todas as casas no Brasil fossem vigiadas a todo tempo. Embora submeter todos os cidadãos anualmente a testes de personalidade e de perfilhamento para verificar suas tendências à violência em instâncias de surtos de raiva e ciúmes, e assim detectar quem deveria ser objeto de medidas preventivas, pudesse conter episódios trágicos e crimes desoladores, isso não trataria pessoas com o respeito e a consideração que devemos um ao outro – e que valorizamos, apesar de que para isso tenhamos de suportar risco maior de sermos vítimas de crimes.

Nós incorremos esse risco tanto por questões práticas como limitação orçamentária (e nosso desejo de direcioná-lo a outras áreas para além da segurança), quanto porque seria degradante para a humanidade esse tipo de tratamento, tendo em vista como vivemos hoje: desconstituiria a premissa de que buscamos viver com dignidade – conduzir nossas vidas sob a responsabilidade pessoal que nos é dada e exigida e cientes de seu valor. Isso nos reserva, por *default,* a expectativa de que exerceremos nossa autonomia moral buscando evitar causar danos deliberados à vida de outras pessoas. Temos direito a esse respeito, mesmo que sem ele a sociedade fosse posta sua situação marginalmente melhor. Essa visão de segurança incompatível com direitos não é uma visão de segurança comprometida com a dignidade (com a promoção da segurança para mantê-la a níveis razoáveis, não absolutos), o que é suficiente para afastar iniciativas nessa linha. Não me reporto a uma *ponderação* de interesses genéricos sobre a vida e a privacidade, mas a um exercício interpretativo sobre nossos valores que envolve a articulação de uma teoria da justiça, em último grau. Se alienígenas invadissem a terra e com eles trouxessem um vírus que aumentasse exponencialmente a tendência de pessoas matarem seus esposos e colegas em crises de raiva e ciúmes (trazendo uma situação de anormalidade), talvez repensássemos a necessidade de realização de testes anuais, mas no nosso modo de vida hoje, seria um erro superestimar o risco de ser morto nessas condições em detrimento de outros dos nossos valores. Não seria medida que compõe um direito à segurança; seria uma medida que persegue *interesses* à segurança, mas que seriam *trunfados* por um direito à privacidade.

Ademais, e no que for passível de regulação, nossas preocupações quanto à fixação de

padrões que asseverem qual o nível de risco de sofrer injustiça estamos dispostos a suportar e como conter o poder do Estado contra acúmulo indevido de poder, abuso e excesso, em tese, permanecem as mesmas que primeiro nortearam aqueles que desenvolvemos no processo penal. Elas devem acompanhar, portanto, tudo o que há de esforço regulatório para novas fronteiras. Inclusive, havendo enorme histórico de abusos em uma polícia como a brasileira, isso pode envolver não admitir certas prerrogativas policiais ou estabelecer arranjos regulatórios que lidem com os riscos específicos que já conhecemos na realidade brasileira (como racismo estrutural). Em outros trabalhos, por exemplo, Zedner avança mais princípios, entre eles um que seria a "presunção contra ameaça" – algo que faria as vezes da presunção de inocência: alguém não poderia ser considerado "ameaçador", perigoso, simplesmente por pertencer a uma classe ou categoria e nem mesmo ao indivíduo mais "ameaçador" no nível de "risco de segurança" seria possível atribuir culpa antes de um evento, preservando assim a ele uma janela de oportunidade de escolher o que é certo em respeito à sua autonomia moral.[133] Há muito a se avançar na discussão se esse tipo de tendência preventiva é aceitável e, na medida que for, como regulá-la.

Além da novidade de toda parte dessa lógica que é alimentada por novas tecnologias, o desafio é, no direito brasileiro, o discurso de "discricionariedade" sobre essas medidas e de "conveniência e oportunidade" sobre escolhas políticas que dificultam revisão a nível administrativo e judicial, ao lado de cobrança histórica por "eficiência" na alocação de recursos para redução e no controle da criminalidade.[134] Há dificuldades institucionais para o aperfeiçoamento de regulação e mecanismos de controle nessa área. Nesse trabalho não preciso me preocupar com essa camada de problema a nível geral, mas com a medida em que ações programáticas promovidas em nome da segurança pública podem interferir com práticas de privacidade e como devem ser reconciliadas com direitos a prerrogativas de privacidade e outras políticas regulatórias – como a de proteção de dados pessoais.

4 Conclusão parcial

Neste capítulo, procurei elaborar, em linhas gerais, o significado e o valor do conceito de segurança. Comecei a partir de observações de Jeremy Waldron sobre os diferentes sentidos em

[133] Zedner, *Security*, 172–73.
[134] Odon, "Segurança pública e análise econômica do crime". Para uma crítica desse tipo de visão, por negligenciar outros valores, ver Zedner, "Too much security?"

que se invoca esse conceito e, almejando expandir e aprofundar a noção de *segurança* enquanto proteção a pessoas de uma comunidade, as suas dimensões possíveis – do seu sentido mínimo como proteção à integridade física às suas relações com o próprio exercício de liberdades. Suas discussões mostram como segurança é um conceito disputado, na política e no direito. Por isso, é inevitável elaborar e discutir qual poderia ser o escopo desse valor.

Liora Lazarus destrinchou o debate em torno de um *direito à segurança*: o atributo de *direito* reporta-se em grande medida ao discurso político de invocar deveres de ação correspondentes do Estado, mas a atribuição de uma concepção abrangente não é atraente. Para Lazarus, a *securitização de direitos,* relacionada a um movimento crescente de reconhecimento de "seguranças" sobre direitos de diversos tipos é perigosa, poluindo disputas ao sacrifício da liberdade. Mais importante para esse trabalho, entretanto, foi identificar que subjacente a essa disputa há uma controvérsia até mesmo sobre a relação da segurança com outros valores: é o valor central, que antecede a própria dignidade? Conferir centralidade à segurança, no entanto, não seria capaz de explicar e justificar diversas práticas em que convivemos com riscos à segurança, inclusive física. Nessa mesma linha, vimos que uma concepção abrangente de segurança que visse em qualquer intervenção a um interesse genérico de segurança uma perda de direito não capta o valor desse conceito.

Por sua vez, uma articulação robusta de como o valor da segurança decorre da própria dignidade traz nuances à concepção dela que não são apreendidas por concepções abrangentes. Como desenvolveu Dworkin em sua teoria da justiça, um sistema de regulação da segurança é necessário para que se possa desenhar uma distribuição igualitária de recursos: as pessoas precisam ter segurança sobre as liberdades que poderão exercer com seus bens e suas próprias vidas. Mais que isso, vimos como a nossa responsabilidade de viver nossas vidas deve incluir um "poder de controle" sobre os atos que serão praticados no exercício dessa responsabilidade que nos foi atribuída (viver uma vida bem vivida) e que "danos deliberados" contra pessoas que firam essa responsabilidade violam a dignidade devida a toda pessoa.

O Estado nos deve – e esse é um direito político básico – uma regulação em matéria de segurança que se mostre ser um esforço razoável de proteção à vida, à integridade física e à propriedade, inclusive por meio de responsabilização criminal, contra intervenções indevidas de terceiros – tanto os demais cidadãos como os próprios agentes/funcionários do Estado. O arranjo concreto é uma questão *política* a ser legislada. Em qualquer caso, entretanto, a regulação é

moldada pela própria dignidade. Não vale tudo pela segurança; ela deve ser compatibilizada com direitos como a liberdade de expressão e privacidades. Deve também ser executada a partir de um compromisso forte com a igualdade no tratamento e no impacto. Sacrificar a segurança de uns para beneficiar a dos outros é incompatível com a igual consideração e respeito.

Para aproximar minhas considerações teóricas do direito brasileiro, esbocei também como áreas específicas do direito compõem essa regulação pública que realiza ou pretende realizar o objetivo político de promover a segurança. De forma específica, destaquei as principais racionalidades do Direito Penal, Direito Processual Penal e Direito Administrativo. Quis mostrar principalmente como a realização dessa regulação não abandona compromissos com a própria dignidade na intencionalidade desses campos de prática jurídica – e com a contenção de poder; deve ser assim para que a própria atuação estatal possa ser justificada. Nesses termos, também sinalizei como a lógica repressiva ou preventiva, individualizada ou generalizada, também invoca diferentes alcances do que se pode fazer pela segurança. Estando a polícia movida a interesses de segurança, e submetendo-se a regimes jurídicos específicos, essa foi uma etapa importante para dar continuidade ao trabalho.

Seja qual for o contexto, se quisermos dar um sentido atraente e consistente ao "direito à segurança" como direito a uma regulação pública, ele deve ser capaz de se conciliar com as demais proteções que irradiam do respeito à dignidade. Medidas de segurança que reduzem a criminalidade, mas provocam tratamento desigual não são compatíveis com a concepção atraente, integrada com a dignidade. Políticas de segurança que reduzem a criminalidade, mas desrespeitam direitos políticos e jurídicos como os de privacidade, tampouco. Isso também vale para a proteção de dados pessoais: medidas de segurança que envolvem uso de dados pessoais devem incorporar as preocupações regulatórias dessa área. No próximo capítulo, avanço nessas frentes.

Capítulo 3 – Um esboço de contextos: exigências de privacidade na atuação estatal pela segurança

No capítulo final da primeira parte deste trabalho, vou tratar de como as considerações que elaborei sobre o sentido do conceito de privacidade no contexto de atuações do Estado pela segurança, e, no caminho oposto, do sentido e alcance do valor da segurança, mais particularmente interagem entre si. Ao longo dos dois capítulos, isso já foi sugerido em diversas oportunidades. Busco, no entanto, oferecer um quadro mais sistemático nesse capítulo. As preocupações com contenção de poder que vimos a partir da análise dos dois conceitos se reforçam do início ao fim. A análise contextual mais concreta permite dizer quais mecanismos de princípio orientam a relação entre esses conceitos em diferentes cenários e que exigências materiais colocam.

1 Razões especiais, fundamentação e procedimentos

No direito brasileiro, ingressar na casa de alguém sem autorização é crime[1], invadir o computador de alguém sem autorização é crime[2], devassar correspondência é crime[3], interceptar

[1] Código Penal: Art. 150: Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências: Pena - detenção, de um a três meses, ou multa.

[2] Código Penal, Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. Em 2021, a redação foi alterada pela Lei nº 14.155: "Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa". Há ainda aumento de pena quando do acesso resultar obtenção de comunicações privadas, segredos comerciais ou industriais, informações sigilosas ou controle remoto não autorizado; quando houver divulgação; quando a vítima por autoridade de alto escalão.

[3] Código Penal, Art. 151: Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena - detenção, de um a seis meses, ou multa.

conversas telefônicas de alguém é crime[4], perseguir alguém é crime[5]. Para Malcolm Thorburn, "a razão pela qual a falta de consentimento é um elemento importante de tantas ofensas é que a injustiça da conduta em questão reside precisamente no fato de que constitui uma usurpação do poder exclusivo de outra pessoa para decidir o que deve ser feito com seu corpo ou propriedade"[6].

Como sugere o comentário, em linha com o que venho apresentando, o que esses tipos penais buscam tratar e proteger são direitos morais: bem ou mal em sua redação final, querem tutelar contra a usurpação de uma prerrogativa que um direito à privacidade garantiria à pessoa diante de algum terceiro, fundado em nossas práticas mais fundamentais sobre o que significa tratar uma pessoa como uma pessoa que é responsável por sua própria vida. No caso brasileiro, a esses direitos morais correspondem também direitos jurídicos – direitos que podem ser exigidos em tribunais. Estes são exemplos paradigmáticos de violações de direitos jurídicos de privacidade que encontram fundamentação moral, mas não necessariamente os únicos que cabe à prática jurídica tutelar – muito menos necessariamente com o direito penal. No direito civil lida-se com uma enorme variedade de questões e possíveis violações.

Apesar de termos uma enorme variedade de direitos à privacidade que, nos mais diversos contextos, podemos reivindicar frente a terceiros, algumas autoridades estatais são excepcionadas para engajar-se em condutas de acesso a informações pessoais, ingresso a espaços e até toques e extração de amostras do corpo, cuja definição e controle, se pode ter interpretação variada conforme os contextos, em geral reservamos à pessoa. Na linguagem recorrente e no contexto que é mais comum a autoridades policiais: elas podem "quebrar o sigilo" ou "afastar a inviolabilidade". Podem também "enquadrar pessoas" e querem poder também muito mais com novos recursos tecnológicos e com a crescente disponibilidade de informações pessoais. Para retomar a linguagem que estipulei, podem "acessar" informações pessoais por meio das mais variadas medidas de vigilância.

---

[4] Lei nº 9.296/96: "Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei: Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa."

[5] Código Penal (redação acrescentada pela Lei Federal nº 14.132, de 31 de março de 2021): "Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa." Há causas de aumento.

[6] Tradução livre. No original: "the reason why lack of consent is an important element of so many offenses is that the wrongness of the conduct in question lies precisely in the fact that it constitutes a usurpation of another person's exclusive power to decide what shall be done with her body or property". Thorburn, "Justifications, Power, and Authority", 1115.

Tendo em vista que nossas práticas paradigmáticas sobre acesso a casas, comunicações privadas, corpo e propriedade conferem especial relevância ao "consentimento" do titular, para se falar em respeito e reconciliação com elas, nessas situações, parece que a justificação deve passar, portanto, por uma explicação da autoridade do Estado para executar a medida de vigilância que o autorize a desconsiderar essa prerrogativa moral, ao mesmo tempo em que mostre respeito a ela. Sugeri que essa autoridade está diretamente relacionada à legitimidade moral e política daquele que vigia – o Estado. Não é autoridade por si só; é a autoridade que mostre respeito à dignidade daqueles que governa, entendida como valor intrínseco de suas vidas conjugada com sua responsabilidade pessoal. Deve haver procedimentos que caracterizem uma interpretação plausível daquilo que significa promover a segurança das pessoas em sua vida, integridade física e propriedade pelo combate à criminalidade violenta, motivo moral distributivo e impessoal, ao mesmo tempo em que acomode riscos de causar injustiças, danos a direitos morais de pessoas inocentes (por excessos, erros, abusos) nessa tarefa.

Nos arranjos de direito processual penal e direito administrativo vistos, e seus princípios subjacentes, pode-se extrair um princípio de igualdade central, repousado na dignidade: "o Estado deve tratar a todos igualmente, até ter boas razões para suspeitar de alguém"[7], na síntese de Thorburn. O elemento da *suspeita individualizada* é tão central em nossa prática jurídica que está imbricado em preocupações que vão além de privacidade: é um elemento que governa o uso da força estatal, limitando discricionariedade e arbítrio, que é apenas reforçado por interesses de proteção à privacidade e aos dados pessoais que temos visto – é um mecanismo que ajusta o nível de risco de sofrer/causar injustiça. Em particular, é um parâmetro que traduz um compromisso moral de evitar criminalizações indevidas[8]: se o próprio processo penal como um todo tem vários instrumentos para assegurar que a pessoa certa (e não um inocente) será condenada na aplicação da lei penal em respeito ao direito moral de não ser condenado se inocente, também precisa acomodar a necessidade de evitar violações a outros direitos ao fazer isso (e ao adotar outras

[7] Malcolm Thorburn, "Identification, Surveillance, and Profiling: On the Use and Abuse of Citizen Data", in *Seeking Security: Pre-empting the Comission of Criminal Harms*, org. G R Sullivan e Ian Dennis (Oxford: Hart Publishing, 2012), 32.

[8] Ver Katerina Hadjimatheou, "Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence", *Philosophy & Technology* 30, nº 1 (1º de março de 2017): 39–54. A autora defende que certos mecanismos de vigilância podem até inocentar pessoas de uma acusação de crime, de modo que não são per se contrários à presunção de inocência enquanto garantia a um *fair trial*. No texto, por outro lado, discute a preocupação com *wrongful criminalization,* uma noção que alcançaria preocupações com vigilância e acho que sintetiza também a ideia que quero passar aqui. Medidas de vigilância que criminalizam pessoas injustamente são um problema.

políticas de segurança que vão além da legislação penal, também, como falarei). Entre eles estão direitos de privacidade e até de reputação – de não ser injustamente tratado como suspeito de ter praticado (ou de que praticará) um crime.

Impõe-se e pode ser justificado por aspectos muito mais gerais de respeito ao valor intrínseco da vida e da responsabilidade pessoal: Estado não pode intervir na vida de alguém sem justa causa; não pode selecionar uma pessoa para submetê-la a restrições de sua liberdade em geral sem que ela tenha feito algo; não pode engatilhar mecanismos de coerção sem atender a parâmetros de justificação que são conhecidos e podem ser contestados.[9]

Repito: não são só direitos fortes à privacidade que governam essa lógica de contenção nem os únicos que impõem limites. O ponto é conter o poder do Estado e fazê-lo atuar legitimamente, respeitando a dignidade: a acomodação da privacidade e da proteção de dados é um reforço à essa ideia e uma perspectiva dela, não o único fator. Dito isso, esse elemento material, combinado com e na medida da necessidade de saber informações, é capaz de constituir uma razão especial para interferir no campo de controle do indivíduo sobre aspecto de relevância pessoal ou em outra prerrogativa moral sua existente no contexto da prática em questão. É relevante que haja decisão política coletiva primária que delimite a possibilidade de se causar dano moral (de violar injustamente uma liberdade valiosa ao conduzir a medida de vigilância) e ajuste o nível de risco a que se está sujeito a tolerar. Como veremos, esse mecanismo é e deve ser importado para nossas decisões sobre meios e métodos de investigação e os limites do que é possível.

Essa observação também coloca em perspectiva as possibilidades e os limites de medidas estatais em matéria de segurança que não se baseiam em suspeita individualizada nem perigo concreto e imediato, e que atingem pessoas de forma generalizada, de forma preventiva, ainda descolada e anterior à notícia de que houve prática de um fato criminoso. Essa área sai pela tangente do processo penal, que tende a receber o centro das atenções, compreensivelmente. É nela, entretanto, como adiantei no capítulo 2, que as mais diversas inovações tecnológicas vêm ocorrendo em nome de políticas de segurança pública mais efetivas. Ao mesmo tempo, é nela que a noção de que direitos morais (fortes) não comportam restrições baseadas apenas em interesse coletivo geral, mesmo que para a segurança pública, é de maior relevância. Interesses comportam restrições para bem geral, ainda que precisem também ser apreciados para que não sejam

[9] Emily Berman, "Individualized Suspicion in the Age of Big Data", *Iowa Law Review* 105 (2020): 478–81.

excessivos, tanto quanto possível. Direitos fortes, não; qualquer regulação não pode coibir nem causar dano sério a seu exercício.

Nesse sentido, como nem todas as atuações policiais pela segurança se inserem no caso focal de restrição à privacidade no processo penal, o cenário da articulação entre privacidade, proteção de dados pessoais e segurança é complexo. Apresento quatro contextos aproximados de atuação estatal que envolvem medidas de vigilância, subdivididos entre (i) atuação repressiva por meios de obtenção de provas, (ii) atuação fronteiriça entre repressão e prevenção para combate a perigos concretos e iminentes, (iii) atuação preventiva focadas em dissuasão/desestímulo à concretização de crimes; e (iv) atuação preventiva focada em auxiliar repressão e detecção de crimes com inteligência – item próximo do anterior, mas que reservo a usos intensivos de dados. Sobrepondo-se a esses grupos, diferencio as medidas como podem ou não afetar direitos à privacidade e as respectivas exigências normativas materiais de justificação.[10] O ponto que não se pode perder de vista e se aplica do início ao fim é o compromisso fundamental com a dignidade como aspecto básico para conter e legitimar o uso da força pelo Estado.

1.1 *Atos de persecução criminal: o caso de meios de obtenção de provas e a relevância da suspeita*

Após um evento criminoso, as próprias razões que fundamentam a legitimidade do Estado – e também fundamentam uma regulação de segurança pública comprometida com a dignidade – exigem que haja mecanismos para investigação e mesmo a responsabilização dos autores. Para atribuição de um fato concreto a alguém, a justificativa sozinha de prevenção geral não serve: a violação à dignidade que a imposição de pena acarreta deve estar atrelada a uma responsabilização

[10] Ver também o artigo Kevin Macnish, "Just Surveillance? Towards a Normative Theory of Surveillance", *Surveillance & Society* 12, nº 1 (2014): 142–53. Para o autor, há nove princípios que influenciam o que ele chama de "ética da vigilância": (i) a existência de justa causa (bases razoáveis para suspeita); (ii) a correta intenção (a intenção por trás da prática da vigilância deve ser correspondente à causa dada para vigilância, não a motivos ulteriores); (iii) a legitimidade do "vigilante"; (iv) a necessidade da medida (que deve ser o último recurso); (v) a notificação sobre a medida (a não ser que acarrete alteração de comportamento e isso não seja pretendido no contexto concreto); (vi) chance razoável de sucesso (deve ser provável que a informação a ser obtida seja a que se deseja tendo em vista o contexto/propósito); (vii) proporcionalidade do dano projetado frente à causa subjacente; (viii) proporcionalidade do meio de vigilância a ser empregado com relação à ocasião (a situação que a motiva); (ix) princípio da discriminação de alvos legítimos (medida deve ser direcionada a sujeitos que aparentem ser culpados segundo a evidência pré-existente). Esse é um esforço analítico relevante para a observação de que a discussão sobre justiça de uma medida de vigilância passa por diversas perspectivas. Esses princípios não são diferenciados conforme o contexto nem destacam necessidade de reconstrução conceitual (fala em proporcionalidade), no que o esforço do autor se diferencia do meu e em que espero oferecer alguma contribuição.

causal específica do ofensor por violação a direitos de outras pessoas ou a outros bens da comunidade cuja importância foi afirmada em decisões políticas coletivas que cidadãos, como parceiros na construção de uma sociedade democrática comprometida com a dignidade, nos propusemos a observar e a respeitar.

Como visto, a imposição de uma pena a alguém, para ser compatível com a dignidade, envolve a observância de um procedimento pelo qual se permita apurar, com certo nível de acurácia, a probabilidade da responsabilidade causal e culpa de alguém sobre um resultado considerado criminoso. Para ser compatível com o direito a não sermos condenados se inocentes, esse procedimento não precisa necessariamente ser o mais preciso possível, mas é importante que seja desenhado de modo a (i) manifestar sensibilidade correta sobre a possibilidade de que as pessoas a ele submetidas sofram dano moral (violação injustificada a direito); (ii) ser coerente com nossas demais práticas sobre proteção a direitos de liberdade (respeito à própria dignidade) – incluindo como calibramos outros riscos. Disse ainda que um mecanismo importante dessa reconciliação é a legalidade: a aprovação por órgão como o Legislativo, sem prejuízo de questionamentos de princípio, para validação das características desse sistema, já que é aí que as escolhas sobre níveis de risco de sofrer injustiça serão feitas e assumidas, sem prejuízo de poderem ser questionadas se não compatíveis com nossas práticas, princípios e materiais jurídicos.

Isso está diretamente ligado, a meu ver, à extensão e aos moldes das prerrogativas de acesso a informações – a "quebras de sigilo" ou outras interferências na privacidade e em dados pessoais no âmbito do processo penal. Apurar informações é etapa necessária para o procedimento de apuração de culpa ou inocência (responsabilidade pessoal), para atribuição e prova suficiente de autoria. Em certas ocasiões, isso envolve apurar informações resguardadas não só genericamente por interesses em privacidade, mas inclusive por direitos à privacidade que a pessoa teria em face de qualquer terceiro em outras circunstâncias. Para que isso seja possível mesmo nas hipóteses em que estamos falando do risco de comprometer um direito, há de existir uma justificativa moral contundente. E mais: não pode nem deve ocorrer de forma ilimitada: a justificativa para a restrição passa necessariamente pela relevância à apuração do fato que está sendo investigado.

Nesse contexto, restrições a direitos de privacidade no processo penal só são possíveis quando há *suspeita* individualizada – um padrão de justificação pelo qual se espera a demonstração não só de que aquele afastamento da privacidade resultará na obtenção de elementos de prova do crime investigado, como de que vai resultar em elementos de prova de que a pessoa implicada está

envolvida em atividade criminosa.[11] A suspeita é, como vimos, um fator material determinante para a própria movimentação da coerção estatal mobilizada pelo direito penal. Faz checagem inclusive das próprias motivações: sobre o quê se suspeita e com base em quê. Ela varia progressivamente: de uma "suspeita inicial" (como uma noticia criminis) até as suspeitas mais fortes tratadas como "indícios suficientes de autoria" (justa causa para denúncia e/ou prisão provisória).[12] Trata-se de padrão que afere a existência de causa justa para a *seleção* de um indivíduo para suportar a coerção estatal em razão da ocorrência de certo crime. Nesse contexto, impõe-se igualmente um padrão de suspeita para meios de obtenção de provas que afetam a privacidade.

Não estou pressupondo que distinguir essas categorias é fácil na prática, muito menos que o que as satisfaz seja fácil de delinear. Como veremos na próxima parte desse trabalho, a jurisprudência constitucional nunca mergulhou no tema de suspeita individualizada, mas já entendeu que esse padrão não se preenche apenas com "denúncia anônima"[13] nem apenas com notícia jornalística, por exemplo. Declarações como essas ainda não podem justificar o tratamento desigual nem admitem desrespeito gratuito à responsabilidade pessoal e a como as pessoas percebem seu valor intrínseco sem qualquer lastro nos seus comportamentos. Declarações de cidadãos comuns testemunhas diretas, de policiais, de informantes, de delatores em colaboração premiada, por outro lado, já recebem outro tratamento – embora o quanto podemos e devemos confiar nelas para constituir suspeitas que acarretam restrições direitos e o quanto precisam de corroboração em outros elementos seja controverso e haja um amplo campo de pesquisa e debate em que este trabalho não se aprofunda. Como evidências empíricas (papeis, vestígios), como o pertencimento da conduta de uma conduta a um perfil de conduta suspeita e como processos

[11] Baseio-me na formulação que encontrei em Berman, "Individualized Suspicion in the Age of Big Data", 472., por sua vez feita com base em julgados da Suprema Corte dos Estados Unidos.

[12] Ver, por exemplo, diferentes categorias de suspeita na Alemanha: Greco, "Introdução – 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)", 51; Luís Greco e Orlandino Gleizer, "A infiltração online no processo penal – Notícia sobre a experiência alemã", *Revista Brasileira de Direito Processual Penal* 5, nº 3 (31 de outubro de 2019): 1498–1500, https://doi.org/10.22197/rbdpp.v5i3.278.

[13] Além dos casos envolvidos no âmbito de interceptações telefônicas referidos no capítulo anterior, ver, por exemplo, afastando denúncia anônima como única base, mas aceitando-a com outras diligências prévias, para dar base a buscas e apreensões: Supremo Tribunal Federal, HC 91350, rel. Min. Ellen Gracie, Segunda Turma, j. 17/06/2008, DJe 29-08-2008.

mecânicos de detecção de possíveis atividades criminosas poderiam ou não satisfazer tais critérios de suspeita individualizada são também matéria para estudo a parte.[14]

Por ora, importa apenas observar que a exigência de suspeita individualizada é um compromisso de princípio embutido nas atividades de obtenção de prova e que o padrão exigível dele pode variar segundo as características do tipo de crime de que se suspeita, segundo o potencial dano moral a direito em questão. Essa calibragem é natural, quando trazemos à luz a ideia de deliberação sobre o nível de risco de injustiça (de *abuso* e de *erro*) a que estamos sujeitos e dispostos a incorrer (riscos razoáveis) para garantir responsabilização criminal, sem fechar os olhos para o fato de que podemos prender, criminalizar e causar diversos tipos de danos de graus diferentes a inocentes. Queremos evitar *abusos* – que servidores abusem de suas prerrogativas com motivações impróprias (como perseguição política e extorsão, por exemplo); e também *erros* – que agentes não façam a "lição de casa" necessária para construir uma hipótese coerente de por que se pensa que alguém está envolvido em crime, impedindo violações gratuitas, como se desimportantes fossem. [15]

Ao lado dessa exigência material, também só é possível restringir a privacidade dentro do escopo necessário para a elucidação do fato investigado, sob pena de causar injustiça pelo *excesso*. A exigência decorre dos pressupostos lógicos de contenção de poder do Estado inclusive traduzidos nos parâmetros iniciais do teste de proporcionalidade. Meios de obtenção de prova e de elementos de informação no processo penal não comportam restrições da privacidade em alcance que não tem relação com o crime, nem de informações que não servem ou que sejam desnecessárias para apurar a conduta. Caso seja necessário buscar informações junto a associações do investigado ou onde mora/trabalha, o vínculo da pertinência e necessidade com a suspeita individualizada deve estar presente. A restrição, para ser justificada, envolve especificidade e delimitação.

---

[14] Enfrentando esse debate nos Estados Unidos, ver Andrew Manuel Crespo, "Probable Cause Pluralism", *Yale Law Journal* 129, nº 5 (2020): 1276–1391.

[15] A discussão regulatória é riquíssima. Por exemplo, ver Hadjimatheou, "Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence". A autora dá o exemplo da política de incluir em equipes policiais um agente responsável por "contrariar" linhas que estejam ganhando força, em detrimento de uma busca por outras possibilidade para explicar o que possa ter ocorrido. Esse é um ajuste regulatório interessante: se alguém é objeto de medidas restritivas de investigação, mas há outras pessoas em situação equivalente, há risco maior de que estamos diante de erro e abuso (perseguição). O agente responsável por contrariar narrativas serviria nesse ponto para garantir mesmo que a suspeita é individualizada – um parâmetro que deve ser interpretado à luz de seu compromisso de evitar injustiças.

Assim, restringir direitos de privacidade de alguém exige razões especiais e um procedimento apropriado de balizas e salvaguardas, que reflita uma decisão da comunidade sobre nível de acurácia da investigação, à luz de nossos valores e convicções – inseridas dentro de um esforço de justificação voltado a mostrar que considerações sobre o respeito ao direito à privacidade foram levadas em conta. Medidas que carregam a possibilidade de infligir danos que consideramos mais graves podem ser reguladas mais estreitamente que outras, desde que seja coerente com o sistema de proteção em geral, mas isso não autoriza a dizer que outras violações a direitos podem ser admitidas. Só assim temos uma moldura da promoção do direito à segurança que é reconciliável com a dignidade. O interesse na responsabilização criminal, para respeitar não só direitos morais específicos à privacidade, mas direitos gerais à responsabilidade pessoal, à independência ética e ao tratamento como igual, deve acomodar e lidar com a possibilidade de arbitrariedades, erros e excessos – situações em que a justificativa moral para o exercício do poder coercitivo do Estado contra certas pessoas não está de fato disponível.

Alguns dos paradigmas de direitos morais e jurídicos à privacidade a que me referi encontram no direito brasileiro engrenagens nessa direção. A própria Constituição Federal prevê que é inviolável o sigilo de comunicações, "salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (art. 5º, XII). Por sua vez, a Lei de Interceptações (Lei nº 9.296/96) regulamenta esse procedimento, notadamente prevendo que, para que seja admitida, deve haver indícios razoáveis da autoria ou participação em infração penal; a prova deve não poder ser feita por outros meios disponíveis; fato investigado deve constituir infração penal punida com pena de reclusão (art. 2º). A autorização judicial deve demonstrar a presença dos requisitos de forma fundamentada.

A inviolabilidade do domicílio também só pode ser afastada sob certas condições (art. 5º, XI, CF/88) vinculadas com a suspeita sobre o crime investigado. No Código de Processo Penal, essa possibilidade está circunscrita a ocasiões em que sirva, mediante fundadas razões, a a) prender criminosos; b) apreender coisas achadas ou obtidas por meios criminosos; c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos; d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso; e) descobrir objetos necessários à prova de infração ou à defesa do réu; f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato; g) apreender pessoas vítimas de crimes; h) colher

qualquer elemento de convicção (art. 240, §1º). Exige-se, como regra, um mandado judicial – mecanismo, pelo qual há o controle da fundamentação da restrição, e sobre o qual se exige "indicar, o mais precisamente possível, a casa em que será realizada a diligência e o nome do respectivo proprietário ou morador; ou, no caso de busca pessoal, o nome da pessoa que terá de sofrê-la ou os sinais que a identifiquem" (art. 240, §2º, I). Exceção são casos de *urgência* – que não deixam de ter de estar vinculados a um tipo equivalente de suspeita individualizada (mas uma de perigo concreto e imediato), ponto revelador, ao qual retornarei na próxima subseção.

Quando essas regras, procedimentos e padrões de justificação que servem à verificação de uma razão especial não são observadas, a noção de que há *violação* do direito moral (e jurídico) à privacidade (por falta de justa causa) retorna. Exemplo paradigmático é o que aconteceu no caso Escher: a Corte Interamericana de Direitos Humanos condenou o Brasil por violar o direito à vida privada e diversas garantias processuais de trabalhadores rurais de cooperativas ligadas ao Movimento Sem-Terra por conta de interceptações telefônicas realizadas de modo irregular no estado do Paraná em 1999. A diligência colecionou uma série de violações às regras da Lei de Interceptações (Lei nº 9.296/96): a medida foi pedida por autoridade não competente (Polícia Militar), fora de uma investigação em curso e sem notificação ao Ministério Público; a decisão que autorizou a medida não foi fundamentada, as interceptações duraram 49 dias; e as gravações foram vazadas e intencionalmente divulgadas em coletiva de imprensa. Em outras palavras: não havia como sustentar a validade desse afastamento da prerrogativa de privacidade.

O direito brasileiro também responde a esse tipo de dano com regras que impõem a inadmissibilidade de prova produzida em violação a normas materiais ou processuais (Constituição Federal, art. 5º, LVI). Notadamente, como veremos na próxima parte, o direito brasileiro considerava interceptações telefônicas, mesmo quando realizadas pela polícia em investigações e mediante ordem judicial, como gravações clandestinas – em 1996, mesmo ano em que a Lei de Interceptações viria a ser aprovada, o STF concedeu habeas corpus afirmando que tal medida era prova ilícita até que editada lei que a regulamente, na forma da Constituição.[16] Mais recentemente, o Superior Tribunal de Justiça também considerou que a prova obtida mediante "espelhamento" de mensagens do WhatsApp pela polícia, mesmo que com ordem judicial, não poderia ser lícita por ausência de previsão legal dessa medida – que não comportaria analogia com nenhuma outra.[17]

[16] Supremo Tribunal Federal, HC 72.588, j. 12 de junho de 1996, Rel. Min. Maurício Correa.
[17] Superior Tribunal de Justiça, RHC 99.735, j. 27 de novembro de 2018, Rel. Min. Laurita Vaz.

No primeiro caso, tratava-se de medida invasiva para as quais ainda não teriam sido fixados os níveis de riscos toleráveis e ajustado o regime regulatório de controle desses riscos – o que só foi feito com a aprovação da Lei nº 9.296/1996. No segundo caso, de novo, essas questões ainda estão em aberto.

Tudo isso reafirma que violar ou não um direito à privacidade no contexto de atuação do Estado pela segurança pode depender de existir uma regulação que mostre respeito a ele e coíba a inviabilização de e *danos sérios* a seu exercício. A regulação de meios e métodos de investigação reflete decisões coletivas sobre nível de risco de que a medida de vigilância importe em violação a um direito à privacidade por decorrer de motivação imprópria; sobre o nível de acurácia que se está disposto a perder no processo penal, em prestígio a outros valores básicos; sobre o padrão de justificação apropriado a mostrar respeito à inviolabilidade da pessoa, diante do risco de que haja erro – o suspeito não seja mesmo responsável – e excessos. A regulação pode ser criticada e questionada quando não demonstra integridade com outros princípios e mecanismos de proteção. Também o pode ser quando é desrespeitada em casos concretos – quando se toma uma nova decisão sobre nível de risco.

Um desafio se coloca quando essa decisão não exista ou seja mal construída. A diligência de quebra de sigilo telemático, por exemplo, enfrenta diversas dificuldades por conta disso: há disputas sobre a interpretação dos direitos jurídicos previstos na Constituição Federal e, assim, sobre quais direitos de privacidade temos. Por decorrência disso, a própria necessidade dessa regulação é questionada. A partir do que vimos aqui, não há saída: se há direitos morais à privacidade em jogo (ou quaisquer outros direitos morais, aliás), tanto a concepção de privacidade como a de segurança que vimos exigem que existam mecanismos de contenção do poder, de contenção de abusos, erros, excessos – de injustiça. Isso vale para os direitos morais que vimos ainda no primeiro capítulo e que ainda não foram consagrados: direitos à privacidade que temos em público, direitos à privacidade que temos sobre dados que vão além de comunicações privadas em fluxo. Voltarei a comentar esse aspecto no capítulo final desse trabalho, já buscando oferecer contribuições concretas à luz do estado da jurisprudência sobre o assunto no Brasil.

1.2 *Entre prevenção e repressão: o caso de emergências*

É também possível restringir direitos de privacidade quando necessário à defesa imediata de direitos, aplicável e referente a uma proteção da independência ética e da responsabilidade

pessoal, e o exercício de sopesamento (reconstrução conceitual) entre o direito ameaçado e esse direito (ambos fortes) assim o sugerir. Essa avaliação é sempre específica e contextual, de interpretação reconstrutiva. São as situações em que se pretende impedir a ocorrência do dano antes que ocorra ou fazê-lo cessar. É o caso de um ingresso a um domicílio para responder a uma emergência: uma denúncia de violência doméstica que esteja ocorrendo ou o resgate de alguém sequestrado em cativeiro, por exemplo. Mas, de novo, para que a restrição não seja indevida, depende da configuração de um perigo que seja tanto concreto quanto imediato. E o que motiva o ingresso é interromper uma conduta criminosa (não é nem mesmo efetivamente fazer uma busca domiciliar para colheita de provas que mais diretamente interfira em interesses de privacidade). Essas variações e nuances quanto às razões e os limites normativos do que autorizam são importantíssimas para o controle de condutas policiais.

Em outras palavras, existem ações do Estado que podem ser justificadas pela própria existência de um perigo – um risco concreto em situação de urgência que ameace direitos de alguém. A lógica é própria de um estado de necessidade, em que a prática de uma conduta que seria em regra ilícita torna-se justificável: se vizinhos escutam uma briga em um lar, com indícios de violência física, chamam a polícia a intervir, a inviolabilidade do domicílio pode ser afastada sem mandado judicial prévio para proteção da vida e da integridade física.[18] A ideia é a defesa imediata do direito concretamente ameaçado e o objetivo é conter o *perturbador*. A interferência em um espaço em que em geral resguardaríamos a prerrogativa do titular de autorizar o acesso é justificada pela razão que o motiva, cuja intencionalidade não desqualifica a dignidade do indivíduo, embora repercuta sobre ela. Essa mesma razão vincula o que o Estado pode ou não fazer a partir do "acesso" que ganhou. Nada mais do que era necessário para controlar o *perigo concreto e imediato* – categoria que vimos para atuação no contexto de atos administrativos ainda, inclusive, e que faz as vezes de razão especial da "suspeita individualizada" nesse contexto; controlado o perigo, o que vem a partir daí se insere no contexto de atos de persecução criminal, sujeito às lógicas da área. Na Constituição Federal brasileira, o art. 5º, XI prevê a possibilidade de intervenções desse tipo quando há flagrante delito, por exemplo.

[18] Em situações extremas e na ausência de autoridades para reagir imediatamente à ameaça, é possível até mesmo imaginar como essa autorização de interferência existe para cidadãos comuns (que poderiam ingressar no lar para parar uma agressão ou salvar alguém de um incêndio) ou mesmo da própria vítima (que poderia gravar uma comunicação telefônica e fornecer a autoridades quando está sendo alvo de extorsão – linha inclusive adotada pelo STF). Cf. Thorburn, "Justifications, Power, and Authority", 1125–29. Isso tem respaldo nas nossas práticas sociais.

Para a justificativa valer, é preciso ter balizas claras sobre o que constitui o preenchimento dos seus requisitos e quais seus limites, refletindo parâmetros de uma decisão da comunidade política. Como visto no capítulo 2, o Estado deve aos cidadãos um tratamento consistente com dignidade do início ao fim em todos os seus atos – isso sequer depende de a medida ser considerada uma restrição a direito de privacidade, aliás. Sem critérios claros sobre sua aplicação e que controlem a discricionariedade policial, não há *accountability* sobre esse tipo de conduta; pelo contrário, há espaço para arbitrariedades e abusos. Afinal, se prerrogativas excepcionais surgem ao Estado sob certas circunstâncias excepcionais, é importante que estejam delimitadas para que não onerem em excesso a liberdade individual para além do necessário e justificável, nem facilite situações de abuso – o que mostraria desrespeito ao direito.

Um campo interessante em que essas discussões são hoje travadas é o das buscas pessoais inibitórias: isto é, revistas baseadas em suspeita de que o indivíduo está prestes a cometer crime ou o está cometendo. Muito embora pareça possível sustentar a legitimidade dessa medida em circunstâncias em que uma situação de perigo concreto possa se dizer imediata, há práticas controversas que daí extrapolam e que não possuem lastro legal. Uma delas é o acesso a celular do portador revistado: se não há nenhuma justa causa nem urgência que vincule o celular à prática do delito de que se suspeitou e à ameaça que se pretendeu controlar, não é possível sustentar essa restrição à privacidade (acesso direto do policial ao celular).[19] Se há algo a ser buscado nessa mídia, o ônus a ser superado de suspeita individualizada sobre o que nele se encontrará e de sua relevância e proporcionalidade para a conduta investigada deve ser demonstrado no Judiciário.

Outra é a fragilidade com que enquadros são conduzidos na praxe policial brasileira – que parecem deliberadamente se afastar de critérios de suspeita e de perigos concretos.[20] O art. 240, §2º do CPP[21] exige fundada suspeita de porte arma ou de objeto que constitua corpo de delito para a possibilidade de realização de busca pessoal. É uma suspeita qualificada, portanto, a certos

[19] Antonialli et al., "Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes".
[20] Sobre o tema, ver Mata, *A política do enquadro*.
[21] Código de Processo Penal (Decreto-lei nº 3.689, de 3 de outubro de 1941): "Art. 240. A busca será domiciliar ou pessoal. § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para: a) prender criminosos; b) apreender coisas achadas ou obtidas por meios criminosos; c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos; d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso; e) descobrir objetos necessários à prova de infração ou à defesa do réu; f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato; g) apreender pessoas vítimas de crimes; h) colher qualquer elemento de convicção. § 2º Proceder-se-á à busca pessoal quando houver fundada suspeita de que alguém oculte consigo arma proibida ou objetos mencionados nas letras *b* a *f* e letra *h* do parágrafo anterior."

objetos. Na prática, no entanto, quando não é feita sem suspeita alguma, a categoria genérica de "atitude suspeita" é invocada para autorizar abordagens policiais: correr da polícia, usar roupas em dissonância com o clima, estar em um local conhecido como ponto de tráfico, haver fluxo de pessoas em um estabelecimento, usar placa de carro de fora da cidade, andar de moto com mais alguém. Vale rememorar: alegadamente, Elize não foi revistada em ruas públicas ao ser parada pela Polícia Federal Rodoviária não porque o objetivo era questioná-la sobre licenciamento atrasado (o que ensejou a parada), mas sob a justificativa de que não apresentou "atitude suspeita". Esses apelos a atitudes veem em certas ações um "perfil" que informa padrões de suspeita.

Embora isso seja admitido em países como os Estados Unidos como apto a alcançar uma "suspeita razoável" individualizada, nunca é tão genérico. A incidência em um "perfil" precisaria estar vinculada a certos tipos de crimes específicos (não a características genéricas que valham para qualquer crime), mediante uma corroboração entre a ação perfilada e a conduta de um indivíduo específico na observação policial, e quando suficiente a destacar a pessoa abordada em comparação com outras pessoas do resto do público.[22] No caso brasileiro, por outro lado, essa prática não é regulamentada em lei nem encontra na jurisprudência, como veremos, critérios hábeis para nortear e balizar a discricionariedade policial – os mecanismos de responsabilização são, portanto, frágeis.[23] O que se vê são categorias muito flexíveis, que dão lugar ao arbítrio. Simplesmente desviar da polícia provoca buscas pessoais, simplesmente usar um casaco provoca buscas pessoais[24], simplesmente ter cor de pele negra provoca buscas pessoais. Sem uma razão

[22] Andrew Guthrie Ferguson, "Predictive Policing and Reasonable Suspicion", *Emory Law Journal* 62, nº 2 (2012): 297–98.

[23] Gisela Wanderley tem uma produção acadêmica relevante sobre como o padrão de justificação qualificado do CPP (vinculado a certo objeto) para buscas pessoais é comumente interpretado de forma aberta e ampla e sobre a contestatação de que milhões de abordagens potenciais sem justa causa potencialmente passam sem questionamento. Ver Wanderley, "Entre a lei processual e a praxe policial"; Gisela Aguiar Wanderley, "A busca pessoal no direito brasileiro: medida processual probatória ou medida de polícia preventiva?", *Revista Brasileira de Direito Processual Penal* 3, nº 3 (set.-dez de 2017): 1117–54.

[24] A Primeira Turma do STF tem precedente antigo sobre o tema: HABEAS CORPUS. TERMO CIRCUNSTANCIADO DE OCORRÊNCIA LAVRADO CONTRA O PACIENTE. RECUSA A SER SUBMETIDO A BUSCA PESSOAL. JUSTA CAUSA PARA A AÇÃO PENAL RECONHECIDA POR TURMA RECURSAL DE JUIZADO ESPECIAL. Competência do STF para o feito já reconhecida por esta Turma no HC n.º 78.317. Termo que, sob pena de excesso de formalismo, não se pode ter por nulo por não registrar as declarações do paciente, nem conter sua assinatura, requisitos não exigidos em lei. A "fundada suspeita", prevista no art. 244 do CPP, não pode fundar-se em parâmetros unicamente subjetivos, exigindo elementos concretos que indiquem a necessidade da revista, em face do constrangimento que causa. Ausência, no caso, de elementos dessa natureza, que não se pode ter por configurados na alegação de que trajava, o paciente, um "blusão" suscetível de esconder uma arma, sob risco de referendo a condutas arbitrárias ofensivas a direitos e garantias individuais e caracterizadoras de abuso de poder. Habeas corpus deferido para determinar-se o arquivamento do Termo. Supremo Tribunal Federal, HC 81305, rel. Min. Ilmar Galvão, j. 13.11.2001, DJ 22.02.2002.

especial, nem um esquema de regulação, tais ações estatais são insustentáveis. Este problema inclusive leva à discussão sobre como implicações à privacidade e a dados pessoais no contexto do direito administrativo, quando desconectado de suspeita e emergência, poderiam ser justificáveis – tema da próxima subseção.

1.3 *Atos administrativos: o caso de medidas generalizadas para dissuasão/desestímulo*

Na ausência de um perigo concreto e imediato e anteriormente à investigação de um fato criminoso específico, a questão sobre os limites do poder do Estado de intervir em direitos de privacidade em nome da segurança pública, de forma geral e ênfase preventiva, é mais complexa. Como poderiam ser justificados, se é que o podem?

A proposta de Barry Friedman

Falando sob o contexto da Quarta Emenda, Barry Friedman faz uma distinção útil para apresentar o ponto, que de certa forma já antecipei. Argumenta que há dois tipos de medidas coercitivas sobre expectativas de privacidade (que por isso configuram "*searches*"/buscas*)*[25]: aquelas baseadas em uma suspeita (*suspicion-based*) e aquelas às quais faltam suspeita (*suspicionless*). Na linha do que apresentei, e como Friedman defende, a exigência clássica de *causa provável* (um padrão de justificação de suspeita individualizada) é o mecanismo que oferece proteção contra ações arbitrárias e discriminatórias do Estado contra alguém – um mecanismo que justifica a seleção de alguém para suportar certa medida individualmente. Sendo assim, faz todo o sentido que seja exigida no contexto investigativo sobre um fato criminoso que ocorreu ou está em vias de ocorrer, em que é preciso reconstruir fatos para identificar o responsável e a polícia trabalha com linhas de investigação.

Por outro lado, autoridades também se engajam em atividades de prevenção (*deterrance*) de forma mais geral em que esse elemento de suspeita não existe; nessas atividades, o propósito é empregar medidas de segurança a ponto de desencorajar tentativas contrárias. Nesses casos,

[25] O "teste" paradigmático da delineação do âmbito de proteção da Quarta Emenda fixado em *Katz* (389 U.S. 347 (1967)) pela Suprema Corte dos Estados Unidos é o da "expectativa razoável de privacidade." Para que essa expectativa seja protegida pela Quarta Emenda, (i) a pessoa em questão deve exibir uma expectativa real (subjetiva) de privacidade e (ii) essa expectativa deve ser uma que a sociedade está preparada para reconhecer como "razoável". Se há expectativa de privacidade, avanços nela são consideradas "search".

Friedman sustenta que, para não haver arbitrariedade e discriminação, a única razão disponível para justificar a medida estatal é distribuí-la igualmente:

> A resposta é que você sujeita todos ao mesmo tratamento. Desse modo, o risco de buscas arbitrárias e discriminatórias desaparece. Isso é o que a Corte de Prouse[26] estava dizendo sobre bloqueios de estradas, e isso é basicamente o que acontece (ou deveria acontecer) nos aeroportos. (…) É claro que revistar todos pode ficar proibitivamente caro, mas há ainda outra opção disponível em muitas circunstâncias: selecionar quem é revistado de uma forma verdadeiramente aleatória.[27]

Nesse contexto, a solução de Friedman para medidas preventivas gerais passa por autorizar restrições a expectativas de privacidade quando aplicáveis de forma geral – e, assim, não arbitrárias e discriminatórias. Esse tipo de medida geral deve ser, sustenta, aprovado pelo público anteriormente – deve ser legislado e regulado. "E com essas buscas sem suspeitas, o Estado tem poucos argumentos sobre a necessidade de mantê-las em segredo. O objetivo das buscas é a dissuasão; as pessoas saberem só ajuda o plano a ter sucesso".[28] Nessas condições, os limites de até onde o Estado pode ir pelo interesse geral se colocariam e seriam filtradas no foro político:

> Encare os fatos - passar pela segurança do aeroporto é uma canseira. Mas, embora as pessoas possam reclamar das filas, não há um apelo generalizado para interromper as buscas. O público está convencido de que vale a pena evitar o terrorismo no transporte aéreo. Observe, porém, que quando o TSA [*Transportation Security Administration*] começou a usar máquinas de raio-X que revelavam muito os corpos das pessoas, houve um clamor imediato e a prática foi interrompida. O público considerou a intrusão muito grande em comparação com a recompensa. Com uma busca verdadeiramente geral, a decisão sobre os interesses legítimos do governo e as intrusões mínimas fica onde deveria: com o público."[29]

---

[26] Referência ao caso Delaware v. Prouse (440 U.S. 648, de 1979) da Suprema Corte dos Estados Unidos em que se entendeu que a polícia não pode parar motoristas sem uma suspeita razoável de que estejam engajados em conduta criminosa apenas para checar seus documentos. Prouse havia sido preso por porte de maconha visto pelo policial em seu carro à plena vista em uma parada. Previamente, o policial não havia observado nenhuma conduta ilegal – nem mesmo violação de regras de trânsito. A abordagem foi considerada inconstitucional.

[27] Tradução livre. No original: "The answer is you subject everyone to the same treatment. In that way the risk of arbitrary, discriminatory searches disappears. That's what the Prouse Court was saying about roadblocks, and that's pretty much what happens (or should happen) at airports." (…) "Of course, searching everyone can get prohibitively expensive, but there is yet another option available in many circumstances: selecting who gets searched in a truly random way." Friedman, *Unwarranted: policing without permission*, 361 (e-book).

[28] Tradução livre. No original: "And with these suspicionless searches, the government has little argument about the need for keeping them secret. The whole point of the searches is deterrence; people knowing only helps the plan succeed."Friedman, 364 (e-book).

[29] Tradução livre. No original: "Face it—going through airport security is a pain in the keister. But while people may grumble about the lines, there is no widespread call to stop the searches. The public is persuaded the inconvenience is worth it to avoid airborne terrorism. Note, though, that when the TSA started to use X-ray machines that were too revealing of people's bodies, there was an immediate outcry and the practice was stopped. The public deemed the intrusion too great given the payoff. With a truly general search, the decision about legitimate government interests and minimal intrusions rests where it should: with the public."Friedman, 364 (e-book).

Os furos

Os argumentos de Friedman sobre medidas de vigilância genéricas parecem a princípio persuasivos em termos de igualdade e não-discriminação. A lei penal, por exemplo, é uma política criminal de prevenção geral para segurança que se aplica a todos; não dizemos que ela per se viola direitos à privacidade (muito embora certos tipos penais ensejem essa discussão, como aborto e uso de drogas, como já comentei). É a aplicação da lei penal a alguém que supostamente se 'auto-selecionou' que atrai as exigências de suspeita individualizada. O que sustenta a validade da lei penal, por ouro lado, não é simplesmente o fato de ser geral e prevista em lei: a existência de uma justificação distributiva que permite a fixação de certos crimes não afastaria a possibilidade de constatação de que essa justificativa pode não estar disponível em certos casos – e para isso precisamos rever a teoria que suporta a regulação e se é uma que tem respaldo em nossos valores.

Nessa linha, os argumentos de Friedman parecem frágeis contra "limites duros" que protejam interesses de privacidade que não sejam só interesses, mas direitos fortes: a conclusão do raciocínio parece ser a de que se uma maioria política aprovar que o Estado sujeite comunicações privadas e casas de todas as pessoas a monitoramento preventivo para fins de segurança, não haveria problema. Passando no foro político, não haveria direito forte constitucional implicado. O desafio seria apenas que a regulação dessas medidas genéricas parta de uma arquitetura institucional e de um arranjo regulatório que alcance todos ou, se não todos, uma amostragem representativa estatisticamente por razões não-discriminatórias.

Desconhecemos uma política pública geral de instalação de câmeras dentro de domicílio de pessoas por parte de autoridades policiais para prevenir crimes ou manter coleta preventiva de provas no caso de ocorrências. Também não se faz gravação preventiva de todas as comunicações no Brasil para os mesmos fins. Nesse sentido, nunca se colocou propriamente a questão de saber se esse é um limite contingente – só não fazemos porque antes não existia a capacidade e ainda é oneroso ou se está fundado mesmo em algum princípio, em um direito moral forte de que o Estado não pode se imiscuir em direitos à privacidade nessa extensão, na linha do que desenvolvemos no capítulo anterior, ainda que isso traga ganhos marginais em segurança.

Para começar, cogitar algo assim perpassaria oferecer uma justificativa. Existe uma justificativa de ordem moral efetivamente disponível? O que disse no capítulo 1 não impede que o exercício de direitos ainda possa ser regulado e restringido para impedir crimes, que afetam direitos básicos alheios. Existe então um vínculo ou correlação clara entre a existência e garantia

de inviolabilidade do domicílio e das comunicações privadas e a prática de violência/crimes para tanto? Para usar as categorias de direito administrativo que vimos, há mesmo um *perigo* a ensejar essa atuação do estado, uma probabilidade de dano? Conseguiria prestar contas de forma bem-sucedida? Embora seja possível supor que a maior parte dos crimes que ocorrem em lares se aproveite dessas prerrogativas de ocultação, se considerarmos as práticas sociais em um país como um todo, também não é difícil supor que seria apenas uma parcela reduzida do valor total. Ademais, é provável que essas garantias na verdade sirvam para coibir diversos crimes e atos ilícitos contra seus titulares. Se for só porque não há essa correlação, esses direitos talvez já ensejem limites em práticas policiais, portanto, simplesmente porque não há uma justificativa moral realmente disponível para justificar restrição à liberdade nessa grandeza.

Na linha do que antecipei, há uma hipótese adicional, mais forte: inviolabilidade do domicílio e das comunicações privadas seriam direitos morais fortes, por sua relevância à independência ética, à responsabilidade pessoal e à democracia. São prerrogativas morais que reconhecemos uns aos outros. Nossas práticas prestigiam, em um conjunto expressivo de cenários, a possibilidade dessas privacidades e, quando dispomos dela, que sejamos consultados. Constituem direitos, não meros interesses, a ponto de que só podem ser afastados por razões especiais em situações excepcionais e específicas, de emergência, em que um direito alheio está em questão. Seriam, assim, trunfos na plenitude do termo – não só contra justificativas éticas mobilizadas pelo Estado: ainda que o interesse geral fosse outro e a maioria se colocasse em uma situação melhor caso esses direitos não existissem ou que o Estado instalasse câmeras em casas e grampeasse todas as comunicações, ainda venceriam qualquer tentativa de afastá-los. Nesse sentido, seria inconcebível um cenário em que autoridades de investigação tivessem acesso a conversas e lares em massa, para monitoramento preventivo de tudo que se fala e se faz, para promover um interesse geral na segurança pública.

Nossas próprias práticas sociais apoiam a noção de que o respeito à dignidade de uma pessoa passa por respeitar o domínio dela sobre seu lar, sobre quem entra nele e quem sabe o que se passa nele; também a prerrogativa sobre para quem essa pessoa compartilha seus pensamentos, o que expressa e com quem se expressa em reserva de outras pessoas. Instalar essas câmeras e capacidades de total monitoramento equivaleria a proibir o exercício de uma prerrogativa de privacidade que valorizamos – o dano que essa política causaria é sério porque seria basicamente impeditivo do exercício do direito. Como o direito à segurança que apresentei não inclui um direito

de ter câmeras instaladas em casa ou conversas monitoradas, se o Estado age a este fim, age na perseguição de meros *interesses* de segurança – que podem ser trunfados por direitos à privacidade.

E averiguações esporádicas aleatórias?

Fazer averiguações eventuais generalizadas, ou mesmo distribuídas aleatoriamente, para prestação de contas sobre o que as pessoas estão fazendo com suas próprias vidas (se não estão cometendo algum crime por aí), por outro lado, mostraria o respeito que esperamos à nossa responsabilidade sobre nossas próprias vidas e às nossas escolhas sobre ela? Alterando um pouco na hipótese, um comentário em voto de caso emblemático que veremos na segunda parte do trabalho sugere que não seria possível *sortear* casas em que se fazer buscas. Diz o Min. Gilmar Mendes: "Imagine-se, por exemplo, que a polícia selecionasse casas por sorteio e, nas escolhidas, realizasse busca e apreensão, independentemente de qualquer informação sobre seus moradores. Certamente, seriam flagrados crimes em algumas delas. O resultado positivo das buscas, no entanto, não justificaria sua realização. O fundamental é que o critério para a decisão de realizar a entrada forçada foi arbitrário"[30]. Nessa hipótese, não há câmera nem policial a todo momento dentro de casa, mas uma busca surpresa em lares aleatórios. O argumento de Friedman tampouco aponta um problema para essa possibilidade; o que o faria? Existe um?

É fato que em certos contextos específicos, como o exemplo de Friedman sinalizava, nos submetemos a certas "averiguações": passar pela segurança do aeroporto é uma delas – medida a que todas as pessoas ficam sujeitas, mas específica ao objetivo concreto de coibir a prática de crimes e atentados em e com transporte aéreo quando o que as pessoas submetidas querem é usar o transporte aéreo. Na nossa prática jurídica, fora do contexto criminal, averiguações generalizadas semelhantes ocorrem em outros contextos muito específicos: agentes de saúde podem forçar ingresso em domicílios para verificar se há foco de mosquitos que transmitem doenças que ameacem a saúde pública;[31] agentes fiscais fazem vistoria sobre informações financeiras

[30] Supremo Tribunal Federal, RE 603616, Min. rel. Gilmar Mendes, Tribunal Pleno, j. 05.11.2015.

[31] Como desenvolvo em outro trabalho, entendo que nesse caso – que envolve também uma medida estatal que atinge pessoas de forma generalizada – há uma necessidade especial (possibilidade de vasos e outros containers em quintais de casas acumularem água parada que levem à proliferação da doença), vinculada a cenário de emergência de saúde pública, em que se autorizou por lei o ingresso excepcional de agentes de saúde para inspecionar e combater locais de possível foco em casos de imóvel abandonado, ausência e recusa – situações cujos critérios estão bem delimitados em lei. Deve haver duas tentativas em horários diferentes antes de ser configurada 'ausência' e toda modalidade de ingresso forçado deve velar pela integridade do imóvel e ser objeto de termo circunstanciado. Entendo que essas

declaradas para fins de pagamento de tributos para respeito à igualdade contributiva; bombeiros fazem vistoria em edificações para verificar sua segurança.

Para justifica-las e diferencia-las das instâncias em que monitoramento preventivo policial é proibido, o esforço é interpretativo e passa pela constatação de que (i) a discussão deixa de ser sobre impedir o exercício de um direito, mas sobre regulação; (ii) há uma justificativa distributiva relevante para tais medidas generalizadas em certos contextos e (iii) a intencionalidade dessas práticas não é uma que vemos como afronta a uma prerrogativa moral de privacidade, não coloca riscos significativos de causar injustiças, não é excessivamente oneroso ao exercício de liberdades que consideramos valiosas. Muito embora, por exemplo, possa ser possível articular um direito à privacidade de nossas informações financeiras em face de terceiros curiosos (pense em seu vizinho), não é possível dizer que esse direito existe em face do Estado a ponto de ser impeditivo da realização de uma política tributária comprometida com igualdade (com a capacidade contributiva) – não existe o direito de omitir essa informação nesse contexto, muito embora possa existir interesse. Há uma justificativa distributiva disponível para essa restrição, portanto.

Os procedimentos de segurança a que nos submetemos no aeroporto, por sua vez, são incidentais ao uso de transporte aéreo – e nossas práticas sobre o que é possível e respeitoso para tanto também leva em conta o que faz sentido e nossas expectativas nesse contexto. Nele, a regulação que obriga a nos identificarmos e minimamente afastarmos dúvidas de que não estamos transportando objetos ilícitos pode fazer sentido dadas as repercussões grandiosas que acidentes podem ter e as complexidades de lidar com interesses soberanos de nações estrangeiras quando cruzamos fronteiras. Por mais que alguém tenha o interesse em não se identificar e não mostrar minimamente que não carrega bomba na mala, nessas circunstâncias (nesse *contexto*), ele não tem esse direito. Nosso direito à segurança inclui não estar sujeitos a riscos irrazoáveis à vida e à integridade física: não fazer checagem nenhuma do que alguém leva a um avião poderia facilitar chocantes desgraças.

Isso não quer dizer que não haja espaço para acomodar interesses de privacidade, conter *excessos* (acessos para além do que a justificativa suporta e que já alcançam prerrogativas morais de privacidade) e evitar um outro tipo de dano moral – tratamento discriminatório –, sobretudo.

condições satisfazem a ideia de não impor ônus excessivo ao direito, vista no capítulo 1. Havia um procedimento adequado que mostrava respeito ao direito (inviolabilidade do domicílio) contra abusos. Abreu, "Privacidade, proteção de dados pessoais e crises epidemiológicas".

Em alguns aeroportos, um formato comum da regulação é que pessoas em geral são objeto de buscas mais aprofundadas, por exemplo, apenas quando um mecanismo como o raio-x detecta algo estranho ou o perfil de viagem sugira alguma anormalidade: a discussão retorna se essas situações atendem a um padrão de suspeita individualizada admissível. Como o que acontece a partir daí então já deixa de ser "suspicionless", porque há *seleção* de alguém, as justificativas próprias se aplicam. Em outros, quando as buscas são completamente aleatórias (aperta-se um "botão" para ver se haverá inspeção), isso não tem impedido a discussão nos Estados Unidos sobre *acesso a dispositivos eletrônicos.*[32] O debate é mais que importante porque tais acessos já ultrapassam os limites do que riscos à segurança pertinentes de serem contidos no ambiente do transporte aéreo suporta – um celular ou um computador e os dados que possuem não carregam ameaça à vida, à integridade nem à propriedade de ninguém.

Como se vê, em sendo uma questão regulatória, é compreensível que Friedman aponte que deveria ficar para o campo político. Nele, haveria delimitação do quanto estamos dispostos a suportar por ganhos gerais em segurança – o que pode em tese também oferecer uma justificativa distributiva para restringir interesses de liberdade. Para avaliar se a medida é válida e possível, entretanto, temos de considerar se impõe danos sérios ao exercício de direitos – de liberdades valiosas do ponto de vista da dignidade: no caso em que a prerrogativa de privacidade domiciliar é basicamente tolhida pela instalação de câmeras para monitoramento constante, essa discussão é tomada já pela constatação de que o exercício do direito é basicamente banido perante o Estado. Precisaríamos olhar para nossa concepção de segurança para verificar se há uma justificativa distributiva razoável no caso para tanto e, com base no que foi visto ainda no capítulo 2 e já adiantei, acredito que a conclusão é que essa justificativa não existiria: é muito descolada de perigos concretos a direitos alheios e excessivamente precaucionária, impedindo exercício de direitos por meras possibilidades abstratas.

No caso de averiguações generalizadas esporádicas e aleatórias, o argumento de que ainda assim há ônus excessivo pode também ser feito, considerando que a medida ainda suspenderia completamente o exercício de privacidade domiciliar em certo momento, ainda que não fosse permanente e contínua; causaria dano gratuito a pessoas inocentes (sempre admitidamente

[32] Hillel R. Smith, "Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?" (Congressional Research Service, 17 de março de 2021); "Border Searches", Electronic Frontier Foundation, acessado 27 de janeiro de 2022, https://www.eff.org/issues/border-searches.

afetadas, já que a política é generalizada e nem todo mundo é criminoso) – por premissa, a hipótese admitiria *erros* e *excessos* (no sentido de injustiças de que tratei no capítulo 1) sem tentativa de contê-los; alimentaria clima de desconfiança entre as pessoas e o Estado e acumularia desnecessariamente poder ao Estado. Nesse sentido, está antenado com a importância que damos ao direito à privacidade domiciliar em nossas práticas o fato de que exigimos *suspeita individualizada* (prévia) necessariamente para que o Estado o restrinja no seu esforço geral de combate ao crime – que reserve intervenções a quando houve violação a direito alheio efetivamente ou quando há um *perigo concreto e imediato* de que existirá lesão a direito alheio. Do direito à segurança, não faz parte nada diferente disso. Esses seriam resultados de um "sopesamento" – não no sentido de "ponderação" de interesses, mas de um exercício de reconstrução conceitual dos valores da privacidade e da segurança e nas concepções que defendi comprometidas com a dignidade.

Em via pública: sobre políticas de enquadros e câmeras

Para além desses exemplos, há ao menos duas práticas reais em que a questão da viabilidade da justificação de medidas generalizadas se apresenta e que vale comentar: (i) buscas pessoais em abordagens policiais "preventivas"/inibitórias de patrulhamento ostensivo, admitidamente sem um nível fundado de suspeita sobre o atingido, como enquadros "protocolares" (que visam bater metas de produtividade), enquadros de saturação (feitos sobre áreas delimitadas de uma cidade) e enquadros de fiscalização (que ocorrem sobretudo no trânsito, para controle de documentos e condições do veículo)[33]; e (ii) coleta e uso de informações para monitoramento, sobretudo em áreas públicas ou semi-públicas, na internet e em vias públicas. Podemos falar em direitos morais fortes capazes de trunfar essas medidas gerais de segurança como foco em *deterrance* – um trunfo que poderia ser suscitado mesmo que a maioria deliberasse por essa medida de segurança?

[33] Essas diferentes classificações de tipos de enquadros foram encontradas em Mata, *A política do enquadro*, 70-71;111. Todos dizem respeito a enquadros "proativos", provocados por autoridades policiais, mas destacados aqui por terem a potencialidade de serem usados como uma medida *generalizada*, desvinculada de suspeitas concretas anteriores contra o alvo afetado. Deixo de mencionar o que a autora chama de "enquadros proativos voluntaristas" (em que o policial teria alguma suspeita) e "enquadros reativos em atenção a chamados". Entendo que o "enquadro proativo voluntarista", para ser legitimado, deve se colocar na situação de "emergência" vista na seção anterior – em que há suspeita concreta de atividade ilícita, que, no caso no CPP brasileiro, é condicionada ao porte de corpo de delito. Já os enquadros reativos por chamados (como os decorrentes do 190), por sua natureza *individualizada*, também estaria submetido ao regime geral do processo penal – por ser provocado *por algo que já aconteceu,* sem ênfase preventiva.

Fora do contexto de ingresso a certos locais que suscitam interesses de segurança específicos (como aeroportos e arenas) que atinge pessoas com objetivos evidentes e pressupostos (usar transporte aéreo, assistir a um show), nossas práticas sociais parecem comportar o reconhecimento de que somos resguardados contra toques e intrusões alheias e ter de dar satisfação sobre quem somos e aonde vamos quando se transita em locais públicos. Naturalmente, a avaliação é contextual: o toque de alguém no ombro de uma pessoa que acaba de deixar cair a carteira na rua não é vista como violação da privacidade; alguém que, por curiosidade e/ou obsessão, insista em saber o nome de uma passageira, de onde veio e para onde vai, o que carrega na bolsa (e em ver o celular) já estaria, por outro lado, quebrando regras sociais de comportamento. Ainda que não chamemos isso de violação da privacidade, falamos em assédio.

No caso policial, a intencionalidade a princípio presumida de uma abordagem pode não ser essa de assediar, mas há uma prerrogativa moral relevante, que deve ser protegida contra abusos, excessos e erros. Mesmo que não comparável em sua importância a outras liberdades que entendamos fundacionais (como talvez a privacidade de nossos lares), ainda há um direito à privacidade em questão (de ser capaz de transitar em ruas sem ter de prestar contas – uma obscuridade). (A polícia que tortura é pior que a polícia que dá beliscões, mas isso não se significa que ela pode sair dando beliscões sistematicamente – o raciocínio é semelhante). Ademais, na medida em que enquadros afetam um grupo de algum modo selecionado de pessoas, há também necessidade de justificar por quê suas condutas ensejaram a seleção para movimentar o sistema de justiça criminal. Esses fatores colocam como contrapartida a essa intervenção do Estado a exigência de suspeita individualizada. O Estado não pode exigir prestação de contas e submeter pessoas a averiguação gratuitamente, para ganhos abstratos em segurança pública.

Na prática administrativa policial brasileira, sobretudo em grandes cidades como São Paulo, enquadros são medidas realizadas em massa, como política institucional, já há muito tempo.[34] Se fossem empregados de forma objetiva e ideal, sem selecionar pessoas por fatores discriminatórios e com protocolos bem delimitados sobre até onde a revista pode ir e o que busca coibir/deter, poderiam colocar um caso bem mais difícil sobre privacidade, com inclinações para se deixar que o jogo político-democrático definisse se os custos aos interesses de privacidade valem os supostos ganhos gerais de uma política pública de segurança generalizada *suspicionless*.

[34] Ver Mata, *A política do enquadro*; Wanderley, "Entre a lei processual e a praxe policial".

Ocorre que a prática brasileira está também longe dessa hipótese teórica: não há efetivamente enquadros completamente aleatórios a que qualquer cidadão esteja sujeito – enquadros de saturação (informados pela área da cidade – por exemplo, uma que tenha mais registros de crime) e enquadros protocolares (feitos aleatoriamente apenas para bater metas) oneram pessoas simplesmente por estarem em certa área da cidade e por cruzarem o caminho de um policial. Ademais, revistas também tendem a se extrapolar sobre os aspectos em que se faz "checagem" da vida pregressa (tornando-se interrogatórios e às vezes vasculhando-se celulares)[35] e são, quando não diretamente, indiretamente discriminatórias (atingindo mais grupos de certo perfil social)[36], caso em que o ganho teórico geral em segurança da população custa liberdades de apenas um grupo de cidadãos. Sem contar a falta de políticas concretas da polícia brasileira sobre o assunto, de transparência, de *accountability* e respaldo em lei delas. Isso torna a medida questionável por muito mais do que "só" deter alguém, obrigar a se identificar, apurar seus precedentes e apalpar seu corpo. Isso joga atenção às repercussões que pode ter a uma prerrogativa moral e à necessidade de proteção regulatória contra abusos, excessos e erros – e assim, à exigência de suspeita individualizada e à desigualdade na prática mesmo que em tese a política de segurança seja de aplicação generalizada.

A parada de Elize Matsunaga, por sua vez, foi provocada por sistema que leu a placa do carro e sinalizou que havia algo de errado no licenciamento do carro. O exemplo extrapola já o recorte criminal, avançando sobre segurança no trânsito, mas mostra como a lógica de "interromper" alguém para que preste contas precisa de algum ensejo que seja coerente com o contexto da medida – algo que faz as vezes da 'suspeita individualizada'. Sem mais, não se poderia justificadamente parar e fazer buscas sobre as coisas que Elize guarda no seu carro. Para fazer blitzes em outras condições para controle de documentação sem essa sinalização automatizada, os critérios que ensejarão parada também demandarão justificativa própria, se fazem sentido junto ao contexto, se possuem justificativa distributiva, se não causam dano sério. (Falarei mais do uso massivo de dados pessoais subjacente a esse tipo de *detecção* no próximo item).

[35] Ver Antonialli et al., "Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes".
[36] Ver Gisela Aguiar Wanderley, "A Quarta Emenda e o controle judicial da atividade policial: busca e apreensão e stop and frisk na jurisprudência da Suprema Corte estadunidense", *Revista de Direito Brasileira* 24, nº 9 (1º de dezembro de 2019): 341–64, https://doi.org/10.26668/IndexLawJournals/2358-1352/2019.v24i9.3259; Mata, *A política do enquadro*; Hadjimatheou, "The Relative Moral Risks of Untargeted and Targeted Surveillance", 192.

Por fim, quanto às medidas de monitoramento público, em linha com o que delineei no primeiro capítulo sobre um direito à privacidade enquanto obscuridade em público, entendo que daí se extrai também um obstáculo fatal para medidas de vigilância que rastreiem todas as pessoas a todo tempo, catalogando seus trajetos. Há uma reivindicação de privacidade que certamente ultrapassa simplificações da separação entre esfera pública e esfera privada: nossas expectativas de controle sobre a privacidade e das dimensões de nossas vidas ao público se erguem sobre certas pressuposições sobre o que é humanamente possível e como se dão comportamentos sociais em grandes cidades:[37] carregamos certa obscuridade em público porque as pessoas em geral não andam com cartões de identificação à mostra, não guardam na memória encontros sobre quem esteve em qual lugar ainda que as tenham visto, nem efetivamente se importam em catalogar o que veem e mesmo ouvem sobre a vida de terceiros estranhos em vias públicas.[38] A partir do momento em que um recurso tecnológico é usado para se sobrepor a essas expectativas, usurpando da pessoa uma capacidade de controle sobre aspectos de sua vida que tinha e valorizava, uma prática de privacidade inerente ao nosso modo de vida fica ameaçada. A ameaça dela por novos recursos tecnológicos nos leva a articular os contornos dessa privacidade como uma prerrogativa moral.

Nessa linha, o esboço dessa defesa pode dizer que essa privacidade é imanente a como nos compreendemos como pessoa: como seres capazes de perceber nossa realidade física como *nossa* por existirem certos rituais de privacidade que resguardam controle razoável sobre os aspectos da nossa realidade que se tornam cognoscíveis a outras pessoas.[39] A partir do momento em que perdemos essa capacidade – que outra pessoa ganha a possibilidade de reconstruir todos os nossos passos e encontros em uma linha do tempo, nossa visão de nossa própria vida muda. Do outro lado, não existe um direito à segurança que ampare o dever e a prerrogativa estatal de rastrear todas as pessoas genericamente a todo tempo, montando linhas do tempo de onde estiveram, o que fizeram, com quem se encontraram. Pode haver interesse e talvez fazer isso fosse trazer ganhos, mas direitos trunfam. Não ausência de um perigo concreto e imediato e de uma suspeita individualizada, não pode existir rastreamento.

O problema é que há outras maneiras de implementar esse tipo de tecnologia de monitoramento que não franqueiam o reconhecimento de violação a um direito forte à privacidade

[37] Selbst, "Contextual Expectations of Privacy", 683.
[38] Woodrow Hartzog e Evan Selinger, "Why You Can No Longer Get Lost in the Crowd", *New York Times*, 17 de abril de 2019, https://www.nytimes.com/2019/04/17/opinion/data-privacy.html?smid=tw-nytopinion&smtyp=cur.
[39] Reiman, "Privacy, Intimacy, and Personhood".

de forma evidente assim e que levam a discussão ao modo como implementadas – câmeras que não possuem as mesmas capacidades de rastreamento e que apenas permitem à polícia o acompanhamento em tempo real de imagens de áreas da cidade em uma central, logo a seguir apagadas, por exemplo. Nessas condições, alguém poderia dizer que já não há riscos de danos sérios a exercício de uma prerrogativa moral de privacidade que proteja a obscuridade, por exemplo (– o que não quer dizer que não haja riscos de outros tipos em que não me aprofundei nesse trabalho, como as preocupações de danos incidentes à coleta de dados pessoais). Comentarei essas dificuldades e nuances regulatórias no último capítulo deste trabalho.

Como se vê, o desafio de todas essas avaliações, sobretudo considerar se há direito forte em jogo e/ou se a regulação concreta é capaz de respeitá-lo com salvaguardas, é que depende do arranjo concreto: dos podes e não podes dessas medidas e como são formatadas. Nesse sentido, cabe notar que, pelo que se viu sobre o ônus de fundamentação aplicável ao Estado em matéria de direito administrativo e mesmo o seu dever de adotar um regime de proteção de dados pessoais, não há ampla discricionariedade do Estado para fazer e implementar tais medidas de qualquer jeito. Precisam ser legisladas, passar por regulamentação, precisam embutir garantias concretas contra arbitrariedades e abusos, contra riscos de danos intencionais ou inadvertidos. Nunca há carta branca. Esse ponto é importante também para a próxima categoria em análise.

1.4 *Prevenção para repressão: o caso de bases de dados para abertura de linhas de investigação (e mais – as promessas do big data)*

Há modalidades adicionais de atuação policial que implicam interesses de privacidade e proteção de dados para se dar conta. Elas giram em torno de medidas administrativas concretas de formação e análise de bases de dados pessoais pensadas para otimizar a abertura de linhas de investigação quando um fato criminoso ocorrer, para garantir a existência de provas que possam vir a ser úteis em processo e para detectar fatos criminosos. Estão insertas no âmbito do direito administrativo que vem sendo impulsionado por noções de segurança precaucionária alimentadas pelo avanço tecnológico e que desafiam as maneiras como até aqui estruturamos o pensamento jurídico sobre contenção do poder do estado.

<u>Bases de dados de identificação</u>

Abrindo essa seção, falei de meios de obtenção de prova como interceptações telefônicas, buscas e apreensões e outras quebras de sigilo. Já ao falar de processo penal, e de sua ênfase repressiva, mencionei também meios de prova voltados à perícia do corpo de delito, os vestígios deixados pelo crime. Falei de análise de impressões datiloscópicas e de DNA (fios de cabelo, sêmen, saliva, sangue e outros fluídos corporais). Esses vestígios auxiliam na triagem de suspeitos e na confirmação de *autoria* de um crime. Imagens das faces capturadas por vídeo e informações sobre aspectos físicos (estrutura corporal, altura, cor da pele, tatuagens) de testemunhas e vítimas em geral também auxiliam na triagem e reconhecimento de suspeitos. Até nomes/apelidos ouvidos e tatuagens vistas por testemunhas do crime/captadas por câmeras também podem ser para úteis abrir linhas de investigação.

Não há nenhum argumento de privacidade que sugira que uma cena de crime não possa ser periciada pela polícia à procura de vestígios para responsabilização criminal, quando é flagrantemente o local do crime. A mata em que o corpo de Marcos Matsunaga foi encontrado foi amplamente analisada em busca de vestígios, inclusive DNA. Não só porque era local público: se o corpo de Marcos tivesse sido encontrado na sua casa por algum terceiro (um funcionário do casal), a denúncia à polícia levaria também à análise do próprio ambiente em que encontrado. Acredito ser assim porque, se é evidente a qualquer um que ocorreu um crime em certo local, não há *erro* nem *abuso* efetivamente possível em analisar o corpo de delito. Há limites contextuais, contra *excessos*: é possível dizer que um latrocínio na porta da casa de alguém não autoriza que a polícia faça buscas pessoais na casa da vítima. Por outro lado, se não é evidente a conexão como local do crime, o elemento de dúvida leva às aplicações do primeiro cenário visto aqui (de exigência de suspeita individualizada): a casa do casal Matsunaga mantinha-se "protegida" e merecedora de proteção regulatória contra abusos, erros, excessos, embora Marcos tivesse sido morto – veio a se descobrir depois – lá.

Dito isso, por sua natureza, e para dizer o óbvio, dados e informações que constituem *vestígios* precisam ser *cruzados* ou *comparados* com outros para levar a algum lugar, para saber a quem pertencem. Quando já há suspeitos, os dados que constituem elementos do corpo de delito são cruzados com os dados do suspeito, voltando à primeira situação analisada acima. Nos casos em que ainda não existem suspeitos identificados, pode não haver com o que se comparar os elementos do corpo de delito. Nesse contexto podemos inserir o interesse de instituições de segurança pública na formação *preventiva* de bancos de dados *pessoais* das mais diversas espécies

– desde dados de identificação comuns (dados pessoais comuns, como nome, endereço e filiação) a dados pessoais sensíveis (impressão digital, material genético, íris, biometria facial) – para auxiliar em propósitos *preventivos gerais* e *repressivos*. Não surpreende que assim seja e o motivo apresentado é relevante: a acurácia na identificação de autoria é importante não só para viabilizar responsabilização penal em geral, mas responsabilização sobre as pessoas *corretas*.

No caso brasileiro, já há anos existem bases de dados de identificação civil junto a secretarias de segurança pública.[40] Mas não para aí: a esses dados são adicionados mais informações quando há interações da pessoa com o sistema de justiça criminal – como quando se faz sua identificação criminal (em que há coleta de impressões digitais, foto e sinais físicos e até material genético, pela Lei nº 12.037/12[41]) e/ou a Lei de Execução Penal assim determina, por conta da modalidade de crime cometido[42]. Para citar movimentações recentes: o Pacote Anticrime expandiu os bancos de dados genéticos de pessoas condenadas já existentes[43], inclusive prevendo um Banco Nacional Multibiométrico e de Impressões Digitais, que fala também de dados de íris, face e voz; a Polícia Federal anunciou que planeja integrar bases de dados biométricos[44] de secretarias, possivelmente em função desse banco nacional; e há até propostas de lei que tramitam para a criação de um banco de dados de material genético (DNA) de toda a população[45].

O que autorizaria iniciativas do tipo e quais os limites? Em certo sentido, tais medidas são também '*suspicionless*': embora em certas instâncias a coleta do dado esteja relacionada a uma

[40] Marta Mourão Kanashiro, "Biometria no Brasil e o registro de identidade civil: novos rumos para a identificação" (Tese de Doutorado, São Paulo, Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo, 2011).

[41] Lei nº 12.037/12: "Art. 5º A identificação criminal incluirá o processo datiloscópico e o fotográfico, que serão juntados aos autos da comunicação da prisão em flagrante, ou do inquérito policial ou outra forma de investigação. Parágrafo único. Na hipótese do inciso IV do art. 3º, a identificação criminal poderá incluir a coleta de material biológico para a obtenção do perfil genético."

[42] Lei de Execução Penal (Lei nº 7.210/84, na redação incluída pela Lei 13.964, de 24 de dezembro de 2019): "Art. 9º-A. O condenado por crime doloso praticado com violência grave contra a pessoa, bem como por crime contra a vida, contra a liberdade sexual ou por crime sexual contra vulnerável, será submetido, obrigatoriamente, à identificação do perfil genético, mediante extração de DNA (ácido desoxirribonucleico), por técnica adequada e indolor, por ocasião do ingresso no estabelecimento prisional."

[43] Cf., ainda comentando o projeto, Dennys Antonialli, Nathalie Fragoso, e Heloísa Massaro, "Da investigação ao encarceramento: as propostas de incremento do uso da tecnologia no Projeto de Lei Anticrime |", *Boletim IBCCRIM* 318 (maio de 2019), https://www.ibccrim.org.br/boletim_artigo/6337-Da-investigacao-ao-encarceramento-as-propostas-de-incremento-do-uso-da-tecnologia-no-Projeto-de-Lei-Anticrime.

[44] Paula Soprana, "PF compra sistema que cruzará dados biométricos de 50 milhões de brasileiros", *Folha de S.Paulo*, 7 de julho de 2021, seç. Tec, https://www1.folha.uol.com.br/tec/2021/07/pf-compra-sistema-que-cruzara-dados-biometricos-de-50-milhoes-de-brasileiros.shtml.

[45] Ver, por exemplo, o projeto de lei nº 1781/2019 proposto pelo Deputado David Soares (DEM-SP), que prevê coleta e armazenamento de material genético de todos os residentes do país.

interação com o sistema de justiça criminal (um evento criminal supostamente já ocorrido), esse tipo de medida de formação de bases de dados mira sobretudo para o futuro, para o próximo caso em que ter aquelas informações possa ser relevante para abrir linhas de investigação sobre autoria. No caso Elize Matsunaga, o DNA de uma terceira pessoa encontrada na sacola em que o corpo foi lançado na mata nunca foi atribuído a ninguém. Ter algo assim poderia em tese encapar esse fio que ficou solto, de que alguém possa ter ficado impune. Isso é suficiente para justificar?

Pela fórmula de Friedman, essas medidas colocam questões a serem decididas no foro político sobre se e como queremos que nossa política criminal repouse nessas bases de dados massivas não só de informações pessoais comuns, mas de dados cada vez mais sensíveis e que podem ser e vem sendo agregados com outros pontos de informação. Por essa e outras razões, muitos pesquisadores alertam sobre o perigo de só analisar as coletas desses dados para formação a partir da obtenção inicial da informação pelo Estado: o uso que é dado depois da coleta pode suscitar diversos questionamentos sobre os riscos a que o cidadão é submetido e pode desencadear diferentes questões sobre privacidade.[46]

No capítulo 1 olhei sobretudo para medidas de vigilância que concedem um *acesso* a uma informação à polícia que não estava ao seu alcance a partir de exemplos mais tradicionais. Neles, dentro do modelo do "terceiro malicioso", era possível mais facilmente comparar a intervenção de um policial à que uma pessoa comum poderia praticar a outra, para cogitar se havia uma prerrogativa moral de privacidade em jogo. Aqui estamos falando de medida anterior a um processo penal e generalizada como política pública de segurança do Estado, voltada à criação de um banco de dados para acesso posterior por autoridades policiais específicas em milhares de investigações. Uma pessoa comum não teria esse poder – constatação suficiente para suscitar preocupações com abusos e excessos.

Há dois momentos: a coleta e inclusão de informação no banco de dados por conta de política pública e, futuramente, os inúmeros acessos a informações desse banco de dados em diversos processos penais (quando pode haver suspeita individualizada para obter o dado ou cruzar o dado de alguém). Meus exemplos não contemplavam essa providência anterior. Daphne Renan chama esse tipo de vigilância de programática, em que se começa por varredura generalizada em

[46] Daniel J. Solove, "Digital Dossiers and the Dissipation of Fourth Amendment Privacy", *Southern California Law Review* 75 (2002 de 2001): 1166–67; Emily Berman, "When Database Queries Are Fourth Amendment Searches", *Minnesota Law Review* 102 (2017): 577–638; Cohen, "How (Not) to Write a Privacy Law".

dados, para depois chegar em individualizações.[47] É baseada não em eventos isolados de interação do indivíduo com a autoridade estatal, mas em ocorrências fluidas, contínuas, cumulativas e agregadas de coleta, uso e análise de dados pessoais que fogem de doutrinas tradicionais de privacidade e requerem, no mínimo, uma estruturação de governança administrativa para seu uso. Cabem alguns comentários.

Nós não temos práticas sociais que manifestamente associem certo valor ao domínio sobre o DNA e à possibilidade de controlar o acesso a ele. Mas as informações que carrega também não são algo que sempre esteve à livre disposição para análise de todos, como se fossem corriqueiras. Também não temos práticas sociais que sugiram que não nos importamos com a catalogação que possa ser feita disso, que seja indiferente ao uso que alguém dará e às consequências para o curso de nossas vidas que isso poderia ter. Se alguma pessoa com hábito duvidoso de coletar, analisar e colecionar dados genéticos de pessoas com quem se encontra por aí, penso que essa conduta seria questionável. Ouso dizer, portanto, que nossas práticas em geral sugerem a possibilidade de articular um direito à privacidade que ressalte a importância que pode ter à nossa autonomia em muitos contextos e que nos obrigar a abrir mão dessa privacidade para fins preventivos gerais pode caracterizar um dano sério a direito. A questão que é posta é se essa medida mostra respeito à nossa autonomia moral e se faz parte de uma visão de segurança comprometida com a dignidade.

A discussão normativa específica é complexa demais para esse trabalho. À primeira luz, entendo que a complexidade passa pelo fato de que a medida inicial de coleta preventiva em si parte da premissa de que supostamente não haverá riscos de causar injustiça a inocentes (da perspectiva de levar à prisão ou à adoção de outras medidas de vigilância invasivas sem que tenham se engajado ou se envolvido em ilícitos), o que afastaria a própria pertinência de invocar a noção de suspeita individualizada enquanto mecanismo de proteção regulatória da privacidade contra abusos, erros e excessos. Se isso é verdade depende não só de argumentos jurídicos sobre a persistente possibilidade de criminalizações indevidas (como implicar o familiar de alguém) e de melhor articulação sobre um direito à privacidade sobre material genético nesse contexto, mas de informações técnicas e científicas sobre esse tipo de prova e da acurácia que se pode esperar dela.

De todo modo, a discussão não para aí. Trata-se de medida que suscita preocupações com riscos de injustiça que a submissão a esse tipo de banco de dados implica da perspectiva de

[47] Daphna Renan, "The Fourth Amendment as Administrative Governance", *Stanford Law Review* 68, nº 5 (2016): 1061.

proteção de dados pessoais. Daí se desencadeiam as questões com o aumento da vulnerabilidade das pessoas e os interesses gerais contra riscos e ameaças que buscamos realizar com instrumentos regulatórios como a Lei Geral de Proteção de Dados Pessoais (riscos de danos – uso secundário e inadvertido do dado de DNA, vazamento, etc)[48]. O risco autoritário desse tipo de medida é também gigantesco; é uma matéria que precisa de deliberação coletiva e pode encontrar limites fundamentais nesses trunfos. Considerando que vivemos em um país que dificulta o rastreamento de *armas*, qualquer mobilização política em favor dessas pretensões fica manchada de enorme hipocrisia.[49] Nessa linha, envolve mergulhar mais nos problemas da visão de política criminal atuarial em que essas tendências se inserem:[50] nós não temos um direito à segurança que autoriza o Estado a anular todo tipo de risco à segurança (e de impunidade), mas um que revele uma atitude de proteção do risco razoável diante de outros dos nossos valores.

Para além disso, a questão de direito moral forte contra a coleta dessas informações e agregação em um banco de dados preventivo aciona a linguagem de um *direito à não-autoincriminação,* por exigir que as pessoas produzam tal informação preventivamente que poderá ser usada contra si, e do *direito ao tratamento como igual*, por ampliar as possibilidades de responsabilização criminal sobre pessoas que já tiveram alguma interação prévia com o sistema de justiça criminal (ampliando suas chances de serem novamente pegos por crimes, em detrimento de outras pessoas em geral). São muitas nuances que extrapolam meu escopo, mas que reiteram a importância de clareza sobre tudo que está em jogo e que, no limite, o ponto é garantir mecanismos hábeis a proteger a direitos morais diante dos poderes coercitivos estatais que os ameaçam.

Bases de dados de muito mais: tudo que virou dado, tudo que se pode integrar

Também ressalvo e ressalto que a tentação por que passam instituições estatais em face do avanço tecnológico é muito grande para se parar na criação de bancos de dados de identificação. O fato de que as formas de identificação já expandem de dados comuns (nome e endereço) para dados em tese capazes de nos identificar inequivocamente e que não podemos alterar é só uma faceta de um fenômeno muito maior de novos interesses com usos de dados. Como coloca Malcolm

[48] Fazendo esse tipo de análise, ver: Luiza Louzada, "Princípios da LGPD e os bancos de perfis genéticos: instrumentalizando a garantia de direitos no processo penal", *Revista do Advogado* 144 (novembro de 2019): 90–98.
[49] Igor Gielow, "Dificuldade de rastreamento afeta metade do arsenal de armas no Brasil", Folha de S.Paulo, 29 de julho de 2021, https://www1.folha.uol.com.br/cotidiano/2021/07/dificuldade-de-rastreamento-afeta-metade-do-arsenal-de-armas-no-brasil.shtml.
[50] Fazendo a ponte entre política criminal atuarial e novas tecnologias, ver Wermuth, "Política criminal atuarial".

Thorburn, e à luz do que já dizia Lucia Zedner, as políticas de combate ao crime mudaram, com crescimento de técnicas de controle situacional, em detrimento de medidas que busquem compreender as causas raízes para atividades criminosas e endereça-las: tem ganhado espaço na política criminal atual modelos em que a estratégia é monitorar "potenciais ofensores tão perto quanto possível, para estruturar o ambiente de modo a fazer o crime mais difícil de ser praticado, e de implementar um conjunto de medidas preventivas para impedir que *eles* ameacem a *nossa* segurança"[51].

Com efeito, como adiantei no capítulo 2, as práticas hoje envolvem não só mais formação de bases de dados para identificação, como também empreender novas modalidades de vigilância e de perfilhamento. Além de bases de dados de identificação, há pretensão de (i) montar bases de dados de mais atividades, como pelo monitoramento de câmeras CCTV e ANPR (leitores automatizados de placas de veículos) (*dragnet surveillance* – vigilância por rede de arrastamento, em que é coletado dados de todas as pessoas, incluindo aí a preponderante maioria de pessoas inocentes, para eventualmente achar alguém criminoso[52]), (ii) reaproveitar bases de dados criadas para fins diferentes[53], inclusive do setor privado (dando lugar ao chamado *function creep*), como já se faz por mecanismos de retenção de dados[54]; e (iii) acumular, agregar e integrar informações para ter à disposição em todas as áreas de atuação policial – da prevenção geral administrativa à execução de penas. A quantidade de informações pessoais detidas pelo Estado sobre o cidadão se amplia, em alcance que se torna mais difícil até de compreender. Se a coleta separada de

[51] Thorburn, "Identification, Surveillance, and Profiling", 16. (tradução livre e destaques do autor)
[52] Sarah Brayne, "The Criminal Law and Law Enforcement Implications of Big Data", *Annual Review of Law and Social Science* 14, nº 1 (2018): 293–308, https://doi.org/10.1146/annurev-lawsocsci-101317-030839.
[53] Victor Martins Pimenta, Izabella Lacerda Pimenta, e Danilo Cesar Maganhoto Doneda, "'Onde eles estavam na hora do crime?': Ilegalidades no tratamento de dados pessoais na monitoração eletrônica", *Revista Brasileira de Segurança Pública* 13, nº 1 (20 de setembro de 2019): 59–75. (mostrando como dados obtidos por tornozeleira eletrônicas para fins de monitoramento de execução de pena é reutilizado por policiais civis na investigação de novos crimes para verificar possibilidade de envolvimento); "TSE e Polícia Federal vão compartilhar banco de dados biométricos", *Tribunal Superior Eleitoral* (blog) (Tribunal Superior Eleitoral, 16 de novembro de 2017), https://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/tse-e-policia-federal-vao-compartilhar-banco-de-dados-biometricos. (anunciando compartilhamento de dados biométricos coletados pela Polícia Federal no âmbito da sua atribuição de expedição de passaportes com os dados biométricos coletados pelo TSE para cadastramento de eleitores, ampliando-se bases de dados disponíveis para o TSE para identificação de eleitores e, para a PF, para investigação).
[54] Sobre obrigações desse tipo para o setor de telecomunicações, ver Jacqueline de Souza Abreu, "Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais", in *¿Nuevos paradigmas de vigilancia? miradas desde América Latina : Memorias del IV Simposio Internacional Lavits, Buenos Aires, 2016*, org. Camilo Rios Rozo, 1º ed (Buenos Aires: Fundación Vía Libre, 2017), 295–306.

determinadas informações pessoais específicas não parecia suscitar interesses de privacidade, o acúmulo e a diversidade de dados integrados o pode.[55]

Dito isso, como para os dados de identificação em si, não é automático que toda crescente vigilância geral esbarre diretamente em direitos de privacidade, nem mesmo na presunção de inocência, por conta das nuances que detalhes regulatórios podem trazer. Como falei ao tratar da regulação de perigos abstratos no capítulo passado, o cenário é nebuloso e as medidas precisam de análises específicas. Se poderia fazer sentido a detecção automatizada pela qual passou Elize para fins de *enforcement* de documentação veicular, não é assim em diversos outros. Vejamos um exemplo. Em linha com tudo o que apresentei no capítulo 1, se o Estado montar uma base de dados de informações de localização de cidadãos, podendo rastrear quem quer que seja a qualquer momento para fins genéricos de promoção de segurança ou recuperar tais informações caso venham a se tornar relevantes para resolver um crime, por exemplo, há uma violação a direito à privacidade devido a cada um deles, que trunfaria essa política. Se esse levantamento é feito "só" em "algumas" vias públicas, por outro lado, e for desenhado e embutido no sistema um esquema de controle sobre as hipóteses específicas em que uma autoridade pode consulta-las e delineadas as condições, a questão fica mais difícil – de repente parece diluir a possibilidade de dano sério a direitos, quando comparado com o cenário mais radical.

É preciso ter frieza sobre essas promessas e sujeitar essas iniciativas a debates informados sobre política criminal e a decisões coletivas sobre o risco de danos morais em que aceitamos incorrer, mesmo quando esses ajustes regulatórios "suavizam" o que seria a versão radical: vigilância pode até inocentar pessoas[56], mas também é uma estrutura que facilita e reproduz discriminação, manipulação e que pode ter efeitos inibidores sobre liberdades,[57] sobretudo a depender do (des-)compromisso do direito penal e das instituições que o aplicam no país com

[55] "'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 própria estrutura da sociedade e do Estado. Nesse nível macro o direito se transforma em uma exigência de separação informacional dos poderes." Greco, "Introdução – 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)", 45.

[56] O Innocence Project mostra como uso de DNA e de materiais de video podem ajudar a diminuir condenações injustas. Ver, por exemplo, "Após quase três anos preso por crimes que não cometeu, jovem é solto com ajuda do Projeto Inocência", G1, acessado 23 de julho de 2021, https://g1.globo.com/fantastico/noticia/2021/07/04/apos-quase-tres-anos-preso-por-crimes-que-nao-cometeu-jovem-e-solto-com-ajuda-do-projeto-inocencia.ghtml.

[57] Richards, "The Dangers of Surveillance".

liberdades democráticas (se ser crítico do governo é ser criminoso ou mesmo terrorista, por exemplo) e de sua seletividade. Impulsiona o tecnoautoritarismo: emergência de práticas autoritárias a partir de mecanismos que a princípio entendemos democráticos.[58] Essa visão de segurança que quer ter controle de tudo não é uma que articula bem aquilo que valorizamos: proteção do risco razoável à vida, à integridade física, à propriedade – o que não envolve tamanhas precauções que contradizem outros dos nossos valores, à privacidade, à autonomia e a outras liberdades (de expressão, de associação) e as características delas em uma democracia.

As preocupações com novas formas de avanço do poder do Estado fazem retornar as preocupações precaucionarias com novos riscos de abuso de poder subjacentes a leis gerais de proteção de dados pessoais e as exigências de fundamentação, justiça, transparência e *accountability*. Além de testar se foram embutidas salvaguardas suficientes para conter um Estado que queira abusar da estrutura para fins tirânicos, não se pode deixar de considerar se a medida ainda assim adiciona riscos novos de injustiça e ônus ao exercício de direitos em comparação com a situação atual – e se isso é algo que queremos, se há um problema real a se resolver que justifique, se não há alternativas. Parte característica dos nossos pleitos históricos de privacidade é conter o poder estatal, fazer essas escolhas difíceis, correr certos riscos porque não admitimos outros: temos a tarefa de honrar essa tradição democrática.

Mineração de dados

Por fim, como falei, há ainda a pretensão de – com as bases de dados montadas e integradas – *minerar* dados, perfilar pessoas para daí extrair novas técnicas (categorias de suspeita) de policiamento e de detecção de atividades criminosas (das suspeitas iniciais ou perfis gerais de suspeita, não ainda do que chamei de suspeita individualizada). Não custa lembrar alguns possíveis direitos implicados: policiar mais um grupo de pessoas que outros pode violar normas de tratamento como igual e policiar por perfil pode esbarrar na premissa embutida na presunção de inocência, de respeito à autonomia moral, de que o que fizemos ontem não prova o que faremos amanhã – muito menos o que pessoas que compartilham uma conexão estatística qualquer o

[58] Alertando sobre esses problemas no Brasil, ver Richard Kemeny, "Brazil Is Sliding into Techno-Authoritarianism", MIT Technology Review, 19 de agosto de 2020, https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/; Centro de Análise da Liberdade e do Autoritarismo e Data Privacy Brasil, "Retrospectiva Tecnoautoritarismo 2020 | Laut e Data Privacy Brasil", LAUT, 26 de janeiro de 2021, https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/.

poderia.[59] Ainda, de novo retorna de forma proeminente a necessidade de o Estado atuar para garantir uma proteção regulatória contra novos riscos decorrentes desses usos que envolvem uso massivo de dados.

Para essas pretensões, fechando o ciclo, a questão inicial da exigência de suspeita retorna: esses tipos de usos de bases de dados (e recursos de *big data*) em alguns casos já envolveriam capitalizar dados pessoais para produzir suspeitas probabilísticas que detectem atividades criminosas automaticamente. Ocorre, atualmente, nesse contexto, um caloroso debate sobre a capacidade de algoritmos preditivos gerarem "suspeitas individualizadas",[60] ao mesmo tempo em que já se discute como cidades e instituições mais "inteligentes" pela coleta massiva de dados e abrirão a possibilidade de que tais dados sejam analisados para detectar condutas criminosas em diversas frentes.[61] O tema é muito mais complexo do que esse trabalho permitiria e se propõe a apresentar, portanto me limitarei a uma observação que considero das mais importantes e ainda dentro do meu propósito de resgatar a necessidade de depurar com cuidado como avaliamos medidas de vigilância estatal.

Emily Berman defende que a suspeita individualizada que permite ao Estado mobilizar a força contra uma pessoa específica é um juízo de probabilidade – mas até aqui sempre esteve envolto em uma justificação narrativa das razões por que se acredita que aquela certa pessoa está envolvida em crime na sua instância particular, não bastando uma mera função estatística de que poderia estar envolvida definida por algoritmo.[62] Algoritmos são probabilísticos, mas não geram

---

[59] Thorburn, "Identification, Surveillance, and Profiling", 32–33.

[60] Ferguson, "Predictive Policing and Reasonable Suspicion"; Berman, "Individualized Suspicion in the Age of Big Data"; Brayne, *Predict and Surveil*. Sobre *big data surveillance*, ver Ferguson, *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*; Brayne, *Predict and Surveil*.

[61] Andrew Ferguson imagina um exemplo que vai além das CCTV sobre áreas públicas: "Other criminal patterns will emerge from mass surveillance technologies embedded in smart city sensors. Sometimes the evidence will be generalized, like the ability of wastewater systems to identify an increase in illegal narcotics from the sewage system. Other times it will be more individualized, like the ability of smart electrical meters to identify suspiciously high home electricity usage (consistent with growing marijuana)".Ver Andrew Guthrie Ferguson, "Structural Sensor Surveillance", *Iowa Law Review* 106 (2021): 63. No Brasil, sobre o uso do software "Detecta", ver Alcides Eduardo dos Reis Peron e Marcos César Alvarez, "Governing the City: The Detecta Surveillance System in São Paulo and the Role of Private Vigilantism in the Public Security", *Sciences Actions Sociales* N° 12, nº 2 (2019): 33–68.

[62] Berman, "Individualized Suspicion in the Age of Big Data", 486–94. A autora chama o exercício de policiais e juízes de articularem as razões de suspeita de um exercício de "normic justification": uma narrativa convincente da crença, no caso, de que o afastamento da privacidade da pessoa resultará em elementos de prova do crime. Esse tipo de proposição seria diferente de meras inferências probabilísticas, porque convida e dá espaço para explicar os erros (as instâncias em que o juízo de *causa provável* que se articulou não se confirma). Dá o exemplo, que aqui simplifico: ocorre um crime na cidade em que o motorista envolvido dirigia ônibus. Pode-se oferecer uma inferência probabilística de que um ônibus azul está envolvido no acidente porque 90% dos ônibus da cidade são azuis, da empresa azul, e se envolvem em 80% dos acidentes. Isso seria diferente do caso em que uma testemunha vê ou pensa que vê um ônibus

esses mesmos tipos de razões.[63] Essa pergunta toca ao tratamento que devemos a pessoas, se não em todas, em partes focais da prática jurídica e que tratam de direitos: os tipos de razões a que podemos nos reportar e quais valem para usar força contra alguém.

Para restrições a direitos morais (fortes), nessa linha, entendo que não há maior reserva do que um papel secundário a essas ferramentas – e ainda assim sob diversas salvaguardas (normas de transparência, explicação, *accountability*, testes contra vieses e problemas de equidade, inacurácia). Isso quando houver algum papel: para algumas intervenções, pode ser que simplesmente não devemos aceitar que o máximo que o direito possa nos dizer é que caímos no campo de imprecisão estatística do algoritmo: nós devemos mais respeito a nós mesmos e uns aos outros.[64] Ademais, quanto mais se puxa essa tendência e se dá esse poder a máquinas, mais encostamos no nosso limite da privacidade na dimensão de contenção de riscos e limitação ao poder. Como vimos, nossa construção do direito penal consagrou que se exige que se possa imputar que a pessoa ingressou, no mínimo, em atos preparatórios para o cometimento do delito – não só que não é uma inferência genérica por seu perfil, mas que também não está só no âmbito de cogitação. O padrão de suspeita individualizada deve respeitar esse princípio.

Isso sem contar as razões de política criminal que desincentivariam a crescente instalação de mecanismos automatizados de detecção de crimes em todo e qualquer lugar, seja porque isso não resolve causas raízes da criminalidade e poderia até levar a encarceramento massivo antes de qualquer prevenção, seja porque deixa de olhar para pessoas como humanos com valor intrínseco e dotados de individualidade e passa a associa-los com índices matemáticos de risco de segurança,

---

azul envolvido e isso é usado como elemento para a suspeita individualizada contra alguém da empresa azul a justificar uma medida coercitiva contra ela, por exemplo. No primeiro caso, se no final das contas não tiver sido um ônibus azul envolvido, o caso só estava inserido na parcela minoritária da estatística (pertencia à parcela porcentual dos casos de acidentes em que ônibus azuis não estão envolvidos). No segundo, precisaríamos de uma explicação de por que a testemunha estava errada (estava escuro, estava sem óculos, mentiu). É desse segundo jogo que fazem parte as razões válidas nessa prática do direito, argumenta. Adiciono o seguinte ponto: essas são as razões válidas porque são as razões relacionadas ao jogo de atribuição de sentido de padrões jurídicos e à abordagem interpretativa com que encaramos a prática jurídica.

[63] Algoritmos que automatizam suspeitas são desafiadores não só porque por vezes não são "transparentes" e "explicáveis", mas porque a lógica com que produzem resultados não compartilha a mesma gramática interpretativa sensível a valores que associamos à prática jurídica no direito penal e processual penal. Ver Mireille Hildebrandt, *Smart Technologies and the End(s) of Law: Novel Entanglements of Law and Technology* (Cheltenham, UK: Edward Elgar Publishing, 2015), 133–81. Para uma reserva desse uso no direito policial, mas ressalvando sua viabilidade para outras áreas, ver Marcela Mattiuzzo, "'Let the Algorithm Decide': Is Human Dignity at Stake?", *Revista Brasileira de Políticas Públicas* 11, nº 1 (2 de abril de 2021), https://www.publicacoes.uniceub.br/RBPP/article/view/6784.

[64] Para um relato dos danos morais e até patrimoniais que esse tipo de problema pode causar, ver Fabiano Bomfim, "'Disseram que eu era traficante', diz pedreiro preso injustamente", *R7.com*, 15 de dezembro de 2021, seç. Brasília, http://noticias.r7.com/brasilia/disseram-que-eu-era-traficante-diz-pedreiro-preso-injustamente-16122021.

seja porque os custos podem não sustentar os ganhos, seja porque dá margem a novos e velhos tipos de atuação discricionária travestidos de objetividade tecnológica,[65] seja porque é uma rendição a uma visão de sociedade de controle de tudo, que tem olhos sobre tudo, seja pelos seus efeitos colaterais em liberdades protegidas, apenas pelo receio da tecnologia e das repercussões de ser equivocadamente enquadrado. Assim, ainda que possa existir campo e interesse para usar tecnologia e big data para detectar suspeitas iniciais por generalizações estatísticas em certos contextos bastante específicos[66], precisamos ter clareza sobre o que colocam em xeque e como não deixar que os fundamentos substantivos que governam nossos compromissos com a exigência de suspeita individualizada não se percam. Esse também é um tema a ser objeto de amplo debate público. A regulação deve estar atenta a todos esses problemas.

2 Uma objeção desconstruída

Nesse momento, penso ser útil e importante mostrar como as discussões acima afastam uma objeção contra pontos-chave do que se desenvolveu até aqui. Em *The Case for Surveillance*[67]*,* Lawrence Rosenthal sustenta que é falso supor que só pode existir vigilância quando existe uma *individualized predication* para que ela ocorra. A tese é relevante porque o que apresentei acima para os contextos de persecução criminal e administrativo policial contra emergências é justamente uma faceta da noção de que a ação de intervenção em direitos de privacidade de alguém (e a

[65] Joh, "The New Surveillance Discretion".

[66] Andrew Crespo defende que os padrões de causa provável (suspeita individualizada) são plurais e variam conforme o contexto, havendo a possibilidade de que alguns deles sejam probabilísticos: como o de um cão que detecta cheiro de drogas e está certo 90% das vezes ou de um policial que, por experiência, chega a um "perfil de conduta suspeita" pela qual em 75% das checagens de quem se insere nela detectam atividade ilícita ocorrendo. Crespo, "Probable Cause Pluralism".O próprio padrão de suspeita individualizada é contextual e, se pode fazer sentido que seja matemático em algum, pode não o ser em outros. Ver ainda Brayne, *Predict and Surveil*, 361–68. A autora argumenta que não há diferença relevante entre uma pessoa suspeitar que uma pessoa carrega uma arma e uma máquina fazer essa mesma avaliação probabilística. Entendo que isso parece ser verdade nesse contexto e aplicação. Porém, à luz das considerações de Emily Berman e do que já apresentei acima sobre generalizações (ações perfiladas), também entendo que essa constatação não poderia gerar e justificar ação policial sem maior corroboração e particularização e aplicáveis a suspeitas específicas sobre certos tipos de crime. Isso porque ações policiais demandam essa fundamentação. Para discutir em um tribunal a validade da abordagem policial da pessoa, é preciso saber as razões dela e não é possível de partida supor que a linguagem matemática atenderá sem discutirmos qual o significado que o padrão de suspeita individualizada deve ter no contexto – se nele, pode ser probabilístico, e até para um humano o é (em 80% dos casos em que há esse volume na barriga, há arma), ou se não é esse tipo de razão que prevelece ou deveria prevalecer. Deixo de firmar conclusões definitivas: o tema é tão complexo que só poderia ser deixado para outro trabalho.

[67] Lawrence Rosenthal, "The Case for Surveillance", in *The Cambridge Handbook of Surveillance Law*, org. David Gray e Stephen Henderson (Cambridge: Cambridge University Press, 2017), 308–29.

seletividade do Estado sobre isso) precisa estar conectada, ligada, predicada a ela de algum modo – a uma suspeita ou a um perigo concreto.

O autor faz uma retrospectiva sobre o papel da polícia para dizer que na época dos *framers* a polícia só *reagia.* Não exercia papel preventivo nem investigava. Podia muito pouco. Pouco a pouco existiu uma reforma para o policiamento "convencional" e assim a polícia ganhou novas atividades. Uma delas foi o policiamento ostensivo – preventivo, em que agentes policiais exerceriam papel de "guardiões" em certas comunidades. Atribui a essa atividade, e aos apoios estatísticos de envio da polícia para *hot spots,* uma das principais causas para redução do crime a partir dos anos 1990 nos EUA. Diz que essa atividade de policiamento não é predicada em nada – então se vigilância dependesse sempre de "um padrão de limiar de predicação individualizado, como suspeita razoável ou causa provável"[68], essas atividades não seriam possíveis. Se para uma investigação começar a polícia já tivesse que reunir muita coisa, seria difícil manter. Daí sustenta que:

> "Em outras palavras, embutido nessa narrativa, está o argumento para a vigilância. A vigilância oficial pode adicionar tutela onde é mais necessária. É garantido, no entanto, apenas naqueles locais em que a tutela adicional é necessária. A vigilância é, portanto, necessária para identificar os locais onde a tutela adicional é necessária e, então, para fornecer essa tutela. Ao mesmo tempo, o argumento para a vigilância não depende de predicação individualizada. Se o estado não pode se envolver em vigilância sem predicação individualizada, então ele não pode oferecer vigilância como uma forma de tutela em pontos críticos [*hot spots*] criminogênicos profilaticamente. Na verdade, se o governo não puder vigiar os pontos críticos até receber informações que representem uma suspeita razoável de que um indivíduo está prestes a cometer um crime, seus esforços subsequentes para fornecer essa tutela provavelmente ocorrerão tarde demais. A tutela funciona profilaticamente e, portanto, exige que a vigilância esteja em vigor antes que um provável infrator chegue ao local.[69]

Diante dessa argumentação, é curioso notar como o autor não define, em nenhum momento, o que está chamando de "vigilância". Tampouco cogita que a exigência de predicação

[68] Tradução livre. No original: "*an individualized threshold standard of predication, such as reasonable suspicion or probable cause*". Rosenthal.

[69] Tradução livre. No original: "Embedded within this narrative, in other words, is the case for surveillance. Official surveillance can add guardianship where it is most needed. It is warranted, however, only at those locations at which additional guardianship is needed. Surveillance is accordingly required both to identify locations where additional guardianship is required and then to supply that guardianship. At the same time, the case for surveillance is not dependent on individualized predication. If the government cannot engage in surveillance absent individualized predication, then it cannot offer surveillance as a form of guardianship at criminogenic hot spots prophylactically. Indeed, if the government cannot surveil hot spots until after it receives information that amounts to reasonable suspicion that an individual is about to commit a crime, its subsequent efforts to provide such guardianship are likely to occur too late. Guardianship works prophylactically, and accordingly requires that surveillance be in place before a likely offender arrives on the scene."Rosenthal, 322.

individualizada pode estar sujeita a gradações e a nuances contextuais. Isto é: intervenções que resvalem em prerrogativas que se assuma como especialmente relevantes podem exigir graus maiores de predicação, em contraposição com práticas que, em rigor, sequer suscitam direitos de privacidade; a predicação para um tipo de crime e vigilância pode ser diferente do que para outro, pela própria natureza da conduta e do que se pretende coibir. O exemplo do autor, aliás, é simplesmente atividade de policiamento ostensivo – em que a polícia conduz atividade *preventiva* para basicamente *marcar presença* em determinada região, observando o que ocorre em tais áreas públicas (vigilância de locais públicos), algo que se espera ter impacto na redução de ilícitos do direito penal clássico contra a vida (violência física) e propriedade (furtos e roubos), e contra a saúde pública (tráfico de entorpecentes). Não está nem mesmo falando de abordagens policiais.

De fato, pelo que foi visto até aqui, não parece existir um direito à privacidade que nos permita obstar pessoas de nos verem enquanto andamos na rua a ponto de impedir a polícia de realizar policiamento ostensivo comum que implica apenas ver o que está acontecendo em vias públicas e mostrar a presença do Estado. Nesse sentido, é certo que a discussão sobre predicação individualizada não pode ser descolada da própria compreensão dos direitos à privacidade, de outras noções de justiça (tratamento como igual, devido processo) – e, sobretudo, do contexto em que estão inseridas (que tipo de medida são). Não é qualquer vigilância que exige predicação individualizada – muito embora as que sejam mais preocupantes em termos de intervenção do Estado o exijam; e o que configura suspeita individualizada para um crime pode variar para outro.

Mais adiante no mesmo texto, Rosenthal dá um exemplo mais difícil – que versaria sobre a vigilância de um ambiente privado, fechado. Ele retoma o julgado United States v. Muller (1976) da Suprema Corte dos Estados Unidos, no qual se teria entendido que a quebra de sigilo bancário não dependeria de um *warrant* (autorização judicial com requisitos rigorosos e estritos de *probable cause*), bastando uma *subpoena* (uma intimação oficial de menor rigor, que carrega um pedido formalizado do requerente por informações que considera relevantes à investigação), porque tais informações não seriam protegidas por expectativa legítima de privacidade[70] em sentido relevante para a Quarta Emenda, já que teriam sido compartilhadas com terceiro (o banco) pelo titular.

[70] Um "teste" paradigmático da delineação do âmbito de proteção da Quarta Emenda é o fixado em *Katz* (389 U.S. 347 (1967)), em que a Suprema Corte desenvolveu o teste da "expectativa razoável de privacidade." Para que essa expectativa seja protegida pela Quarta Emenda, (i) a pessoa em questão deve exibir uma expectativa real (subjetiva) de privacidade e (ii) essa expectativa deve ser uma que a sociedade está preparada para reconhecer como 'razoável'.

Reflexo da *third party doctrine*[71] – jurisprudência em torno da Quarta Emenda que considera que quaisquer atividades que ocorrem em âmbito público ou quaisquer informações compartilhadas com terceiros (inclusive aquelas compartilhadas com o fim de executar um contrato ou ter acesso a um serviço) perdem sua expectativa de privacidade.

Para o autor, seria trágico para persecução penal se informações bancárias só pudessem ser obtidas depois que autoridades tivessem já obtido um conjunto expressivo de provas de ilícito, porque seria muito mais fácil esconder atividades ilícitas. "Em um regime em que o Estado tem permissão para regular uma ampla variedade de atividades financeiras, circunscrever a capacidade do Estado de realizar a vigilância da atividade financeira irá circunscrever de forma semelhante a eficácia de qualquer regime regulatório"[72]. A seguir, ainda lamenta que, pela decisão, o Estado não teria condições de saber por antecipação a quem direcionar *subpoenas*, já que ainda precisaria de uma investigação aberta. Nesse ponto, enaltece os modelos regulatórios de "*cash transaction report*" pelo qual instituições bancárias devem reportar ao *Internal Revenue Service* a identificação de transações em dinheiro a partir de certa quantia e as análises de risco feitas pelo *Securities and Exchange Commission* para identificação de operações suspeitas. Nesse contexto, defende que um sistema que foca apenas na vigilância de locais públicos pode até ter um impacto díspar sobre determinados grupos.

Também aqui, suas observações – e as limitações delas para a conclusão que propõe – são úteis para os propósitos do trabalho a fim de esclarecer aspectos do que apresentei nas seções anteriores. Primeiro, para observar que o caso é até hoje objeto de controvérsia justamente por ter fixado um "padrão de justificação" concebido como frouxo e insuficiente sob uma leitura de um direito à confidencialidade de informações bancárias e de *suspeita individualizada*.[73] A visão de que a pessoa entregou "voluntariamente" informações a um banco a ponto de ter aberto mão de qualquer expectativa de privacidade simplesmente não corresponde à realidade de como nos relacionamos com essas entidades nem ao papel que essas instituições têm para nos permitir conduzir nossas vidas. Nesse contexto, o padrão de justificação de "*subpoenas*", que por vezes deixam a pessoa vulnerável a meras curiosidades de autoridades, pode ser considerado baixo na

[71] Solove, *Understanding Privacy*, 282 (Kindle Location).
[72] Tradução livre. No original: "In a regime in which the government is permitted to regulate a wide variety of financial activity, circumscribing the government's ability to undertake surveillance of financial activity will similarly circumscribe the efficacy of any regulatory regime." Rosenthal, "The Case for Surveillance", 328.
[73] Ver, por exemplo, Christopher Slobogin, "Subpoenas and Privacy", *DePaul Law Review* 54 (2005): 805–45.

calibração de risco de dano moral contra arbitrariedades. No caso, por exemplo, a quebra de sigilo não se dava a partir do nada: xerifes de Houston County na Georgia descobriram uma destilaria de whiskey sem os documentos apropriados e pediram informações bancárias do seu dono, mas também não se dava a partir de uma suspeita mais consistente. Ademais, se existe uma dificuldade específica para identificar certos tipos de crimes que envolvem transações financeiras (que não gerariam vestígios nem flagrância comparáveis a um homicídio, por exemplo) e formar a suspeita individualizada mais robusta antes da obtenção de certos documentos, isso não deveria significar flexibilização geral da *individualized predication* para informações detidas por terceiros.[74] Também é possível calibrar o papel de subpoenas para pedidos que investigam empresas (não pessoas físicas específicas), antes de facilitação geral.[75] O fato de que existem essas discussões apenas reforça a importância que se dá a predicações individualizadas.

Segundo, as considerações de Rosenthal servem para reforçar que diferentes contextos e motivações para intervenções suscitam padrões diferentes de justificação da compatibilidade com direitos à privacidade. Olhemos para o Brasil. A Receita Federal brasileira recebe anualmente declarações de renda de boa parte da população brasileira (recortada a partir de critérios objetivos), para fins de apuração do imposto devido sobre a renda; também recebe de instituições financeiras informações de montantes globais de seus clientes. Tais informações são cobertas por "*sigilo fiscal"*. Para além disso, a Lei Complementar nº 105/2001 autoriza auditores a examinar documentos, livros e registros de instituições financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso. Essas requisições são reguladas de forma específica no Decreto nº 3.724/2001. Não é estranho que, havendo uma justificativa distributiva e impessoal para tanto, implemente-se essa medida geral – muito embora ela envolva obtenção de informações pessoais e que podem revelar aspectos da vida privada de cidadãos ao Estado: no caso, aspectos sobre a capacidade financeira, mas em regra não detalhes. Nos casos específicos que atendam a algum padrão de justificação para a seleção – os indícios que ensejam a abertura de certos procedimentos – mais informações podem ser solicitadas sobre pessoas específicas. Assim, a partir do momento que há seleção e maior invasividade para um grupo específico de pessoas, a exigência de predicação individualizada retorna.

[74] Slobogin, 835–40.
[75] Slobogin, 837–44.

O COAF (Conselho de Controle de Atividades Financeiras) também representa um modelo de atuação preventiva digno de nota. A Lei nº 9.613/1998 autoriza/obriga instituições financeiras a comunicarem operações suspeitas a esse órgão, criado para prevenção e combate sobretudo à lavagem de dinheiro, corrupção, crime organizado e financiamento ao terrorismo – tipos penais específicos, que não geram violência física, flagrância, nem outros vestígios imediatamente notórios a qualquer pessoa que com as transações se deparem. Estabelece, portanto, um dever de monitoramento *geral* de todas as pessoas e suas movimentações financeiras, implementadas diretamente pelos atores principais desse mercado e dentro de seus sistemas. A ideia é deter esse tipo de crime por conta de suas próprias características; não há suspeita prévia a essa checagem geral.

A comunicação de instituições financeiras ao COAF, entretanto, que envolve o Estado ganhar acesso e fazer análises de informações bancárias, e poder requisitar mais informações, depende, por outro lado, de novo de um nível, ainda que baixo, de *suspeita:* operações em espécie que ultrapassem determinada quantidade ou que apresentem irregularidades entre particularidades do cliente e a transação realizada – parâmetros fixados em lei.[76] Para comunicar as autoridades competentes, a unidade faz ainda mais análises para arquivar ou levar adiante os chamados em que conclui haver fundados indícios de ocorrência de ilício. Nesse sentido, é um modelo que combina as lógicas que vimos acima: a de monitoramento geral (*inteligência financeira*), para dissuasão e detecção de crimes específicos facilitados pela obscuridade de transações no sistema financeiro, com as medidas individualizadas do processo penal.

Por essas características, o modelo regulatório inclusive aparenta, em tese, acomodar um direito moral à privacidade que, em outras circunstâncias em face de terceiros (reporto-me ao "modelo do terceiro malicioso"), teríamos sobre as informações financeiras que mantemos em instituições financeiras: as informações só são acessadas por instituições estatais mediante indícios de alguma suspeita – podemos debater sobre esses níveis, sobre a seletividade das operações suspeitas que efetivamente virão a ser analisadas e sobre mecanismos de supervisão do sistema (bem como os riscos inerentes a uso massivo de dados pessoais), mas ainda reconhecer que almeja

[76] Nina Ribeiro Nery de Oliveira, "O Conselho de Controle de Atividades Financeiras – COAF e a Nulidade das Provas" (Monografia (Especialização), Brasília, Instituto Brasiliense de Direito Público - IDP, 2016), 43; Coaf – Conselho de Controle de Atividades Financeiras, "Relatório de Atividades 2020" (Brasília, 2021), 15, https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/relatorio-de-atividades-2020-publicado-20210303.pdf.

implementar uma política de detecção de crimes no sistema financeiro sem, em tese (o tema mereceria, de novo, estudo próprio), onerar excessivamente o exercício desse direito à privacidade. A ideia é deter esse tipo particular de crimes que não geram flagrância, é que não ocorram – mas se fatos criminosos forem verificados, as medidas investigativas que daí decorreram devem estar/são predicadas. Caso algum desses órgãos (Receita, COAF) identifique indícios de infração penal, a acionar persecução penal, o acesso das autoridades competentes passa a necessitar da predicação individualizada típica dessa área do direito para medidas investigativas sobre fatos específicos e da decorrente seleção específica de pessoas para suportá-las. Nesse contexto, meu ponto é que, ao contrário do que faz parecer Rosenthal, esse não é um exemplo para afastar os pressupostos normativos que defendi.

A maneira como sistemas regulatórios devem conter e controlar avanços sobre liberdades obedece a premissas fundamentais: devem ser evitados arbítrio, erros, injustiças e excessos. O lugar de direitos e interesses em privacidade e proteção de dados nessa regulação é de reforço à essa lógica: não pode avançar sem ter razão; deve mostrar respeito à dignidade – ao valor intrínseco das vidas e à responsabilidade pessoal. Como vimos, é cada vez mais difícil separar contextos em que o Estado atua entre direito processual penal e direito administrativo: busca-se segurança de diversas formas, o que *borra* conceitos e categorias que possam ter sido úteis no passado. Mas não há outra saída. Quando a complexidade de medidas pela segurança aumenta, a regulação deve acompanha-la – e endereça-la analiticamente, sem por nossos compromissos fundamentais a perder.

3 Conclusão parcial

Esse capítulo buscou mostrar como ocorre a articulação normativa entre questões de privacidade e proteção de dados nas áreas do direito dedicadas a promover a segurança contra crimes. Em matéria de promoção da segurança, como apontei acima, há diferentes justificativas que podem estar disponíveis ao Estado: (i) pós-crime, no cenário repressivo, o Estado atua para *punir* alguém pela violação da direitos de terceiros e outros bens jurídicos relevantes objeto de proteção por lei penal e por isso atua para obter informações que reconstruam o ocorrido para fins de atribuição de responsabilidade; (ii) pré ou durante-crime, no cenário preventivo e diante de um perigo concreto e imediato, o Estado atua para garantir o direito individual à segurança de alguém

sobre bens como a vida, integridade física e propriedade, também protegidos pela lei penal, que estejam sob ameaça e para isso pode necessitar obter informações e ingressar em espaços para neutralizar tal perigo concreto; (iii) desconectado de crime concreto, no cenário preventivo voltado a perigos abstratos em geral, o Estado atua em nome de política pública de segurança e para tanto pode almejar fazer diversas análises com informações de todas as pessoas governadas.

Na linha do que construí, o Estado pode ter, em tese, justificativas razoáveis para afastar direitos de privacidade no primeiro e no segundo caso ((i) e (ii)). São *razões especiais* para limitar direitos – especiais não porque eu as acho importantes e as chamei assim, mas porque oferecem e se reportam a uma interpretação coerente dos valores que constituem uma comunidade jurídica, pela qual excepcionalmente o Estado pode afastar um direito à privacidade sem deixar de notar que é um direito moral e sob o compromisso de resguardá-lo de abusos, erros e excessos. Essa atuação coercitiva só é autorizada em face de alguém ou de um grupo de pessoas – isto é, seletivamente – mediante uma justa causa: uma suspeita individualizada ou um perigo concreto e iminente. Tudo isso precisa ser legislado, pois os padrões finais desse procedimento, o nível de risco de sofrer injustiça/dano moral, é algo a ser fixado coletivamente, tendo de levar em conta os demais princípios que caracterizam nosso sistema de garantias e sendo vedadas incoerências que importem em retrocessos, e *justificado* no caso concreto. Por outro lado, o caso (iii) não autoriza afastamentos de direitos de privacidade: medidas generalizadas voltadas à promoção de interesses coletivos na segurança pública não superam trunfos – não podem coibir seu exercício.

Desafiadoras são as medidas de vigilância que prometem reduzir a impunidade e aumentar a eficiência do sistema de justiça criminal e da prevenção de crimes, ao mesmo tempo em que exigem a articulação e reconhecimento de novos direitos de privacidade (como um direito à privacidade no sentido de obscuridade em público) ou até extrapolam a linguagem de privacidade, sem deixar de colocar diversos outros problemas de justiça. Mapeei algumas aqui, mas penso que precisam de análises específicas por conta dos detalhes de sua estruturação. De todo modo, já observei que essas iniciativas parecem apelar a uma visão de segurança largamente precaucionária, que aparenta querer rastrear todo tipo de interesse em segurança que alguém poderia ter, sem considerar que comportamos riscos para viver em um Estado comprometido com certas liberdades que igualmente valorizamos. A pertinência de reduzir problemas de segurança pública a "riscos" dessa maneira e preferir medidas de controle e monitoramento desses "riscos" é discussão importante de política criminal – nela, de como melhor realizar o direito à segurança enquanto

proteção regulatória – uma proteção do risco razoável à vida, à integridade, à propriedade enquanto). Abraçar medidas de vigilância modernas pode significar, em diversas oportunidades, preterir o tratamento do fenômeno da criminalidade enquanto um problema social que poderia e deveria ser visto não só à luz do direito penal (embora a responsabilização seja uma peça crucial), mas também ao lado de políticas sociais de educação, trabalho, saúde, redução da desigualdade.

Dito isso, nada afasta as exigências de que o Estado leve em conta interesses privados de forma geral em suas estratégias regulatórias, não onere direitos em excesso e enderece riscos de danos. O Estado tem obrigação de justificar toda a sua atuação e de não onerar pessoas mais do que o necessário. Também cabe frisar que dei destaque para limites postos e ligados a direitos de privacidade, mas nada disso afasta outros direitos que também reconhecemos em nossa prática jurídica: não falei do princípio da não-autoincriminação, por exemplo, nem investiguei a fundo a sua fundamentação, mas essa exploração poderia resultar em mais limites. Também apenas tangenciei riscos de danos morais que o direito da proteção de dados pessoais busca endereçar e que estão postos também nas práticas estatais que envolvem o uso massivo de dados pessoais: sobretudo problemas de justiça, de tratamento desigual quando não há razão para tanto. Por fim, ainda que algo seja viável de uma perspectiva de princípio de direito e em tese, pode ser fortemente desaconselhável por uma perspectiva de política e na prática. O risco é, diversas vezes, demais para se assumir.

Ao resgatar todas essas nuances da interação entre a noção de privacidade e a noção de segurança, espero ter mostrado tudo que deixamos escapar quando damos de barato que privacidade perde da segurança, pressupomos que interesses coletivos prevalecem sobre interesses públicos ou generalizamos os problemas sobre a linguagem de proporcionalidade, para fazer "ponderação". Embora acredite que fazemos e devemos fazer perguntas como a de "adequação" e "necessidade" de uma medida estatal (e que elas já podem encerrar controvérsias), o teste não capta aspectos da maior importância, sobretudo agora que estão em constante provocação de avanços tecnológicos: suas definições abrangentes (e convencionais) de direitos ocultam discussões normativas relevantes sobre o que valorizamos sobre privacidade e segurança que moldam e devem moldar arranjos regulatórios e mesmo casos constitucionais. Na próxima parte, vou explorar a conexão interna entre garantir privacidade e garantir segurança concretamente no direito constitucional brasileiro, com destaque a como o STF tem tratado o tema.

PARTE II – JURISPRUDÊNCIA, REGULAÇÃO E PRÁTICA: UM OLHAR RECONSTRUTIVO, CRÍTICO E PROPOSITIVO A PARTIR DA TEORIA

Na segunda parte deste trabalho, e partir das considerações teóricas vistas na primeira parte, volto-me a considerações mais práticas atinentes ao direito brasileiro. No capítulo 4, reconstruo a jurisprudência constitucional brasileira sobre privacidade sobretudo no campo das atividades de segurança, para apresentar como se deu o desenvolvimento histórico dos paradigmas jurídicos dessa área no direito brasileiro. Além de constituir um registro sobre o pensamento jurídico sobre privacidade no Brasil, esse exercício recupera as origens e raízes de certos entendimentos sobre o escopo de direitos constitucionais e ilustra o que guardam de semelhança com a teoria sobre a articulação entre privacidade e segurança que apresentei na primeira parte, e no que se distanciam ou incorrem nos problemas que identifiquei.

No capítulo 5, destaco alguns aspectos da jurisprudência do STF que considero particularmente problemáticos à luz da teoria apresentada na primeira parte do trabalho. Em especial, e fechando o ciclo, retorno a onde comecei: demonstro a urgência do abandono de referências puramente retóricas de que privacidade não serve a acobertar ilícitos – o que mais polui reflexões do que as aprofunda; comento o papel protagonista do controle judicial de intervenções a privacidades e o localizo sob a perspectiva de outros instrumentos regulatórios imprescindíveis para completar o cenário de salvaguardas, sobretudo frente ao avanço tecnológico; e examino criticamente particularmente duas discussões sobre "sigilo telemático" e outra sobre "privacidade em público" que hoje mais sofrem dos problemas que identifiquei ainda no capítulo 1 e que precisam de revisão urgente.

Capítulo 4 – Privacidade e segurança na jurisprudência constitucional brasileira

Minhas explorações até aqui dos conceitos de privacidade e segurança refletiram um esforço teórico. O próximo passo natural é mostrar como essas reflexões servem para revermos questões que afetam o direito brasileiro. Neste capítulo, busco reconstruir como a jurisprudência do STF lida com casos que aparentam opor interesses de privacidade e segurança. Começo apresentando as garantias constitucionais em torno dos quais giram esse empreendimento. A seguir, revejo casos emblemáticos que chegaram à Corte desde 1949, com referência ao regime legal e constitucional subjacente às decisões. Planejo assim jogar luz sobre os traços da prática jurídica brasileira sobre prerrogativas do Estado quanto à obtenção de informações sobre seus cidadãos. A ênfase está no contexto penal, mas trato também de casos cíveis e administrativos que tenham relevância histórica sobre certas doutrinas e entendimentos que repercutiram na esfera penal.

Como passo a mostrar, nossos dispositivos constitucionais carregam um vínculo com as proteções jurídicas tradicionais de privacidade que se alimentam na lógica de um direito à privacidade como um direito a um "âmbito privado" e por isso buscam identificar e traçar os limites desse âmbito como se buscassem um critério capaz de fazer essa identificação do que está dentro e o que está fora. A noção de "inviolabilidade" associada a esses dispositivos, por sua vez, é em muitas oportunidades vista como uma ameaça de uma proteção absoluta que não existiria frente ao Estado-penal e precisaria ser combatida, ofuscando os reais debates subjacentes aos casos em favor de lugares-comuns sobre privacidade em face do Estado no âmbito de investigações criminais e atividades de segurança pública. De partida, portanto, revejo essas leituras à luz das discussões trazidas na primeira parte.

As discussões mais controvertidas na jurisprudência constitucional brasileira reverberam esses problemas. Grande parte delas se dá quanto (i) à qualidade da informação, das atividades e dos espaços que seriam protegidos por um direito constitucional à privacidade, em maior ou menor grau, por exemplo; e (ii) à necessidade ou não de autorização judicial para acesso – aspecto que tem como principal consequência, no processo penal, poder levar à supressão da prova ilicitamente obtida caso a eventual exigência não esteja satisfeita. Se esse repertório funcionou por um longo tempo tanto para proteger a "casa" e "comunicações telefônicas" quanto para enunciar quando não são "invioláveis", dá sinais de completa exaustão para lidar com problemas de privacidade na nova era tecnológica, como as considerações que antecipei no capítulo 1 já antecipavam.

Nesse sentido, considerando a intenção desse trabalho de contribuir notadamente para o enfrentamento de novos desafios decorrentes do avanço tecnológico, mostro como a área de *sigilo telemático* está vulnerável a uma proteção fragilizada tanto pela menor regulação, quanto por interpretações do escopo constitucional que anulam efeitos desse direito – pela aplicação de testes binários que vimos no capítulo 1 falharem para identificar quando há um direito em jogo. Nesse aspecto, destaco como a discussão em torno da necessidade ou não de uma autorização judicial por vezes polui e tira a atenção de outros aspectos que deveriam ser igualmente relevantes para a averiguação da existência de razões apropriadas para a restrição à privacidade – como a própria regulação da prerrogativa e de seus limites em lei, parâmetros relevantes para a garantia de que nosso avanço do valor da segurança será reconciliado com e acomodará o respeito a direitos.

Para além disso, a revisão de casos emblemáticos de privacidade relativos a diversos "objetos", inclusive os mais "tradicionais", feita neste capítulo traz a oportunidade de mostrar algumas premissas centrais que vão na direção de noções que apresentei na primeira parte desta tese sobre a articulação entre segurança e privacidade: em geral e apesar de ainda limitada, a jurisprudência incorpora a noção de que o "afastamento" da privacidade – isto é, a atuação contrária a uma prerrogativa de privacidade que a pessoa teria com base em nossas práticas – ocorre e só pode ocorrer mediante a apresentação de boas razões para tanto em contextos específicos – destacadas por nossa prática processual penal e administrativo policial, dando espaço para *categorias* que qualificam essas situações (suspeita, perigo), não adotando um regime amplo de *ponderação* para medir quando a privacidade precisa abrir espaço para a segurança. Essa observação, bem como diversas outras que farei ao longo do capítulo, não afastam a nota de que há muito a avançar, mas são importantes para afastar uma inclinação a adotar a solução da

proporcionalidade e da ponderação como o instrumento naturalmente hábil a lidar com os novos problemas gerados pela tecnologia, sem dar espaço à análise conceitual.

1 Breves notas iniciais

1.1 *Um brevíssimo retrato da privacidade no direito constitucional*

A interpretação constitucional sobre privacidade gira em torno de dispositivos constitucionais que apontam para um compromisso fundamental com esse valor. No caso da Constituição Federal brasileira de 1988, há ao menos três. Primeiro, quando diz serem "invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (inciso X); a seguir, quando garante ser a casa "asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo no caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" (inciso XI); terceiro, quando assegura ser "inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (inciso XII).

A doutrina constitucional destaca esse compromisso. José Afonso da Silva, por exemplo, organiza "todas essas manifestações da esfera íntima, privada e da personalidade, que o texto constitucional em exame consagrou" sob a alcunha genérica e ampla de "direito à privacidade".[1] A partir do trabalho de René Ariel Dotti, entende que "a intimidade se caracteriza como a 'esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais'".[2] Abrangeria a inviolabilidade do domicílio, o sigilo da correspondência e o segredo profissional – os dois primeiros também formas de direito à segurança pessoal[3]. Em particular, a inviolabilidade do domicílio garantida pela Constituição consistiria no reconhecimento de que "o homem tem um direito fundamental a um lugar em que, só ou com sua família, gozará de uma esfera jurídica privada e íntima que terá que ser respeitada como sagrada manifestação da pessoa humana"[4]. Já o

[1] José Afonso da Silva, *Curso de Direito Constitucional Positivo* (São Paulo: Malheiros, 2009), 206.
[2] Afonso da Silva, 206.
[3] Afonso da Silva, 437–38.
[4] Afonso da Silva, 207.

sigilo da correspondência abarcaria tanto o direito de expressão e de comunicação quanto "nele é que se encontra a proteção dos segredos pessoais, que se dizem apenas aos correspondentes. Aí é que, não raro, as pessoas expandem suas confissões íntimas na confiança de que se deu pura *confidência*"[5]. Por fim, o segredo profissional imporia o dever a quem exerce profissão pela qual toma conhecimento do segredo de outra pessoa a guarda-lo com fidelidade. "Profissional médico, advogado e também o padro-confessor" não podem liberar o segredo de que se teve conhecimento, devassando a esfera íntima do titular.

Em contraste com a intimidade, a vida privada seria um conceito mais abrangente, "como direito de o indivíduo viver sua própria vida". Partiria de uma constatação de que a vida das pessoas compreenderia um aspecto voltado ao exterior e outro, ao interior. A vida exterior envolveria "a pessoa nas relações sociais e nas atividades públicas" e poderia "ser objeto das pesquisas e das divulgações de terceiros, porque é pública". [6] A vida interior, por sua vez, seria efetivamente a vida privada, que "se debruça sobre a mesma pessoa, sobre os membros de sua família e sobre seus amigos"[7]. Nesse contexto, a tutela constitucional abarcaria tanto o "segredo da vida privada" como a "liberdade da vida privada". "O segredo da vida privada é condição de expansão da personalidade. Para tanto, é indispensável que a pessoa tenha ampla liberdade de realizar sua vida privada, sem perturbação de terceiros."[8] Os atentados a esse direito se dariam por *divulgação* (levar fatos e eventos da vida pessoal e familiar a conhecimento público); *investigação* (pesquisa referente a acontecimentos referentes à vida pessoal e familiar); e *conservação* de um documento relativo à pessoa obtido por meios ilícitos.[9]

Como se vê, buscando definir os contornos da privacidade, o constitucionalista delineia nuances nos significados de *intimidade* e *vida privada* e como esses conceitos interagem com a inviolabilidade do domicílio, o sigilo de correspondência e o segredo profissional. Já vimos no capítulo 1 que, se esse tipo de esforço de definição de um conceito tem espaço em um manual de direito constitucional, ele dificilmente será pacificado a ponto de servir para resolver um caso constitucional difícil, que verse fundamentalmente sobre a pergunta sobre se existe um direito à privacidade que teria sido violado em certo cenário ou sobre o que um direito à privacidade requer

[5] Afonso da Silva, 207.
[6] Afonso da Silva, 208.
[7] Afonso da Silva, 208.
[8] Afonso da Silva, 208.
[9] Afonso da Silva, 208.

como freio a uma atuação do Estado no caso concreto. Há um limite para a compreensão dogmática da privacidade – momento em que articular o conceito a um valor, a uma teoria, é inevitável.

De fato, nem mesmo nesse esforço de manual há concordância sobre como melhor registrar os valores com que esses dispositivos constitucionais estariam comprometidos. Nem todos apelam unicamente a noções de privacidade para explicar o conteúdo deles, a começar. Manuel Gonçalves Ferreira Filho, sem falar em direito à privacidade, por exemplo, limita-se a tratar os três dispositivos centrais da Constituição como relativos (i) à "inviolabilidade da intimidade", contida no inciso X e parte em que a Constituição teria inovado ao "tornar explícitos os chamados 'direitos à integridade moral'"; (ii) a inviolabilidade do domicílio, entendido como residência do indivíduo, contida no inciso XI e que seria um direito relativo à "segurança pessoal"; e (iii) à manifestação de pensamento sigilosa por correspondência de uma pessoa para outra não presente (inciso XII) como uma dimensão da liberdade de expressão.[10] Isto é: apela também a outros conceitos e valores que, se não afastam a noção comum de privacidade, ao menos mostraria como pode se combinar com diferentes lógicas e enfatizar diferentes propósitos. Não surpreende que existam essas variações: como o próprio conceito de privacidade, também o conceito juridicamente relevante de direitos à privacidade é interpretativo.

Dito isso, os dispositivos mencionados – as garantias de "inviolabilidade" da intimidade, da vida privada, do domicílio e do sigilo das comunicações – apresentam certas semelhanças e interconexões textuais. Falo do atributo da "inviolabilidade" que unifica a linguagem dos dispositivos na próxima seção. Por ora, cabe aqui observar, emprestando um diagnóstico de Helen Nissenbaum para o direito americano, que podemos enxergar certas dicotomias implícitas nesses dispositivos: entre (i) informação sensível (como comunicações privadas) e não sensível; (ii) espaço público e espaço privado (domicílio); e (iii) entre aspectos da vida pública e da vida privada (e da intimidade), que responderiam de forma geral à distinção entre "público e privado" de que falei no capítulo 1.[11] Daí nasce o impulso de ler direitos à privacidade a partir dessa separação – depurar o que é, portanto, do *âmbito privado*, nesses diferentes sentidos, buscando-se um critério que separe tipos de informações protegidas das não protegidas, o território público do privado, as áreas privadas da vida daquelas abertas. Controvérsias acerca de direitos à privacidade girariam

[10] Manoel Gonçalves Ferreira Filho, *Curso de Direito Constitucional*, 35º ed (São Paulo: Saraiva, 2009), 300; 307.
[11] Nissenbaum, "Privacy as Contextual Integrity", 136.

em torno da discussão sobre o que faz parte do *âmbito privado* nesses sentidos que o fazem merecedor de ser protegido – e o que não faz parte dele e, portanto, não deve ser protegido.

Esses são, no entanto, "proxies", generalizações, de proteções da privacidade – não valem para todo contexto e, se serviram de algum modo bem para muitos deles no passado, já nem tanto: como já sinalizei, se a proteção jurídica da casa ficar limitada a quem *penetrar* nesse ambiente, não teremos o que fazer quanto a máquinas que conseguem ver entre paredes; e, mais, se acharmos que só temos privacidade quando estamos em ambientes fechados, assistiremos a um assalto ao valor da obscuridade sem ter o que fazer. Nessa mesma linha, se só protegermos "comunicações privadas em fluxo", prerrogativas de privacidade que envolvem outros tipos de dados terão de ser abandonadas. Com isso não quero simplesmente dizer que não podemos ser literais na aplicação do texto constitucional, mas que há um claro convite a revisitar a teoria subjacente a esses dispositivos e a manter integridade com o valor que resguardam.

Em manuais mais recentes de direito constitucional, grupo do qual tomo a obra de Virgílio Afonso da Silva como referência, as distinções inerentes ao texto ainda existem em comentários sobre o "âmbito de proteção" de tais dispositivos constitucionais. Quanto ao inciso X, o autor se limita a argumentar que "não importa se, na definição de intimidade, a ênfase recaia sobre o domínio do próprio corpo, a relação entre corpos, a sexualidade, a afetividade, os segredos íntimos, as comunicações pessoais, a vida doméstica, todas essas esferas estão contidas também no conceito de vida privada"[12]. Destaca que por "casa" vem sendo entendido como moradia "seja própria ou não, seja uma casa ou apenas um quarto em habitação coletiva", abrangendo terreno privado (áreas construídas ou não) e até quarto de hotel.[13] Já para o sigilo das comunicações, interagindo com discussões interpretativas de longa data e que veremos adiante ao mergulhar sobre a jurisprudência, defende que o dispositivo protege diversas formas de *comunicações* – a autorização para a interceptação excepcional das *telefônicas* já constaria no texto, ao passo que restrições das demais comunicações "dependem de robusta fundamentação e têm que passar pelo teste de proporcionalidade"[14]. Assim, o autor agrupa todos esses temas, e a proteção de dados pessoais, sob o tema da "privacidade": dentro dela, tanto o texto constrange a leitura quanto a orientação final para saber se há um direito à privacidade concreto é abertamente o teste de proporcionalidade.

[12] Afonso da Silva, *Direito Constitucional Brasileiro*, 204.
[13] Afonso da Silva, 209.
[14] Afonso da Silva, 214.

Definições genéricas, que rastreiam todo tipo de interesse, oferecem uma alternativa limitada. Como sugeri no capítulo 1, o valor que associamos a certas informações, espaços, relações e atividades está muito mais relacionada ao significado delas no contexto de nossas práticas sociais do que de a qualquer aspecto imanente a elas. Se quisermos protege-las, é importante olhar se o contexto suporta o reconhecimento de uma regra social intersubjetiva que ampare essa proteção em respeito à pessoal naquelas circunstâncias – se comporta a articulação de um direito moral – e se o reconhecimento de certa proteção jurídica à privacidade é reivindicável. Precisamos de uma teoria sobre nossos valores para tanto – algo que a teoria da proporcionalidade não oferece. No caso da atuação do Estado, a proteção é devida na forma de razões que limitam os tipos de ações que podem motivar legitimamente a polícia e o Estado em geral a intervir e sob quais condições, para que ainda mostre respeito ao direito e não imponha dano sério ao exercício deles. Isso é e deve ser levado para regras e procedimentos aplicáveis à sua atuação.

Isso nos ajuda a explicar como o tratamento de uma "mesma privacidade" – um toque, por exemplo, ou mesmo sobre o que dizemos a outras pessoas em conversas das quais não participaram mais ninguém – pode receber tratamentos tão diferentes a depender do contexto em que a pergunta sobre o direito à privacidade em questão se impõe e qual resposta merece. Deve também nos fazer suspeitar de testes binários que possam ter servido no passado em situações sociais menos complexas e que limitem inapropriadamente o próprio reconhecimento de que há direitos morais à privacidade em jogo e que comportam proteção jurídica. Nosso direito constitucional consagrou certas "generalizações" de prerrogativas de privacidade tradicionais ao desenhar proteções jurídicas, o que transparece no texto e reverbera a leitura doutrinária, mas o compromisso moral com prerrogativas de privacidade e uma rede de valores incorporado e invocado nesses dispositivos é o que não se pode perder de vista e é inescapável em qualquer caso que tem não tem resposta fácil.

1.2 *Inviolabilidades em retrospectiva*

Traço comum que chama atenção no texto da Constituição Federal brasileira, e que também aparece nos materiais históricos associados à sua articulação desses direitos, é a linguagem de *inviolabilidade.* Por que esses diferentes aspectos de um âmbito privado da vida seriam

"invioláveis" para a Constituição Federal? Que sentido de inviolabilidade é esse? Uma breve perspectiva história sobre a forma como o direito ocidental de tradição liberal incorporou a proteção do "lar" enquanto "castelo", estabelecendo regras acerca da inviolabilidade do domicílio, é uma boa porta de entrada para esse ponto, considerando os propósitos desse capítulo.[15] Daniel Solove sustenta que a noção de "inviolabilidade" da casa contra intrusões remonta a tempos antigos. Em fontes jurídicas ocidentais, demarca mais precisamente a sua introdução no direito inglês em 1604, no caso *Semayne*, em que se estabeleceu que a *"[T]he house of every one is to him as his castle and fortress*".[16] A proclamação famosa da ideia, atribuída a William Pitt, em 1763, diz que: "*O homem mais pobre pode em sua casa desafiar a Coroa. Pode ser frágil - seu telhado pode tremer - o vento pode entrar - a chuva pode entrar - mas o rei da Inglaterra não pode entrar - todas as suas forças não ousam cruzar a soleira do cortiço em ruínas!*"[17].

Como relata Laura Donahue, a preocupação principal à época dos *framers* da Constituição dos Estados Unidos, na linha da tradição inglesa que primeiro a inseriu em texto jurídico, também advinha de invasões de funcionários do Estado à "santidade do lar" e à esfera em que "pensamentos, crenças, escritos e relações íntimas são protegidas de inspeção exterior".[18] Dessa preocupação teria surgido a tutela jurídica relativa às hipóteses e condições em que o Estado poderia adentrar não só ao lar, mas a algum aspecto que fosse da "esfera privada" de cidadãos. No caso do direito americano, resultou no texto da Quarta Emenda à Constituição dos EUA, de 1798: "*O direito do povo de estar seguro em suas pessoas, casas, papéis e haveres, contra buscas e apreensões irrazoáveis, não será infringido, e não se expedirá mandado a não ser mediante causa provável, apoiada por juramento ou declaração, e descrevendo-se particularmente o lugar da busca e as pessoas ou coisas a serem apreendidas*." Tal garantia incorpora a noção de estar *seguro* – e contra o Estado – associação também feita por um dos constitucionalistas brasileiros, como se viu.

As reivindicações do "sagrado" do lar que resultaram nessas proteções naturalmente não brotaram do nada. A estrutura física da casa, como um tipo de demarcação de uma fronteira entre

---

[15] Daniel Solove, "A Brief History of Information Privacy Law", in *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, org. Christopher Wolf (Practising Law Institute, 2006), §1:2.
[16] Solove, *Understanding Privacy*, Kindle Locations 739-742.
[17] Tradução livre. No original: "*The poorest man may in his cottage bid defiance to the Crown. It may be frail-its roof may shake-the wind may enter-the rain may enter-but the King of England cannot enter-all his force dares not cross the threshold of the ruined tenement!*". William Pitt, Earl of Chatam. Speech, March 1763, in Lord Brougham *Historical Sketches of Statesmen in the Time of George III* First Series (1845) vol. 1.
[18] Laura Donohue, "The Original Fourth Amendment", *University of Chicago Law Review* 83 (2016): 1195.

o que é público e o que é privado[19], e a significação disso como separação entre aquilo que diz respeito ao indivíduo e sua família em contraste com aquilo que é da comunidade é atribuída em estudos antropológicos e sociológicos à percepção da família e, finalmente, do indivíduo como entidades sociais autônomas.[20] Proteger a privacidade doméstica significaria prestigiar um abrigo para a personalidade de indivíduos[21], protegendo-os contra olhos curiosos.

Essa proteção também seria mobilizada para a demarcação da liberdade em face autoridades públicas no Brasil: o "sagrado do lar" que fez a Constituição do Império de 1824 garantir a preservação da casa como "asylo inviolável" permitiu espaços de contestação[22] de "sediciosos" que finalmente levaram à independência do Brasil, por exemplo. Isso não significa que sempre foi invocada por motivos nobres: chegou a ser reivindicada contra autoridades que ameaçavam usar escravos como delatores contra seus senhores[23]. Se hoje somos capazes de colocar

[19] Não estou dizendo que sempre foi assim. Como relata Stuart Shapiro, as quatro paredes de casas conviveram com períodos de ampla circulação de pessoas em diversas sociedades. Leila Algranti relata isso também para o período colonial brasileiro. Dito isso, a arquitetura de domicílios enseja um tipo de separação entre o que seria público e o que seria privado que hoje associamos com a ideia de privacidade. Stuart Shapiro, "Places and Spaces: The Historical Interaction of Technology, Home, and Privacy", *The Information Society* 14, nº 4 (1º de novembro de 1998): 275–84, https://doi.org/10.1080/019722498128728; Leila Mezan Algranti, "Famílias e vida doméstica", in *História da Vida Privada no Brasil: Cotidiano e vida privada na América portuguesa*, org. Laura de Mello e Souza, 1ª edição, vol. 1 (São Paulo: Companhia de Bolso, 2018), 62–119.

[20] Shapiro, "Places and Spaces", 277–78.: "One of the hallmarks of the modern era in the West has been the rise of the individual as a social entity thoroughly distinct from the kinship unit and the larger community. This is a point worth bearing in mind, for it helps explain the changing situation within the home during this period."

[21] Richard Sennett, *The Fall of Public Man* (Penguin UK, 2003), 97.: "(…) the family became the proper place for the natural simplicity of adults to express itself. Here was a dimension of the psyche, and of expression, which possessed an integrity and dignity, no matter what the circumstances of any individual. (...)Thus did the recognition of a common nature and the theory of natural dependency become the psychic foundation of certain political rights."

[22] István Jancsó, "A sedução da liberdade: cotidiano e contestação política no final do século XVIII", in *História da Vida Privada no Brasil: Cotidiano e vida privada na América portuguesa*, org. Laura de Mello e Souza, 1ª edição, vol. 1 (São Paulo: Companhia de Bolso, 2018), 310.: "Se os locais privilegiados de conspiração nas Minas Gerais são as casas, é porque os homens que aí conspiravam as possuíam em condições de assegurar a privacidade necessária para fazê-lo. Era o que se dava quanto aos membros da elite baiana, dez anos mais tarde, mas para os homens pobres que aí sonharam com liberdade, o espaço de privacidade estava principalmente nas ruas e locais ermos da cidade por motive de sua condição. E percebe-se que a própria casa, local privilegiado da vida privada, tem seu significado enriquecido. Os membros da Sociedade Literária do Rio de Janeiro, ainda que implantando novas formas de sociabilidade de autorreferência estamental e radicada no escravismo, circunscreviam às residências particulares o espaço efetivo da prática da liberdade, na revelação de que os ensaios de ruptura dos limites da vida pública se engendravam no interior do espaço privado."

[23] Relatando disputas de poder no Primeiro Reinado, Luiz Felipe de Alencastro cita trecho do jornal Bemtevi, "órgão do autonomismo maranhense", que continha reclamação sobre a nomeação de "prefeitos da comarca" pela Coroa portuguesa, ameaçando a ordem social vigente: "Um prefeito tem espalhados tantos quantos oficiais de polícia, espiões, ele quer para saber do que se passa for a e dentro das casas! Adeus sagrado das famílias! Os prefeitos chamarão e corromperão nossos escravos para dizerem tudo que em nossas casas se faz e se diz, e acrescentarem o mais que nem se faz, nem se diz! Com uma autoridade tão absoluta quem se julgará Seguro! Quem os poderá ter mão! Mil maldições pesem sobre a cabeça de quem pediu e sancionou uma tal lei!". Luiz Felipe de Alencastro, "Vida privada e

essa reivindicação em perspectiva e criticar esse alcance da noção de privacidade do lar, é porque aperfeiçoamos a compreensão do tipo de *sagrado* que essa inviolabilidade protege, mesmo em face de autoridades.

As origens da associação da ideia de "inviolabilidade" ao sigilo das comunicações também são instrutivas das preocupações que resultaram na consagração de um direito em documentos jurídicos. A capacidade de privacidade de cartas trocadas entre pessoas à distância dependia da guarda da confidencialidade de seu teor enquanto estivesse trânsito: enquanto viaja de uma *casa* à outra, de um indivíduo ao outro. Segundo Neil Richards e Daniel Solove recontam também da perspectiva dos Estados Unidos, em tempos coloniais, era difícil *selar* uma carta a ponto de impedir que fosse lida por terceiros.[24] Serviços postais logo então começaram a cobrar esse dever de seus funcionários e surgiram leis ainda em 1710 que impediam a abertura, detenção e atraso de cartas. Em 1877, em *Ex parte Jackson,* a Suprema Corte dos Estados Unidos entendeu que "*o fato de que as pessoas dão voluntariamente ao Estado suas cartas para entrega não renuncia a proteção, já que era esperado do Estado que mantenha a confidencialidade*"[25] – não afastando a proteção da Quarta Emenda para tais objetos simplesmente porque tais papéis passavam a ser detidos e transmitidos por órgãos estatais. Nesse bojo de transformações sociais e expectativas culturais que refletia nas fontes jurídicas e na linguagem que veiculavam via-se a atribuição da noção de objeto "sagrado" às ideias e imagens expressadas por pessoas em cartas, o que exigia respeito.[26] Essas proteções garantiam um "espaço privado" mesmo fora do "local privado" da casa.[27] Após as cartas, mantiveram-se as preocupações em garantir que novos órgãos públicos e sobretudo empresas encarregadas de viabilizar comunicações à distância respeitassem a inviolabilidade de correspondências. As invenções do telégrafo e do telefone foram objeto de apropriação social e respostas regulatórias semelhantes.[28] No Brasil, passaram a ter referência

ordem privada no Império", in *História da Vida Privada no Brasil: Império e a modernidade nacional*, org. Luiz Felipe de Alencastro, 1ª edição, vol. 2 (São Paulo: Companhia de Bolso, 2019), 17.

[24] Solove e Richards, "Privacy's Other Path", 141–42.

[25] *Ex parte Jackson,* 96 US 727 (1877).

[26] Solove e Richards, "Privacy's Other Path", 142–43. Era reforçada ainda, segundo os autores, por doutrinas de *direitos autorais* pelo qual "expressões não publicadas [fixadas] em cartas" seriam protegidas contra publicação involuntária: não precisavam ser íntimas a ponto de ferir sentimentos de autor – a própria noção de propriedade veiculava esse interesse e essa proteção.

[27] Shapiro, "Places and Spaces", 278–79.

[28] Solove e Richards, "Privacy's Other Path", 144–45; Shapiro, "Places and Spaces", 280.

constitucional a partir da Constituição Federal de 1966. Em 1988, "dados" foram incluídos "por exigência da nossa época"[29].

Enquanto as *inviolabilidades* sobre correspondências e domicílio, que influenciaram a inclusão dessas garantias ou de alguma forma delas desde a primeira Constituição brasileira ainda no Império em 1824[30], encontram certa precedência histórica e desde logo calibre constitucional, a ideia de inviolabilidade da intimidade e da vida privada demorou mais a se consagrar a nível constitucional no Brasil. No *common law* que acima usei de comparativo, o *direito à privacidade* apareceu veiculado sobretudo a demandas cíveis. A formulação se tornou célebre através do artigo *The Right to Privacy*[31] de Warren e Brandeis, de 1890, destinado a proteger o que é de "ocorrência doméstica", nos termos que já comentei no capítulo 1, e que deu origem aos *privacy torts*[32]. Nessa dimensão da privacidade, a inviolabilidade é da personalidade.

No Brasil, a inclusão de um dispositivo constitucional capaz de acomodar pleitos mais gerais de privacidade como o inciso X que protege a inviolabilidade da "intimidade" e "vida privada" é atribuída a antecedentes legislativos inaugurados no Código Penal de 1969, no qual foi previsto o crime de "violar, mediante processo técnico, o direito à intimidade da vida privada ou o direito ao resguardo das palavras ou discursos que não forem pronunciados pùblicamente".[33] A discussão sobre "direitos de personalidade" e a necessidade de dar tratamento constitucional e

---

[29] Palavras do Constituinte Adolfo Oliveira (PFL), defendendo o Substitutivo 2. Ver Assembleia Nacional Constituinte, "Diário da Assembléia Nacional Constituinte (Suplemento 'C')" (Brasília, 1987), 186, https://www.senado.leg.br/publicacoes/anais/constituinte/9b_Sistematizacao.pdf. A primeira menção a 'dados' no contexto Constituinte apareceu no tal Substitutivo 2 do Relator, ao que se permite extrair dos arquivos da Assembleia Nacional Constituinte, acolhendo emenda de Artur da Távola (PMDB/RJ) de que o "sigilo clássico" deveria agora abranger também a hipótese de "comunicação de dados", "no mundo contemporâneo". A redação dada no substitutivo foi: "É inviolável o sigilo da correspondência e das comunicações telegráficas, telefônicas e de dados, salvo por ordem judicial, nos casos e na forma que a lei estabelecer, para fins de instrução processual. Na fase final de redação, foi aprovada sugestão de Hélio Braun (PMDB/RS) de que o que se deve "fixar é a inviolabilidade do sigilo de dados e não precipuamente o sigilo das comunicações de dados", acolhida na versão aprovada e promulgada, após intercessão de Ricardo Fiuza (PFL) no Plenário. Ver Câmara dos Deputados, *A construção do artigo 5º da Constituição de 1988* (Brasília: Câmara dos Deputados, Edições Câmara, 2013), 79-82;1545;1751; Assembleia Nacional Constituinte, "Diário da Assembléia Nacional Constituinte (Suplemento 'B')" (Brasília, 1988), 213, http://imagem.camara.gov.br/Imagem/d/pdf/307anc23set1988SUPB.pdf.

[30] Constituição Política do Império do Brazil (de 25 de março de 1824):

VII. Todo o Cidadão tem em sua casa um asylo inviolavel. De noite não se poderá entrar nella, senão por seu consentimento, ou para o defender de incendio, ou inundação; e de dia só será franqueada a sua entrada nos casos, e pela maneira, que a Lei determinar.

XXVII. O Segredo das Cartas é inviolável. A Administração do Correio fica rigorosamente responsavel por qualquer infracção deste Artigo.

[31] Warren e Brandeis, "The Right to Privacy".

[32] Prosser, "Privacy". Ver também a primeira seção do capítulo 1.

[33] Doneda, *Da Privacidade à Proteção de Dados Pessoais*, 2019, 103.

legislativo a eles, aí incluindo intimidade e vida privada, é registrada em artigos da década que antecedeu a CF/88.[34] Antes disso, tratados de direito civil já discutiam um "direito a velar pela intimidade"[35] a partir da Constituição Federal e de dispositivos penais. O Código Civil de 2002, por sua vez, consagrou o alinhamento às proteções asseguradas pela Constituição na seção de "direitos de personalidade", sem aprofundar os conceitos a ponto de facilitar a identificação de atos ilícitos de "privacidade", dos danos morais à personalidade que esses direitos coíbem.[36]

Nessa perspectiva, o conceito de inviolabilidade associado aos dispositivos constitucionais passa a ideia de que seu objeto não deve ser violado, de que deve ser mantido em *segurança* contra invasões, intrusões e profanações por ser de algum modo *sagrado* e exigir assim respeito por se referir à própria personalidade.[37] Na jurisprudência constitucional brasileira, como se verá adiante, essa locução gerou e ainda gera enormes discussões e, a meu ver, confusões – sobretudo pela leitura (que buscam de vários modos combater) de que "inviolável" significaria portar certa proteção *absoluta,* de modo a afastar esses campos da vida de qualquer interferência mesmo quando observado devido processo legal. Não precisa ser esse o sentido e, em consonância com o que apresentei na primeira parte da tese, acredito que não é.

Inviolabilidade pode significar certa *imunidade* contra certos tipos de ações – aquelas cuja intencionalidade desafiar um valor que prezamos segundo o contexto.[38] Inviolabilidade pode reportar-se ao status moral da pessoa detentora desses direitos, no sentido de que tais aspectos de sua vida não se pode violar *de certas maneiras*.[39] A violação ocorreria quando tratamento inadmissível ocorresse, porque negaria o status moral de pessoa cuja vida tem valor intrínseco e que tem responsabilidade para conduzi-la em certo contexto. Para o Estado, no campo da segurança pública e do processo penal, a inviolabilidade não significa inacessibilidade absoluta sobre

[34] Antônio Chaves, "Os direitos fundamentais da personalidade moral (à integridade psíquica, à segurança, à honra, ao nome, à imagem, à intimidade)", *Revista de Informação Legislativa* 15, nº 58 (abril de 1978): 157–80; René Ariel Dotti, "A liberdade e o direito à intimidade", *Revista de Informação Legislativa* 16, nº 66 (1980): 125–52.
[35] Miranda, *Tratado de Direito Privado: Parte Especial – Tomo VII: Direito de personalidade, Direito de Família*, 196-211 (§755 Direito a velar a intimidade). Os tomos que compõem o tratado foram originalmente publicados entre 1954 e 1969.
[36] Anderson Schreiber identifica e comenta mais de 30 casos que versariam sobre direitos de privacidade em sua obra sobre direitos de personalidade, mas critica a parca orientação do Código para lidar com as complexidades do tema e "ponderações" exigidas. Anderson Schreiber, *Direitos de personalidade*, 2º ed (São Paulo: Atlas, 2013), 133–86.
[37] Linda McClain, "Inviolability and Privacy: The Castle, the Sanctuary, and the Body", *Yale Journal of Law & the Humanities* 7, nº 1 (8 de maio de 2013): 198.
[38] McClain, 205.
[39] Thomas Nagel, "The Value of Inviolability", in *Morality and Self-Interest*, org. Paul Bloomfield (Oxford: Oxford University Press, 2007), 107.

aspectos privados da vida de alguém. Em geral, significa ter de respeitar e observar exigências formais e materiais de fundamentação que garantam respeito a tais direitos contra abusos, erros e excessos – procedimentos que visam impedir o afastamento ilegítimo e injustificado desses direitos e que são corroboradas pelas nossas práticas, convicções e expectativas sobre o tratamento que o Estado deve a nós nessas situações. Tudo isso calibrado ao contexto em que se insere.

1.3 *A pesquisa*

Nesse contexto, passo à análise dos casos de controle constitucional de prerrogativas estatais sobre a privacidade. Como adiantei, foi feita uma pesquisa no repositório eletrônico de jurisprudência do STF com termos relativos a "sigilo", "intimidade", "privacidade" e "inviolabilidade" entre os dias 13 e 17 de janeiro de 2021. O repositório eletrônico do STF contempla acórdãos publicados após 06/07/1950 e a busca abrange a identificação desses elementos de busca na ementa e na indexação dada aos acórdãos – os resultados refletem o que existia disponível ao tempo da pesquisa.[40] Entre os acórdãos catalogados, com antecipei, busquei analisar aqueles que discutem questões de privacidade frente a medidas estatais sobretudo no contexto processual penal e administrativo de segurança pública, buscando aqueles mais emblemáticos – que delimitaram as fronteiras e formularam doutrinas.

Para facilitar a análise e localização dos julgados paradigmáticos, tais acórdãos foram estruturados cronologicamente pela data de julgamento e então categorizados em planilhas segundo "objetos" de privacidade sobre os quais versavam (sigilo bancário, sigilo fiscal, sigilo de chamadas telefônicas, sigilo de registros telefônicos, sigilo telemático, aspectos físicos do corpo, ou 'outros') e o contexto em que a discussão se deu (matéria cível, processual penal ou administrativa). A partir da análise da ementa e, quando esta não permitia, do relatório, identifiquei em novas colunas o tema em discussão e descartei aqueles que não interessavam ao tema do trabalho, como os casos que lidavam com discussões sobre transparência do Poder Público, sigilo processual (acesso aos autos/segredo de justiça), sigilo do voto e liberdade de expressão ou de imprensa.

[40] Cf. STF, Dicas de Pesquisa, disponível em: http://portal.stf.jus.br/textos/verTexto.asp?servico=jurisprudenciaPesquisaGeralNovoPortal&pagina=Dicas_de_pesquisa Acessado em 15.01.2021.

Muito embora o meu interesse seja a matéria penal (da perspectiva de prerrogativas do Estado), ao fazer a triagem dos casos, observei que as discussões de privacidade nesse contexto não eram impermeáveis às discussões tidas em disputas cíveis, entre agentes privados, e administrativas para além de segurança pública. São esses, aliás, os contextos dos primeiros casos que apelam a noções de privacidade que aparecem na busca, ainda que o conceito não seja discutido explicitamente. Pela sua importância no retrato de como se pensava e se pensa sobre privacidade nos julgados do STF, incluí essas decisões mais antigas na reconstrução elaborada adiante, ainda que de outras áreas. Desde logo, também registro que não se pode extrair das decisões abaixo inovação histórica definitiva sobre o que se argumentou – sobre linhas de argumentação –, por conta da limitação do recurso que usei de fonte. No entanto, no mínimo, a semelhança com argumentos vistos hoje permite verificar a continuidade de tais racionalidades.

Nesse contexto, minha reconstrução é voltada à *ratio decidendi,* aos fatores e argumentos que ensejam uma posição em detrimento de outra que compunha a controvérsia sobre privacidade e proteção de dados frente ao Estado. Comento ideias centrais e observo problemas de consistência. Não há qualquer pretensão de exaurir a matéria, mas existiu o esforço de identificar discussões centrais – focais à compreensão dos limites do poder do Estado penal frente a interesses de privacidade e dados pessoais no direito brasileiro. Destaquei decisões que, na minha leitura do problema de privacidade em questão, pareceram lidar com questões novas dentro do período estudado. Dentro da mesma linha temática de discussão, destaquei os fundamentos lançados e a revisão e o amadurecimento deles ao longo do tempo. Todas as citações em aspas referem-se a trechos do acórdão que estiver comentando; a indicação de páginas de citações de votos foi acrescentada quando possível – e quando os acórdãos do STF começam a ficar caracteristicamente longos. Quando pertinente, acrescentei as referências de textos normativos em rodapé.

Sob essas premissas, o exercício é admitidamente limitado em termos de quantidade de julgados selecionados e analisados. Naturalmente, a busca em si desse tipo de caso também carece de outros tipos de limitações: apenas algumas reivindicações de privacidade chegam ao judiciário e, dentre elas, apenas uma parte muito reduzida se torna casos constitucionais. Ainda assim, para o propósito de apontar como se pensa o assunto e o estado em que jurisprudência se encontra à luz da teoria que apresentei na primeira parte da tese, ainda relevante e pertinente.

2 Sigilo bancário[41]

O acórdão mais antigo localizado versa sobre sigilo bancário. No MS nº 1047-SP, julgado em 6 de setembro de 1949[42], 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 letigimamente 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[43]); (b) se a determinação consistia em exibição de documentos, deveria ter sido observado o procedimento do art. 220 do Código de Processo Civil[44]; (c) a medida violaria os arts.

[41] Assim agrupei os casos que lidam com informações que pessoas mantêm junto a instituições financeiras. A categoria também é utilizada pelo STF.

[42] O primeiro acórdão listado aqui não compõe, ou pelo menos não compunha, o repositório eletrônico do STF, que contempla decisões a partir de 1950, ao tempo em que fiz a pesquisa. No entanto, como os primeiros acórdãos analisados se referiam a esse MS como paradigmático, foi solicitada a cópia eletrônica do acórdão. Supremo Tribunal Federal, MS 1047, Min. rel. Ribeiro da Costa, Tribunal Pleno, j. 06.09.1949.

[43] 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: (…)"

[44] 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 exibí-lo, poderá o juiz designar audiência especial, afim de, ouvidos o requerente e o terceiro, proferir despacho."

17, 18 e 19 do Código Comercial[45], 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 registou 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.[46] 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[47]. 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

[45] 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.
[46] Supremo Tribunal Federal, RE 2172, Min. rel. Nelson Hungria, Tribunal Pleno, j. 10.07.1953.
[47] 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: (…)"

'confidentes necessários' e, como tais, obrigados a sigilo 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. Não se fala em "quebra de sigilo" – a ideia é que o sigilo sequer é oposto à autoridade pública nessas situações. 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. 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.

Em 13 de setembro de 1961, o STF apreciou outro caso sobre sigilo profissional bancário que traçou um limite sobre as possibilidades de acesso.[48] O Banco Hipotecário e Agrícola para o Estado de Minas Gerais impetrou mandado de segurança contra ato de juiz da 2ª Vara Cível de Belo Horizonte que determinou, ao que alegou, 'verdadeira devassa em seus livros e escrita' (em uma ação relativa a um particular). "É certo que o sigilo bancário não é absoluto e ele cede, muitas vezes, a valores dignos de consideração, como se dá para a perfeita instrução de processos criminais, como decidira esta Suprema Corte, no RMS 1.047 (...) [m]as, nas questões de ordem patrimonial, os exames hão de se fazer com cautela". Aos "peritos se poderá dar o privilégio, apenas porque são peritos, de se inteirarem dos negócios do Banco. Sua atuação há de limitar-se aos quesitos, no que interessa às partes em litígio. Quaisquer dúvidas, que surgirem, devem ser

[48] Supremo Tribunal Federal, RMS 9057, Rel. Min. Gonçalves de Oliveira, Tribunal Pleno, j. 13.09.1961, DJ 26.10.1961.

solvidas pelo Juiz, nesta orientação a que ainda agora aludimos. De qualquer forma excluem-se do exame, no caso, o cadastro, as fichas cadastrais".

Nesse último ponto, há referência ao RMS 2574[49], de 1957, pelo qual "não há lei que obrigue um banco a exibir o seu fichário cadastral, de natureza sigilar e uso privado. Assim é ilegal e pode ser anulado por mandado de segurança, a ordem judicial de exibição". Nessa ocasião, o STF entendeu não ser cabível decisão judicial que autorize o acesso a ficha cadastral de cliente para análise pericial de operações realizadas por certo indivíduo – o que foi solicitado por esposa com relação ao marido em ação de desquite para compreensão de sua situação patrimonial. Esse fichário cadastral seria organizado pelo banco para fins exclusivos e teria "informações várias sobre idoneidade financeira e moral dos que operam na praça". Não se tratava, assim, de informação que, nos termos dos arts. 216 a 222 do CPC (1939)[50], pudessem ser exibidas por terceiros, já que não diziam respeito a documento pertencente ao requerente nem documento comum ao requerente e ao banco. Sendo assim, a recusa do banco quanto à ficha não poderia ser interpretada como falta de colaboração com a Justiça.

Além de sublinhar a necessidade de vínculo entre o escopo das informações a serem fornecidas ao que é pertinente e necessário à elucidação do litígio, os julgados também destacam uma limitação de acesso a bases cadastrais de clientes de bancos, sobretudo pela ausência de

---

[49] Supremo Tribunal Federal, RMS 2574, Rel. Min. Antonio Villas Boas, Tribunal Pleno, j. 08.07.1957, DJ 08.08.1957. Muito embora a publicação se refira a período após 06/07/1950, o referido acórdão não foi detectado no repositório eletrônico do STF, o que sugere que o repositório não é completo, apesar das informações que constam no site.

[50] Código de Processo Civil de 1939 (Decreto-Lei nº 1.608, de 18 de setembro de 1939). Art. 216. O interessado poderá solicitar ao juiz que ordene a exibição de documento e de coisa que se ache em poder da parte contrária.
Art. 217. O pedido de exibição de documento conterá: I - a designação do documento; II - a indicação, tão completa quanto possivel, de seu conteúdo; III - a enumeração dos fatos que devem ser provados com ele; IV - a indicação das circunstâncias em que o requerente se funda para afirmar que o documento existe e se acha em poder da parte contrária.
Art. 218. A exibição do documento não poderá ser negada: I - si houver obrigação legal de o exibir; II - si aquele que o tiver em seu poder, a ele houver feito referência na causa com o propósito de constituir prova; III - si o documento, em virtude de seu conteudo, for comum ao requerente e ao detentor. *Parágrafo único.* O documento considerar-se-á comum às pessôas cujas relações jurídicas forem nele determinadas e àquelas em cujo interesse houver sido elaborado.
Art. 219. Desde que só o exame do documento possa confirmar ou destruir as alegações do requerente, o juiz poderá considerá-las provadas, si forem verosímeis e estiverem coerentes com as demais provas dos autos: I - quando a parte condenada a exibí-lo negar que o possua, ou recusar a exibição; II - quando as circunstâncias convecerem de que a parte condenada à exibição ocultou ou inutilizou o documento, para impedir-lhe o uso pelo requerente. 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 exibí-lo, poderá o juiz designar audiência especial, afim de, ouvidos o requerente e o terceiro, proferir despacho.
Art. 221. Si o terceiro, notificado, não exibir o documento, poderá o interessado cobrar-lhe, por ação direta, a indenização dos danos sofridos, sem prejuizo da responsabilidade penal por desobediência.
Art. 222. A exibição de coisa obedecerá, no que fôr aplicavel, ao disposto para a exibição de documento.

obrigação legal de fornecimento e apresentação de algo dessa natureza. Esse não foi um elemento propriamente destacado antes. Pela lógica dos acórdãos anteriores, tudo o que serve para elucidar conflitos na Justiça deveria estar disponível, de modo que é a primeira vez que se vê o STF traçar uma linha. Considerando as observações sobre o "conceito moral" contida nas fichas elaboradas pelo banco, a hipótese seria a de que dados arregimentados no âmbito de relações de clientela, que poderiam conter avaliações negativas sobre a pessoa e que hoje conhecemos como histórico de crédito e forma pontuação de crédito, não poderiam ser exibidas naqueles contextos. De novo, entretanto, tal argumento não é formulado como um de privacidade.

Em 20 de maio de 1966, no RMS 15925, a discussão do sigilo bancário é pela primeira vez – nos acórdãos identificados – tratada no contexto de uma requisição administrativa – isto é, não mais em caso cível envolvendo agentes privados, mas uma requisição diretamente de interesse de agente público no exercício de atividades públicas.[51] O Banco Francês e Italiano para a América do Sul recebeu pedido de agentes fiscais para prestar informações sobre operações de uma empresa e uma pessoa física, mas recusou e foi autuado por embaraço à ação fiscal. Acolhendo parecer da procuradoria, o STF entende que não há "perigo de devassa ou quebra de sigilo bancário" no caso porque "[o] sigilo bancário tem por finalidade a proteção contra a divulgação ao público dos negócios do banco, ou dos negócios dos seus clientes" e "agentes fiscais do Imposto de Renda são obrigados ao sigilo (art. 201, Decreto nº 47.373/59[52])".

Como veremos mais a frente, essa lógica de "transferência de sigilo" para afastar o argumento de que haveria "quebra de sigilo" ao encaminhar dados a alguém segue bastante comum no contexto de compartilhamento de informações entre autoridades estatais. O ponto mais relevante do acórdão, no entanto, considerando que a novidade aqui é permitir um acesso *direto*, sem intermediação de autoridade judicial, é a indicação de que existe uma prerrogativa de uma autoridade pública, prevista em lei, para tanto. A justificativa distributiva subjacente que a tornaria válida é tomada por natural: sequer se problematiza a constitucionalidade da atuação do Estado para fiscalização tributária – que incluiria um poder de ter acesso a informações financeiras dos cidadãos e empresas. Essa observação é reforçada no AI 40883[53], de 1967, que envolvia as mesmas

[51] Supremo Tribunal Federal, RMS 15925, rel. Min. Gonçalves de Oliveira, Tribunal Pleno, j. 20.05.1966, DJ 24.06.1966.
[52] Decreto nº 47.373/59 ("Regulamento para a cobrança e fiscalização do impôsto de renda"): "Art. 201. Aquele, que, em serviço do Impôsto de Renda, revelar informações que tiver obtido no cumprimento do dever profissional, ou no exercício do oficio ou emprêgo, será responsabilizado como violador de segredo, de acôrdo com a lei penal."
[53] Supremo Tribunal Federal, AI 40883, rel. Min Hermes Lima, Terceira Turma, j. 10.11.1967, DJ 08.03.1968.

partes e a mesma questão: agentes do Fisco exigiram informações sobre correntistas de banco. Com a recusa, o banco foi autuado. Nele, o STF confirmou o entendimento de que antes da entrada em vigor da Lei n. 4.154/62[54] bancos não estavam obrigados a exibir à fiscalização esses materiais diretamente. Antes disso só por exibição "parcial e determinada, por decreto judicial".

Em decisão do AI 40812[55], também de 1967, o STF afirmou a necessidade de que tais requisições sejam precedidas da abertura de um procedimento fiscal, não sendo admitidas sem tal lastro. Isto é: além da previsão em lei de uma tal prerrogativa, seria preciso que diga respeito a um procedimento formalizado – outro parâmetro procedimental que delimita o objeto. No caso, agentes do Fisco exigiram de um banco a apresentação de "relação discriminada de promissórias rurais descontadas na sua agência local". O acórdão afastou essa exigência sob a lógica de que não havia sido ainda instalado um procedimento fiscal contra o banco – que no caso era o contribuinte em questão. O STF fundamentalmente não conhece do recurso, mas o relator Min. Djaci Falcão faz questão de registrar que a Lei nº 4.595/64 que resguarda sigilo bancário realmente exigiria essa instauração prévia.[56]

Observe-se que até aqui não tratei de decisão em matéria de processo penal. De fato, nenhuma das decisões sobre sigilo bancário localizadas pré-Constituição Federal de 1988 no STF versaram sobre prerrogativas de autoridades de investigação. Não posso afirmar que não existiram – apenas que não constam no repositório da partir dos termos buscados. Tampouco foram as decisões vistas até aqui decididas com referência explícita a noções de direito à privacidade e à intimidade dos correntistas, como antecipei. Não chega a ser surpresa, considerando que as Constituições de 1946 e de 1967, que abrangem o período dos julgados, não garantiam um direito

[54] Lei nº 4.154/1962: "Art. 7º Os estabelecimentos bancários, inclusive as Caixas Econômicas, não poderão eximir-se de fornecer à fiscalização do impôsto de renda, em cada caso especificado em despacho do diretor, dos delegados regionais ou seccionais e dos inspetores do impôsto de renda, cópias das contas correntes de seus depositantes e de outras pessoas que tenham relações com tais estabelecimentos, nem de prestar informações ou quaisquer esclarecimentos solicitados."

[55] Supremo Tribunal Federal, AI 40812, Min rel. Djaci Falcão, Primeira Turma, j. 21.08.1967.

[56] As referências são aos §§5º e 6º do art. 38 da Lei nº 4.595/64: "Art. 38. As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados.
§ 5º Os agentes fiscais tributários do Ministério da Fazenda e dos Estados somente poderão proceder a exames de documentos, livros e registros de contas de depósitos, quando houver processo instaurado e os mesmos forem considerados indispensáveis pela autoridade competente.
§ 6º O disposto no parágrafo anterior se aplica igualmente à prestação de esclarecimentos e informes pelas instituições financeiras às autoridades fiscais, devendo sempre estas e os exames serem conservados em sigilo, não podendo ser utilizados senão reservadamente."

à vida privada e à intimidade;[57] apenas tratavam de sigilo de correspondência e comunicações. De todo modo, o contexto penal logo aparece como um tema central entre os acórdãos já promulgados com a nova Constituição. O cenário político muda, o discurso muda.

Em 25 de março de 1992, o STF apreciou petição de Delegado da Polícia Federal que buscava autorização judicial para a quebra de sigilo do ex-Ministro do Trabalho Antonio Rogério Magri, demitido em janeiro daquele ano pelo Presidente Fernando Collor de Mello em meio a acusações de corrupção.[58] O pedido para fornecimento de extratos bancários de 1991 e 1992 dele e da esposa se baseava unicamente em publicação na imprensa segundo a qual cintas de dinheiro teriam sido encontradas no lixo de sua residência. O relator, Min. Carlos Velloso, na mesma linha que o parecer da Procuradoria-Geral da República, sustenta que "o sigilo bancário protege interesses privados. É ele espécie de direito à privacidade, inerente à personalidade das pessoas e que a Constituição consagra (C.F., art. 5º, X), além de atender 'a uma finalidade de ordem pública, qual seja a de proteção do sistema de crédito' (...)".

Como seria comum a todos os votos – e é um chavão quase que obrigatório em decisões de quebras de sigilo como se vê desde 1949 – a observação seguinte do Ministro é a de que "não é ele um direito absoluto, devendo ceder, é certo, diante do interesse público, do interesse da justiça, do interesse social, conforme, aliás, tem decidido essa Corte". Em tese, portanto, não haveria dúvidas da possibilidade de quebra de sigilo bancário com autorização judicial. Complementa: "pode o Judiciário requisitar, relativamente a pessoa e instituições, informações que implicam quebra do sigilo (Lei 4.595/64, art. 38, § 1º). A faculdade conferida ao judiciário pressupõe, entretanto, que a autoridade judiciária procederá com cautela, prudência e moderação, virtudes inerentes à magistratura, ou que os magistrados devem possuir". Ocorre aqui que o pedido não está instruído "com os elementos de prova mínimos de autoria de delito, aptos a justificar a autorização judicial pretendida". "Aliás, não há notícia do delito que teria sido praticado". Não havia, para usar a terminologia vista ao fim da primeira parte da tese, suspeita individualizada suficiente.

O Min. Celso de Mello seguiu o mesmo raciocínio. Frisou que a intimidade é "valor constitucionalmente assegurado (CF, art. 5º, X), cuja proteção normativa busca erigir e reservar,

[57] Havia diversas discussões em torno de um direito à intimidade pré-1988, mas elas se davam no direito civil. Cf. Chaves, "Os direitos fundamentais da personalidade moral (à integridade psíquica, à segurança, à honra, ao nome, à imagem, à intimidade)"; Dotti, "A liberdade e o direito à intimidade".
[58] Supremo Tribunal Federal, Pet 557 QO, Min rel. Carlos Velloso, Tribunal Pleno, j. 25.03.1992.

em favor do indivíduo – e contra a ação expansiva do arbítrio do Estado – uma esfera de autonomia intangível e indevassável pela atividade persecutória do Poder Público, apta a inibir e a vedar o próprio acesso dos agentes governamentais". É um direito de caráter relativo, que cederia "pela preponderância axiológica e jurídico-social do interesse público". Ao mesmo tempo, a pesquisa da verdade real "sofre os necessários condicionamentos que a ordem jurídica impõe à ação persecutória do Estado". No caso, "sem elementos fundados de suspeita, como a existência concreta de indícios idôneos e reveladores de possível autoria de prática delituosa, não há como autorizar o '*disclosure*' das informações bancárias reservadas". Destacou ainda que a "notoriedade" dos fatos "não dispensa a autoridade" da comprovação. No final, o requerimento foi indeferido por maioria, que registrou que não haveria prejuízo para avaliação de nova representação fundamentada. Ficou vencido o Min. Marco Aurélio que, localizando o sigilo bancário no art. 5º, XII da CF/88, entendia que bastava a existência de uma investigação criminal para que o sigilo de *dados* bancários pudesse ser quebrado e que havia um "anseio da própria sociedade em ver esclarecidos os fatos que reiteradamente vêm sendo noticiados".

O caso é de especial relevância por ser o primeiro que traz questões de sigilo bancário associado a um direito à privacidade, por demonstrar a relevância de *indícios fundados* de possível prática delituosa para restrições da privacidade para fins de investigação criminal e por sinalizar como o mecanismo de controle da legitimidade de restrições à privacidade em matéria penal que ganhará mais destaque é a revisão/autorização judicial, combinada com padrões de justificação/fundamentação da decisão. O relator vê no sigilo bancário um interesse privado vinculado a direitos de personalidade; o Min. Celso de Mello o localiza na esfera privada, a ser protegida de avanços do Estado. Sequer questionam que o direito constitucional à privacidade não cobriria tais informações. Sendo esse ponto incontroverso, a discussão é a que tipo de exigência a interferência no direito processual penal exigiria: uma autorização judicial, mas que estivesse baseada em indícios mais robustos que uma notícia na imprensa. O voto do Min. Marco Aurélio, por sua vez, já é um exemplar de uma abordagem flexibilizadora para casos de grande repercussão, diante do "clamor da sociedade".

Em 1995, o STF ressalvou a exigência de ordem judicial para certos tipos de requisições de informações bancárias. A Corte denegou mandado de segurança impetrado pelo Banco do Brasil contra requisição do Ministério Público Federal de informações sobre beneficiários de empréstimos subsidiados pelo Tesouro Nacional do setor sucroalcooleiro para instrução de

procedimentos administrativos.[59] Em síntese, e acolhendo a tese do MPF, o Tribunal do Pleno do STF, pela maioria apertada de 6 votos a 5, entendeu que operações envolvendo recursos públicos não estão cobertas pela "vida privada" nem por sigilo; nesse caso, a regra seria a da publicidade. Como o MPF teria prerrogativa legal de requisitar tais informações pelo art. 129, VI, VIII da CF/88[60] e pelo art. 8º da LC nº 75/93[61] e se tratava aqui de investigação para defesa do patrimônio público, não haveria necessidade de autorização judicial e os dados deveriam ser entregues.

Após os votos do relator Min. Marco Aurélio, do Min. Celso de Mello, do Min. Maurício Correia, todos eles destacando a longa jurisprudência do STF pela qual a quebra do sigilo bancário dependeria de autorização judicial, o Min. Francisco Rezek abriu a divergência. Para ele o sigilo bancário seria "instituto que protege certo domínio – de resto nada transcendental, mas bastante prosaico – da vida das pessoas e das empresas, contra a curiosidade gratuita, acaso malévola, de outros particulares, e sempre até o exato ponto onde alguma forma de interesse público reclame sua justificada prevalência". Entende que "o inciso X do rol de direitos fala assim numa intimidade

[59] 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. Também Tânia Nigri, *O Sigilo Bancário e a Jurisprudência do Supremo Tribunal Federal* (São Paulo: IASP, 2016), 131–36.

[60] Constituição Federal do Brasil de 1988: "Art. 129. São funções institucionais do Ministério Público": "VI - expedir notificações nos procedimentos administrativos de sua competência, requisitando informações e documentos para instruí-los, na forma da lei complementar respectiva"; "VIII - requisitar diligências investigatórias e a instauração de inquérito policial, indicados os fundamentos jurídicos de suas manifestações processuais;".

[61] Lei Complementar nº 75, de 20 de maio de 1993 (Dispõe sobre a organização, as atribuições e o estatuto do Ministério Público da União): Art. 8º Para o exercício de suas atribuições, o Ministério Público da União poderá, nos procedimentos de sua competência: I - notificar testemunhas e requisitar sua condução coercitiva, no caso de ausência injustificada; II - requisitar informações, exames, perícias e documentos de autoridades da Administração Pública direta ou indireta; III - requisitar da Administração Pública serviços temporários de seus servidores e meios materiais necessários para a realização de atividades específicas; IV - requisitar informações e documentos a entidades privadas; V - realizar inspeções e diligências investigatórias; VI - ter livre acesso a qualquer local público ou privado, respeitadas as normas constitucionais pertinentes à inviolabilidade do domicílio; VII - expedir notificações e intimações necessárias aos procedimentos e inquéritos que instaurar; VIII - ter acesso incondicional a qualquer banco de dados de caráter público ou relativo a serviço de relevância pública; IX - requisitar o auxílio de força policial. § 1º O membro do Ministério Público será civil e criminalmente responsável pelo uso indevido das informações e documentos que requisitar; a ação penal, na hipótese, poderá ser proposta também pelo ofendido, subsidiariamente, na forma da lei processual penal. § 2º Nenhuma autoridade poderá opor ao Ministério Público, sob qualquer pretexto, a exceção de sigilo, sem prejuízo da subsistência do caráter sigiloso da informação, do registro, do dado ou do documento que lhe seja fornecido. § 3º A falta injustificada e o retardamento indevido do cumprimento das requisições do Ministério Público implicarão a responsabilidade de quem lhe der causa. § 4º As correspondências, notificações, requisições e intimações do Ministério Público quando tiverem como destinatário o Presidente da República, o Vice-Presidente da República, membro do Congresso Nacional, Ministro do Supremo Tribunal Federal, Ministro de Estado, Ministro de Tribunal Superior, Ministro do Tribunal de Contas da União ou chefe de missão diplomática de caráter permanente serão encaminhadas e levadas a efeito pelo Procurador-Geral da República ou outro órgão do Ministério Público a quem essa atribuição seja delegada, cabendo às autoridades mencionadas fixar data, hora e local em que puderem ser ouvidas, se for o caso. § 5º As requisições do Ministério Público serão feitas fixando-se prazo razoável de até dez dias úteis para atendimento, prorrogável mediante solicitação justificada.

onde a meu ver seria extraordinário agasalhar a contabilidade, mesmo o das pessoas naturais, e por melhor razão o das empresas". E continua:

> Do inciso XII, por seu turno, é de ciência corrente que ele se refere ao terreno das comunicações: a correspondência comum, as mensagens telegráficas, a comunicação de dados, e a comunicação telefônica. Sobre o disparate que resultaria do entendimento de que, fora do domínio das comunicações em geral – e a seu reboque o cadastro bancário – são invioláveis, não há o que dizer. O funcionamento mesmo do Estado e do setor privado enfrentaria um bloqueio.

Como veremos mais à frente, essa interpretação do inciso XII terá especial repercussão para questões de sigilo telefônico e telemático. E, por isso, vale aqui registrar a digressão do Ministro Rezek sobre por que o Constituinte não teria dado ao

> cadastro bancário proteção igual à das comunicações telefônicas, só devassáveis mediante endosso judiciário à autoridade executiva investigante. Quer parecer-me, desde logo, que a comunicação telefônica cobre nas mais das vezes aquela estrita privacidade pessoal de cuja importância já falara o inciso X do rol das garantias, distinguindo-se nesse ponto da relação contábil entre uma casa bancária e seus clientes.

Isto é: os requisitos para a intervenção em comunicações telefônica seriam mais rigorosos porque essa medida seria mais invasiva à "estrita privacidade pessoal" – o que isso quer dizer e seu escopo não é totalmente claro. De todo modo, como veremos mais à frente, esse raciocínio se perderá – o STF não olhará para o que seria mais invasivo a uma privacidade pessoal que as pessoas possam esperar, apenas ao que é *comunicação.*

Por fim, 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". É o tipo de medida que poderia dar lugar a muitos abusos, por isso a exigência. No caso da quebra de sigilo bancário ordenada 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 se sabe, grande parte das interceptações telefônicas são feitas hoje obrigando-se empresas de telefonia a retransmitir ligações.[62] Nesse aspecto, portanto, há algum tipo de formalização. Não fosse pela consideração sobre invasividade anterior, portanto, até parece que o Ministro poderia admitir interceptações telefônicas sem autorização judicial nos dias de hoje.

Digressão à parte, o voto vencedor ficou a cargo do Min. Néri da Silveira, que endereçou o tema de forma bem mais delimitada ao que estava em discussão, como o fez também o Min.

[62] Miguel Ângelo Duarte Ticom et al., "Histórico, implementação e uso do Sistema Guardião® de interceptação de dados de informática e telemática nas garantias do cidadão", *Cadernos de Segurança Pública* 12 (setembro de 2020).

Octavio Gallotti: "se se trata de operação em que há dinheiro público, a publicidade deve ser nota característica dessa operação. Não há razão, portanto, para o banco não dizer quem são os beneficiados por esses empréstimos. (...) O sigilo bancário não pode englobar esse tipo de informação, em se cuidando da aplicação de recursos públicos". A argumentação repousou sobretudo nos poderes requisitórios do MP e sua conjugação com o princípio da publicidade, em ordem com o art. 37 da Constituição Federal, sem se debruçar com as garantias do art. 5º. O Min. Sepúlveda Pertence, por sua vez, consignou que sigilo bancário não seria garantia que tem status constitucional: não seria coberto pela intimidade, nem pelo "sigilo de dados" que abarcaria apenas comunicação de dados. Muito embora tenha manifestado dúvida sobre a possibilidade de incluir o Banco do Brasil entre as "autoridades" que não poderiam opor sigilo ao acesso a uma informação pelo MP nos termos da lei[63], concluiu que o caso se resolvia pela premissa mais simples de que "em matéria de gestão de dinheiro público, não há sigilo privado".

Além de ser um acórdão em que há delimitação daquilo que compõe o próprio sigilo bancário – concluindo-se pela exclusão de operações com financiamento público – cabe observar como a discussão não versou sobre a fundamentação da requisição. Aqui, a requisição do MPF se baseava em notícia de jornal – algo que no caso Magri não foi suficiente para autorizar a quebra de sigilo. A explicação possível para a distinção, se tentássemos encontrar uma, seria o fato de que no primeiro caso a quebra versava sobre investigação criminal e era mais abrangente (abarcava mais de um ano de extratos bancários sobre duas pessoas específicas), ao passo que aqui instruiria um procedimento administrativo e abrangia pessoas que foram beneficiárias de uma operação com dinheiro público[64] – a única informação revelada seria essa: de que participaram da operação. Nessa linha, o lastro causal para a requisição a bancos sobre gastos públicos poderia ser diferente. Do STF, entretanto, não veio esse esforço de esclarecimento da consistência das decisões nesse aspecto, nos diferentes domínios.

---

[63] Lei Complementar nº 75/1993: Art. 8º, § 2º Nenhuma autoridade poderá opor ao Ministério Público, sob qualquer pretexto, a exceção de sigilo, sem prejuízo da subsistência do caráter sigiloso da informação, do registro, do dado ou do documento que lhe seja fornecido.

[64] Outro ponto que reforçaria essa conclusão é o fato de que em duas oportunidades em 2006 o STF vedou pedidos sobre conjunto indeterminado de clientes e períodos inespecíficos. Cf. Supremo Tribunal Federal, HC 84.758-7 GO, Min. rel. Celso de Mello, Tribunal Pleno, j. 25.05.2006 (concedendo habeas corpus impetrado por funcionários do Banco Itaú que deixaram de atender a ordens judiciais do Tribunal Regional Eleitoral em Goiás por necessidade de identificação dos titulares (CPFs) e do período de interesse). E Supremo Tribunal Federal, Inq 2206 AgR, Min. rel. Joaquim Barbosa, Tribunal Pleno, j. 29.11.2006 (provendo parcialmente agravo regimental contra requisição de listagem genérica de clientes que tivessem certo tipo de conta bancária, por afetar pessoas não relacionadas com a investigação).

(Em outra controvérsia famosa, contexto diferente, e mais recentemente, o STF viria a entender pela constitucionalidade da disponibilização de nomes, vencimentos e vantagens de servidores da Administração Pública em nome da transparência – mostrando também preferência sobre ampla publicidade de gastos públicos em detrimento de interesses de intimidade, vida privada e segurança pessoal.[65] Nesse mesmo espírito, também já recentemente barrou que a prestação de contas de partidos políticos pudesse ser feita sem a individualização dos doadores.[66] Isto é, embora tenha faltado à época, e sobre o diploma do sigilo bancário, há alguma consistência quando visto da perspectiva de gastos públicos. Desrespeitaria, entretanto, o contexto da decisão, se fosse levada para apoiar flexibilizações sobre sigilo bancário de forma geral, quando essas razões não se apliquem.)

Alguns anos depois, a 2ª Turma (liderada por Ministros vencidos pelo julgado anterior) não conheceu de recurso extraordinário interposto pelo MPF em face de acórdão do TRF-5 que concedeu a ordem em habeas corpus impetrado por gerente do BANESPA para trancar ação penal decorrente de negativas de entrega de movimentações bancárias de dois clientes. Entenderam que a solicitação importaria quebra de um "direito inerente à privacidade", o que só caberia a uma "autoridade judiciária com dever de ser imparcial, procedendo com cautela, com prudência e com moderação"[67] decidir, repetindo as palavras do paradigma de 1992. As prerrogativas de requisição do MP não poderiam ser interpretadas de modo a se estender sobre informações protegidas por sigilo bancário. Na 1ª Turma, essa exigência de autorização judicial em regra frente a pedidos do MP acaba também sendo reafirmada em outros julgados de matéria penal – a discussão nesses casos, aliás, é sobre problemas de fundamentação das decisões, que geravam nulidade.[68]

---

[65] Supremo Tribunal Federal, ARE 657.777-SP RG, rel. Min. Teoria Zavascki, Tribunal Pleno, j. 23.04.2015, fazendo ampla referiencia ao acórdão da SS 3902 AgRg-segundo, rel. Min. Ayres Britto, Tribunal Pleno, j. 03.10.2011. Sobre o ponto das informações: "Não cabe, no caso, falar de intimidade ou de vida privada, pois os dados objeto da divulgação em causa dizem respeito a agentes públicos enquanto agentes públicos mesmos; ou, na linguagem da própria Constituição, agentes estatais agindo "nessa qualidade" (§6º do art. 37). E quanto à segurança física ou corporal dos servidores, seja pessoal, seja familiarmente, claro que ela resultará um tanto ou quanto fragilizada com a divulgação nominalizada dos dados em debate, mas é um tipo de risco pessoal e familiar que se atenua com a proibição de se revelar o endereço residencial, o CPF e a CI de cada servidor. No mais, é o preço que se paga pela opção por uma carreira pública no seio de um Estado republicano." Seriam informações de interesse coletivo. Prevalece o princípio da publicidade administrativa, que seria inclusive uma forma de concretizar a República como forma de governo.

[66] Supremo Tribunal Federal, ADI 5.494, rel. Min. Alexandre de Moraes, Tribunal Pleno, j. 22.03.2018. A medida cautelar (indeferida) já havia sido discutida em 11.12.2015, ainda sob relatoria do Min. Teori Zavascki.

[67] Nigri, *O Sigilo Bancário e a Jurisprudência do Supremo Tribunal Federal*, 139. Com referência a Supremo Tribunal Federal, RE 215301/CE, Rel Min. Carlos Velloso, Segunda Turma, j. 13/04/1999, DJ 28/05/1999.

[68] Supremo Tribunal Federal, HC 80724, Rel. Min. Ellen Gracie, Primeira Turma, j. 20.03.2001 e Supremo Tribunal Federal, HC 85455, Rel. Min. Marco Aurélio, Primeira Turma, j. 8.03.2005.

Esse tema foi amplamente debatido no contexto de ordens decretadas por Comissões Parlamentares de Inquérito no início dos 2000 – sem ser exclusividade do sigilo de dados *bancários*, mas abrangendo também dados fiscais e dados (de registros) telefônicos. O *leading case* de diversos mandados de segurança é acórdão da lavra do Min. Celso de Mello no MS 23.452, de 16 de setembro de 1999, que destacava a possibilidade dessa decretação sem reserva judicial, nos termos do art. 58, §3º da CF/88, desde que fundamentada. Em particular, ressalta que as decisões,

> relativamente a pessoas por elas investigadas, devem demonstrar, a partir de meros indícios, a existência concreta de causa provável que legitime a medida excepcional (ruptura da esfera de intimidade de quem se ache sob investigação), justificando a necessidade de sua efetivação no procedimento de ampla investigação dos fatos determinados que deram causa à instauração do inquérito parlamentar[69].

No 23.879-8, de 03 de outubro de 2001, o relator Min. Maurício Correa complementaria que "meras conjecturas não são suficientes para fundamentar a quebra de sigilos, que dizem respeito à intimidade da vida privada das pessoas, prerrogativa protegida pelo art. 5º, X, da Constituição Federal.[70] "Dados, suspeitas e suposições apenas enunciados, sem qualquer base empírica" não são aceitos, disse recuperando termos do relator Min. Sepúlveda Pertence no MS 23.991. Outra vez, observações sobre parâmetros de "suspeita individualizada".

De volta ao campo da fiscalização tributária, a exigência de autorização judicial para acesso da Receita Federal foi afirmada em julgamento apertado (5x4) de um recurso extraordinário de 2010, para depois ser revista em 2016, também apertado, em sede de controle abstrato de constitucionalidade de dispositivos da Lei Complementar nº 105/01[71] que dispensavam a autorização judicial para obtenção informações bancárias pelo Fisco.[72] Na primeira ocasião, em 2010, aqueles que defendiam a possibilidade de acesso direto destacaram a previsão constitucional de que a Receita Federal identifique o patrimônio, rendimentos e atividades econômicas de

[69] Supremo Tribunal Federal, MS 23452, Rel. Min. Celso de Mello, Tribunal Pleno, j. 16.09.1999.
[70] Supremo Tribunal Federal, MS 23.879, Rel. Min. Maurício Correa, Tribunal Pleno, j. 03.10.2001.
[71] Lei Complementar nº 105/01: "Art. 6º As autoridades e os agentes fiscais tributários da União, dos Estados, do Distrito Federal e dos Municípios somente poderão examinar documentos, livros e registros de instituições financeiras, inclusive os referentes a contas de depósitos e aplicações financeiras, quando houver processo administrativo instaurado ou procedimento fiscal em curso e tais exames sejam considerados indispensáveis pela autoridade administrativa competente. Parágrafo único. O resultado dos exames, as informações e os documentos a que se refere este artigo serão conservados em sigilo, observada a legislação tributária."
[72] Supremo Tribunal Federal, RE 389.808/PR, Rel. Min. Marco Aurélio, Tribunal Pleno, j. 15.12.2010 (por maioria apertada, entendendo que a Receita Federal não pode requisitar, no âmbito de fiscalização tributária, sem ordem judicial, o acesso a dados bancários). Supremo Tribunal Federal, RE 601.314-SP, Rel. Min. Edson Fachin, Tribunal Pleno, j. 24.02.2016 (entendendo que o art. 6º da LC 105/2001 não fere a Constituição ao permitir requisição de dados bancários pelo Fisco pois haveria apenas "transferência de sigilo").

contribuintes (art. 145, §1º[73]), "respeitados os direitos e garantias individuais e nos termos da lei", papel que preencheria a LC nº 105/01, permitindo o acesso. No mais, em fundamento vocalizado principalmente pelo Min. Dias Toffoli, sustentavam que não há "quebra de sigilo", mas "transferência de sigilo" – Fisco não poderia dar publicidade às informações a serem recebidas. Como se vê, a racionalidade de julgados da década de 1960 do STF sobre o mesmo tema retornava. A maioria, entretanto, encabeçada pelo voto do rel. Min. Marco Aurélio, entende que o *sigilo de dados* bancários submete-se à guarda do art. 5º, XII, CF/88, a partir do qual a matéria ficaria sob reserva de jurisdição. A Receita, que é parte na relação jurídico-tributária, não poderia ter maior acesso direto, sem intermediação de órgão equidistante como o Judiciário.

No segundo caso, em 2016, a fundamentação para essa possibilidade foi afirmada no voto do Min. Edson Fachin, na lógica de que a norma realizaria a igualdade em relação aos cidadãos, por meio do princípio da capacidade contributiva. Para ele, embora o sigilo bancário esteja protegido pelo art. 5º, X, CF/88 como direito da personalidade "que se traduz em ter suas atividades e informações bancárias livres de ingerências ou ofensas, qualificadas como arbitrárias ou ilegais, de quem quer que seja, inclusive do Estado ou da própria instituição financeira" (p. 33), "essa constatação tem reflexos óbvios na questão da oponibilidade do sigilo bancário contra a Administração Tributária, porquanto limita o exercício do direito subjetivo à privacidade, na medida em que reputa ilegítimo utilizar o figurino do segredo bancário com a finalidade de elidir os tributos devidos por uma pessoa" (p. 34).

Conjuntamente, na ocasião, o STF julgava uma série de ações diretas de inconstitucionalidade contra os dispositivos da LC nº 105, nelas prevalecendo o voto do relator Min. Dias Toffoli na compreensão sobre transferência de sigilo e na observação de que o sistema seria calibrado quanto às informações repassadas em duas etapas:

> O primeiro elemento que evidencia esse conjunto protetivo do cidadão é o sigilo fiscal: conforme já mencionado neste voto, os dados obtidos perante as instituições financeiras são mantidos em sigilo (art. 5º, § 5º, e art. 6º, parágrafo único), tanto que os servidores responsáveis por eventual extravasamento dessas informações devem ser responsabilizados administrativa e criminalmente (arts. 10 e 11).
> Em seguida, pode-se observar o desenvolvimento paulatino da atuação fiscalizatória, que se inicia com meios menos gravosos ao contribuinte: é que a natureza das informações acessadas pelo Fisco na forma do art. 5º da lei complementar é, inicialmente, bastante

[73] Constituição Federal do Brasil de 1988: "Art. 145. A União, os Estados, o Distrito Federal e os Municípios poderão instituir os seguintes tributos: (…) § 1º Sempre que possível, os impostos terão caráter pessoal e serão graduados segundo a capacidade econômica do contribuinte, facultado à administração tributária, especialmente para conferir efetividade a esses objetivos, identificar, respeitados os direitos individuais e nos termos da lei, o patrimônio, os rendimentos e as atividades econômicas do contribuinte."

> restrita, limitando-se, conforme dispõe o seu § 2º, à identificação dos "titulares das operações e dos montantes globais mensalmente movimentados, sendo vedada a inclusão de qualquer elemento que permita identificar sua origem ou a natureza dos gastos a partir deles efetuados" .
> Perceba-se, pois, que, com base nesse dispositivo, a Administração tem acesso apenas a dados genéricos e cadastrais dos correntistas. Essas informações obtidas na forma do art. 5º da LC são cruzadas com os dados fornecidos anualmente pelas próprias pessoas físicas e jurídicas via declaração anual de imposto de renda, de modo que tais informações, do ponto de vista da Administração Tributária, já não são, a rigor, sigilosas.
> Apenas se, no cotejo dessas informações, forem "detectados indícios de falhas, incorreções ou omissões, ou de cometimento de ilícito fiscal, a autoridade interessada poderá requisitar as informações e os documentos de que necessitar, bem como realizar fiscalização ou auditoria para a adequada apuração dos fatos" (§ 4º do art. 5º).[74] (p. 29)

As premissas quanto à proteção garantida pela Constituição ao sigilo bancário não pareciam ser compartilhadas por todos que aderiram aos votos: o Min. Teori Zawaski, por exemplo, assevera sem aprofundar que "O Supremo, por uma maioria representativa, considera que a formatação do chamado sigilo bancário e do sigilo fiscal é eminentemente infraconstitucional" (p. 97). No final, de todo modo, prevaleceu o entendimento aplicado pré-1988, que, como apontei, apela a uma justificativa distributiva suficiente para essa medida estatal de revelação de informações bancárias ao Fisco, que pode alcançar qualquer pessoa indistintamente e em tese vale a todos de forma comum.

Ficaram vencidos os Ministros Marco Aurélio e Celso de Mello. Este último também entendia pela relevância da intermediação judicial: que "provenha de ato emanado de órgão do Poder Judiciário, cuja intervenção moderadora na resolução dos litígios, insista-se, revela-se garantia de respeito tanto ao regime das liberdades fundamentais quanto à supremacia do interesse público." (p. 154). Reafirmava ser "imprescindível a existência de causa provável, vale dizer, de fundada suspeita quanto à ocorrência de fato cuja apuração resulte exigida pelo interesse público" para tanto (p. 149). Nesse contexto,

> A tutela do valor pertinente ao sigilo bancário não significa qualquer restrição ao poder de investigar e/ou de fiscalizar do Estado, eis que o Ministério Público, as corporações policiais e os órgãos incumbidos da Administração Tributária e previdenciária do Poder Público sempre poderão requerer aos juízes e Tribunais que ordenem às instituições financeiras o fornecimento das informações reputadas essenciais à apuração dos fatos. (p. 152)

Em 2019, as transferências de dados de autoridades administrativas como a Receita Federal e o COAF (Conselho de Controle de Atividades Financeiras) para o Ministério Público, para fins

[74] Supremo Tribunal Federal, ADI nº 2859/DF, Rel. Min. Dias Toffoli, Tribunal Pleno, j. 24.02.2016 (vencidos Min. Marco Aurélio e Celso de Mello).

de investigação criminal, ganharam proeminência.[75] A discussão é interessante porque finalmente lida com a colisão de finalidades: se para a Receita Federal haveria justificativa razoável e fundamentação legal para o acesso direto mediante requisição, ao passo que para o Ministério Público era necessária a intervenção judicial, sobretudo para investigação criminal, o que dizer da situação em que a Receita Federal repassa informações bancárias (e, agora, *fiscais*) ao MP?

Embora o STF tenha reafirmado um direito à privacidade sobre informações bancárias, restou dispensada a autorização judicial prévia, desde que realizada na forma prevista em legislação – que reservaria tais transferências aos materiais relativos a representações fiscais para fins penais elaboradas pelo Fisco (art. 198, Código Tributário Nacional[76]). Expandindo e antecipando discussões em meio ao calor político da ocasião, também já definiu que relatórios de inteligência sobre operações suspeitas elaborados pelo COAF podem ser repassados sem autorização judicial prévia (art. 15 da Lei nº 9.613/98[77]) quando presentes indícios de ilícitos. Para fins de tese de repercussão geral, fica definido que deve ser resguardado o "sigilo das informações em procedimentos formalmente instaurados e sujeitos a posterior controle jurisdicional". Podem ser feitos "unicamente por meio de comunicações formais, com garantia de sigilo, certificação do destinatário e estabelecimento de instrumentos efetivos de apuração e correção de eventuais desvios".

Isto é, a Corte concluiu que o encaminhamento para o Ministério Público não necessitaria de uma *autorização judicial* por se tratar de "transferência de sigilo" e não "quebra de sigilo" e porque o mecanismo está previsto em lei. Assim, o STF salientou a existência de certos elementos procedimentais balizadores e reafirmou parâmetros formais e materiais previstos na lei específica

[75] Supremo Tribunal Federal, RE 1.055.941/SP, Rel. Min. Dias Toffoli, Tribunal Pleno, j. 04.12.2019.

[76] Lei nº 5.172/66 (Código Tributário Nacional): "Art. 198. Sem prejuízo do disposto na legislação criminal, é vedada a divulgação, por parte da Fazenda Pública ou de seus servidores, de informação obtida em razão do ofício sobre a situação econômica ou financeira do sujeito passivo ou de terceiros e sobre a natureza e o estado de seus negócios ou atividades. § 1o Excetuam-se do disposto neste artigo, além dos casos previstos no art. 199, os seguintes: I – requisição de autoridade judiciária no interesse da justiça; II – solicitações de autoridade administrativa no interesse da Administração Pública, desde que seja comprovada a instauração regular de processo administrativo, no órgão ou na entidade respectiva, com o objetivo de investigar o sujeito passivo a que se refere a informação, por prática de infração administrativa. § 2o O intercâmbio de informação sigilosa, no âmbito da Administração Pública, será realizado mediante processo regularmente instaurado, e a entrega será feita pessoalmente à autoridade solicitante, mediante recibo, que formalize a transferência e assegure a preservação do sigilo. § 3o Não é vedada a divulgação de informações relativas a: I – representações fiscais para fins penais; II – inscrições na Dívida Ativa da Fazenda Pública; III – parcelamento ou moratória."

[77] Lei nº 9.613/18: "Art. 15. O COAF comunicará às autoridades competentes para a instauração dos procedimentos cabíveis, quando concluir pela existência de crimes previstos nesta Lei, de fundados indícios de sua prática, ou de qualquer outro ilícito."

que tange tais transferências de dados. Ainda que tenha dispensado ordem judicial, não é possível dizer que dispensou também que repasses ao MP, que possuem repercussões penais, não devam estar vinculadas a *suspeitas* e *indícios* contra pessoas específicas. Não se ocupou em registrar na tese de repercussão qualquer observação sobre esse aspecto, embora do julgado se extraia que não podem ocorrer genericamente.

À luz do que foi visto na primeira parte da tese, é possível fazer três observações: (i) não faz sentido falar em transferência de sigilo para legitimar transferências entre órgãos públicos com competências distintas – não é qualquer tipo de transferência que é autorizada, as finalidades/competências/justificativas importam, e não se dribla implicações a direitos à privacidade pela manutenção de sigilo (pela não-divulgação). Se essa fosse uma razão para autorizar qualquer medida estatal que implique a privacidade, seria possível haver amplo fluxo de dados entre entidades estatais, desde que tudo fosse mantido em segredo. Não é assim e não deve ser assim.

Por outro lado, (ii) um modelo procedimental bem desenhado, previsto em lei poderia, em certas ocasiões, ser capaz de oferecer salvaguardas contra arbitrariedades equivalentes ao que usualmente se associa ao crivo judicial – no caso, o arranjo de supervisão do sistema financeiro segmentado em etapas, atores e critérios de fluxo supostamente possuiria salvaguardas equivalentes que atenderiam exigências para sua fundamentação, considerando o ambiente opaco do sistema financeiro. Ocorre que (iii) o apelo dos recorrentes à tese de exigência de "ordem judicial" prévia ao compartilhamento parece se reportar a outro incômodo mais fundamental, de princípio: a uma possível inexistência de suspeita *individualizada* ou a uma seletividade arbitrária sobre quem é objeto de *detecção* de atividades ilícitas. Faltariam mecanismos claros e justos que fossem hábeis a justificar porque *essa pessoa* e não outra está sendo alvo da investigação pelo MP a partir de informações do COAF.

Como este não é um trabalho sobre o COAF e as críticas a como funciona ultrapassam a realidade do que é previsto texto da lei, vou parar por aqui, mas a observação é relevante se quisermos que a jurisprudência do STF seja revista e amadureça frente ao avanço tecnológico movido a *big data* de forma íntegra e consistente. Discussões relevantes ficam para trás quando só se concentra na discussão binária se precisa de ordem judicial e princípios relevantes ao processo penal (como suspeita individualizada), deixam de ser reafirmados.

3 Inviolabilidade do domicílio

O mais antigo acórdão que lida com inviolabilidade do domicílio como garantia em matéria penal localizado no repositório eletrônico do STF durante a pesquisa é de 1960.[78] O relatório não dá detalhes e o voto é curto. Tratava-se de RHC impetrado em favor de pessoa presa em flagrante "por prática de curandeirismo, na sua Tenda de Umbanda", a seguir liberada provisoriamente mediante fiança.[79] Alegando que "a autoridade policial está ameaçando o livre exercício de culto na referida Tenda ou Terreiro, e a incolumidade do seu domicílio, em contrastes com o art. 141, §§7º e 15º", da Constituição de 1946[80], impetrou habeas corpus preventivo, negado nas instâncias inferiores. O relator Min. Nelson Hungria vota pela denegação da ordem: "O que a autoridade policial está tentando fazer é impedir a prática de curandeirismo na Tenda de Umbanda dirigida pelo recorrente, tendo ali surpreendido agentes do curandeirismo em plena atuação. Nenhum crime pode acobertar-se sob a capa de culto religioso ou de inviolabilidade do domicílio". O julgamento foi unânime.

Em 1971, essa racionalidade volta a ser indiretamente afirmada, em prisão em flagrante de praticantes de jogo do bicho.[81] Em 1977, também:

> a casa é asilo inviolável do indivíduo sem dúvida, porém não pode ser transformada em garantia de impunidade de crimes que em seu interior se praticam (...). Em se tratando de flagrante delito, não é necessário mandado de busca e apreensão domiciliar, pois o próprio texto constitucional admite que se penetre na casa, mesmo à noite, e sem consentimento do morador, em caso de crime e desastre (...). 'Não verificadas as exceções admitidas no texto

[78] Também localizei o RE 22255, Rel. Min. Afrânio Costa, Segunda Turma, j. 24.04.1953, que considera que quem ingressa clandestinamente em escritório de fábrica, depois de encerrado o expediente e encerrado o acesso ao público, também incorre no crime de violação a domicílio. Como a inviolabilidade, nesse caso, é suscitada pela vítima do crime, não pelo autor/investigado, tomei o próximo como marco.

[79] Supremo Tribunal Federal, RHC 38039, Rel. Min. Nelson Hungria, Tribunal Pleno, j. 12.10.1960.

[80] Constituição dos Estados Unidos do Brasil de 18 de setembro de 1946. Art 141 - A Constituição assegura aos brasileiros e aos estrangeiros residentes no País a inviolabilidade dos direitos concernentes à vida, à liberdade, a segurança individual e à propriedade, nos termos seguintes: § 7º - É inviolável a liberdade de consciência e de crença e assegurado o livre exercício dos cultos religiosos, salvo o dos que contrariem a ordem pública ou os bons costumes. As associações religiosas adquirirão personalidade jurídica na forma da lei civil. § 15 - A casa é o asilo inviolável do indivíduo. Ninguém, poderá nela penetrar à noite, sem consentimento do morador, a não ser para acudir a vitimas de crime ou desastre, nem durante o dia, fora dos casos e pela forma que a lei estabelecer.

[81] Suprema Tribunal Federal, HC 48934, Rel. Min. Raphael de Barros Monteiro, Primeira Turma, j. 19.11.1971. "Indiretamente" porque naquela ocasião a discussão se centrou mais em se uma *contravenção* se incluía entre os flagrantes possíveis de excepcionar a garantia de inviolabilidade prevista na Emenda Constitucional n. 1 de 1969. Por ela: Art 153 - A Constituição assegura aos brasileiros e aos estrangeiros residentes no Pais a inviolabilidade dos direitos concernentes à vida, à liberdade, à segurança e à propriedade, nos termos seguintes: § 10 - A casa é o asilo inviolável. do indivíduo; ninguém pode penetrar nela, à noite, sem consentimento do morador, a não ser em caso de crime ou desastre, nem durante o dia, fora dos casos e na forma que a lei estabelecer.

> constitucional, responderão os agentes da autoridade pelos erros ou abusos que tenham praticado'.[82]

Sob a égide da Constituição Federal de 1988, a conclusão não mudaria. O primeiro acórdão de relevância encontrado sobre esse tema é o HC 70.909, de 1994.[83] Nele, a 2ª Turma do STF denegou habeas corpus em que se sustentava ilicitude da prova pelo ingresso em domicílio sem mandado judicial. Acolhendo parecer do MP, e a partir da observação de que foi encontrado entorpecente na casa, a Corte entendeu que havia um fundamento independente para justificar a medida: a flagrância de crime permanente, nos termos do art. 303 do CPP[84]. A 1ª Turma manteria o mesmo entendimento no HC 74.963, apreciado em 25 de março de 1997, também sobre tráfico de entorpecentes.[85] No mês seguinte a 2ª Turma voltou a chegar à mesma conclusão, dessa vez no contexto do crime de quadrilha.[86]

Os acórdãos não oferecem qualquer balizamento sobre quais condições prévias ao ingresso deveriam estar presentes – como uma suspeita, minimamente. No último caso, é feita menção a "diligências no local" que policiais teriam feito até se convencerem da ocorrência de crime. Nos demais, o destaque é ao resultado do que foi encontrado no ingresso (droga apreendida), que comprovaria a prática delituosa em flagrante. Se confirmado, dispensam-se maiores explicações. Esse elemento foi a novidade no julgamento paradigmático do RE 603.616 duas décadas depois – em 2015. O rel. Min. Gilmar Mendes assim sintetizou o paradoxo que a interpretação ensejava:

> Considerado o entendimento atual, o policial ingressará na casa sem a certeza de que a situação de flagrante delito, de fato, ocorre. Se concretizar a prisão, poderá dar seu dever por cumprido. Em caso contrário, terá, ao menos em tese, incorrido no crime de violação de domicílio, majorado pela sua qualidade de funcionário público, agindo fora dos casos legais – art. 150, §2º, do CP.
> Ou seja, o policial estaria assumindo o risco de perpetrar um crime, salvo se tiver sucesso em sua diligência. Isso dá ao policial um perigoso incentivo. Ou desvenda o crime, ou responde pessoal e criminalmente pela violação de domicílio.
> Caso o policial não encontre a droga e venha a ser acusado criminalmente, transferir-se-á a escolha dramática para a fase de punição do agente público. A tese defensiva natural será o estrito cumprimento do dever legal putativo – o policial alegará que achava que havia um crime em andamento dentro da casa invadida.
> Se rejeitar a defesa, o julgador pune um policial que acreditava estar cumprindo seu dever.

[82] Supremo Tribunal Federal, RE 86926 PR, Min. rel. Cordeiro Guerra, Segunda Turma, j. 21.10.1977.
[83] Supremo Tribunal Federal, HC 70909, Min. rel. Paulo Brossard, Segunda Turma, j. 11.10.1994.
[84] Código de Processo Penal (Decreto-lei nº 3.689, de 3 de outubro de 1941): "Art. 303. Nas infrações permanentes, entende-se o agente em flagrante delito enquanto não cessar a permanência."
[85] Supremo Tribunal Federal, HC 74963, Min. rel. Ilmar Galvão, Primeira Turma, j. 25.03.1997.
[86] Supremo Tribunal Federal, HC 74127-4 RJ, Min. rel. Carlos Velloso, Segunda Turma, j. 15.04.1997.

> Se a acolher, aniquila a garantia da inviolabilidade do domicílio. Qualquer alegação por parte de policiais de que tinham informação de que havia um crime em andamento afastaria a inviolabilidade domiciliar.[87]

Nesse contexto, propõe que as buscas sejam avaliadas pelo que se sabia antes da diligência, não depois. Para ilustrar, diz, como antecipei na primeira parte: "Imagine-se, por exemplo, que a polícia selecionasse casas por sorteio e, nas escolhidas, realizasse busca e apreensão, independentemente de qualquer informação sobre seus moradores. Certamente, seriam flagrados crimes em algumas delas. O resultado positivo das buscas, no entanto, não justificaria sua realização. O fundamental é que o critério para a decisão de realizar a entrada forçada foi arbitrário". Nesse contexto, o flagrante é, nos termos do voto do relator,

> exceção à exigência de prévia ordem escrita da autoridade judiciária para a prisão, fundada na urgência em fazer cessar a prática de crime e na evidência de sua autoria. No entanto, é indispensável o controle da medida a posteriori, mediante imediata comunicação ao juiz, que analisa a legalidade da prisão em flagrante – art. 5º, LXII, da CF. (…) O modelo probatório é o mesmo da busca e apreensão domiciliar – fundadas razões, art. 240, §1º, do CPP. Trata-se de exigência modesta, compatível com a fase de obtenção de provas.

Comentando o julgado, Gisela Wanderley observa que a distinção traçada pelo acórdão de que os julgados até ali tratados se validavam pelo resultado, não pelos fundamentos, nunca foi uma doutrina explicitamente enunciada. Na prática, o que se via era uma admissão da "mera intuição ou suspeita genérica da prática de crime permanente como motivação suficiente para a prática da busca e, assim, não fornece critérios e parâmetros que delimitem a validade da motivação da busca."[88] Nesse contexto, haveria uma "validação virtualmente automática das buscas nos casos de crimes permanentes". Com respeito a que critérios e parâmetros concretos seriam esses, aliás, o STF não teria dado muita direção no julgado histórico. Assim, muito embora tenha dado passos importantes quanto ao que poderia fundamentar o ingresso excepcional sem ordem judicial, os

[87] Supremo Tribunal Federal, RE 603616, Min. rel. Gilmar Mendes, Tribunal Pleno, j. 05.11.2015.
[88] Gisela Aguiar Wanderley, "Comentário ao STF - RE 603.616/RO: Busca domiciliar sem mandado judicial em situação de flagrante de crime permanente", *Revista dos Tribunais* 966 (2016): 337–59.

requisitos firmados ainda seriam frouxos e, superficialmente, apenas reafirmaram exigência que o CPP (art. 240, §1º)[89] já prevê.[90]

Para ser justa, o relator chegou a dizer que "provas ilícitas, informações de inteligência policial – denúncias anônimas, afirmações de "informantes policiais" (pessoas ligadas ao crime que repassam informações aos policiais, mediante compromisso de não serem identificadas), por exemplo – e, em geral, elementos que não têm força probatória em juízo não servem para demonstrar a justa causa" (p. 23). Essa é uma observação que oferece um parâmetro sobre o que não atenderia a noção normativa de suspeita individualizada que esperamos ser atendida para que se fale em uma situação excepcional em que o poder público está autorizado a ingressar em lares, mesmo contra a vontade de seus donos. Mas, como na crítica de Gisela Wanderley, ainda é uma observação tímida que inclusive não dialoga com a suspeita *qualificada* que o CPP exige – enquanto um parâmetro fixado de proteção contra invasões arbitrárias que comporta certo nível de risco que assumimos de termos o direito violado indevidamente. Na melhor leitura, no máximo, apenas reafirma o que o CPP já prescreve, no sentido de que a suspeita deve ter base em fatos e circunstâncias prévias.

De fato, nessa observação, é sintomático que o único voto divergente no caso – do Min. Marco Aurélio – discordava da conclusão do relator de que, no caso concreto, haveria sim justa causa para o ingresso em domicílio sem autorização judicial prévia. Muito embora tenha destacado diligências prévias que apontassem para envolvimento do recorrente em tráfico de drogas, o relator não teria oferecido qualquer razão que justificasse *urgência* no ingresso em domicílio sem autorização judicial prévia após a prisão de comparsa com carga de drogas – a partir desses

[89] Código de Processo Penal (Decreto-lei nº 3.689, de 3 de outubro de 1941): "Art. 240. A busca será domiciliar ou pessoal. § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para: a) prender criminosos; b) apreender coisas achadas ou obtidas por meios criminosos; c) apreender instrumentos de falsificação ou de contrafação e objetos falsificados ou contrafeitos; d) apreender armas e munições, instrumentos utilizados na prática de crime ou destinados a fim delituoso; e) descobrir objetos necessários à prova de infração ou à defesa do réu; f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato; g) apreender pessoas vítimas de crimes; h) colher qualquer elemento de convicção. § 2º Proceder-se-á à busca pessoal quando houver fundada suspeita de que alguém oculte consigo arma proibida ou objetos mencionados nas letras *b* a *f* e letra *h* do parágrafo anterior."

[90] Para além do contexto de buscas domiciliares, Wanderley tem uma produção acadêmica relevante sobre como o padrão de justificação qualificado do CPP (vinculado a certo objeto) para buscas pessoais é comumente interpretado de forma aberta e ampla. Essa constatação será retomada adiante, mas a sinalizo aqui pelo fato curioso de que o voto fala genericamente em "fundadas razões", sem incluir os itens elencados no CPP que precisam predicar tais razões. Cf. Wanderley, "Entre a lei processual e a praxe policial"; Wanderley, "A busca pessoal no direito brasileiro: medida processual probatória ou medida de polícia preventiva?"

mesmos indícios.[91] Pelo contrário, em certo momento parece pressupor que será sempre esse o caso para certos tipos de crime[92]. O Min. Fachin, ao votar com o relator, também apenas reverbera o entendimento que supostamente estava sendo superado: assenta que a autoridade policial precisa de "fundadas razões para o flagrante, que, na hipótese do caso concreto, o ter em depósito, na condição de crime permanente, funda o flagrante que justifica a afirmação da tese." Mesmo o Min. Celso de Mello, notável defensor da "causa provável" em seus votos, pontuou: "Vê-se, portanto, que o agente em questão foi surpreendido na prática de crime permanente, o que tornou legítimo o ingresso forçado, em seu domicílio, da Polícia, eis que, naquele momento, o delinquente estava cometendo uma infração penal." Atualmente, quem se debruça com requisitos e delineamento de critérios do que constituem as fundadas razões é sobretudo o STJ[93] – casos mais recentes, que poderiam suscitar questões concretas do balizamento, vêm sendo sistematicamente barrados em critérios de admissibilidade pelo STF (Súmula nº 279).

Para além das discussões sobre os critérios de justificação do ingresso em domicílio, há também casos que versam sobre o escopo dessa garantia à luz do próprio conceito de domicílio. O STF já foi provocado várias vezes a se manifestar acerca dos espaços que estariam englobados por essa proteção. Em decisões de 2005, 2008 e 2012, a 2ª Turma considerou que a apreensão de livros contábeis e documentos fiscais em escritório de contabilidade por agentes fazendários e policiais federais sem mandado judicial seria ilegal. O escritório seria um espaço privado, não aberto ao público, que seria alcançado pelo conceito de "casa" e por isso seria protegido.[94] Em 2007, também considerou que quarto de hotel ainda ocupado seria protegido pelo dispositivo constitucional, de

[91] No caso, a conclusão do relator foi a de que havia fundadas razões para se suspeitar da situação de flagrante delito: comparsa foi preso com caminhão carregado de drogas, que saíra da casa do recorrente.

[92] Voto do Min. Gilmar Mendes: "Nós estamos aqui a fazer um exercício, tendo em vista essas várias situações, tudo nos crimes permanentes, como esse caso de depósito de drogas, ou porte de drogas, ou extorsão mediante sequestro, cárcere privado. Então, todas essas situações exigem uma ação imediata da Polícia. Aqui nós estamos falando exatamente da possibilidade de um necessário controle a posteriori que vai permitir, então, fazer essa aferição para evitar exatamente os abusos que se perpetram sistematicamente." Supremo Tribunal Federal, RE 603616, Rel. Min. Gilmar Mendes, Tribunal Pleno, j. 05.11.2015.

[93] Ver Daniel Nicory do Prado, "Prisão em flagrante em domicílio: um olhar empírico", *Revista Direito GV* 16, nº 2 (2020): e1962, https://doi.org/10.1590/2317-6172201962. Sintomaticamente, em março de 2021, a 6ª Turma do STJ firmou precedente pela exigência de fundadas razões ("aferidas de modo objetivo e devidamente justificadas, de maneira a indicar que dentro da casa ocorre situação de flagrante delito"), e a preferência da autorização judicial prévia inclusive para casos de crime permanente exceto em casos de urgência em que prova do crime pode se perder, além de estabelecer condições claras para a validade de consentimento de moradores. Ver Superior Tribunal de Justiça, HC 598.051-SP, Rel. Min. Rogério Schietti Cruz, Sexta Turma, j. 02.03.2021, DJE 15.03.2021.

[94] Supremo Tribunal Federal, HC 103325, Rel. Min. Celso de Mello, Segunda Turma, j. 03.04.2012; Supremo Tribunal Federal, HC 93050, Rel. Min. Celso de Mello, Segunda Turma, j. 10.06.2008; Supremo Tribunal Federal, HC 82788, Rel. Min. Celso de Mello, Segunda Turma, j. 12.04.2005.

forma que apenas poderia ocorrer busca e apreensão de materiais e equipamentos por autoridades policiais mediante mandado judicial.[95] Isto é, são espaços protegidos por direito à privacidade e, não sendo o caso de emergência, desastre ou consentimento, só podem ser ingressados por agentes do Estado mediante mandado judicial.

Para fiscalização tributária, a lógica vista para sigilo bancário não encontra eco aqui. Para buscar documentos em domicílios que sirvam à fiscalização tributária, o STF entende que é necessária a autorização judicial prévia, à luz da Constituição Federal, não sendo o caso de nenhuma exceção. O *leading case* da fase pós-1988 é o HC 79.512, de 1999.[96] Nele, o MPF "provocou" – nos termos do relatório – a Receita Federal a fazer uma fiscalização na empresa Cavalo Marinho Ltda. O contato resultou na apreensão de 7 caixas de documentos no escritório da empresa por agentes fiscais e repasse das informações ao MP, que a seguir ainda também solicitou judicialmente quebra de sigilo bancário e deu origem a processo penal. O relator Min. Sepúlveda Pertence sustentou que a legislação infraconstitucional que autoriza agentes do Fisco a fazer apreensão de documentos, prévia à Constituição Federal de 1988, não poderia ser lida de forma a autorizar o ingresso forçado em domicílio, inclusive. Seria preciso autorização judicial ou uma das outras exceções (flagrante, socorro ou desastre).

Entretanto, o ministro estabelece uma espécie de presunção de consentimento que poderia validar o ocorrido. Registra que "é um dado elementar da incidência da garantia constitucional do domicílio o não consentimento do morador ao questionado ingresso de terceiro". Como nos autos não havia prova de que se deu sem consentimento e nem se trataria de um caso "das famigeradas batidas policiais no domicílio de indefesos favelados" que pudesse indicar "*metus publicae potestati*"[97], não teria existido ilegalidade. Há discussão levantada pelo Min. Marco Aurélio de que, tivesse sido seguido o procedimento legal, o contribuinte teria sido primeiro intimado a exibir os livros e não seria dessa maneira, mas sai vencido. Ademais, e embora o elevado volume de informações, característico de devassa, tenha sido pontuado, não se torna um problema no posicionamento final do Tribunal. O entendimento volta a ser aplicado em dois casos do ministro

[95] Supremo Tribunal Federal, RHC 90376, Rel. Min. Celso de Mello, Segunda Turma, j. 03.04.2007.
[96] Supremo Tribunal Federal, HC 79512, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, j. 16.12.1999.
[97] Brocardo que se refere ao temor do particular sobre autoridade pública em face de sua posição de autoridade.

na Primeira Turma em 2004, em ambos para outra vez concluir que não houve demonstração de que não houve consentimento/ não seria possível revisar tal matéria factual.[98]

Já em 2005, 2008 e 2012, o Min. Celso de Mello é relator de três habeas corpus relacionados (já referidos quando falei sobre o que se considera *domicílio*) na Segunda Turma.[99] Muito embora sustente a mesma conclusão quanto aos limites das prerrogativas da administração tributária e faça menção da possibilidade de consentimento, a exigência de *demonstração* de que não existiu aceitação não tem qualquer destaque. Isto é: ao contrário dos primeiros julgados, não há uma presunção de consentimento em operação. Ademais, o voto trata agentes públicos indistintamente: tais limites seriam iguais tanto em matéria de fiscalização tributária como no campo processual penal. Em 2014, a Primeira Turma, em caso relatado pelo Min. Dias Toffoli, nega seguimento a recurso extraordinário sobre a mesma matéria voltando a dar ênfase na necessidade de demonstração de ausência de consentimento.[100]

À luz do que foi visto sobre fundamentação de ações do Estado, prestação de contas e necessidade de fixação de um parâmetro de risco que aceitamos incorrer de sofrer dano moral, não faz sentido algum que a demonstração de *ausência de consentimento* seja ônus do acusado, nem que, na ausência de uma lei que fixe esse ônus da prova, a possível exceção constitucional à inviolabilidade do domicílio – que não está em seu texto, mas é inerente à razão de ser desse direito – seja interpretada de tal modo.

4 Sigilo de papeis: documentos e correspondência

Que tipo de proteção é conferida a *papeis* de alguém*,* sejam eles documentos relativos à própria pessoa, a uma empresa, a um diário pessoal ou cartas trocadas com interlocutores*?* Em 1963, sob a Constituição Federal de 1946, que já garantia ser "inviolável o sigilo da correspondência" (art. 141, § 6º), o STF negou provimento a recurso em mandado de segurança impetrado em face de intimação de procuradores da Fazenda para que empresa exibisse "papeis

[98] Supremo Tribunal Federal, RE 331303 AgR, Rel. Min. Sepúlveda Pertence, Primeira Turma, j. 10.02.2004 e Supremo Tribunal Federal, RE 230020, Rel. Min. Sepúlveda Pertence, Primeira Turma, j. 06.04.2004.
[99] Supremo Tribunal Federal, HC 103325, Rel. Min. Celso de Mello, Segunda Turma, j. 03.04.2012; Supremo Tribunal Federal, HC 93050, Rel. Min. Celso de Mello, Segunda Turma, j. 10.06.2008; Supremo Tribunal Federal, HC 82788, Rel. Min. Celso de Mello, Segunda Turma, j. 12.04.2005.
[100] Supremo Tribunal Federal, RE 767180 AgR, Rel. Min. Dias Toffoli, Primeira Turma, j. 19.08.2014.

existentes em seus arquivos sobre seus negócios comerciais" com outras três empresas.[101] O acórdão entendeu que a então vigente Lei do Sêlo previa que contratos realizados por meio de correspondência não ficam isentos de selo e o art. 58[102] dela autorizaria fiscalização. Dialogando com a garantia constitucional, o voto condutor entendeu que "A inviolabilidade da correspondência assegurada na Constituição não envolve, evidentemente, a correspondência comercial, para efeitos de fiscalização, quando a carta já chegou ao destinatário." Como concluiu o relator: "O comerciante tem indiscutível direito a que sua correspondência trafegue pelas repartições postais sem ser violada, mas, uma vez incorporada sua correspondência aos arquivos comerciais, fica ela sujeita à verificação dos agentes fiscais do estado."[103]

O caso anterior não trata de sigilo que sirva a uma privacidade *pessoal.* Como se vê, protege o negócio de empresas – o "sigilo comercial". Curiosamente, essa temática compõe todos os casos identificados pré-1988 sobre *documentos* e *cartas* em geral e, como o caso apresentado, tratam de contexto cível ou administrativo – não penal. O precedente mencionado é relevante porque até hoje o STF entende que o inciso XII do art. 5º protege o *fluxo de comunicações*, não os objetos da comunicação em si. Essa é, de fato, como visto, uma interpretação que ecoa historicamente de uma preocupação com a integridade de sistemas de comunicações: uma vez que um objeto *comunicado* a alguém é compartilhado com um *condutor* para ser dirigido ao seu destinatário, é necessário que seja garantido que essa condução ocorra de forma segura, sem interferências de terceiros. Isso não impediria, entretanto, que tais objetos fossem apreendidos ou analisados junto ao remetente ou destinatário.

Essa compreensão do STF não era descolada de uma preocupação com o alcance dessa busca e apreensão sobre o que já não estivesse *em fluxo,* mas diretamente na posse de detentor de direito. Para o sigilo comercial, em casos cíveis, ao mesmo tempo em que já se reverberava que não é "muralha chineza, cortina de ferro, para acobertar apontadas lesões praticadas por comerciantes contra terceiros"[104], a jurisprudência do STF destacava uma vinculação à finalidade e à necessidade para buscas e apreensões de documentos: um perito contratado para apurar cheques

[101] Supremo Tribunal Federal, RMS 11274-PE, Rel. Min. Evandro Lins Silva, Tribunal Pleno, j. 27.11.1963.
[102] Decreto-Lei nº 4.655/1942: "Art. 58. Os estabelecimentos comerciais e industriais, as sociedades civis que revestirem forma comercial, os serventuários de ofício e todos os que são obrigados a manter escrituração não poderão excusar-se, sob pretexto algum, de exibir aos encarregados da fiscalização do selo os papéis e livros de sua escrituração e arquivo."
[103] Supremo Tribunal Federal, RMS 11274-PE, Rel. Min. Evandro Lins Silva, Tribunal Pleno, j. 27.11.1963.
[104] Supremo Tribunal Federal, RE 22175-MG, Rel Min. conv. Afrânio Costa, Segunda Turma, j. 9.01.1953.

fraudulentos não poderia se estender a outras documentações que comprometessem sigilo comercial. Para fiscalização trabalhista, por sua vez, o STF já entendia que "a lei autoriza o Ministério do Trabalho [o Instituto de Aposentadorias e Pensões dos Industriários] a fazer essa verificação que se deve restringir à matéria específica, ou seja, o interesse de verificar a escrituração comercial relativa aos compromissos da firma dos empregados, em face dos interesses do empregador."[105] Se ocorrer necessidade de ir além, precisa requerer a juiz "fazendo demonstração, evidentemente, dessa necessidade"[106]. A justiça determinaria a extensão desse exame, caso houvesse controvérsia.

Saltando para a Constituição atual, o primeiro caso identificado e de expressão – propriamente sobre sigilo de correspondência e arquivos *pessoais* – foi o HC 70814, em 1994.[107] O objeto da impetração foi uma sentença condenatória que teria se apoiado em carta obtida de forma criminosa. Além de entender que a tal carta não era a única prova nos autos que sustentava a condenação, o relator Min. Celso de Mello votou entendendo que, de fato, o CPP veda a utilização em juízo de cartas particulares obtidas por meios criminosos (art. 233[108]), mas que a tal carta não foi obtida de forma criminosa. Ela foi enviada pelo paciente, enquanto preso, a outro preso em regime aberto. Invocando o art. 41, parágrafo único, da Lei de Execução Penal[109], fundamenta que há permissão excepcional para o acesso a cartas, "eis que a cláusula tutelar da inviolabilidade do sigilo epistolar não pode constituir instrumento de salvaguardas de práticas ilícitas". Cita Julio Fabbrini Mirabete nesse sentido, em trecho que destaca ocasiões em que essa restrição poderia ocorrer (estão na lista do autor a suspeita de prática de infração penal, o envio de objetos proibidos, dúvidas quanto à identidade de remetente e destinatário, a segurança de presídios). Muito embora as circunstâncias sugiram que houve intromissão de terceiro no próprio *fluxo* de cartas, o que em tese seria contraditório com a leitura recorrente dada ao art. 5º, XII, o ponto não é problematizado. Isto é, muito embora a linguagem de muitas decisões atribua um senso

[105] Supremo Tribunal Federal, RE 27596 EI, Rel. Min. Barros Barreto, Tribunal Pleno, j. 17.10.1958.
[106] Supremo Tribunal Federal, RE 27596 EI, Rel. Min. Barros Barreto, Tribunal Pleno, j. 17.10.1958.
[107] Supremo Tribunal Federal, HC 70814, Rel. Min. Celso de Mello, Primeira Turma, j. 01.03.1994.
[108] Código de Processo Penal (Decreto-lei nº 3.689, de 3 de outubro de 1941): "Art. 233. As cartas particulares, interceptadas ou obtidas por meios criminosos, não serão admitidas em juízo. Parágrafo único. As cartas poderão ser exibidas em juízo pelo respectivo destinatário, para a defesa de seu direito, ainda que não haja consentimento do signatário."
[109] Lei de Execuções Penais (Lei nº 7.210/1984): "Art. 41 - Constituem direitos do preso: XV - contato com o mundo exterior por meio de correspondência escrita, da leitura e de outros meios de informação que não comprometam a moral e os bons costumes. Parágrafo único. Os direitos previstos nos incisos V, X e XV poderão ser suspensos ou restringidos mediante ato motivado do diretor do estabelecimento".

quase até de uma proteção absoluta ao que está em fluxo, em contraste com o que está "armazenado", esse sequer é o ponto aqui – pela previsão legal de permissão administrativa-penitenciária, entende-se que a prova era lícita.

Mais recentemente, discussão semelhante voltou à Suprema Corte. O STF teve de decidir se prova obtida por meio de abertura de pacote postado nos Correios viola o sigilo de correspondência. Note-se que historicamente a preocupação constitui justamente interferências de terceiros no fluxo – explicitamente os próprios Correios. Nesse caso, colocava-se uma discussão anterior sobre a proteção do pacote: seria equivalente a cartas? Ao contrário do que fez na ADPF 46 sobre o escopo do monopólio dos Correios, aqui o STF não diferenciaria correspondência pessoal de encomendas. Entendeu que estas também são protegidas. O relator, Min. Marco Aurélio, entendia que o sigilo de comunicações protege comunicações entre pessoas, independentemente do meio pelo qual ocorre (se carta ou pacote). Havendo suspeita, caberia ter buscado autorização judicial para intervir.

A maioria, no entanto, e para fins de tese fixada, aderiu ao voto-vogal do Min. Fachin, pelo qual, não havendo autorização judicial, nem existindo hipótese legal em que se insira esse tipo de acesso na legislação que trata de serviços postais, houve violação do sigilo de correspondência.[110] O Min. Alexandre de Moraes restou vencido: para ele, seria possível o acesso sem autorização judicial prévia quando verificados fundados indícios da prática de atividades ilícitas. Como se vê, e ao contrário da retórica já encontrada em acórdãos, o STF reconhece a possibilidade de intervenção inclusive no fluxo de correspondência, não apenas nos objetos em si, desde que haja previsão legal ou autorização judicial.

O que isso sugere, no mínimo, é que a distinção feita entre *comunicações* e os objetos em si para moderar e flexibilizar acessos a objetos arquivados com alguém, em contraste com o que está em fluxo, é uma generalização convencional que não se presta a uma distinção normativa aplicável de forma consistente. Em linha com o que tenho defendido, são as razões subjacentes de procedimento e de suspeita que sustentam uma *justa causa* para acesso que constituem o cerne da fundamentação. Não é só autorização judicial nem só previsão legal genericamente, e por isso até mesmo a tese do Min. Fachin merece reparo para não perder de vista os princípios em jogo: a autorização judicial deve atender a padrões de justificação da privacidade no contexto e a previsão

[110] Supremo Tribunal Federal, RE 1116949, Rel. Min. Marco Aurélio, Redator p/ acórdão Min. Edson Fachin, Tribunal Pleno, j. 18.08.2020.

legal deve deliminar as hipóteses específicas de aplicação, os parâmetros a serem atendidos para conter riscos de erros, abusos e excessos, e os cenários a que se refere de forma consistente com o respeito ao direito que está em questão.

Paralelamente, é de se notar que, para *cartas e documentos pessoais em si,* o STF já sinalizou a possibilidade de que haja limites duros ao aproveitamento como prova. No julgamento do RHC 115983[111] sobre cartas amorosas, foi reconhecido que a apreensão de cartas pessoais para ser usada como prova era uma questão constitucional relevante. Uma mulher foi condenada por homicídio qualificado por ter persuadido amante a contratar uma pessoa para matar o marido e questionava a licitude das "cartas de amor" utilizadas no julgamento, dizendo que o art. 240, §1º, f do CPP[112] não foi recepcionado pela CF/88. De fato, o CPP permite busca e apreensão de cartas com mandado judicial desde que úteis à elucidação de fato criminoso. O ponto suscitado é se aquelas cartas compunham algum núcleo de intimidade que poderia representar um limite; em países como a Alemanha, o uso de diários como prova já foi densamente debatido em Tribunais Superiores.[113]

A questão não é, entretanto, efetivamente debatida pela Turma: o relator Min. Ricardo Lewandowski entendeu que não era necessário analisar sob essa perspectiva porque a condenação dela se baseou em outros elementos de prova, servindo as cartas unicamente de indicativo da relação extraconjugal. Sem enfrentar a questão difícil, não deixa, entretanto, de citar precedentes pelos quais sigilo não poderia encobrir ilícitos.[114] Tendo em vista todas as ilustrações a partir do caso Elize Matsunaga, o foco seria menos se existiria algum tipo de carta de caráter íntimo que

[111] Supremo Tribunal Federal, RHC 115983, Rel. Min. Ricardo Lewandowski, Segunda Turma, j. 16/04/2013.

[112] Código de Processo Penal (Decreto-Lei nº 3.689/1941): Art. 240. A busca será domiciliar ou pessoal. § 1º Proceder-se-á à busca domiciliar, quando fundadas razões a autorizarem, para: f) apreender cartas, abertas ou não, destinadas ao acusado ou em seu poder, quando haja suspeita de que o conhecimento do seu conteúdo possa ser útil à elucidação do fato;

[113] Cf. Greco, "Introdução – 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)", 69–72. Na Alemanha, o *Bundesgerightshof* já se manifestou ao menos duas vezes sobre a questão: na primeira, em 1967, entendeu que diários não poderiam ser valorados em acusação relativa a falso testemunho por contar informações privadas relativas à própria dignidade da pessoa (BGHst 19, 325). Deixou em aberto, entretanto, a possibilidade de ponderação com interesses de persecução penal leve a outra conclusão em outra ocasião. Em 1987, essa possibilidade se concretizou e diários que continham informações sobre crimes que o acusado pensava em cometer contra acusados foram valorados (BGHSt 34, 397). Em recurso, no *Bundesverfassunggericht* (Tribunal Constitucional), houve empate (4x4) – o que no resultado levou à compreensão de que a valoração dos diários não violava a Constituição no caso (BVerfGE 80, 367).

[114] Questões processuais de não revolvimento de prova pesam também entre os demais ministros. De forma específica, o Ministro Teori Zawascki e a Min. Cármen Lúcia explicitamente deixam de se manifestar sobre uso de cartas pessoais como prova já que não seria necessário.

está fora do alcance como prova e mais se, no contexto específico do crime investigado, faria minimamente algum sentido que o trabalho investigativo envolvesse tomar conhecimento sobre elas.

5 Sigilo profissional

Tratei já de um tipo de sigilo profissional – o sigilo bancário – de maneira destacada. Agora agrupo aqui outras questões de privacidade que aparecerem incidentes ao exercício de outras profissões. Em 1962, a polícia recebeu notícia de que uma jovem havia abortado em um hospital público e iniciou investigações para apuração de crime. Uma das diligências foi requisitar a ficha médica de seu atendimento. O superintendente do hospital se recusou a fornecer as informações com base no dever de segredo profissional, mesmo diante de determinação judicial, tendo sido impetrado habeas corpus a seu favor. Por 7 votos a 3, o habeas corpus foi concedido pelo Supremo Tribunal Federal – após uma vibrante discussão. A maioria entendeu, a partir do voto do Min. Pedro Chaves, que a ficha médica é protegida por sigilo e que a ordem expunha o superintendente a violação de segredo profissional e de sua consciência, sem justa causa. Se qualquer crime fosse "causa" para revelação, nunca haveria sigilo profissional, nesse caso, entendeu o Min. Victor Nunes Leal. A divergência, liderada pelo relator Min. Ary Franco, entendia que existia a justa causa para fornecimento pois a polícia estaria tentando "habilitar a justiça", o superintendente não seria diretamente o médico e não estava sendo obrigado a prestar depoimento, o hospital era público (devendo comunicar crimes de que tem notícia) e insinuando que, tivesse sido ordenada a busca e apreensão da ficha, o superintendente não teria o que impedir.[115]

Pouco tempo depois, em 1966, a então Terceira Turma do STF daria provimento a um recurso extraordinário do IPASE (Instituto de Previdência e Assistência dos Servidores do Estado) de Guanabara contra decisões que lhe impunham o dever de fornecer a uma pessoa natural – não qualificada no acórdão – uma certidão que devassaria "sigilo profissional a que está obrigado o médico, pois refere-se a ficha hospitalar de terceiros, dos quais se quer informações sobre diagnósticos e resultados de exame radiológicos a que se submeteram".[116] O min. Luiz Gallotti reporta-se ao seu voto no HC acima, pelo que a lei daria prevalência ao resguardo do sigilo frente

[115] Supremo Tribunal Federal, HC 39.308, Rel. Min. Ary Franco, Min. p. acórdão Pedro Chaves (voto vencedor), Tribunal Pleno, j. 19.09.1962.
[116] Supremo Tribuna Federal, RE 60.176, rel. Min. Luiz Gallotti, Terceira Turma, j. 17.06.1966, DJ 9.11.1966.

ao interesse na repressão ao crime, não havendo justa causa. Ainda, apontou que a recusa no fornecimento não foi completa, mas que se exigiu que o interessado demonstrasse como o que buscava lhe serviria em sua defesa, o que não foi satisfeito. Também não impediu que juízo criminal requisitasse informações eventualmente necessárias – hipótese em que seriam aplicáveis as devidas cautelas, não satisfeitas dada a "amplitude" do pedido. Foi unânime.

Em 1981, o tema outra vez se colocou – agora na Segunda Turma e o resultado foi apertado (3x2). Juiz de São Paulo determinou, para instrução de inquérito policial, a apresentação de fichas clínicas de mulher que fora atendida pela Santa Casa de Misericórdia, supostamente como paciente de aborto consentido. O hospital opôs o sigilo médico para se negar ao fornecimento diretamente ao juiz, mas informou ter compartilhado o material com peritos para elaboração do laudo do Instituto Médico Legal – que incluiu não haver ocorrido aborto, mas "gravidez ectópica rota". O rel. Min. Djaci Falcão entendeu que o sigilo profissional não seria absoluto e que o Código de Ética Médica permitiria revelação em caso de investigação de abortamento criminoso, resguardados interesses do cliente (art. 38, alínea g)[117]. No caso, como houve compartilhamento com peritos, a cautela com o segredo profissional já estava presente. Foi acompanhado dos Ministros Décio Miranda (que não teceu mais considerações) e Firmino Paz, pelo qual haveria um "direito subjetivo à abstenção de se lhe impedir de guardar segredo profissional" (p. 323) e, a partir de comentários de Nelson Hungria, conclui que a legislação penal não autorizou médicos a serem delatores de crimes, embora permitam informações quando pacientes são vítimas e a revelação não lhes cause prejuízo. A minoria formada pelos Ministros Cordeiro Guerra e Moreira Alves acreditava, respectivamente, que o acesso era "elemento valioso na apreciação da verdade" e não poderia "proteger um delinquente" (p. 299) e que, se houve compartilhamento com peritos, deveria ser compartilhado com juiz, que não seria obrigado a acolher o laudo pericial (p. 307).

Não foram encontrados mais acórdãos desse tema na minha pesquisa no STF.[118] A discussão neles, entretanto, não deixa de valer a observação de que se preocupam com o médico e

[117] Código de Ética da Associação Médica Brasileira então vigente, segundo transcrições do acórdão: "Art. 38. A revelação do segredo medico faz-se necessária: g) nos casos de abortamento criminoso, desde que ressalvados os interesses do cliente."

[118] Esse tipo de discussão existe até hoje no STJ, embora com a variação de que não é se a polícia pode buscar materiais de sigilo médico e forçar a entrega, mas a validade de informações já repassadas a policiais – julgados relativamente recentes entenderam que não há sigilo profissional para prática de crimes, havendo justa causa para que médico delate/denuncie a ocorrência de um aborto. *Ver*, por exemplo, Superior Tribunal de Justiça, HC 514.617 SP, Rel. Ministro Ribeiro Dantas, Quinta Turma, j. 10/09/2019, DJe 16/09/2019. Como essa variação esbarra na questão de *divulgação* e por discurso, com que esse trabalho não se ocupou, e porque não fiz pesquisa no repositório do STJ, deixo de tecer mais comentários.

com como forçar-lo a prestar informações poderia fazê-lo incorrer em uma violação moral junto a seu paciente, que nele confiou informações. Não se fala em privacidade da paciente, mas é o elemento que coloca o problema. Esse é um elemento, no entanto, em linha com o visto, em que poderia haver interferência quando essas informações são relevantes para apurar crime e há suspeita individualizada – ponto em que insiste a divergência e que não é estranho, tendo em vista como lidamos com outros tipos de privacidade.

Com a reserva de que a criminalização de certas condutas (como aborto) é questionável do ponto de vista da autonomia ética (no caso, procriativa), colocando uma questão anterior e fundamental sobre se essa conduta poderia ser proibida, vemos operar razões instrumentais para a garantia da privacidade nessas situações. Informações sobre a saúde são protegidas porque se verifica que a garantia de sigilo promove a qualidade da relação entre médicos e pacientes e, assim, o próprio tratamento recebido (uma razão de política, não de princípio). Isso não significa que a tutela de informações desse tipo é só resguardada por razões do tipo em qualquer contexto. Não autorizamos, entretanto, nem na hipótese em que há crime, pelo prejuízo que isso pode causar à relação entre médico-paciente, plantando desconfiança e potencialmente desencorajando idas a hospitais.

Para outras profissões é assim também. Em 1978, chegou ao STF o pleito de contadores que impugnavam multas decorrentes de decreto estadual do Rio Grande do Sul que os obrigava a, como viam, delatar seus clientes: deveriam informar ao Fisco a existência de débitos em atraso de estabelecimentos contribuintes que deixassem seus livros fiscais com os contabilistas, para fins de escrituração. O voto do relator Min. Xavier de Albuquerque resolveu o caso por interpretação da legislação infraconstitucional: o contabilista tem o dever de manter sigilo sobre o que souber em razão de suas funções, segundo previsto em Código de Ética (art. 2º, II da Resolução 290/70 do Conselho de classe, cuja edição era determinada por Decreto-Lei nº 1.040/69); o que seria reforçado pelo parágrafo único do art. 197 do CTN[119] e pelo art. 144 do Código Civil[120]. Ao

[119] Código Tributário Nacional: "Art. 197. Mediante intimação escrita, são obrigados a prestar à autoridade administrativa todas as informações de que disponham com relação aos bens, negócios ou atividades de terceiros: I - os tabeliães, escrivães e demais serventuários de ofício; II - os bancos, casas bancárias, Caixas Econômicas e demais instituições financeiras; III - as empresas de administração de bens; IV - os corretores, leiloeiros e despachantes oficiais; V - os inventariantes; VI - os síndicos, comissários e liquidatários; VII - quaisquer outras entidades ou pessoas que a lei designe, em razão de seu cargo, ofício, função, ministério, atividade ou profissão. Parágrafo único. A obrigação prevista neste artigo não abrange a prestação de informações quanto a fatos sobre os quais o informante esteja legalmente obrigado a observar segredo em razão de cargo, ofício, função, ministério, atividade ou profissão."
[120] Código Civil de 1916: "Art. 144. Ninguém pode ser obrigado a depor de fatos, a cujo respeito, por estado ou profissão, deva guardar segredo."

contrário do que pensaram as instâncias inferiores e a autoridade coatora, não se poderia dizer que havia "consentimento" dos contribuintes que dispensava o sigilo profissional: "os critérios deontológicos [do contabilista] não se acham necessariamente subordinados às manifestações de vontade de seus clientes" (p. 579).[121]

Os casos de sigilo profissional de advogado também suscitam questões semelhantes. Em 1978 a Primeira Turma do STF entendeu, por maioria, que advogado não poderia ser obrigado a depor como testemunha sobre documentos supostamente falsos juntados a mandado de segurança.[122] O ministro Cordeiro Guerra, vencido, entendia que não se pode invocar sigilo profissional para responder sobre sua própria atuação (juntada de um documento falso e possível favorecimento pessoal a seus clientes): "o nobre múnus da advocacia não se confunde com uma espécie de cumplicidade post factum com o cliente". O voto que abriu a divergência e foi seguido pelos demais foi o do Min. Décio Miranda, para o qual o sigilo profissional imposto pelo Estatuto da Ordem dos Advogados é claro no sentido de que o advogado tem o dever de recusar-se a depor como testemunha sobre fatos relacionados a seus clientes.[123] A diferença entre ser testemunha e ser indiciado era crucial: se a polícia lhe imputasse cumplicidade, aí o encaminhamento seria outro – haveria possibilidade de depoimento. No caso, não houve, o que sugeria não haver indícios de participação dele.[124]

Com a nova Constituição Federal, e mesmo com a alteração do Estatuto da Ordem (Lei nº 8.906/1994), é difícil enxergar grandes diferenças no pensamento. Quando são investigados por ilícitos, advogados podem ter seus bens e escritórios objeto de busca e apreensão, sendo constitucional que se imponha por lei que a OAB seja informada para que alguém possa acompanhar a diligências,[125] mas podem também ser alvo de interceptações telefônicas e até de escutas ambientais: instalação de microfones e câmeras de captação por agentes estatais em seus

[121] Supremo Tribunal Federal, RE 86420-RS, rel. Min. Xavier de Albuquerque, Primeira Turma, j. 16.05.1978, DJ 02.06.1978.
[122] Supremo Tribunal Federal, HC 56563-SP, rel. Min. Cordeiro Guerra, rel. p/ acórdão Min. Decio Miranda, Segunda Turma, j. 20.10.1978, DJ 28.12.1978.
[123] Lei Federal nº 4215/63: Art. 87 - São deveres do advogado e do provisionado: XVI - recusar-se a depor como testemunha em processo no qual funcionou ou deva funcionar, ou sôbre fato relacionado com pessoa de quem seja ou foi advogado, mesmo quando autorizado ou solicitado pelo constituinte; Art. 89. São direitos do advogado: XIX - recusar-se a depor no caso do art. 87, inciso XVI, e a informar o que constitua sigilo professional.
[124] No RHC 66278, dez anos depois, esse ponto restou mais esclarecido: a Segunda Turma negou provimento a recurso de advogado que buscava ser dispensado de depoimento, porque era indiciado, diretamente suspeito de práticas delituosas e os fatos que teria de esclarecer supostamente não diriam respeito a cliente. Ver Supremo Tribunal Federal, RHC 66278-PR, rel. Min. Aldir Passarinho, Segunda Turma, j. 17.05.1988, DJ 17.06.1988.
[125] Supremo Tribuna Federal, ADI 1127, rel. Min. Marco Aurélio, Tribunal Pleno, j. 17.05.2006, DJ 11.06.2010.

locais de trabalho.[126] Intimados a depor como testemunhas, devem se apresentar, embora seja possível que fiquem em silêncio quando os atos versarem sobre causas de seus clientes.[127]

Por fim, cabe mencionar um caso emblemático de sigilo de fonte jornalística. Em 2011, o jornalista Allan de Abreu produziu matéria para o Jornal da Região, de São José do Rio Preto, em que reproduziu teor de conversas telefônicas interceptadas pela Polícia Federal no âmbito da operação Tamburucapa, que apurava indícios de corrupção na cidade. O MPF o questiona sobre fonte; ele se recusa a entregar; eles pedem quebra de sigilo telefônico. O agravo regimental na reclamação é improvido – porque afastam a aplicação do paradigma (censura prévia/lei da imprensa – ADPF 130), mas é concedido HC de ofício para trancar o inquérito contra o jornalista (porque não poderia ser acusado de quebrar o sigilo /segredo de justiça) e também para suspender a determinação de que operadoras de telefonia, a partir do CPF do jornalista e do CNPJ do jornal em que trabalha, fossem indicados os números relacionados. Assevera o rel. Min. Dias Toffoli:

> Diante dessa justa recusa do jornalista em indicar sua fonte, orientou-se o inquérito para a identificação de seus terminais telefônicos e dos da empresa para a qual trabalha. Essa medida invasiva, por si só, traduz ofensa ao sigilo de fonte, constitucionalmente assegurado (art. 5º, XIV, CF), a qual poderia desbordar, na sequência, para uma teratológica devassa de todas as ligações efetuadas ou recebidas a partir de terminais telefônicos do jornalista e da empresa que edita o Diário da Região.[128] (p.36-7)

O voto se preocupa com a repercussão que a fragilização desse tipo de sigilo poderia causar à imprensa e a quem com ela colabora, muito embora isso também dificulte a apuração de um crime.

6 Sigilo de conversas orais privadas[129]

[126] Supremo Tribunal Federal, Inq 2424, rel. Min. Cezar Peluso, Tribunal Pleno, j. 26.11.2008, DJ 26.03.2010.
[127] Supremo Tribunal Federal, AP 470 QO-QO, rel. Min. Joaquim Barbosa, Tribunal Pleno, j. 22.10.2008, DJ 30.04.2009.
[128] Supremo Tribunal Federal, Rcl 19464 AgR, rel. Min. Dias Toffoli, Segunda Turma, j. 10.10.2020, DJe 14.12.2020.
[129] Essa seção aborda casos que tratam de comunicações orais, tanto entre pessoas presentes (que estejam em um mesmo ambiente) quanto entre ausentes (por telefone). Embora essa distinção seja relevante para discussão de matéria regulatória (sobre quando se aplica a lei de interceptações telefônicas, apenas recentemente ampliada para incluir explicitamente interceptações ambientais, por exemplo), para as discussões sobre violação a direitos constitucionais, não me pareceu determinante separá-las nessa apresentação. Não encontrei julgados em que essa distinção em si foi crucial para o resultado do caso.

Como para sigilo bancário, os casos mais antigos que lidam com sigilo de comunicações orais são ambientalizados na esfera cível. Em 1977, a 2ª Turma do STF apreciou o caso de um marido que, desconfiado de que era traído e já não mais morando no mesmo domicílio, instalou um gravador no telefone da esposa. A seguir, pretendeu utilizar as gravações magnéticas como prova de adultério em ação de desquite. Em parecer, o MP opinou tanto pela violação à inviolabilidade do domicílio como das comunicações. A Corte, discutindo a legalidade da prova à luz do art. 332[130] e 383[131] do CPC/1973, entendeu que a prova era inaproveitável: "tenho como patente, por outro lado, à luz do que dispõem a respeito o Código Penal[132]e o Código Brasileiro de Telecomunicações[133], a ilegalidade do meio probatório de que se valeu, até aqui com aquiescência das instâncias ordinárias, o recorrido, meio que também não pode ser considerado moralmente legítimo, por mais progressistas e elásticos que sejam os padrões de moralidade que se possam utilizar"[134]. Não há nenhuma elaboração da posição. Ficou determinado, assim, o desentranhamento da prova.

Em 1984, a 1ª Turma enfrentou a matéria também na seara cível.[135] Um inquilino de imóvel sob disputa judicial forneceu declaração usada para fundamentar Embargos de Terceiro. A advogada dos embargados fez contato telefônico e gravou conversa em que ele basicamente assumia a falsidade de sua declaração quanto à identidade do locador do imóvel. Contra a admissão dessa prova, o inquilino impetrou mandado de segurança alegando violação ao sigilo de suas comunicações, sobretudo considerando que não seria parte no processo em que usado. O STF,

---

[130] Lei nº 5.869/1973 (Código de Processo Civil): "Art. 332. Todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, são hábeis para provar a verdade dos fatos, em que se funda a ação ou a defesa."

[131] Lei nº 5.869/1973 (Código de Processo Civil): Art. 383. Qualquer reprodução mecânica, como a fotográfica, cinematográfica, fonográfica ou de outra espécie, faz prova dos fatos ou das coisas representadas, se aquele contra quem foi produzida lhe admitir a conformidade. Parágrafo único. Impugnada a autenticidade da reprodução mecânica, o juiz ordenará a realização de exame pericial.

[132] Decreto-Lei nº 2.848/1940 (Código Penal): Art. 151 - Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem: Pena - detenção, de um a seis meses, ou multa.

§ 1º - Na mesma pena incorre: II - quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas;

[133] Lei 4.117/1962 (Código Brasileiro de Telecomunicações): "Art. 55. É inviolável a telecomunicação nos têrmos desta lei.

Art. 56. Pratica crime de violação de telecomunicação quem, transgredindo lei ou regulamento, exiba autógrafo ou qualquer documento do arquivo, divulgue ou comunique, informe ou capte, transmita a outrem ou utilize o conteúdo, resumo, significado, interpretação, indicação ou efeito de qualquer comunicação dirigida a terceiro. § 1º Pratica, também, crime de violação de telecomunicações quem ilegalmente receber, divulgar ou utilizar, telecomunicação interceptada.

[134] Supremo Tribunal Federal, RE 85.439, Rel. Min Xavier de Albuquerque, Segunda Turma, j. 11.11.1977.

[135] Supremo Tribunal Federal, RE 100.094-PR, Rel. Min Rafael Mayer, Segunda Turma, j. 28.06.1984.

então, entende que "o modo de captação desse meio de prova, feito à socapa, para servir, com a inciência do declarante, como dado a comprometer a sua integridade pessoal, incorre na infringência dos mais elementares princípios da ética e do mínimo de lealdade que deve presidir as relações humanas". Outra vez, portanto, assenta a ilegitimidade moral desse tipo de prova. Quanto ao argumento de que o sigilo seria inoponível a um participante da própria conversa, registra que isso "importa, na verdade, em mutilar a garantia da inviolabilidade do sigilo das comunicações telefônicas, notadamente quando ela é quebrada em audiência pública com divulgação para conhecimento geral". Nessa linha, fala em "direito ao recato" de comunicação telefônica e preservação da vida privada da indiscrição alheia.

É a partir desse contexto que a discussão chega na esfera criminal. Em 1986, a 2ª Turma do STF apreciou recurso em habeas corpus de médico – servidor da Previdência Social e perito em casos criminais. A partir de gravações clandestinas fornecidas por advogado (que não teve de informar a origem delas por proteção a sigilo profissional) de acusados em casos em que o médico tinha atuado, a 3ª Vara Federal de São Paulo determinou a instauração de inquérito e o médico foi chamado a prestar esclarecimentos a Delegado da Polícia Federal/DOPS. Para o STF, não havia dúvidas de que a Constituição Federal[136] não admitiria a licitude de tal prova. Para o relator Min. Aldir Passarinho, apenas em estado de sítio é que se excepcionava o direito ao sigilo de comunicações. No entanto, por meio de citações doutrinárias, sobretudo de Ada Pellegrini Grinover, já se começava a manifestar desconforto com a leitura da Constituição vigente em termos de que a linguagem de inviolabilidade sem ressalvas importaria em impossibilidade absoluta de aproveitamento de correspondências e comunicações telegráficas e telefônicas como prova e a sinalizar a defesa de restrições previstas em lei.

As manifestações do Min. Francisco Rezek melhor condensam a antecipação da revisão de entendimentos que em breve aconteceria: "O autor de uma carta tem o direito de dar ciência do seu conteúdo a outras pessoas que não o destinatário; o destinatário tem o direito de dar ciência do seu conteúdo a outras pessoas que não o remetente; penso que uma ideia analógica deveria presidir nossas convicções a respeito da comunicação telefônica (...)". Tinha em mente casos de sequestro e extorsão, como faz transparecer pelos exemplos que invoca. E seguia:

> À luz da Constituição vigente no Brasil, esse gênero de prova não pode ter valor algum. Não escondo minha convicção no sentido de que deveríamos, mediante nova disciplina

[136] Emenda Constitucional nº 01/1969: "Art. 153. § 9º - São invioláveis a correspondência e o sigilo das comunicações telegráficas e telefônicas."

> constitucional e legal, adotar sistema inspirado no modelo norte-americano: a interceptação telefônica é possível em caso de investigação de crime grave, mediante autorização prévia, plena responsabilidade e controle absoluto do magistrado. Este é quem autoriza, sempre por antecipação, a medida excepcional. Ele a controla. E, sobretudo, é ele historicamente o responsável por aquilo que está sendo feito. Tal quadro, deve ser possível que se quebre a norma da privacidade em nome de um elevado interesse público. Mas isso ainda não é possível no Brasil de hoje, sob a Constituição em vigor, e num quadro de normalidade política.[137]

Em matéria penal, nunca se questionou que conversas que não são dirigidas a público são protegidas pelo sigilo de comunicações. Comunicações *privadas* são o ponto focal da proteção. Nesse contexto, a discussão sobre a matéria logo se deu sobre a possibilidade em tese da obtenção e uso desse tipo de material em processo e os limites do consentimento de um dos participantes, sem elaboração de *por que* conversas privadas seriam protegidas.

Nos primeiros casos de Turma pós-1988, a discussão era ainda justamente sobre limites do consentimento, com temperos sobre o escopo do direito ao sigilo. Em 1989, no RHC 67.058[138], uma autoridade fazendária aduaneira foi gravada em conversa com proprietários de empresas de importação e exportação, o que ensejou abertura de inquérito por supostas ameaças. Quanto ao argumento suscitado pelo paciente – a autoridade, no caso – de que a gravação seria ilícita, o Min. Francisco Rezek, relator, pontuou em linha com o precedente anterior que, além de não haver objeção para participante de conversa "dar ciência" do conteúdo a outrem, não haveria dever de sigilo quanto ao "tipo de evento" gravado: "um funcionário público dissertando sobre tópicos inerentes à sua função".[139]

Em 1992, foi o caso do HC 69.818[140]: agentes policiais gravaram o que foi chamado de "entrevista" com dois indiciados. Uma terceira pessoa, delatada nessa conversa, impetrou habeas corpus sustentando a ilegalidade da prova. STF afasta a compreensão de que havia ilegalidade, entendendo que o contexto e o teor da conversa não deixavam crer que não houve consentimento, ainda que tenha existido arrependimento posteriormente. Ademais, e com relação ao princípio da não-autoincriminação, ainda que tenha existido constrangimento psíquico dos entrevistados e senso de oportunidade aproveitado pelos policiais, o Tribunal entendeu que essa garantia não serviria a terceiros mencionados. O "direito ao recato" sobre comunicações, se protege de

[137] Supremo Tribunal Federal, RHC 63834-SP, Min. Aldir Passarinho, Segunda Turma, j. 18.12.1986, voto do Min. Francisco Rezek (p. 120).
[138] Supremo Tribunal Federal, RHC 67058-RS, Min. Francisco Rezek, Segunda Turma, j. 03.03.1989.
[139] Ainda assim, e muito embora não houvesse razão para conhecimento do recurso pela novidade do argumento, foi provido habeas corpus de ofício, pelo entendimento de que não havia nada de ilegal no conteúdo da gravação.
[140] Supremo Tribunal Federal, RHC 69818-SP, Min. Sepúlveda Pertence, Primeira Turma, 03.11.1992.

intervenções de terceiros, já não é nesses casos oponível a participantes da própria comunicação – que poderiam captar a conversa e usá-la em processo penal.

Em 1993, o Plenário também teve de lidar com as implicações de gravações de conversas por interlocutor na esfera criminal, de novo em caso envolvendo o ex-ministro Antônio Rogério Magri.[141] Tendo sido convidado a participar de esquema de corrupção, Volnei Abreu Ávila, diretor de arrecadação e fiscalização do INSS, gravou conversa que teve com o então ministro, em que este relatava ter recebido U$ 30.000,00 pela agilização de processos de parcelamento de débitos previdenciários. Segundo o relatório, foi preparado para conversa com gravador no bolso, já que suas tentativas prévias de chamar a atenção do Presidente da República sobre o ocorrido restaram frustradas. Votando pelo recebimento da denúncia, o relator Min. Carlos Velloso sustentou que "não há, ao que penso, ilicitude em alguém gravar uma conversa que mantém com outrem, com a finalidade de documenta-la futuramente, em caso de negativa. A alegação talvez pudesse encontrar ressonância no campo ético, não no âmbito do direito" (p. 218).

O Min. Rezek acompanhou, seguindo o raciocínio já exposto nos casos prévios: "é a interferência do terceiro" que feriria a Constituição. Para ele:

> Quando, entretanto, um dos participantes da comunicação oral ou escrita entende de documenta-la de algum modo, ainda que na inconsciência da outra parte, isso não configura, em princípio, afronta à regra do sigilo. O resultado pode variar entre a indiscrição inofensiva e a mais reprovável vilania; mas não há, aí, um ato ilícito. Admitiria que as normas protetivas da privacidade, de estatura também constitucional, poderiam ser invocadas em repressão ao uso que um dos interlocutores queira fazer da carta ou da gravação do entendimento a dois, quando visa, por exemplo, a auferir lucro à custa da notoriedade da imagem alheia; um propósito bem diverso daquele de desencadear a ação da Justiça Pública.[142]

Entre manifestações tanto no sentido de que a gravação com eventual confissão não seria suficiente para comprovar crime quanto de que a licitude da prova não seria tema a ser tratado para recebimento da denúncia, a discussão sobre existência de violação ao sigilo de comunicações ficou escanteada. Também admitindo a denúncia, o único a registrar desde logo a sua posição pela ilicitude da prova foi o Min. Celso de Mello.[143]

---

[141] Supremo Tribunal Federal, Inq 657, Min. rel. Carlos Velloso, Tribunal Pleno, j. 30.09.1993.

[142] Supremo Tribunal Federal, Inq 657, Min. rel. Carlos Velloso, Tribunal Pleno, j. 30.09.1993, voto do Min. Francisco Rezek, p. 220-1.

[143] "[O] reconhecimento constitucional do direito à privacidade (CF, art. 5º, X) desautoriza o valor probante do valor do conteúdo da fita magnética que registra, de forma clandestina, o diálogo mantido com alguém que venha a sofrer a persecução penal do Estado. A gravação de diálogos privados, quando executada com total desconhecimento de um de seus partícipes, apresenta-se eivada de absoluta desvalia, especialmente quando o órgão de acusação postula, com base exclusivamente nela, a prolação de um decreto condenatório". Supremo Tribunal Federal, Inq 657, Min. rel. Carlos Velloso, Tribunal Pleno, j. 30.09.1993, voto do Min. Celso de Mello, p. 241.

Na AP 307, de 1994, em que o ex-Presidente da República Fernando Collor de Mello figurava como réu principal, também foi suscitada a questão da inadmissibilidade de gravações feitas por interlocutor – no caso, por Sebastião Curió, com respeito a conversas telefônicas tidas com o ex-tesoureiro de campanha Paulo César Farias e o ex-Ministro Bernardo Cabral (mas sem conhecimento deles).[144] O relator Min. Ilmar Galvão votou pela inadmissão por não terem sido respeitadas as condições impostas pela Constituição Federal: "previsão legal, autorização judicial e observância de forma estabelecida pelo legislador" (p. 2178), disse ele, citando os precedentes antigos de área cível que "projetaram-se no campo penal" sobre gravações feitas por interlocutor (p. 2177).

O revisor Min. Moreira Alves adota a mesma linha de raciocínio: destaca que a gravação telefônica clandestina, se pode ser feita para defesa de direito por um interlocutor (quando é vítima de extorsão, por exemplo), não valeria naquele caso em que Sebastião Curió não gravou as conversas para defesa de direito seu. Exceto pelos Min. Carlos Velloso, Sepúlveda Pertence e Néri da Silveira, os demais entendem pela ilegalidade, nos termos do voto do relator. Para os dois primeiros, a proteção de sigilo é contra terceiros, não contra interlocutor; para o terceiro, as ligações gravadas não poderiam ser desconsideradas na medida que referidas em depoimentos. Nesse ponto, cumpre registrar uma observação final de um trecho raro em votos do STF por se enveredar nos propósitos subjacentes do dispositivo. O Min. Sepúlveda Pertence registra que

> muito se falou aqui, também, em proteção da intimidade. E dela se tem falado alhures, a propósito, também, do problema da gravação de telefonemas por um dos interlocutores. Creio que, na linha da melhor doutrina e da jurisprudência prevalente no direito comparado, o problema não admite uma solução apriorística: a proteção da intimidade, é tautológico, tem o seu círculo próprio no âmbito da intimidade. Não é o simples fato de a conversa se passar entre duas pessoas que dá, ao diálogo, a nota de intimidade, a confiabilidade na discrição do interlocutor, a favor do qual, aí sim, caberia invocar o princípio constitucional da inviolabilidade do círculo de intimidade, assim como da vida privada. Não é o caso, evidentemente, de nenhum dos três diálogos em questão. (p. 2642-3).

No HC 75338, de 1998, um juiz teve conversa telefônica com Tabelião gravada, quando este se sentiu extorquido para que pagasse US$ 100.0000,00 para o juiz "influir junto ao Corregedor-Geral de Justiça" do TJRJ para "solucionar" a situação do notário em um procedimento disciplinar.[145] As gravações foram entregues a desembargadores no TJ. Investigado pelo crime de exploração de prestígio, o juiz impetrou o habeas corpus para que a prova fosse

[144] Supremo Tribunal Federal, AP 307, Rel. Min. Ilmar Galvão, Tribunal Pleno, j. 13.12.1994.
[145] Supremo Tribunal Federal, HC 75338, Rel. Min. Nelson Jobim, Tribunal Pleno, j. 11.03.1998.

desentranhada e a ação penal trancada. Nessa oportunidade, o Tribunal Pleno do STF volta à questão[146] e tem a oportunidade de refinar o tratamento jurídico à matéria. Para o relator Min. Nelson Jobim, a gravação – se autêntica – era lícita, porque havia justa causa: "é inconsistente e fere o senso comum – fonte última da proporcionalidade – falar-se em violação do direito à privacidade quando a própria vítima grava diálogo com sequestradores, estelionatários ou qualquer outro tipo de chantagista". O Min. Ilmar Galvão o acompanha – curiosamente "corrigindo" alusões à AP 307, porque lá teria estado em questão o "sigilo de dados". (De fato, essa questão também foi debatida, mas não só, como visto; voltarei ao ponto adiante).

Os ministros Maurício Corrêa, Carlos Velloso e Sepúlveda Pertence voltam a reafirmar a noção de que a proteção do art. 5º, XII é contra terceiros interceptando conversa de duas outras pessoas – não um interlocutor. Como faria em outros votos paradigmáticos, o Min. Sepúlveda Pertence não deixa de analisar a questão também sob o prisma do inciso X, a proteção da intimidade. Para ele, poderia incidir proibições decorrentes de deveres legais de sigilo aplicáveis a advogado, médico, confessor, e "até em outras relações" em que se pudesse invocar "traição a deveres nascidos da esfera da intimidade em que se tenha passado: aí vem a tona outra garantia individual; a que protege a intimidade e impõe a reserva a todos que dela participem" (p. 109-10). Também poderia ser o caso de atentar-se à garantia contra a autoincriminação, como também suscitou no julgado mencionado de 1992. Mas nada disso estaria em questão aqui. O Min. Marco Aurélio – para o qual a exceção constitucional era uma (existir autorização judicial, na forma da lei) e a prova seria usada para acusar alguém, não para a defesa do interlocutor – e o Min. Celso de Mello ficam vencidos.

No RE 583937 QO-RG, de 2009, é firmada a tese de repercussão geral "É lícita a prova consistente na gravação ambiental realizada por um dos interlocutores sem conhecimento do outro", lastreada em diversos acórdãos do Tribunal, por maioria (vencido Min. Marco Aurélio). Reproduzindo voto em outro RE, o rel. Min. Cezar Peluso sustenta:

> (...) não há licitude alguma no uso de gravação de conversação telefônica feita por um dos interlocutores, sem conhecimento do outro, com a intenção de produzir prova do intercurso, sobretudo para defesa própria em processo criminal, se não pese, contra tal divulgação, alguma específica razão jurídica de sigilo nem de reserva, como a que, por exemplo, decorra de relações profissionais ou ministeriais, de particular tutela da intimidade, ou

[146] O Min. Nelson Jobim retoma o paradigma firmado no anterior, mas abre discordando da conclusão do relator vencedor naquela ocasião de que as conclusões a que se chegou na esfera cível sobre uso de gravações se projetariam na penal. Ele não havia participado do julgamento.

> doutro valor jurídico superior. A gravação aí é clandestina, mas não ilícita, nem ilícito é seu uso, em particular como meio de prova.[147] (p. 1745).

Vale frisar que essas observações sobre possibilidade de gravação por interlocutor pressupõem expectativa de privacidade da conversa. Quando a conversa não é tida por "privada", outros argumentos aparecem, como o RHC 67.058 comentado já sinalizava: em 2011, por exemplo, a 1ª Turma enfrentou questionamento da licitude de prova de vídeo gravado por jornalistas, sem conhecimento dos envolvidos, registrando abordagem policial em que pediam propina aos abordados sob pena de forjarem flagrante por tráfico de drogas. A ação foi considerada uma gravação ambiental clandestina, mas a solução do voto do Min. Luiz Fux destacou que "sequer cabe falar em intimidade, uma vez que os envolvidos, policiais civis, em local público e no exercício de função pública"[148] (p. 50).

À luz do que foi visto na primeira parte da tese, a validade da prática de gravar uma conversa de que se é participante e a seguir usá-la como prova em algum procedimento sempre dependeria de análise contextual. Certos tipos de conversas presenciais entre pessoas pressupõem certa privacidade – ou pelo menos uma expectativa de que as informações e diálogo trocado será usado segundo os pressupostos da relação entre os interlocutores. Naturalmente, nos contextos em que essa expectativa de privacidade é uma que nossas práticas sociais permitiriam sustentar que a pessoa tinha, é certo que há sempre o risco de *traição* – de que o interlocutor grave, ou menos espalhe informação, de forma contrária aos interesses do interlocutor ou para expô-lo indevidamente. Com frequência, em casos cíveis, a fase de *divulgação* aciona interesses de privacidade combinados com a proteção de reputação que comentei ainda no início do trabalho.

No contexto em que a gravação é registro de que alguém está sendo vítima de um crime ou de que está ocorrendo crime, não há nada que suporte que o agressor pode esperar que uma regra social de privacidade o protegerá. Nossas práticas passam longe de criticar alguém por ter deixado de revelar um crime de que foi vítima. Por outro lado, como visto no capítulo 1, isso não é desculpa que legitime gravações clandestinas da polícia: se do ponto de vista de um terceiro ao diálogo há um direito à privacidade em face dele em jogo, devemos pensar o mesmo da polícia. As expectativas, regras e preocupações acerca de legítimo uso da força se aplicam e, portanto, há riscos de abuso, erro, excesso com os quais se precisa lidar. Nessa linha, é também um limite

[147] Supremo Tribunal Federal, RE 583937 QO-RG, Rel. Min. Cezar Peluso, Tribunal Pleno, j. 19/11/2009.
[148] Supremo Tribunal Federal, RHC 108.156/SP, rel. Min. Luiz Fux, Primeira Turma, j. 28.06.2011.

importante que autoridades policiais não simplesmente aliciem pessoas do círculo de um investigado para fazer gravações enquanto interlocutor: isso não afastaria questões de privacidade, porque aí ele se tornaria agente do próprio Estado.

Registrado e comentado esse desfecho (provisório?[149]) para gravações feitas por interlocutores, vale retornar a 1993. Havia outra temática emblemática que ocupava o STF. O Tribunal Pleno tinha de analisar a relevância de autorização judicial para a licitude da prova obtida mediante interceptações telefônicas em investigação de tráfico de drogas. Foi o *leading case* sobre o status da matéria sob a nova Constituição Federal e ainda sob o trauma recente em que escutas telefônicas eram constantemente utilizadas clandestinamente pelo próprio aparato estatal.[150] O relator, Min. Sepúlveda Pertence, proferiu voto sustentando que a autorização judicial não era suficiente à luz da Constituição Federal de 1988. Nas decisões recorridas, entendeu-se que o Código Brasileiro de Telecomunicações[151] permitia a medida, ao prever que "não constitui violação de telecomunicação o conhecimento dado a juiz competente, mediante requisição ou intimação deste". No entanto, para o relator, a respectiva lei não poderia ser interpretada no sentido de consagrar a "genérica possibilidade de escuta telefônica", o que a faria ser "inconstitucional desde a origem" pela Constituição que vigia. De todo modo, também aqui amparado na obra de Ada Pellegrini Grinover, sustenta que não serviria para atender ao "nas hipóteses e na forma que a lei estabelecer" previsto no art. 5º, XII da Constituição Federal: a Lei de Telecomunicações "nada especifica" quanto ao procedimento. A seguir, consigna que o direito comparado prestigia o entendimento:

> [N]a América do Norte, como na Europa, as leis que regem a autorização judicial à escuta telefônica para fins de investigação criminal, fiéis à natureza da exceção à garantia constitucional que a permissão há de ter, são todas minuciosas, começando pela enumeração taxativa dos delitos cuja repressão possibilitará, em tese, a interceptação e

[149] Em 2019, foi adicionado à Lei nº 9.296/96, a Lei de Interceptações, dispositivo que diz "A captação ambiental feita por um dos interlocutores sem o prévio conhecimento da autoridade policial ou do Ministério Público poderá ser utilizada, em matéria de defesa, quando demonstrada a integridade da gravação." Por conta de receios de que a redação importe em limitações à utilização de gravação feita por interlocutor como prova para acusação de alguém em qualquer circunstância (e não apenas quando isso tiver sido previamente combinado com a polícia pelo interlocutor), é possível que as discussões constitucionais retornem.

[150] "De sua vez, é notório que a escuta telefônica foi amplamente utilizada, sob o regime autoritário, pelos organismos de informação e de repressão política: a questão de sua ilicitude não se constituiu, porém, senão rarissimamente, em tema de discussão judicial, fosse pela vigência exclusivamente nominal das garantias constitucionais, fosse porque, efetivada clandestinamente, poucas vezes a "degravação" das conversas telefônicas interceptadas tenha sido levada aos autos dos processos". Supremo Tribunal Federal, RHC 69912-RS, Min. Sepúlveda Pertence, Tribunal Pleno, j. 30/06/1993, p. 328.

[151] Lei nº 4.117/62: "Art 57. Não constitui violação de telecomunicação: II - O conhecimento dado: e) ao juiz competente, mediante requisição ou intimação dêste.

> determinam disciplina procedimental rígida do pedido, da autorização e da execução da diligência, de modo a restringi-la ao estritamente necessário.[152]

A garantia constitucional seria esvaziada, caso não se entendesse assim.

Nessa discussão, a maioria dos ministros entendeu que a realização de interceptações telefônicas de forma lícita dependeria de elaboração legislativa específica, nos termos do voto do relator. A divergência do Min. Brossard ponderava que "decorrerá daí" [ausência de edição de lei] que a regra constitucional que admite interceptações "permanecerá em estado de sonolência (...) até que a lei seja promulgada?" Para ele, a autorização judicial permitiria a ação de forma inequívoca nos casos de investigação de crime de tráfico, aos quais a própria Constituição Federal teria tratado com "atenção particular". Nesse ponto, o Min. Moreira Alves concordava. Entretanto, a controvérsia que realmente dividiu o Plenário foi a repercussão que o entendimento sobre a ilicitude da prova deveria ter no processo (a doutrina de *fruit of the poisonous tree*), se havia provas autônomas e, de forma relacionada, se as conclusões sobre a independência de outros elementos de prova dos autos poderiam ser revistas em sede de habeas corpus – aspectos que renderam mais discussão. Em tom de alerta nessa disputa, o Min. Carlos Velloso pontuava que "A Corte Suprema há de ser sensível, então, ao clamor da sociedade, que se sente indefesa, e não deve colaborar para que não haja punição para os traficantes" (p.352). [153]

A possibilidade de interceptação mediante ordem judicial, mas ainda sem lei regulamentadora, voltou ao Pleno outras vezes em 1996, mesmo ano em que a Lei nº 9.296 – a Lei de Interceptações – entraria em vigor. Sempre, a discussão foi apertada – o lado que entendia pela admissibilidade era ainda fortemente influenciado por preocupações com as repercussões da ilicitude da prova para o resto do conjunto probatório. O último julgado de relevância do período versou sobre escuta ambiental em telefone público instalado em presídio.[154] Outra vez, o escopo do art. 5º, XII voltou à tona: divergindo do entendimento que prevaleceu no STJ, o relator Min. Maurício Corrêa consignou que

> a garantia que a Constituição dá, até que a lei o defina, não poderá distinguir entre o telefone público e o particular, pois o bem que visa proteger é a privacidade. Imagine-se se essa construção prevalecesse; geraria incontornável constrangimento para os funcionários

[152] Supremo Tribunal Federal, RHC 69912-RS, Min. Sepúlveda Pertence, Tribunal Pleno, j. 30/06/1993.
[153] No final das contas, no caso, o relator, que deferia o habeas corpus, restou vencido por 6 a 5. No entanto, o julgamento foi anulado por impedimento do Min. Neri da Silveira, que votou pelo indeferimento e que não foi apontado na ocasião. No novo julgamento ocorrido em 25/11/1993, o habeas corpus restou deferido, prevalecendo o entendimento de que a prova obtida pelas interceptações contaminou as que daí decorreram e que teriam sido cruciais para a condenação, por maioria de 5 a 4, na ausência do Min. Moreira Alves e impedimento do Min. Neri da Silveira.
[154] Supremo Tribunal Federal, HC 72.588-PA, Min. Rel. Maurício Corrêa, Tribunal Pleno, j. 12/06/1996.

> públicos, transformando as suas vidas em verdadeiro pandemônio, além do maléfico incentivo da indústria da delação que ganharia total permissividade para a proliferação generalizada dos 'grampos' oficiais. Ademais, ainda que se admitisse tal extravagância, restaria o direito à privacidade do uso do telefone que a Constituição erigiu como prerrogativa dogmática do cidadão, do interlocutor de quem a escuta verdadeiramente se destina. (p. 307-8)

O voto termina com desabafo do ministro quanto a grampos dos quais foi alvo durante o regime militar e reiteração do sentido de que "Enquanto não houver lei que nas hipóteses e na forma da lei autorize essas gravações, creio não dever o Supremo Tribunal Federal emprestar a sua interpretação para que continue a perpeturar esse achincalhe e ultraje em que se tem transformado a escuta telefônica para fins tão baixos, pérfidos e soezes, em prejuízo da privacidade que a Constituição Federal garante aos cidadãos" (p. 309). Ao final, pela maioria apertada de 6 a 5, o HC foi deferido.

Pouco depois, a Lei de Interceptações (Lei nº 9.296/96) regulamentou a exceção da Constituição Federal de que é inviolável o sigilo de comunicações, "salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal" (art. 5º, XII). Estabeleceu um regime bastante semelhante ao que o Min. Francisco Rezek ansiava em 1986: para que seja admitida, deve haver indícios razoáveis da autoria ou participação em infração penal; a prova deve não poder ser feita por outros meios disponíveis; fato investigado não deve constituir infração penal punida com pena de reclusão (art. 2º). É necessária autorização judicial, expedida de ofício ou a requerimento da autoridade policial ou do MP (art. 3º). Há deveres de fundamentação, limites temporais e obrigação de descarte do que não interessar (arts. 5º e 9º). Na teoria, a medida segue diversos parâmetros de alta proteção regulatória à privacidade.

Desde então as principais discussões do STF se dão justamente sobre o atendimento dos requisitos de fundamentação (se pode ser *per relationem* e quais os elementos mínimos que autorizam a medida, se denúncia anônima os satisfaz, por exemplo)[155] e comprovação de

[155] Por exemplo, Supremo Tribunal Federal, HC 95244, rel. Min. Dias Toffoli, Primeira Turma, j. 23/03/2010, DJe 30.04.2010 (mantendo validade de quebra de sigilo telefônico originada de denúncia anônima, mas precedida de outras apurações). Em geral, faz-se referência a HC nº 84.827/TO, rel. Min. Marco Aurélio, Primeira Turma, j. 07.08.2007, DJ de 23/11/07, para sustentar que a autoridade policial deve realizar diligências preliminar para apurar se os fatos da denúncia são verdadeiros (no caso original, considerou-se que isso não existiu – levando ao afastamento de denúncia proposta). Também Supremo Tribunal Federal, HC 121271 AgR,rel. Min. Celso de Mello, Segunda Turma, j. 13.05.2014, (pela possibilidade da técnica *per relationem* e considerando que existiu 'averiguação sumária' para analisar verossimilhança de fatos delatados); Supremo Tribunal Federal, HC 94.028, rel. Min. Cármen Lucia, Primeira Turma, j. 22.04.2008; Supremo Tribunal Federal, HC 99490, rel. Min. Joaquim Barbosa, Segunda Turma, j. 23/11/2010, DJe 01.02.2011.

necessidade, bem como sobre os limites temporais desse tipo de prova (a possibilidade de renovação e as exigências para tanto).[156] Também debate as possibilidades de compartilhamento e uso de interceptações como *prova emprestada*[157] e o que fazer com *encontro fortuitos* (em que a medida acaba levando a elementos de prova de outros crimes, diferentes dos que originalmente ensejaram a interceptação). Em 2008, o STF não tratou um meio de prova novo – a interceptação ambiental – que combinaria não só a captação de sons, mas também de imagens –, com a mesma necessidade de regulamento detalhado em lei que primeiro levou a todo o debate em torno de interceptações – serviria a previsão genérica desse tipo de medida nos arts. 1º e 2º, IV, da Lei nº 9.034/95, com a redação da Lei nº 10.217/01,[158] com autorização judicial diante de indícios de crime de organização criminosa.

Como adiantei ainda na primeira parte, o modelo da lei de interceptações combinado com a Constituição Federal pode, em muitos aspectos, ser considerado exemplar no papel aos propósitos de garantir contenção do poder do Estado e assim proteger a dignidade, autonomia e privacidade. Ele afirma a exigência de suspeita individualizada, reserva a medida a crimes mais graves e a combina com noções de necessidade que o juiz deve verificar se estão atendidos na prática, além de impor segredo às gravações e descarte do excesso. Poderia ser melhor, como comentarei no próximo capítulo, mas já não é o pior cenário. Apesar disso, a realidade dá sinais de que é bem diferente: doente de todos os vícios imagináveis de automatização, validação de qualquer pedido genericamente dizendo que é proporcional e não há direito absoluto, e muito atropelo a uma apuração do que realmente pode ser suspeita individualizada.

---

[156] Ver, por exemplo, Supremo Tribunal Federal, HC 83515, rel. Min. Nelson Jobim, Tribunal Pleno, j. 16.09.2004 (lidando com elementos mínimos para decretação, demonstração de necessidade, possibilidade de renovação, tipos de crimes que podem ensejar a medida e com (des-)necessidade de transcrição complete de gravações, entre outros questionamentos). O ponto sobre renovação é tema de repercussão geral (661) desde 2013, mas é um tema não-grato: no Inq 2424, julgado em 2008, o Min. Cezar Peluso chegou a admitir renovações de interceptações que ultrapassaram um ano. A denúncia que teve origem nessas interceptações foi recebida pelo Plenário, entendendo-se possível a renovação. Ver Supremo Tribunal Federal, Inq 2424, rel. Min Cezar Peluso, Tribunal Pleno, j. 26.11.2008, DJ 26.03.2010.

[157] Ver, por exemplo, Supremo Tribunal Federal, Inq 2424 QO-QO, rel. Min. Cezar Peluso, Tribunal Pleno, j. 20.06.2007 (lidando com a possibilidade de compartilhar provas produzidas por interceptações em processo criminal em processo administrativo disciplinar contra as mesmas pessoas); e Supremo Tribunal Federal, Inq 3014 AgR, rel. Min. Marco Aurelio, Tribunal Pleno, j. 13.12.2012 (pela impossibilidade de compartilhamento).

[158] Lei nº 9.034/95 (antiga Lei das Organizações Criminosas), com a redação da Lei nº 10.217/01: Art. 1º Esta Lei define e regula meios de prova e procedimentos investigatórios que versem sobre ilícitos decorrentes de ações praticadas por quadrilha ou bando ou organizações ou associações criminosas de qualquer tipo.
Art. 2º Em qualquer fase de persecução criminal são permitidos, sem prejuízo dos já previstos em lei, os seguintes procedimentos de investigação e formação de provas: IV – a captação e a interceptação ambiental de sinais eletromagnéticos, óticos ou acústicos, e o seu registro e análise, mediante circunstanciada autorização judicial;

Para ter uma visão mais qualificada e menos esparsa de quão bem o modelo (não) funciona na prática, é necessária a condução de pesquisa empírica de jurisprudência muito mais rigorosa, envolvendo mais tribunais, e com maior nível de detalhes sobre o caso e informações sobre o processo. O sigilo de processos criminais impõe desafios para essa tarefa. As parcas modalidades de transparência de medidas de vigilância tampouco ajudam: por exemplo, embora o Conselho Nacional de Justiça divulgue quantas medidas de interceptação supostamente foram deferidas por mês, não informa quantas foram indeferidas – de modo que não há indícios concretos sobre como a avaliação é feita. Há muito a se avançar.

7 Sigilo de registros telefônicos

Quando uma conversa ocorre pelo telefone, essa ocorrência deixa um *registro* junto à operadora de que o número X ligou ao ou recebeu ligação do número Y, em certo horário, e que a conexão foi viabilizada pelo sinal de certa torre (Estação Rádio-Base). Geradas automaticamente para uso do serviço e mantidas por empresas para fins de bilhetagem/cobrança e hoje objeto de obrigações legais de guarda obrigatória por até 5 anos[159], pouco a pouco, essas informações passaram a instruir diversas investigações e as controvérsias jurídicas surgiram.

O primeiro acórdão localizado do STF que trata de *registros telefônicos,* termo que seria usado para se referir a dados relativos a registros de chamadas e outros metadados gerados pelo uso de telefonia fixa ou celular (e que já cheguei a mencionar acima quando falei de sigilo bancário), é o HC 75232, de 1997.[160] A discussão desse caso é notadamente processual sobre cabimento de *habeas corpus* baseado exclusivamente na tutela da intimidade e se dá no contexto de decretação de quebra de sigilo de extrato de conta de telefone de Pedro Neiva Filho pela CPI dos Títulos Públicos. A maioria do Tribunal Pleno não conhece do recurso, sustentando o não-cabimento. Os que conhecem já partem para discussão de mérito: sobre a proteção das informações e os contornos dos poderes investigativos de CPIs. O relator Min. Carlos Velloso entende que os dados referidos incluem-se no

> sistema de comunicação telefônica. É dizer, comunicações telefônicas não significam, apenas, as conversas havidas por telefone, mas tudo o que com elas – comunicações

[159] Abreu, "Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais".
[160] Supremo Tribunal Federal, HC 75232-2-RJ, Rel. Min. Carlos Velloso, Tribunal Pleno, j. 05.07.1997.

> telefônicas – se relaciona. Em certos casos poderá interessar muito mais ao indivíduo o sigilo dos mencionados dados do que a própria conversa. Figuremos um exemplo: um cidadão, de boa conduta, exemplar comportamento público, chefe de família mantém romance com mulher casada. Trocam telefonemas. Para muitos isso é reprovável. É certo, entretanto, que esse comportamento se insere no direito à intimidade e à vida privada do indivíduo, direitos que a Constituição proclama invioláveis (CF, art. 5º, X), porque inerentes à personalidade das pessoas, já que não seria possível que a vida destes pudesse ser exposta a terceiros.

Não seria, entretanto, de nenhum modo um direito absoluto. Cita trecho de trabalho doutrinário de Luis Flávio Gomes em que este sustenta que a quebra de registros telefônicos é possível e seria diferente da diligência da Lei 9.296/96 (p. 731). Demandaria autorização judicial e justa causa – mas apenas quando houvesse autorização legal. O relator Min. Carlos Velloso rejeita que, não havendo lei específica, não poderia quebrar sigilo de registros telefônicos. E a seguir retorna ao raciocínio de que essa quebra se insere no sistema de comunicação telefônica, para o qual já existe lei – Lei 9.296/96 (p. 733). Conclui que CPIs podem decretar esse tipo de sigilo, por gozarem de poderes investigatórios próprios das autoridades judiciais (art. 58, §3º, CF/88), mas devendo observar a referida lei. Na hipótese, os seus requisitos não estavam presentes– notadamente por falta de fundamentação, de demonstração da necessidade, de observância do segredo de justiça na quebra, de delimitação do objeto da investigação.

O Min. Sepúlveda Pertence aderiu ao voto do Min. Neri Silveira, para o qual a ameaça a direito em investigação criminal permitiria o manejo do HC. Faz uma reserva, entretanto, à qual retornaria diversas vezes – e seria duradoura no entendimento do STF: não poderia incluir o sigilo dos dados em questão no inciso XII. "Que não se trata de interceptação telefônica, com todas as vênias, parece-me claro; e que os dados que ali se protege não são os dados em si, mas a 'comunicação de dados', também me parece evidente, sob pena de chegarmos ao resultado kafkiano de que toda investigação, seja ela parlamentar, policial, administrativa ou judicial, não possa se valer de nenhum arquivo de dados". Por isso não poderia limitar o uso dessas informações à investigação de matéria criminal, podendo também a CPI em sua atividade fiscalizadora também obtê-las.

A discussão retoma com força no MS 23452[161], de 1999, em que o STF debateu a possibilidade de CPI decretar quebra de sigilo bancário, fiscal e de registros telefônicos (ao qual já me referi acima e aqui retomo mais detidamente). O relator Min. Celso de Mello proferiu voto em que sustentou que

[161] Supremo Tribunal Federal, MS 23452, Rel. Min. Celso de Mello, Tribunal Pleno, j. 16.09.1999.

> Cabe traçar aqui, por necessário, uma distinção entre interceptação ("escuta") das comunicações telefônicas, inteiramente submetida ao princípio constitucional da reserva de jurisdição (CF, art. 5º, XII), de um lado, e a quebra de sigilo do sigilo dos dados (registros) telefônicos, de outro, cuja tutela deriva da cláusula de proteção à intimidade inscrita no artigo 5º, X, da Carta Política. (p. 121)

Mencionando obra de Tercio Sampaio Ferraz Jr, sustenta que o inciso XII protegeria a ação comunicativa, não os dados comunicados e estes, tutelados pela intimidade, "não constituem limite absoluto à ação do Poder Público" (p. 122). "Qualquer outra interpretação, de que podem resultar efeitos inibitórios sobre a atividade desenvolvida por uma CPI, certamente frustraria, de modo ilegítimo, o exercício, por esse órgão do Legislativo, da competência investigatória que lhe outorgou a própria Constituição da República" (p. 122). Por essa razão, não seria matéria fora do alcance de CPIs – estas não poderiam decretar apenas prisão, interceptação telefônica e busca e apreensão domiciliar (p. 137), para as quais a CF imporia a reserva de jurisdição. Por fim, fecha o voto alertando para a possibilidade de excessos que comprometam sigilo profissional do advogado e entendendo que, de todo modo, não se poderia cogitar da validade da quebra na hipótese por problemas de fundamentação do pedido, inclusive da falta de demonstração de necessidade (p. 141).

Cinco Ministros (Sidney Sanches, Maurício Correa, Octavio Gallotti, Néri da Silveira e Moreira Alves) apenas concordam quanto ao ponto de que a requisição não estava fundamentada, em linha com outro precedente do STF já sobre esse tema (MS 23454), também do contexto de CPIs. São três os Ministros que votam integralmente com o relator inclusive no ponto quanto a que tipos de diligências pode ou não a CPI determinar. Outra vez, vale destacar o voto vogal de Sepúlveda Pertence.

> Entendo tratar-se de sigilos relativos, que podem ser quebrados, observado o 'due process of law', por determinação judicial, extensível, em princípio, ao âmbito de poderes das comissões parlamentares de inquérito". (…)"Com relação especificamente à requisição dos dados telefônicos – que aqui só enfrentou de raspão – a minha convicção é a de que o problema há de ser encarado à luz do princípio da proteção constitucional da privacidade e da intimidade, e não propriamente do inciso XII do art. 5º, que diz respeito ao sigilo das comunicações, em suas diversas modalidades: são desdobramentos que a tecnologia impôs ao multissecular princípio da correspondência. O que ali se protege, pois, é a comunicação telemática dos dados: a não ser assim, então, todos os dados, todos os apontamentos, todos os fichários antigos e modernos existentes no mundo estariam protegidos por uma reserva que até se pode sustentar absoluta, porque a alusão ao final do inciso XII do art. 5º é restrita às comunicações telefônicas. A meu ver, o absurdo a que levaria conferir quanto a tudo o mais uma reserva absoluta mostra que, naquele inciso, só se cogitou das diversas técnicas de comunicação. E, por isso mesmo, teve-se de resguardar mesmo de intromissão judicial

> o próprio ato de comunicação, salvo se cuida da comunicação telefônica, porque não deixa prova de seu conteúdo.[162]

Como também se verá a seguir ao se tratar de sigilo telemático, o STF desenvolvera uma longa história mal resolvida com relação à proteção constitucional do sigilo de registros telefônicos. Se aqui a narrativa que adentrou no mérito era de que a CPI poderia diretamente (sem uma autorização judicial) decretar a quebra porque detém poderes equivalentes de autoridades judiciárias e que a Constituição não protege tais informações com alguma reserva especial de jurisdição, não se descartava a relevância de tais informações para a intimidade. Pouco a pouco, entretanto, esses aspectos vão se perdendo e a falta de um entendimento claro sobre o assunto vai produzindo decisões curiosas e baseadas em razões difíceis de reconciliar.

Em julgado de 2003, por exemplo, sinaliza-se que a distinção entre interceptações telefônicas e quebra de registros telefônicos poderia permitir a dispensa de autorização judicial para obtenção de registros em investigação criminal. Nesse caso, a discussão subjacente é uma alegação de prova ilícita porque houve "rastreamento de telefones", descobrindo-se o conjunto de chamadas feitas antes e depois de um crime, entre investigados, sem autorização judicial.[163] A 1ª Turma entende que esse ponto foi suscitado tardiamente e se recusa a rever. Ainda assim, a relatora Min. Ellen Gracie registra que

> Não custa lembrar, também, que a garantia constitucional instituída no art. 5º, XII, da Carta Política que objetiva preservar a inviolabilidade do sigilo das comunicações telefônicas, não se confunde com a cláusula prevista do art. 5º, X, da mesma Carta, que tutela o direito à intimidade. Estes autos, entretanto, não cuidam de ofensa à inviolabilidade das comunicações telefônicas, de sorte que a invocação, no extraordinário, do art. 5º, XII, da CF, foi impertinente. Cuidam, sim, de dados/registros telefônicos que poderiam se inserir no âmbito da intimidade tutelada no inciso X, do art. 5º da Carta Política, norma esta que não foi objeto do recurso extraordinário. De qualquer sorte, é sabido que o direito à intimidade, embora constitucionalmente tutelado, não pode erigir-se num limite absoluto à ação do Poder Publico. Principalmente na hipótese dos autos quando se investiga a autoria intelectual de um homicídio encomendado. (p. 453)

Como se viu: não era isso o que se extraia dos casos anteriores, mas é como foi usado no caso. De fato, ao longo dos anos, e em termos de exigências materiais para quebras de sigilo de registros telefônicos junto a operadoras de telefonia, o STF não deixou de exigir fundamentações de decisões judiciais, mediante demonstração de indícios de envolvimento em infração penal e de

[162] Supremo Tribunal Federal, MS 23452, Rel. Min. Celso de Mello, Tribunal Pleno, j. 16.09.1999, voto do Min. Sepúlveda Pertence, p. 154.
[163] Supremo Tribunal Federal, RE 327717 AgR-ED, Rel. Min. Ellen Gracie, j. 04.11.2003.

necessidade para a apuração. No HC 89083, em 2008, por exemplo, a 1ª Turma manteve ordem judicial de quebra de sigilo de dados telefônicos para instrução de inquérito, porque "há referência à suspeita de envolvimento do paciente no crime que o inquérito visa a elucidar" nos autos.[164] A ementa registrou o entendimento da seguinte maneira: "Embora a regra seja a privacidade, mostra-se possível o acesso a dados sigilosos, para o efeito de inquérito ou persecução criminais e por ordem judicial, ante indícios de prática criminosa".

Na AP 1003, de 2018, a 2ª Turma também afastou questionamentos dirigidos à validade de ordem judicial de quebra de sigilo de registros telefônicos (registros de chamada e localização de ERB) das pessoas e empresas investigadas porque o tema já estava precluso e, destacou o relator Min. Edson Fachin, "[d]e qualquer maneira, *ainda que superado o óbice apontado*, impende enfatizar, *por relevante,* que restou configurada, *na espécie*, a imprescindibilidade da referida quebra de sigilo telefônico, até mesmo *em razão da necessidade* demonstrada pelos órgãos de persecução penal para a formação de sólido acervo probatório apto a viabilizar eventual oferecimento de denúncia." E também que "era absolutamente pertinente e necessário o afastamento do sigilo telefônico em questão diante *dos indícios existentes* e *das referências* feitas em depoimentos colhidos nas investigações sobre a realização de contatos telefônicos voltados *à alegada* execução dos ilícitos penais descritos na denúncia, conforme restou *devidamente fundamentado* na decisão que ordenou a efetivação de mencionada providência"[165].

Nos casos acima, a exigência de decisão judicial não estava diretamente em questão – e sim os parâmetros que ela deve observar. Como se verá mais à frente, esse cenário fica ainda mais complexo pela influência da compreensão de que o acesso a registros telefônicos (histórico de chamadas) *no celular* seria admitido sem ordem judicial (entendimento firmado em hipótese de prisão em flagrante e que tratarei ao falar de sigilo telemático). Essas distinções e variações contextuais, entretanto, não são feitas de forma clara, de modo que hoje o STJ mantém que é dispensada a autorização judicial para acesso a registros telefônicos – o que significa que é admitido pela segunda principal Corte do país que não seja feito o controle independente e imparcial para o uso dessas medidas investigativas – independentemente do impacto que possa ter para a intimidade e para outros sigilos constitucionais, da necessidade para a investigação e da

[164] Supremo Tribunal Federal, HC 89083-MS, Rel. Min. Marco Aurélio, Primeira Turma, j. 19.08.2008.
[165] Supremo Tribunal Federal, AP 1003, Rel. Min. Edson Fachin, Segunda Turma, j. 19.06.2018, p. 3646.

existência concreta de indícios de envolvimento dos alvos em crime.[166] Como no STF, afastam-se as exigências da Lei nº 9.296/96 quando se obteve alguma ordem judicial[167] e, mesmo quando a autorização judicial não existiu, também essa exigência – por conta da natureza dos dados requisitados[168]. Como muitos recursos extraordinários simplesmente não são admitidos por necessidade de revolvimento em matéria fático-probatória, essa compreensão acaba se mantendo e prevalecendo. À luz do que foi visto na primeira parte da tese, esse descarte completo de relevância e de regulação clara e coerente não faz sentido nenhum e expõe pessoas à arbitrariedade sem qualquer salvaguarda.

Há outros exemplos recentes de aplicações fora de contexto e inconsistentes da distinção entre quebras de registros telefônicos e interceptações telefônicas. Também em 2018, por exemplo, a 2ª Turma apreciou caso em que a defesa em ação penal requereu quebra de sigilo de dados telefônicos do Núcleo de Inteligência da Polícia Federal para que fosse apurado quem seria o autor de denúncia anônima.[169] Embora também não se trate de interceptação telefônica, o relator Min. Edson Fachin invocou a Lei nº 9.296/96 para sustentar que a medida não poderia ser autorizada porque

> não tem por objeto qualquer investigação da prática de uma infração penal, como exige a Lei 9.296/1996, mas apenas a ciência de quem seria o autor de notícia criminal que culminou com diligência de busca e apreensão. Assim, aos agravantes falta legitimidade ao exercício da pretensão, nos termos do art. 3º[[170]] do aludido diploma legal.

---

[166] Jacqueline de Souza Abreu, "Comentário ao STJ – REsp 1.782.386/RJ: Acesso a Agenda de Contatos de Celular por Autoridade Policial sem Autorização Judicial", *Revista dos Tribunais* 1026 (2021): 371–406.

[167] Cf., por exemplo, Superior Tribunal de Justiça, RHC 53.541/RJ, Rel. Min. Jorge Mussi, Quinta Turma, j. 12/09/2017, DJe 20/09/2017: "a quebra do sigilo de dados telefônicos, consistentes no histórico de chamadas, dados cadastrais e extratos de ligações, não se submete à disciplina da Lei 9.296/1996, que trata da interceptação das comunicações telefônicas. [...] Na espécie, o magistrado singular justificou a quebra do sigilo dos dados telefônico dos recorrentes com base, essencialmente, nas informações coletadas pela autoridade policial e pelo Ministério Público indicativas da prática criminosa atribuída aos investigados, inexistindo, assim, qualquer nulidade apta a contaminar as provas dela decorrentes".

[168] Cf., por exemplo, Superior Tribunal de Justiça, AgRg no REsp 1760815/PR, Rel. Min. Laurita Vaz, Sexta Turma, j. 23/10/2018, DJe 13/11/2018: "De fato, exige-se decisão judicial fundamentada para obter o teor da comunicação ou do que é transmitido pelo interlocutor. A proteção constitucional não abrange, contudo, os dados cadastrais do usuários, relações de números de chamadas, horário, duração, dentre outros registros similares, que são informes externos à comunicação telemática." No contexto do caso, também se arguia que a autorização para acesso sem autorização judicial seria dada pelos arts. 3, 15 e 17 da Lei nº 12.850/13 (Lei das Organizações Criminosas). No STF, essa legislação (art. 15 e 16) foi aplicada para autorizar acesso direto pela autoridade policial a documentos e registros de viagens realizadas por investigado, por exemplo, no HC 139749 MG, Rel. Min. Marco Aurélio, Primeira Turma, j. 16.06.2020.

[169] Supremo Tribunal Federal, AP 1030 Ag-Rg, Rel. Min. Edson Fachin, Segunda Turma, j. 25.09.2018.

[170] Lei nº 9.296/1996: "Art. 3° A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento: I - da autoridade policial, na investigação criminal; II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.

O entendimento ressoa o antigo voto do Min. Carlos Velloso – para quem as exigências da referida lei se estenderiam a quebras de registros telefônicos. Não há, entretanto, qualquer tentativa de reconciliar tal entendimento com os longos anos de distinção entre interceptações telefônicas e registros telefônicos, nem com as flexibilizações possibilitadas para diversos contextos em razão desse entendimento "bipartite". A razão talvez mais influente do resultado, de política pública, contra a medida requerida, é só apresentada de forma secundária e breve nova: a medida também encontraria "óbice no art. 3º da Lei 13.608/2018, que protege o sigilo dos dados de informante que se utiliza de serviço telefônico de recebimento de denúncias".

8 Dados pessoais: dados cadastrais

Há ainda um conjunto de casos em que não é requerido o histórico de ligações, mas informações cadastrais – o que faz parte disso é em si disputado, mas em geral o termo se refere a informações usadas para um *cadastro* em algum serviço, que pode conter nome, endereço, e outros dados pessoais, inclusive qual o identificador *de cadastro* (como o número do telefone) – de alguém.

No HC 124322 AgR, de 2016, a 1ª Turma do STF trata de uma questão nova, mas sem reconhecer essa novidade. Habeas corpus foi impetrado contra acórdão do STJ que manteve o entendimento de licitude de prova obtida a partir de informações sobre as linhas de telefones de usuários de telefonia (dados cadastrais) que estiveram em certa localidade em horário em que ocorreu o crime.[171] Esse tipo de medida é diametralmente diferente das usuais quebras de sigilo em investigações – que giram em torno de um suspeito. Nela, a estrutura da empresa operadora de telefonia e seu reservatório de dados de clientes é utilizada para que se busque coletividades de pessoas – *pool* em que então se identificaria quem poderia ser um suspeito. No caso, a diligência da autoridade policial foi providenciada ainda diretamente (sem ordem judicial) e a defesa sustentava justamente a violação do sigilo de comunicações e da privacidade. É negado seguimento ao recurso por aspecto processual – utilização de habeas corpus como substitutivo de recurso ordinário –, mas é feito registro sobre o mérito: os acórdãos do STJ e do TRF-4 não estariam em desacordo com a jurisprudência sobre o inciso XII, pela qual protege-se a

[171] Supremo Tribunal Federal, HC 124322 AgR, Rel. Min. Luis Roberto Barroso, Primeira Turma, j. 12.09.2016.

comunicação de dados, não os dados. Apelando também à distinção entre conteúdo e "informes externos à comunicação", também afasta a proteção constitucional de dados cadastrais. Cita um julgado sobre dados telemáticos e outro de acesso a celular (aos quais retornarei adiante). O julgamento foi unânime (firmado em sede de agravo regimental, passou sem maiores discussões nos termos do voto do relator). Embora o tipo de medida não seja regulado em lei e por premissa alcance diversas pessoas sem relação com o crime, o comentário focou na natureza dos dados cadastrais a serem entregues, agrupados com base em dados de localização, descartando a necessidade de qualquer outra avaliação sobre a medida.

Outra manifestação curiosa nessa linha ocorrera mais de uma década antes, no julgamento de uma Ação Direta de Inconstitucionalidade, apreciada pelo Plenário em 2007. O caso não versa sobre matéria penal, mas é elucidativo da superficialidade com que se carrega certas doutrinas de forma inerte ao contexto. Tratava de lei de Santa Catarina que obrigou veículos de transporte de cargas e passageiros a indicar número de telefone na parte traseira. O STF entendeu que a obrigação não contrariaria o inc. XII do art. 5º da Constituição Federal. Nos termos do voto da relatora Min. Cármen Lúcia, "A proibição contida nessa norma constitucional refere-se à interceptação e à conseqüente captação de conversa, por terceira pessoa, sem a autorização e/ou o conhecimento dos interlocutores e interessados na conversa telefônica. A informação de número telefone para contato não implica quebra de sigilo telefônico".

De fato, não estava em questão interceptação de conversas nem mesmo fornecimento de registros de chamada pertinentes à intimidade e à vida privada de ninguém e é justamente o contexto que revela não haver comprometimento algum a um direito à privacidade. Não há, entretanto, qualquer elaboração quanto a esses aspectos para se justificar a constitucionalidade de instituir uma obrigação de exibição de dados – apenas uma reverberação quase aleatória da compreensão sobre o tema que aparenta se encaixar na hipótese por mero acaso. Afinal, se a lei determinasse que todo e qualquer cidadão exibisse seu número de telefone em seus carros, é improvável que a matéria tivesse passado com tanta facilidade ou que fundamentar da mesma maneira tivesse funcionado. A razão invocada é tão genérica e simplificadora, entretanto, que até parece autorizar medidas assim.

Informações para contato são, ironicamente, aquelas que provocaram a definição de novo marco para a jurisprudência do STF. Em 2020, o STF julgou pedido de medida cautelar em cinco ações diretas de inconstitucionalidade no STF (ADI 6387, 6388, 6389, 6390 e 6393) contra a

Medida Provisória 954 de 2020, que dispôs que "as empresas de telecomunicação prestadoras do STFC [Serviço Telefônico Fixo Comutado] e do SMP [Serviço Móvel Pessoal] deverão disponibilizar à Fundação IBGE, em meio eletrônico, a relação dos nomes, dos números de telefone e dos endereços de seus consumidores, pessoas físicas ou jurídicas" (art. 2º). Em síntese, os diferentes autores sustentaram que a medida instituiria uma "estrutura contemporânea de vigilância da população", e que a concentração de dados facilitaria abusos e vazamentos e outras "ilegítimas interferências" sobre as pessoas. Implicaria desrespeito a princípios elementares do direito à proteção de dados pessoais, que podem ser extraídos das proteções constitucionais da intimidade e do sigilo de dados e do remédio do habeas data. A Advocacia-Geral da União, o Ministério Público Federal e o IBGE, por sua vez, defenderam que não se poderia pressupor que haveria uso abusivo, que a medida envolveria apenas dados cadastrais e que não seria hipótese de quebra de sigilo, mas sim de "transferência de sigilo" (de empresas para o IBGE).

O STF foi contundente. O voto da relatora Min. Rosa Weber manejou, de forma sofisticada, diversos aspectos do direito da proteção de dados pessoais, desde a suspensão liminar – referendada pelo Plenário[172]. Assentou, de forma paradigmática, que também os dados que foram objeto do pedido são protegidos constitucionalmente e que a medida, com escopo ambíguo e alcance excessivo, não poderia ser admitida. A finalidade declarada – "produção de estatística oficial" – seria inespecífica, o que comprometeria também a avaliação sobre o atendimento do princípio da necessidade. Ademais, não teria sido elencada qualquer indicação da necessidade de uma coleta massiva de todos os dados, principalmente para pesquisas que, segundo o próprio IBGE declarou, seriam feitas por amostragem. Nesse aspecto, sinalizou que as principais pesquisas já estavam sendo realizadas remotamente, por dados já existentes. Por fim, também observou que não foram previstas medidas de segurança. Todos esses problemas seriam potencializados pela ausência de uma autoridade de controle e supervisão – visto que a Autoridade Nacional de Proteção de Dados prevista na Lei nº 13.709/18 ainda não havia sido criada – e pelo adiamento da entrada em vigor da Lei Geral de Proteção de Dados. A relatora foi seguida pela maioria. Apenas o Min. Marco Aurélio discordou: entendeu haver "razão suficiente" para o compartilhamento de dados entre teles e IBGE e que ele não seria submetido a prazo indeterminado.

[172] Supremo Tribunal Federal, Referendo da MC nas ADIs nº 6387, 6388, 6389, 6390 e 6393, Rel. Min. Rosa Weber, Tribunal Pleno, j. 07.05.2020, DJE 12.11.2020.

Resta ver como esse reconhecimento de um direito à proteção de dados pessoais influenciará o contexto penal. No período analisado, a matéria não foi enfrentada no contexto processual penal. A única manifestação que existiu foi em medida cautelar em ADI contra lei de Tocantins que criava "Cadastro Estadual de Usuários e Dependentes de Drogas", a ser mantido pela Secretaria Estadual de Segurança Pública.[173] A cautelar é deferida e referendada no Plenário, nos termos do voto do relator Min. Edson Fachin, não só por inconstitucionalidade formal, mas também material: tem "viés de seletividade e higienização social incompatível com o Estado de Direito democrático e os direitos fundamentais que a Constituição de 1988 protege, especialmente, a igualdade (CRFB, art. 5º, caput), a dignidade da pessoa humana (CRFB, art. 1º, III), o direito à intimidade e à vida privada (CRFB, art. 5º, X) e o devido processo legal (CRFB, art. 5º, LIV)". Em termos de proteção de dados, adiciona que dados referentes à saúde são sensíveis e se submetem a tratamento jurídico especial na LGPD (Lei nº 13.709/18) e consigna:

> Esse sistema constitucional especial de proteção é violado pela lei impugnada, a qual, ademais, não prevê formas de controle prévio à inclusão no cadastro, não prevê a comunicação e o consentimento do interessado e, para a sua exclusão, exige laudo médico e informação oficial sobre a não reincidência. Tampouco existe protocolo claro de proteção e tratamento desses dados.

Também em 2020, o STF barrou a elaboração de dossiês de informações de servidores públicos integrantes do movimento "antifascista" pela Secretaria de Operações Integradas do Ministério da Justiça por ter como único critério o posicionamento político. O tal dossiê reunia típicos "dados cadastrais": nomes e, em certos casos, fotos e endereços de perfis de redes sociais". Para a relatora da medida cautelar referendada no Plenário, "O uso – ou o abuso – da máquina estatal para a colheita de informações de servidores com postura política contrária ao governo caracteriza desvio de finalidade."[174] Um relatório com esse escopo, ainda que tenha sido feito para "inteligência", seria incompatível com a democracia. É um caso que mostra que mesmo dados simples e comuns podem despertar a proteção de um direito à privacidade se o contexto permitir dizer que é um que a pessoa tem: a autenticidade na perspectiva de independência ética barra esse tipo de medida do Estado – ninguém deve ser catalogado pelo Estado por suas opiniões políticas.

[173] Supremo Tribunal Federal, MC na ADI 6561 TO, Rel. Min. Edson Fachin, Tribunal Pleno, j. 13.10.2020.

[174] Supremo Tribunal Federal, ADPF 722 MC, Rel. Min. Cármen Lúcia, Tribunal Pleno, j. 20.08.2020, DJE 22.10.2020. Vencido apenas o Min. Márco Aurélio. Ressalvo que o acórdão não apareceu na minha extração de resultados, possivelmente por não ter sido analisado à luz de noções de privacidade, mas sim de liberdade de expressão e associação. Pela relevância, incluo-o aqui.

Dias antes, o STF havia apreciado pedido de medida cautelar na ADI 6529, proposta pelo Partido Socialista Brasileiro e pela Rede Sustentabilidade contra artigo de lei de mais de 20 anos (parágrafo único do art. 4º da Lei nº 9.883/1999), acerca dos limites das transferências de dados de órgãos pertencentes ao Sistema Brasileiro de Inteligência à Agência Brasileira de Inteligência.[175] Por conta de mudanças recentes veiculadas no Decreto nº 10.445/2020, a tese levada era que havia o risco de compartilhamento de informações sigilosas mediante mera requisição da agência. O caso não trata apenas de dados cadastrais e, na falta de lugar melhor, é mencionado aqui, na medida em que o resultado do caso foi repisar uma distinção genérica entre informações pessoais de qualquer tipo e "dados sigilosos": "dados referentes às comunicações telefônicas ou dados sujeitos à reserva de jurisdição", quando submetidos a condições de compartilhamento balizado em lei, que ainda precisaria ser respeitado. Para além disso, compartilhamentos ficaram autorizados quando há interesse público, solicitação motivada e mediante procedimento formalmente instaurado e sistema eletrônico de segurança e registro de acesso.

Fora isso, ainda não há grandes precedentes firmados sobre o tema. A situação é temporária. Atualmente, 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 (retornando à discussão do item anterior) – sem ordem judicial. Por exemplo, na 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 sem autorização judicial; na ADI 4906, sobre art. 17-B da Lei de Lavagem de Dinheiro (Lei nº 9.613/98), que permite a autoridades e ao MP acesso a dados cadastrais mantidas por certas entidades públicas e privadas, sem autorização judicial prévia; ADI 5642, 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. [176] Nos dois últimos casos, os relatores Min. Nunes Marques e Edson Fachin, respectivamente, já votaram pela improcedência, mas o julgamento foi interrompido por conta de

[175] Supremo Tribunal Federal, ADI 6529 MC, Rel. Min. Cármen Lúcia, Tribunal Pleno, 13.08.2020, DJE 15.10.2020.

[176] Cf. Jacqueline de Souza Abreu e Dennys Antonialli, "Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais" (São Paulo: InternetLab, 2017), 27 e 35, http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf.

pedidos de vista. Algumas empresas também questionam pedidos específicos que lhes parecem abusivos.[177]

Ao analisar e deliberar sobre essas questões, será importante ter em mente que não há dados banais a ponto de flexibilizar qualquer acesso. A finalidade de uso importa e a existência e possibilidade defesa da privacidade deles em relação a terceiros em certo contexto, também. Fricções no seu acesso – a necessidade de formalização de uma petição justificada, preferencialmente em face de autoridade judicial que verifique atendimento de exigências de suspeita individualizada e necessidade, tende a mostrar o respeito que direitos à privacidade merecem. Sendo essa uma questão eminentemente regulatória e contextual, é possível imaginar que uma lei estabeleça a possibilidade de acesso apenas mediante pedido policial para certos tipos de crime cujas características autorizem maior rapidez e eficiência no acesso aos dados, mas que equipare com salvaguardas posteriores. Pode ser uma avaliação diferente, portanto, quando comparamos o uso disso para investigações de lavagem de dinheiro com quando estamos diante de um furto. Ainda, o cardápio de instrumentos regulatórios oferece outras formas de *accountability* sobre o uso que é feito das informações obtidas; as leis que estabelecem essas possibilidades de acesso direto devem, portanto, se utilizar delas. Falarei mais disso no próximo capítulo – o STF está na posição para dar visibilidade a essas opções e impulsioná-las.

9 Dados pessoais sensíveis: DNA

Cabe registrar a existência de um conjunto de casos que envolve um dado pessoal "sensível" – terminologia, no caso, que tomo emprestada do direito da proteção de dados pessoais que aqui uso para me referir a uma categoria de informação sobre uma pessoa que ela não consegue mudar: DNA. Em 1994, o STF enfrentou pela primeira vez a possibilidade de obrigar alguém a entregar material genético para produção de prova.[178] O caso é cível – uma ação de investigação de paternidade em que foi determinado tal exame pericial, sob condução coativa. Além de suscitar violação ao art. 5º, X, CF/88, o interessado sustentava violação ao art. 5º, II, CF/88, por não haver

[177] Por exemplo, casos em que se defere a criação de uma "senha" para acesso ao banco de dados da empresa de telefonia. Cf. Jacqueline de Souza Abreu, "Quebras de sigilo e privacidade: três casos idênticos, três resultados diversos", *Gazeta do Povo*, 6 de dezembro de 2017, https://www.gazetadopovo.com.br/opiniao/artigos/quebras-de-sigilo-e-privacidade-tres-casos-identicos-tres-resultados-diversos-1zo7q26et3qh31cd42u88k6sh/.
[178] Supremo Tribunal Federal, HC 71736, Rel. Min. Francisco Rezek, rel. p/ acórdão Min. Marco Aurélio, Tribunal Pleno, j. 10.11.1994, DJE 22.11.1996.

dispositivo legal impondo-lhe a submissão. O julgamento foi apertado (6x4). O relator Min. Francisco Rezek votou pelo indeferimento de habeas corpus, entendendo prevalecer os interesses pela verdade real, o dever de colaborar com o Judiciário (art. 339[179]) e o direito à identidade da criança: a "incolumidade corporal deve ceder a um interesse preponderante" (p. 411). Acolhe o parecer do MPF no ponto de que "a afirmação ou não do vínculo familiar não se pode opor ao direito ao próprio recato" (p. 414). Ainda, considera que juízes podem determinar as provas necessárias à instrução do processo. Foi acompanhado dos ministros Ilmar Galvão, Carlos Velloso e Sepúlveda Pertence.

Abriu a divergência o Min. Marco Aurélio, para quem não existe lei que amparasse tal ordem judicial de condução "debaixo de vara". Se tivesse, seria inconstitucional:

> é irrecusável o direito do Paciente de não permitir que se lhe retire, das próprias veias, porção de sangue, por menor que seja, para a realização de exame. A recusa do paciente há de ser resolvida não no campo da violência física, da ofensa à dignidade humana, mas no plano instrumental – reservado ao juízo competente – ou seja, o da investigação de paternidade – a análise cabível e a definição, sopesadas a prova coligida e a recusa do réu (p. 420).

Acompanharam os Min. Celso de Mello, Sidney Sanches, Néri da Silvera, Moreira Alves e Octavio Gallotti. A posição prevaleceu.

Pouco tempo depois, em ação em que um terceiro buscava ser reconhecido como pai de criança em lugar do pai presumido (pelo casamento com a mãe), o Min. Sepúlveda Pertence mudou de lado – pela "desproporcionalidade" do pedido, que seria mera "prova de reforço", já constando nos autos exames do autor, da criança e da mãe.[180] Os demais que compuseram o julgamento unânime haviam votado da mesma maneira no primeiro caso.

No início dos anos 2000, a questão ressurgiu em um caso criminal. Gloria Trevi, cantora mexicana, grávida e extraditanda presa nas dependências da Polícia Federal ajuizou petição, recebida no STF como reclamação, para, com base nos arts. 5º X e XLIX[181] da CF/88, impedir que, no parto, fosse colhido material genético da sua placenta para averiguar a paternidade de seu filho.[182] A PF se mobilizava para apurar a origem de sua gravidez, em meio a notícias com

[179] Código de Processo Civil (Lei nº 5.869) de 1973: "Art. 339. Ninguém se exime do dever de colaborar com o Poder Judiciário para o descobrimento da verdade."
[180] Supremo Tribunal Federal, HC 76.760, Rel. Min. Sepúlveda Pertence, Primeira Turma, j. 31.03.1998, DJE 15.05.1998. O caso não constou na minha busca, mas como foi referido no precedente seguinte, eu o incluí.
[181] Constituição Federal de 1988, art. 5º: "XLIX - é assegurado aos presos o respeito à integridade física e moral;",
[182] Supremo Tribunal Federal, Rcl 2.040-QO, Rel. Min. Néri da Silveira, Tribunal Pleno, j. 21.02.2002, DJE 27.06.2003. Participaram do julgamento os ministros Marco Aurélio, Moreira Alves, Néri da Silveira, Sydney Sanches, Sepúlveda Pertence, Celso de Mello, Ilmar Galvão, Maurício Correa, Nelson Jobim e Ellen Gracie.

alegações de que teria sido estuprada por funcionários da instituição. Sua defesa chegou a alegar nos autos do seu processo de extradição ter sido vítima de estupro carcerário ao pleitear por liberdade provisória, apesar de ela não ter representado formalmente sobre a ocorrência do crime. Foi recolhido, espontaneamente, material de 61 homens para comparação para se resolver o que era posto como "enigma".

O relator Min. Néri da Silveira viu um conflito entre a intimidade e vida privada da cantora e a honra e imagem dos policiais que impunha o esclarecimento da verdade quanto à participação dos servidores no ato de alegada violência sexual, destacando a repercussão do caso e argumentos suscitados pela defesa mesmo da moralidade das instituições brasileiras implicadas, além do caráter não invasivo do teste que se basearia em um material residual ao parto. No seu voto, o Min. Carlos Velloso destacou o que seria a pretensão legítima de policiais, que estariam sob suspeita de terem cometido crime, de provarem sua inocência. Restou vencido apenas o Min. Marco Aurélio, para quem o inquérito policial que deu origem ao pedido não tem pedido claro: mesmo que averiguada a paternidade, nunca se chegaria a uma prova de calúnia que permitisse a criminalização da cantora, já que ela não representou formalmente sobre a ocorrência de crime; no máximo, o resultado seria uma responsabilização administrativa disciplinar. O respeito à integridade moral da extraditanda e sua intimidade deveriam ser preservadas.

Nessa temática, o STF tem casos pendentes envolvendo ainda a coleta obrigatória fixada em lei municipal de material genético de bebês recém-nascidos com a finalidade de evitar trocas de crianças (ADI 5545) e também sobre a constitucionalidade da formação de bancos de dados de material genético de pessoas condenadas por crimes violentos ou hediondos (RE 973837 MG).

Esses casos merecem análises específicas. No primeiro caso, seria necessário, antes mesmo de começarem as questões difíceis de princípio, se há um risco real de segurança que precisa ser dirimido, se precisa ser dirimido mesmo dessa maneira e, se a alternativa de reservar essa coleta a famílias que tem receio real de serem vítimas desse problema já não resolveria o problema. É preciso saber também quais as formas de uso e guarda dessas informações. Certamente há um direito à privacidade que protege contra essas políticas públicas ruins e excessivas, que oneram o exercício da privacidade excessivamente, considerando que material genético é um material único, cuja guarda merece o maior dos cuidados em termos de contenção de risco de sofrer injustiça pelo abuso dessa informação.

O segundo caso, por sua vez, coloca uma discussão sobre não-autoincriminação que merece pesquisa própria se seria suficiente para barrar esse tipo de iniciativa, como adiantei ainda no final da primeira parte. De todo modo, é possível ver como as variações dos contextos ainda importarão nessa análise: a possibilidade de se exigir DNA da placenta de Gloria Trevia para inocentar pessoas de estupro não significa necessariamente que será possível coletar genericamente dados genéticos de pessoas condenadas. O primeiro caso é específico às circunstâncias e a uma suspeita de mentira – fato concreto que já ocorreu; a segunda, é geral sobre um grupo específico da população e prospectiva para prevenção de diversos crimes. Nesse exemplo, aliás, é de se perguntar se é compatível com o direito de tratar pessoas como igual que apenas essa parcela da população seja sujeitada a uma possibilidade estatisticamente muito maior de ter seu envolvimento em crimes descoberto do que o resto da população em geral.

10 Sigilo telemático

Como casos de "sigilo telemático" classifiquei todos aqueles que versam sobre acesso a mídias eletrônicas (como computadores e celulares), captação de fluxo de pacotes de internet ou obtenção de informações armazenadas junto a provedores de aplicações de internet. Nessas informações, inclui tudo que poderia ser incluído em "eletrônico": dados digitais em geral, inclusive *conteúdo* de comunicações, quando eletrônicas. Embora o STF diferencie o tratamento dentro desse universo, como veremos a seguir, quis nessa categoria agrupar o "ambiente digital" e como a sua novidade está sendo enfrentada.

O primeiro caso localizado que se insere nesse grupo é a AP 307, de 1994, em que o ex-Presidente da República Fernando Collor de Mello figurava como réu principal.[183] Nele se suscitava a inadmissibilidade de gravações feitas por Sebastião Curió de conversas telefônicas tidas com o ex-tesoureiro de campanha Paulo César Farias e o ex-Ministro Bernardo Cabral (mas sem conhecimento deles) e obtenção de memória de computadores por busca e apreensão domiciliar no escritório da empresa de PC Farias. Já tratei da parte das gravações acima, então aqui vou focar apenas nos computadores.

Com relação aos computadores, o relator Ministro Ilmar Galvão relata que ficou apurado que foram inicialmente apreendidos por agentes da Receita Federal durante diligência de natureza

[183] Supremo Tribunal Federal, AP 307, Rel. Min. Ilmar Galvão, j. 13.12.1994, Tribunal Pleno.

fiscal (p. 2179) e depois encaminhados à Polícia Federal, onde foram degravados. Em contraste com o que antes ocorria, afirma então que a Constituição Federal de 1988 não admite o ingresso em domicílio durante o dia mesmo de agentes do Fisco no exercício de sua função sem autorização judicial prévia. Este seria, portanto, um vício de origem (p. 2187). O entendimento é consistente com o que se viu acima ao tratar de inviolabilidade de domicílio. De todo modo, ainda que essa parte tivesse ocorrido de forma regular, o acesso à memória do computador não poderia:

> a Polícia Federal não poderia ter-se apropriado dos dados contidos naquele micro-computador, para mandar decodifica-los ao seu alvedrio, como fez, acobertados que se achavam pelo sigilo, o qual, conquanto se possa ter por corolário da inviolabilidade do próprio recinto dos escritórios da empresa, acha-se especificamente contemplado no inciso XII, do mesmo artigo, ao lado da correspondência e das comunicações telegráficas e telefônicas. (p. 2187)

Referia-se ao sigilo de dados. Continuou:

> Aliás, nos tempos modernos, em que todos os aparelhos datilográficos das empresas é realizado por meio de digitação, a invasão da memória dos computadores implica fatalmente a quebra do sigilo não apenas dos dados em geral, desde os relativos a simples agenda até os relacionados a fórmulas e cálculos, mas também de toda correspondência, epistolar e telegráfica, em relação aos quais o manto constitucional é de natureza absoluta, já que não deixou espaço reservado ao trabalho normativo do legislador ordinário, como se fez com as comunicações telefônicas. (p. 2188)

O revisor Min. Moreira Alves adota a mesma linha de raciocínio: além do mesmo vício de origem já pontuado, entendeu que "com relação aos dados em geral – e, consequentemente, os constantes de computador que pode armazenar as mais sigilosas informações de seu proprietário – estão eles cobertos pela garantia do disposto no inciso XII do artigo 5º da Constituição" (p. 2440-1). Não dá, entretanto, o mesmo ar de proteção absoluta que o relator, apesar de ressaltar a necessidade de regulamentação:

> Pelos termos em que está redigido esse dispositivo, é possível sustentar que as demais inviolabilidades só admitem sejam afastadas por texto constitucional expresso. Mas, ainda quando se admita que possam ser postas de lado nas hipóteses e na forma prevista na lei, o que é certo é que não há lei que disponha a respeito no concernente – que é o que importa no momento – à inviolabilidade dos dados aludidos no citado texto constitucional. (p. 2441)

Os min. Carlos Velloso, Celso de Mello, Néri da Silveira, Sepúlveda Pertence, Sidney Sanchez e Octavio Gallotti concordam quanto à ilegalidade da prova obtida pela degravação da memória de computar, sobretudo por ter sido obtida por busca e apreensão domiciliar sem autorização judicial.[184] O Min. Sepúlveda Pertence ressalva que

[184] Não participaram os Ministros Marco Aurélio, Francisco Rezek e Maurício Corrêa.

> Basta-me aí a ilegalidade quanto à apreensão, à vista do inciso XI, da Constituição. Não me comprometo, por ora, consequentemente, com o problema do que se chamou "sigilo de dados": continuo um tanto perplexo, no que toca a saber se, no art. 5º, inciso XII, da Constituição, o que se protegeu foi o sigilo de qualquer dado armazenado por alguém ou o sigilo da comunicação de dados, uma vez que se trata naquele inciso, de diversas formas de comunicação intersubjetiva e não do sigilo de arquivos. Basta-me, portanto, a ilicitude da apreensão, à falta de autorização judicial à diligência dos agentes do Fisco. (p. 2637)

Em 1996, a discussão que chegou ao STF foi a constitucionalidade da previsão de interceptação telemática, estabelecida no parágrafo único do art. 1º da Lei nº 9.296/96 (Lei de Interceptações).[185] A Associação dos Delegados de Polícia do Brasil propôs a ADI 1.488, cujo pedido liminar para suspender o dispositivo – por "atentar contra a inviolabilidade do sigilo das comunicações no âmbito do processamento de dados (art. 5º, inciso XII, C.F.), inadmissível como prova (art. 5º, inciso LVI, C.F.), eis que resultará em laudos de degravação de computadores que, no caso concreto, ocorrerá sempre ao arrepio da garantia de inviolabilidade da intimidade das pessoas (art. 5º, inciso X, C.F.)" – foi julgado pelo Plenário no mesmo ano.

O relator Min. Néri da Silveira reconhece que existe uma controvérsia relativa à interpretação apropriada do inciso XII do art. 5º e a qual grupo de comunicações/objetos se referiria a exceção que admite o afastamento do sigilo "no último caso".[186] A defender a possibilidade cravada na Lei nº 9.296/96 estaria o entendimento segundo o qual "comunicações de telemática e informática" estariam abrangidas em "comunicações telefônicas" (p. 68), o que seria a realidade "no estágio atual do desenvolvimento tecnológico" (p. 70). Nessa linha, o relator cita trabalho de Ivan de Lira Carvalho para o qual a Constituinte teria admitido interferência em *informes em tráfego* – inclusive das comunicações de dados que se dão através de linha telefônica. Avançando para ponto que depois geraria distinções duradouras, o relator também registra a defesa deste autor de que, se a Constituição admitiu a interferência para tanto, também o fez sobre "dados estáticos" parados em computador ("se pode mais, pode menos", era a lógica). Daí recorda o entendimento do STF na AP 307, em que teria decidido "no sentido da inviolabilidade de dados constantes de

[185] Supremo Tribunal Federal, MC na ADI 1488, rel. Min. Néri da Silveira, Tribunal Pleno, j. 07.11.1996. Lei nº 9.296/96: "Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça. Parágrafo único. O disposto nesta Lei aplica-se à interceptação do fluxo de comunicações em sistemas de informática e telemática."

[186] Para um retrospectiva do processo legislativo sobre esse ponto e como a discussão se desdobra até hoje, ver Rafael Mafei Rabelo Queiroz, "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*, org. Danilo Doneda (São Paulo: Thomson Reuters Brasil, 2018), 13–26.

computador". A ação proposta carregaria, então, "fundamentos relevantes". O acórdão fecha, entretanto, com julgamento unânime de que não haveria "periculum in mora" a justificar a suspensão da norma. O pedido de mérito nunca foi a julgamento.

O Min. Sepúlveda Pertence retomaria a discussão sobre sigilo telemático de computadores exatamente de onde ela parou na AP 307. No RE 418416, de 2006, abre esclarecendo que o caso foi afetado ao Plenário após insistência do advogado, pelo qual o seu voto no caso estaria em desacordo com o entendimento firmado na AP do Collor.[187] O ministro sustenta que nunca houve entendimento pacificado de que o sigilo de dados seria absoluto – muito embora esse pareça ter sido o entendimento do relator ministro Ilmar Galvão naquele caso e, em alguma medida, também do revisor Moreira Alves. A maioria focou na ausência de mandado de busca e apreensão *domiciliar* e os que concordaram com relator e revisor não se manifestaram explicitamente quanto à compreensão sobre sigilo de dados. É nesse caso que o Min. Sepúlveda Pertence vai proferir o voto que mais marcará a jurisprudência do STF sobre esse tema.

Tratava-se de busca e apreensão feita em sede de empresa para apuração de crimes fiscais. Diferente do que ocorreu na Ação Penal, aqui a apreensão de computadores se deu mediante cumprimento de mandado judicial de busca e apreensão relativamente específico – no sentido de que ao menos continha a previsão de que equipamentos informáticos poderiam ser apreendidos e selecionados aqueles "interessantes à investigação" – criminal. Nesse sentido, não se colocava a questão de violação a domicílio (art. 5º, XI), que esteve no fundo do caso anterior. Aqui, sendo o mandado específico para incluir esses objetos, era válido, e a prova, lícita. Nesse contexto, sobrava saber se a apreensão da mídia em si representava uma violação.

Neste ponto, o ministro retomará entendimento a que já sinalizava em votos anteriores – nos mais diversos contextos, e notadamente no MS 21.729, de 1995, que tratava de sigilo bancário de beneficiários de recursos públicos. Para ele: "na espécie, não há violação do art. 5º, XII, da Constituição que, conforme se acentuou na sentença, não se aplica ao caso, pois não houve 'quebra de sigilo de comunicações de dados (interceptação das comunicações), mas sim apreensão de base física na qual se encontravam os dados, mediante prévia e fundamentada decisão judicial'" (p.

[187] Supremo Tribunal Federal, RE 418.416-SC, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, j. 10.05.2006; DJe 02.02.2007.

1264). Ampara-se em trabalho de Tercio Sampaio Ferraz Jr. para a distinção – o mesmo que já mencionei outras vezes.[188]

O Plenário acompanha o ministro na tese. Em seus comentários na convergência, o Min. Cezar Peluso diz ser pouco razoável entender-se que a CF trataria de sigilo *dos dados*. Nessa linha "bastaria que a prova do crime fosse sempre registrada no computador, o que tornaria inviável a persecução criminal". (p. 1275). Também o Min. Gilmar Mendes: "entendo que não se pode interpretar essa cláusula do artigo 5º, XII, no sentido de proteção aos dados enquanto registro, depósito registral." O contrário reforçaria uma ideia de "um tipo de paraíso da impunidade ou da criminalidade" (p. 1314). De novo, os intérpretes parecem recear que reconhecer a proteção de sigilo de dados no inciso XII signifique conferir uma proteção absoluta a todo tipo de dado.

Nos debates, o Min. Sepúlveda Pertence ressalvaria que "o que merece proteção está protegido sobre o outro inciso, o que protege a intimidade" (p. 1289), ponto que o Min. Lewandowski também faria. É do Min. Carlos Ayres Britto, também concordando com Pertence, as observações mais elaboradas sobre privacidade e como aquela discussão se encaixava diante das proteções dos incisos X, XI e XII do art. 5º da CF/88:

> A matéria está toda imbricada, não é a toa que a Constituição cuida dos três incisos assim, um atrás do outro - só faço uma distinção: a Constituição não confunde privacidade com intimidade. Tanto que usa de duas palavras diferentes, ligando uma à outra pela conjunção aditiva 'e'. Privacidade, para mim, é uma comunicação reservada entre pessoas, digamos, *'en petit comité'*. É a pessoa se relacionando com seus amigos, com seus parentes. Ao passo que a intimidade é a pessoa consigo mesma, sozinha. Exemplo: alguém escrevendo um diário - está no uso de sua intimidade. (...)
> Os três círculos da doutrina europeia. Ao passo que uma comunicação por 'e-mail' já é privacidade; uma carta já é privacidade. Porém um diário, não; é absolutamente intimidade. Quando a pessoa está consigo mesma, é intimidade; quando está com os seus - amigos, parentes -, aí se dá a privacidade. Agora tanto a intimidade como a privacidade têm o seu locus, o seu habitat na casa em que se mora ou em que se trabalha. Vejam como os três incisos se entrelaçam. E a interpretação do Ministro Sepúlveda Pertence não só nos possibilita conhecer o conteúdo e o alcance do inciso XII, como nos auxilia a conhecer o conteúdo e o alcance dos incisos imediatamente anteriores. (p. 1303-4).

Apesar do cenário pintado sobre privacidade, e o entrelaçamento com outros dispositivos, de modo que a discussão não se encerraria no art. 5º, XII, essa ideia não permaneceria, isto é, não seria transportada a outros julgados. É na síntese do Min. Marco Aurélio que se vê a ideia que permaneceria e repercutiria, suprimindo-se o "no caso": "comungo inteiramente com a afirmação dos colegas de não haver, no caso, a proteção quanto a dados armazenados."(p. 1317). Não se

[188] Tercio Sampaio Ferraz Junior, "Sigilo de Dados: o direito à privacidade and os limites da função fiscalizadora do Estado", *Revista da Faculdade de Direito da Universidade de São Paulo* 88 (1993): 439–59.

presta ao esforço de reconciliar sua visão aqui com as que manifesta sobre sigilo de dados bancários, embora a posição de que no caso houve decisão judicial específica estivesse disponível aqui. O único que não se posicionou sobre o tema foi o Min. Joaquim Barbosa – concordando no resultando, mas destacando outros aspectos no acórdão: para ele a decisão era fundamentada, teve origem em documentos nos quais se vislumbrou a possível prática de sonegação de tributos e na verificação de uma série de discrepâncias entre declarações e faturas (p. 1306).

No HC 91.867, de 2012, a 2ª Turma apreciou a licitude de provas obtidas pela verificação do histórico de chamadas de dois celulares apreendidos com preso em flagrante – os fatos são de 2004.[189] Referi-me a esse julgado quando tratei de sigilo de registros telefônicos acima. O voto do relator Min. Gilmar Mendes, em linha com o que se viu até aqui, abre com um "destaque" que na verdade se refere a duas postulações distintas, mas cujo sentido se mesclaria no voto e na jurisprudência formada a partir daí: a *primeira,* de que "não se confundem *comunicação telefônica* e os *registros telefônicos*, recebendo, inclusive, proteção jurídica distinta" (p. 9). Realmente, conversas não se confundem com os dados relativos ao histórico de chamadas recebidas e efetuadas – que realmente recebem tratamento distinto, como já se viu. A seguir, consigna que "não se pode interpretar a cláusula do artigo 5º, XII, da CF, no sentido de proteção aos dados enquanto registro, depósito registral. A proteção constitucional *é da comunicação 'de dados' e não os 'dados'*." (p. 10). Cita jurisprudência que afirma essa interpretação e a clássica obra de Tercio Sampaio Ferraz Junior.

Após a abertura, recorre aos argumentos de que (i) pelo art. 6º do CPP "a autoridade policial tem o dever de proceder à coleta do material comprobatório da prática da infração penal, impondo-lhe determinar, se for o caso, que se proceda a exame de corpo de delito, apreender os objetos que tiverem relação com o fato delituoso, colher as provas que servirem para esclarecimento do fato e suas circunstâncias, ouvir o ofendido, ouvir o indiciado, dentre outras diligências. Em princípio, foi como agiu a autoridade policial que, ao prender em flagrante delito o corréu, tomou a cautela de colher todo material com potencial interesse para investigação."; (ii) "os números — registros de ligação no aparelho — estavam acessíveis à autoridade policial, mediante simples exame do objeto apreendido, circunstância que, de fato, diferencia do acesso a informações registradas na empresa de telefonia"; e (iii) o exame teria indicado apenas um número de telefone, dado que não

[189] Supremo Tribunal Federal, HC 91.867, Rel. Min. Gilmar Mendes, Segunda Turma, j. 24.04.2012, DJe 20.09.2012.

se conectaria a nenhum valor constitucionalmente protegido nem teria de per se nenhum significado. Procede a um conjunto de perguntas retóricas ante à conclusão:

> *Ad argumentadum*, abstraindo-se do meio material em que o dado estava registrado (aparelho celular), indago: e se o número estivesse em um pedaço de papel no bolso da camisa usada pelo réu no dia do crime, seria ilícito o acesso pela autoridade policial? E se o número estivesse anotado nas antigas agendas de papel ou em um caderno que estava junto com o réu no momento da prisão? Ademais, impende lembrar que a Constituição Federal excepcionou a inviolabilidade domiciliar na hipótese de flagrante delito (art. 5º, XI). A própria liberdade sofre restrição no flagrante delito. Um aparelho de celular receberia proteção diversa? A obviedade que resulta da resposta a essas indagações, denota que, não raras vezes, na construção argumentativa desvia-se o foco da tutela constitucional. A proteção jurídica à intimidade, à vida privada, não me parece que tenha o alcance pretendido pelo impetrante." (p. 14).

Nesse contexto, conclui que a atitude dos policiais foi "perfeitamente razoável, não havendo que se falar de lesão à intimidade ou privacidade" dos corréus. Não deixa de também registrar o chavão típico, "Não há direitos e garantias fundamentais de caráter absoluto, sendo certo, também, que esses não podem, a qualquer pretexto, servir de manto protetor de práticas escusas" (p. 16-7). O julgamento foi unânime.

No HC 103425, também de 2012, a 2ª Turma do STF lidou com um caso sobre validade do consentimento no cenário do sigilo telemático.[190] Um militar divulgou panfletos críticos pela internet, a partir da *lan house,* em que teria "incitado militares à desobediência, à indisciplina, à prática de crimes, além de ofendido a dignidade e desacatado diversos militares". Descoberta a origem dos envios, investigador foi ao local; o proprietário confirmou, por reconhecimento fotográfico, que o réu esteve no local no horário indicado, e permitiu que o conteúdo do computador fosse periciado. O paciente sustentou violação da privacidade sem sua autorização nem autorização judicial.

A relatora Min. Rosa Weber afasta a tese de violação atacando as bases do argumento. De um lado, ressalta que as diligências não implicaram revelação do conteúdo de comunicação – este que já seria conhecido pelos que receberam as mensagens e provocou a investigação. Para ela:

> Não há falar, nessa perspectiva, em qualquer violação do direito de privacidade do paciente em relação ao conteúdo de comunicações que teria mantido com terceiros, já que ele próprio as disponibilizou a esses terceiros e esses escolheram revelá-las às instituições militares, por seu teor criminoso. Feitas as devidas adaptações, seria como se pretender violação de privacidade pelo fato de o destinatário de carta com ameaças as revelar às autoridades policiais. (p. 2)

[190] Supremo Tribunal Federal, HC 103425, rel. Min. Rosa Weber, Primeira Turma, j. 26.06.2012.

De outro, a obtenção dos dados do computador que ligaram as mensagens à identidade do paciente

> foram mantidos em computador pertencente a terceiro que, manuseando-o, poderia ter acesso a esses dados e, igualmente, poderia validamente compartilhá-los com os agentes da investigação. Se o terceiro proprietário do computador permitiu o acesso a ele pelos agentes da investigação, não houve intromissão estatal sem o assentimento da pessoa que possuía a disponibilidade dos dados nele contidos. (p. 3).

Faz a analogia com a possibilidade de busca e apreensão domiciliar com consentimento do proprietário, dispensada a autorização judicial. O julgamento foi unânime.[191]

No HC 176766 de 2020, a 1ª Turma afastou a aplicação do art. 2º, II da Lei nº 9.296/96, que desautoriza a realização de interceptações quando "a prova puder ser feita por outros meios disponíveis" no contexto de celulares apreendidos em local de abordagem policial.[192] O relatório da decisão informa que estavam "abandonados" onde "olheiros" foram presos em flagrante e que o acesso ao conteúdo dos celulares, mediante autorização judicial, levou a informações sobre existência de grupo criminoso voltado ao tráfico de entorpecentes – cujos membros foram então acusados. O acórdão não destaca esses pontos, entretanto: apenas afasta genericamente a aplicação da lei a "dados armazenados em dispositivo de telefonia".

No HC 170376 AgR, do mesmo ano, a 1ª Turma afastou outros limites da Lei nº 9.296/96 a esse contexto.[193] Na hipótese, a defesa questionava o deferimento de quebra de sigilo de e-mails, que alcançou longo período (2008 a 2015), em decisão que seria padronizada e teria deixado de especificar o período de abrangência. O voto da relatora Min. Rosa Weber entendeu que o "*decisum* endereçou justificativa própria, ainda que sucinta, para o deferimento do pedido e, no essencial, fez referência à documentação trazida pelo Ministério Público, sitou (*sic*) o contexto investigativo, registrou a imprescindibilidade da medida e individualizou o que se buscava apurar" (p. 7). Fez-se uso de fundamentação *per relationem*, que seria válida pela jurisprudência do STF. Ademais, não identificou "violação à Lei 9.296/96, a qual '*não estabeleceu um limite temporal para o acesso, pelas autoridades estatais, a comunicações pretéritas*', nem à Lei 12.965/2014 (Marco Civil da Internet), cujo artigo 22, p.u , III, é inaplicável às quebras de sigilo telemático -

[191] Depois desse caso, o STF já decidiu outros casos em que assenta a possibilidade de acesso a celulares e computadores mediante consentimento: RHC 132062, Rel. Min. Marco Aurélio, Primeira Turma, j. 22.11.2017; HC 152836 AgR, Rel. Min. Gilmar Mendes, Segunda Turma, j. 22.06.2018; RHC 169682 AgR, Rel. Min. Luiz Fux, Primeira Turma, j. 03.04.2020.
[192] Supremo Tribunal Federal, HC 176766, Rel. Min. Marco Aurélio, Primeira Turma, j. 04.05.2020.
[193] Supremo Tribunal Federal, HC 170376 AgR, Rel. Min. Rosa Weber, Primeira Turma, j. 08.06.2020.

voltadas ao conteúdo de comunicações privadas -, pois orientado a '*informações de início e de término de uma conexão à internet ou de uso de determinada aplicação, incluindo o número do endereço IP utilizado*'" (p. 8). Nesse contexto, "não configurada ilegalidade na operacionalização da quebra entre 2008 a 2015 (período 'contemporâneo às práticas delitivas'), porque proporcional ao período da denúncia, a qual data de 2017 e abrange o período de supostas fraudes licitatórias de caráter permanente a partir de 2009".

No HC 168052, pela 2ª Turma, de 2020, o cenário voltou a se agitar. O paciente foi preso por tráfico de entorpecentes, encontrados em seu domicílio, após denúncia anônima que levou a uma abordagem policial na calçada de sua casa, momento em que houve verificação do celular (inclusive mensagens de WhatsApp), cujo teor originou a ação de busca e apreensão em sua residência. Para o relator Min Gilmar Mendes, que em 2012 votou pela possibilidade do acesso a registros telefônicos em celular, houve "mutação constitucional", em razão "[d]a modificação das circunstâncias fáticas e jurídicas, [d]a promulgação de leis posteriores e [d]o significativo desenvolvimento das tecnologias da comunicação, do tráfego de dados e dos aparelhos *smart phones*"[194]. O ministro deixa em aberto o debate sobre o âmbito de proteção do inciso XII, mas reconhece a proteção sobretudo a partir da proteção da intimidade e vida privada do art. 5º, X e avanços infraconstitucionais como o Marco Civil da Internet – pelo qual comunicações privadas armazenadas só poderiam ser acessadas mediante ordem judicial (art. 7º, III). Conclui que

> uma vez que a apreensão das drogas e da arma, que ensejou a condenação do paciente, somente ocorreu após o acesso indevido a seu celular e o ingresso desautorizado em sua residência [ambos sem prévia autorização judicial], concluo pela ilicitude das provas que deram origem à apuração e de todo o processo penal, com base no art. 5º, X, XI e LVI, da CF/88 e nos fundamentos acima transcritos. (p. 13)

Observa ainda que "a permissão de acesso direto a aparelhos telefônicos, por autoridades policiais, pode servir de estímulo para que pressões indevidas sejam exercidas sobre os acusados para o fornecimento de senhas de acesso e informações confidenciais." (p. 13). Refere-se a relatos

[194] Supremo Tribunal Federal, HC 168052, rel. Min. Gilmar Mendes, Segunda Turma, j. 20.10.2020, p. 3. Continua: "Nos dias atuais, esses aparelhos são capazes de registrar as mais variadas informações sobre seus usuários, como a sua precisa localização por sistema GPS ou estações de rádio base, as chamadas realizadas e recebidas, os registros da agenda telefônica, os dados bancários dos usuários, informações armazenadas em nuvem, os sites e endereços eletrônicos acessados, lista de e-mail, mensagens por aplicativos de telefone, fotos e vídeos pessoais, entre outros. Além disso, a conexão de todos esses aparelhos à rede mundial de computadores faz com que estejamos todos integralmente conectados, o tempo todo, fornecendo dados e informações para órgãos públicos e privados. Conforme noticiado pelos meios de comunicação, os celulares são a principal forma de acesso dos brasileiros e cidadãos do país à internet. Esse motivo, por si só, já seria suficiente para concluir pela incidência das normas acima descritas no que toca à proteção dos dados, fluxos de dados e demais informações contidas nesses dispositivos." (p. 5).

de policiais segundo os quais pessoas teriam assentido com acessos ou prestado depoimentos informais, sempre contestados pela defesa. E continua:

> Nesse sentido, o acesso direto a aparelhos telefônicos e a residência de suspeitos, sem autorização judicial, fora das hipóteses de flagrante e com o não estabelecimento de procedimentos bem delimitados que garantam a observância dos direitos fundamentais dos indivíduos também conflita com o direito fundamental à não autoincriminação (art. 5º, LVII, da CF/88). É por isso que essas medidas devem ser submetidas à prévia decisão judicial, enquanto garantia procedimental in concreto através da qual sejam analisados e registrados, especificamente, os fundamentos que possam afastar os direitos fundamentais envolvidos. Ou seja, a existência de prévia decisão judicial é capaz de demonstrar a necessidade, adequação e proporcionalidade da pretensão dos órgãos de segurança de acesso aos dados, informações e residência dos suspeitos. Permite, ainda, o controle desses fundamentos. A transcrição, assinatura e registro formal do depoimento dos investigados, com a declaração de ciência de seus direitos constitucionais, impede que investigações sejam realizadas e condenações sustentadas com base em confissões informais prestadas durante o ato de prisão e sob fortes suspeitas de violação de direitos. (p. 14)

Termina com um convite a que "STF poderia caminhar para a criação de uma fórmula de garantia dos direitos das pessoas investigadas cuja inobservância leve à nulidade dos atos de investigação e coleta de provas, mesmo que durante o inquérito policial – tal como ocorreu no relevante precedente estabelecido pela Suprema Corte dos Estados Unidos em 1966, no julgamento do caso Miranda v. Arizona (384 U.S. 436)." (p. 14). A ideia veiculada é que não seria possível apelar a um *consentimento* do acusado ou a declarações prestadas antes que ficasse comprovado que foram observados certos procedimentos de resguardo ao direito à não-incriminação.

A ministra Cármen Lúcia pediu vista "nem tanto porque estou com tendência à divergência, mas porque realmente, hoje, é um dos temas que mais me chamam a atenção." (p. 19) No retorno, apresentou voto-vista em que sustenta que, apesar de o paciente ter alegado não ter autorizado o acesso de policiais ao celular nem à casa, "não foi juntado aos autos documentos referentes à fase de instrução do processo, o que dificulta a análise dessas alegações" (p. 26). No caso, a versão acusatória só é corroborada por depoimentos de policiais, o que seria insuficiente para higidez da prova e confere plausibilidade às alegações. A ministra, no entanto, se recusa a extrair daí a possibilidade de anular todo o processo, pois a sentença teria sugerido existência de fonte autônoma em relação àquela colhida no celular – que a perícia realizada posteriormente teria inclusive concluído ser inútil. Não há indicação de qual fonte autônoma seria essa e silencia-se quanto à questão da violação do domicílio. O julgamento se encerra pela maioria apertada de 3x2.[195]

[195] Ministros Gilmar Mendes, Celso de Mello e Ricardo Lewandowski x Ministra Cármen Lúcia e Ministro Edson Fachin.

Essa discussão agora se coloca no Plenário – misturada com as discussões sobre proteção devida a "registros telefônicos". No ARE 1042075, Tema 977 de repercussão geral do STF –, discute-se a possibilidade de acesso quando, após um assalto "saidinha de banco", celular caído é encontrado no local do crime e acessado sem autorização judicial prévia. A polícia consultou a agenda de contatos, as últimas chamadas no histórico e as fotografias – diligência que serviu à identificação do autor e para condenação. O relator Min. Dias Toffoli votou mantendo o paradigma de 2012, agora capitalizando na distinção entre "registros" e "acesso ao conteúdo de eventuais informações transmitidas via aplicativos (ex: WhatsApp), e-mail ou mensagem eletrônica". Logo depois, abriu a divergência o Min. Gilmar Mendes, adotando a linha de seus votos mais recentes, já acompanhado do Min. Edson Fachin. O julgamento foi interrompido após pedido de vista do Min. Alexandre de Moraes.

Vou comentar essas controvérsias particulares sobre sigilo telemático no próximo capítulo.

11 Conclusões parciais

Nesse capítulo, apresentei um brevíssimo retrato da doutrina constitucional e igualmente brevíssima recapitulação do histórico de dispositivos constitucionais, em preparação para uma reconstrução da jurisprudência constitucional brasileira sobre privacidade e segurança. A partir da retrospectiva que elaborei, tive a oportunidade de fazer diversos comentários sobre o estado da jurisprudência à luz da teoria apresentada na primeira parte deste trabalho e pude chamar atenção a alguns traços gerais de como são analisados casos que tocam questões de privacidade em matéria criminal no Brasil.

Se a conclusão for de que o espaço ou a informação não é protegida, não há condicionamentos para acessos e usos na atuação policial. Se é considerada protegida, pode haver a invocação de alguma exigência para que o espaço ou a informação possam ser acessados/obtidos/usados – como a exigência de autorização judicial prévia ou alguma previsão legal. Quando alguma exigência é posta, sobretudo quando há algum tipo de previsão legal explícita, critérios materiais (causa e proporcionalidade) podem se tornar objeto de atenção ou análise mais detida (exemplo: denúncia anônima ou matéria de jornal como justa causa insuficiente). Embora se fale em proporcionalidade e por vezes em ponderação, há amplo espaço para padrões que não se explicam por essa lógica – como e sobretudo a exigência de justa causa.

Falta profundidade e clareza quanto aos princípios normativos subjacentes aos traços fundamentais da articulação entre privacidade e segurança no direito constitucional. Embora haja discussão sobre noções que giram em torno da "suspeita individualizada" aqui e ali, ela aparenta não ser percebida como um elemento fundamental de avaliação substantiva – por vezes se perde em um reforço genérico de que certa ação policial simplesmente precisa de autorização judicial. Ainda, embora claramente se façam análises sensíveis ao contexto, essa percepção parece que nem sempre existe e entendimentos são arrastados entre um e outro às vezes de forma completamente aleatória e aplicados sem qualquer reflexão.

Mesmo se desconsiderarmos o quadro que apresentei na primeira parte dessa tese, é notória a falta de consistência interna dessa jurisprudência constitucional, que vem à tona por amplos contrastes entre áreas "tradicionais" e a área de sigilo telemático – um campo novo de discussões sobre privacidade. No campo de dados telemáticos, como ou (i) se conclui que não há proteção porque o dado não passa o teste criterial ou (ii) apenas um requisito formal de exigência de ordem judicial é reafirmado, outras discussões e nuances se perdem.

Por exemplo, a jurisprudência sobre sigilo de documentos e cartas mostra as origens da compreensão que enfatiza a proteção do *fluxo* de comunicações ao interpretar o art. 5º, XII, da CF/88 – um tipo de teste criterial binário que faz separação daquilo que seria protegido do que não seria. Considerando-se a necessidade de confiar cartas e sistemas de telefonia a *terceiros,* encarregados de viabilizar a *comunicação* à distância, era preciso afirmar um dever de sigilo enquanto essa comunicação *viaja*, para que a privacidade das pessoas e sua confiança nesse sistema de comunicação não estivessem completamente vulneráveis. Se essa mesma preocupação ainda é válida hoje para comunicações telemáticas que dependem enormemente de terceiros (*provedores de aplicações de internet*, por exemplo) à comunicação para que esta seja viabilizada, e que assim pode se expor enquanto está "em fluxo" ou em geral detida por este terceiro, nada disso sugere que o teor da comunicação em si e a atividade a que se relaciona não possam compor uma prática de privacidade que valorizamos e por isso ser relevantes para uma prerrogativa de privacidade de alguém.

Cartas já recebidas e diários mantidos podem estar envoltas de expectativas relevantes de privacidade daqueles que as legitimamente detém – e não só por força de estarem guardadas em ambientes privados (dentro de um domicílio). Nesse sentido, o caráter *estático* de *dados telemáticos* não deveria ser nunca suficiente para afastar questões constitucionais de privacidade.

Ademais, a constatação de que a mesma jurisprudência constitucional permite a *interceptação* de cartas e documentos havendo na presença de determinados requisitos formais e materiais mostra que é falsa a noção de que o fluxo de comunicações só seria violável para comunicações telemáticas e telefônicas na forma da Lei nº 9.296/96. Por trás da reverberação irrefletida da diferenciação binária entre estático/dinâmico para fixar o que no mundo digital é protegido pela Constituição, compreensão que repercute em todos os tribunais do Brasil,[196] perdem-se as discussões sobre quando há expectativas legítimas de privacidade em jogo apoiadas em nossas práticas sociais e sob quais condições acessos estatais a informações digitais estão legitimados.

Com efeito, a jurisprudência sobre inviolabilidade do domicílio mostra como se considera que mesmo espaços protegidos como parte de noções de privacidade e "intimidade doméstica" podem ser *acessados* em certas situações – mediante autorização judicial, flagrância ou desastre. O que caracteriza essas circunstâncias autorizadoras é de extrema relevância, como visto na primeira parte, e é a aplicação rigorosa e consistente delas que seria capaz de balizar atuações policiais em respeito a direitos de privacidade. Nessa linha, caso se entenda que hoje dispositivos como celulares, computadores e serviços de computação em nuvem suscitam proteções semelhantes de privacidade como as que estão na base da proteção ao domicílio e, se não as mesmas, também preocupações com abusos, erros e excessos, a mesma atenção ao ônus de justificação e proteção regulatória que deve ser superado em diferentes contextos deve ser conferida.

Já os casos sobre registros telefônicos mostram como a jurisprudência sobre *metadados* incidentes a uma comunicação – ao uso de uma tecnologia – reconheceu desde o início como podem também ser relevantes para a privacidade, chegando-se a cogitar que a Lei nº 9.296/96 também se aplicasse a acessos a tais informações. No entanto, a distinção entre "comunicações de dados" e "dados em si" para interpretar art. 5º, XII chegou a tal ponto que apagou a discussão sobre critérios de acesso e, para o processo penal, reduziu a importância de tais informações para a privacidade a níveis irrisórios. Nesse contexto, é interessante observar como até casos que envolvem não um amplo conjunto de registros, mas *dados cadastrais* já suscitaram questões de privacidade ou, ao menos, questões sob a etiqueta de *proteção de dados pessoais*. Se o contexto processual penal confere certas prerrogativas para acessos a certos tipos de dados, inclusive de forma menos rigorosa que outras informações que se tenha por mais sensíveis, são de novo os

[196] Ver, por exemplo, em Antonialli et al., "Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes".

critérios que constituem a *justa causa* – os padrões de justificação – que devem ser discutidos e afinados, sem deixar de afastar outras preocupações básicas de arranjo regulatório (como até mesmo a noção de necessidade). Assim, simplesmente afastar a discussão sobre proteção de certos dados nos afasta das questões importantes.

Já os casos de sigilo bancário mostram como informações bancárias de clientes são associadas a um aspecto da intimidade (art. 5º, X), em contraste com noções de publicidade de operações envolvendo o Poder Público, e como, ao mesmo tempo em que há expectativas de que empresas que detêm dados colaborem com a busca da verdade, há diversas leis para dar base e nortear tais quebras de sigilo e compartilhamento de dados. Nesse sentido, as informações que empresas de tecnologia hoje carregam sobre seus usuários deveriam ser igualmente – quando não mais – consideradas do ponto de vista da necessidade de proteção da intimidade e da vida privada, ao mesmo tempo em que é de se esperar que as eventuais colaborações desses atores com agentes públicos para investigações e segurança pública estejam balizadas em lei.

Por fim, a proteção a conversas telefônicas que hoje existe no Brasil é fruto da herança de um passado sombrio em que as próprias autoridades se tornavam alvo de grampos irregulares. Se é fundado o receio e legítima a preocupação que motivaram a proteção reforçada de conversas telefônicas na ordem jurídica brasileira e que a fizeram receber tratamento especial para obtenção de provas desse tipo, cabe também observar que as práticas de comunicação mudaram e se espalharam por outras ferramentas. Nesse sentido, concentrar a proteção a essa modalidade de medida, sem balizar outras, deixa novos campos desprotegidos ou ao menos fragilizados, de forma incoerente com práticas de privacidade que valorizamos. Os mesmos receios que motivaram o balizamento de interceptações telefônicas deveriam se mover para conter outros ardis: se um regime autoritário tivesse os recursos tecnológicos de hoje em dia, como os usaria? E a partir daí desenhar a regulação e checar se possui mecanismos de contenção de poder. Por outro lado, se o padrão rigoroso da Lei nº 9.296/96 foi concebido porque se entendeu que conversas privadas são tão relevantes para a liberdade individual que só poderiam ser capturadas por terceiros em condições bastante rigorosas, não há por que não levar o mesmo raciocínio e nível de proteção a

contextos que mereçam proteção equivalente a não ser por um apego ao texto literal que deixa a proteção constitucional refém do tempo.[197]

Nesse contexto, para início de conversa, um esforço básico de integridade já será crucial ao STF para enfrentar novos desafios da era tecnológica.

No próximo e último capítulo, para fechar o ciclo, revisito o repetido truísmo que vimos em julgados do STF de que a privacidade não serve para cobrir ilícitos, para outra vez desconstruí-lo; comento estratégias regulatórias que ainda estão longe do cardápio nacional para temas do campo (o que talvez não seja culpa do STF, mas que não é ajudado por sua ênfase em usar a "necessidade" ou não de ordem judicial prévia como meio de pensar o tema); e por fim busco oferecer caminhos para recolocar a jurisprudência nos trilhos para enfrentar a era digital movida a dados.

[197] Nesse sentido, também Gisela Aguiar Wanderley, "Privacidade e Cidadania: os limites jurídicos da atividade investigativa e a legalidade do acesso policial a aparelhos celulares", in *Direitos Fundamentais e Processo Penal na Era Digital*, org. Dennys Antonialli e Nathalie Fragoso, vol. 2 (São Paulo: InternetLab, 2019), 125–26.

Capítulo 5 – Reparos e encaminhamentos

Neste capítulo, discuto três características específicas da jurisprudência do STF vista no capítulo anterior, a partir das premissas teóricas assentadas na primeira parte deste trabalho. Juntas, acredito que compõem os problemas mais urgentes que nossa jurisprudência constitucional tem de revisitar se quiser não só sofisticar como lida com questões de privacidade e segurança em geral, mas manter sua tarefa de ser guardiã da Constituição Federal e dos princípios lá consagrados frente a avanços tecnológicos cada vez mais rápidos e avassaladores de práticas sociais.

Começo retomando a ideia de que situações que afetam interesses de privacidade e autodeterminação informacional, e podem também afetar direitos à privacidade (e outros que não são meu enfoque) exigem por parte do Estado a adoção de procedimentos, requisitos e exigências de fundamentação que mostrem *respeito* às pessoas, não as onerando de forma excessiva em suas atividades e cuidando para que danos morais a seus direitos não ocorram. Nesse sentido, quando estamos falando de privacidade no contexto de investigações e segurança pública, dizer que a privacidade não serve para ocultar atividades ilícitas – como faz o STF em várias oportunidades – não serve para encerrar qualquer discussão. É apenas uma distração; uma falácia. O valor da privacidade no contexto de investigações e segurança pública está imbricado com a ideia de contenção do poder, de abusos, de demonstração de respeito – e é esse o sentido que está posto e que pode ser cobrado. Não se pode confundir esse recurso retórico com qualquer aparência de ser fundamento normativo. Se é para parar aí, qualquer esforço de conter a vigilância estatal àquilo que faça sentido em uma democracia liberal igualitária resta frustrado antes de começar.

A seguir, discuto o papel do controle judicial para dar conta de problemas de privacidade e segurança. Como se viu no capítulo passado, desde sempre se deu um papel fundamental à supervisão judicial para casos em que há restrições de direito a "sigilo". A função é resultado de uma combinação de crenças de que o sigilo não pode ser obstáculo para *habilitar a justiça* nem para *esconder ilícitos*, ao mesmo tempo em que se coloca no juiz a imagem tradicional de árbitro independente e neutro. Essa avaliação não pode, no entanto, ser vista só como um obstáculo formal, esquecendo-se das exigências materiais que a autorização judicial deve analisar e atender. Ainda: os direitos à privacidade não se reduzem àqueles a que atribuímos reserva de jurisdição. Nesse sentido, não é todo problema de privacidade que é suficientemente endereçado assim em termos de contenção de riscos; para alguns, pode nem fazer sentido. Em linha com essa constatação, e para enriquecer a prática jurídica brasileira que discute reforma, apresento um arsenal de recursos procedimentais para regulação em matéria de proteção das privacidades e de dados pessoais em face do Estado na área de segurança pública e investigações criminais. O debate deve se mover para tais recursos e como melhor aperfeiçoar o que existe hoje. Observo ainda que há desafios institucionais que tornam o STF, e outros tribunais, palco incapaz de dar conta de implementar esse ferramental sozinho, embora esteja em posição única de impulsioná-lo.

No fim, apresento desafios *tecnológicos* que se impõem para a área do "sigilo telemático", que no capítulo anterior já concluí padecer de diversas incoerências internas perante o resto da jurisprudência do STF. Comento três casos específicos (i) acesso a informações armazenadas em celulares; (ii) a obtenção de dados junto a empresas controladoras de dados; e (iii) uso de reconhecimento facial em locais públicos – e aponto para a postura com que enfrenta-los – os dois primeiros mais tipicamente insertos em "sigilo telemático" e o terceiro que hoje recebe atenção na linguagem de "dados pessoais" ou de privacidade em público. Como mostro, a percepção sobre diferentes contextos é crucial para o endereçamento dessas questões.

1 Privacidade e Crime: sem lugar para lugares-comuns

No capítulo 1, afirmei que, nos contextos em que privacidade e segurança se encontram ou aparentam "colidir", não é incomum a invocação de truísmos como o de que quem não deve não teme e de que privacidade não serve para acobertar ilícitos para reforçar a validade de medidas

invasivas adotadas em nome da segurança. Como expus, o apelo dessas colocações quer ser intuitivo: reporta-se à noção de que não temos a prerrogativa de reivindicar um direito à privacidade para sermos capazes de cometer crimes – instâncias de violação a direitos morais de outras pessoas e a obrigações políticas de observância de regras da comunidade, que devem ensejar nossa responsabilização. Pela elaboração vista no capítulo 1, realmente não temos esse direito moral. Como se viu, entre nossas liberdades protegidas não há nada que sugira minimamente um direito de interferir na dignidade alheia pela prática de ilícitos.

Isso autoriza o STF a usar essa afirmação como se fundamento fosse – um atalho para encerrar logo a discussão? O desconforto entre reconhecer a inexistência desse direito e comprar a justificativa encontrada ainda hoje em tribunais para facilitar prerrogativas estatais mora no fato de que não é este o ponto: mesmo entre ativistas de privacidade, é difícil encontrar alguém que defenda seriamente que a privacidade seja absoluta ou que sustente que a privacidade serve mesmo para praticar ilícitos e assim deve ser. Reivindicações de privacidade e proteção de dados pessoais em face do Estado no contexto de regulação pública da segurança não possuem essa intencionalidade. Nesse sentido, reduzir o debate a essas alegações deixa de capturar o sentido de uma reivindicação potencialmente relevante e apenas alimenta a impressão de que postulações baseadas em privacidade não devem ser levadas à sério, de que não há nada de valor a se opor contra postulações do Estado em nome da segurança.

De fato, essa visão é incoerente com a própria jurisprudência do STF, que não admite vigilantismo: não aceitamos que terceiros interfiram na privacidade alheia *para* demonstrar que ocorre crime. O STF tem uma série de julgados que impedem o aproveitamento de determinadas provas porque obtidas de forma criminosa – e, assim, aplicando o art. 5º, LVI, CF/88. Em 2000, por exemplo, o Min. Celso de Mello julgou caso em que um terceiro invadiu consultório odontológico, obteve fotos guardadas em cofre que exibiam práticas ilícitas e as entregou à polícia. Muito embora o material fotográfico comprovasse a prática ilícita, não poderia ser aproveitado: ao consultório de cirurgião dentista se estenderia a inviolabilidade do domicílio, pois "consentânea com a liberdade individual e a privacidade pessoal."[1] Intervenções nesse direito dependem do

[1] Supremo Tribunal Federal, RE 251.445-GO, Rel. Min. Celso de Mello, j. 21.06.2000, DJE 03.08.2000 (monocrática de não-conhecimento). Eu poderia ter mencionado outros exemplos: Em 2002, o Tribunal Pleno do STF referendou liminar que impediu a TV Globo de divulgar conversas telefônicas interceptadas que mostrariam que o ex-governador do Rio de Janeiro Anthony Garotinho participava de esquema de suborno. O relator Min. Sepúlveda Pertence entendeu que o material é produto de violação de terceiro a sigilo de comunicações e, assim, tinha origem criminosa – uma interceptação ilegal. Afirmou ainda que "a garantia do sigilo das diversas modalidades técnicas de comunicação

preenchimento de condições e requisitos de fundamentação que não foram observados no caso para que fosse válida.

O chavão de que "a privacidade não serve para acobertar ilícitos" poderia ser invocado para bancar a licitude da prova, pelo menos a inexistência de violação a uma norma de direito constitucional que protege a privacidade. Mas não se faz nem se fez isso. Veja-se que a premissa é que a privacidade cobria ilícito, mas não se admite vigilantismo para justificar a violação à privacidade ali perpetrada. "A privacidade não serve para acobertar ilícitos" não constitui justificativa suficiente para validar *intrusões* a uma prerrogativa de controle sobre quem ingressa a um espaço como o do domicílio, que reservamos ao indivíduo, em conformidade com práticas de privacidade fundadas em compromisso com a personalidade de cada um.

Essa observação reforça o argumento de que restrições realizadas por autoridades estatais sobre direitos jurídicos de privacidade que em geral teríamos sobre terceiros do público em geral só são legítimas quando presentes certos requisitos e observado certo procedimento, como exigência de fundamentação de sua legitimidade em face da pessoa em cujos interesses se intervém, contra erros, excessos e abusos. É uma questão de contenção de poder. É nisso, portanto, que repousa a justificação para a restrição legítima a esses sentidos de privacidade. Se essas condições não forem atendidas, ainda que a privacidade em questão esteja "acobertando ilícitos", a intervenção estatal não será legítima. Por essa razão, é inconsistente, insuficiente e frustrante que também o STF invoque razões desse tipo para fazer valer certas quebras de sigilo – esse chavão não resolve a questão e não serve para justificar um enorme conjunto de casos: os de vigilantismo, como mencionei, mas também os das próprias autoridades, quando extrapolam permissões legais – a disciplina de ilicitude das provas no processo penal simplesmente não existiria se esse tipo de razão estivesse disponível para justificar atuação estatal.

Isso não significa, por outro lado, que não há lugar para as intuições de que a privacidade pode ser afastada quando o seu titular agride direito forte alheio e/ou outros bens e valores tutelados pelo direito penal, em situações em que obter informações pessoais dele pode jogar luz sobre fatos

---

pessoal – objeto do art. 5º, XII – independe do conteúdo da mensagem transmitida". Cf. Superior Tribunal Federal, Pet. 2702, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, j. 18.09.2002. Mais recentemente, a Segunda Turma do STF voltou a chegar à mesma conclusão em caso análogo com as mesmas partes. Cf. Superior Tribunal Federal, RE 638360 AgR-segundo, Rel. Min. Dias Toffoli, Segunda Turma, j. 27.04.2020. Como tais casos envolvem liberdade de imprensa, que influi considerações diferentes, não os destaquei. Mas não deixam de ilustrar a ideia de que "a privacidade não serve para acobertar ilícitos" não é uma razão jurídica relevante. Acobertando ilícitos, noções de direito à privacidade já venceram até a liberdade de imprensa.

que interessam à apuração sobre a culpa ou a inocência desse titular acerca de um fato criminoso (sua responsabilidade pessoal). Existe: os requisitos e procedimentos de fundamentação que exigimos de autoridades policiais giram em grande parte em torno dessa ideia e decorrem de uma decisão política coletiva sobre os riscos de causar e sofrer danos morais inerentes a essas atuações. Padrões de justificação – de verificação de justa causa – para quebras de sigilo, nada mais fazem do que isso: estabelecem uma métrica individualizada das causas suficientes para acreditar que medidas de vigilância (que acarretem obtenção de informações) sobre certas pessoas mostrarão elementos de prova de atividade criminosa.[2] Querem garantir que a invasão não se dá por razões aleatórias, por arbitrariedades, por discriminação, por erro, desnecessariamente.

Cabe, portanto, o convite para que a inclusão do chavão em votos e acórdãos seja substituída por razões substantivas que se debrucem sobre as salvaguardas ao controle do poder do Estado, cabíveis em todo caso de privacidade em matéria criminal.

2 Regulação: um esquema de ferramentas e parâmetros

2.1 *A centralidade do papel do controle judicial e seu significado*

Como se viu ao longo do capítulo 4, desde sempre se deu um papel fundamental à supervisão judicial para casos em que há mitigações a direitos à privacidade. Na maioria dos casos em que se identifica um interesse de privacidade relevante e não há consentimento, emergência nem motivo distributivo associado a uma medida generalizada, a conclusão é que a ordem judicial é necessária para a intervenção de alguém. Em muitos casos, isso se dá sob o pano de fundo de alguma legislação – até do texto da Constituição Federal; em outros, a exigência nasce da jurisprudência na lacuna de lei. Naqueles em que a autorização prévia é dispensada, o elemento não deixa de mostrar seu protagonismo: há vários casos em que foi essa a possível exigência procedimental em discussão.

A relevância da autorização judicial em questões de intervenções a direitos à privacidade, ou pelo menos a origem dela, não é equivocada. Como e quando uma prerrogativa de privacidade

[2] Renan, "The Fourth Amendment as Administrative Governance", 1052; Friedman, *Unwarranted: policing without permission*, 352 (e-book); David Gray, *The Fourth Amendment in an Age of Surveillance* (Cambridge: Cambridge University Press, 2017), 94.

que o indivíduo em regra teria em face de terceiros está ameaçada, é importante que haja ferramentas que contenham excessos, erros e abusos de autoridades estatais, como vimos. Malcolm Thorburn propõe ver da seguinte maneira: como nessas situações deve ser superado o que seria o consentimento do titular do direito para executar a medida e viabilizar a investigação, a autoridade judicial deve se encarregar, de um ponto de vista independente do das autoridades de investigação, de avaliar se há legitimidade no pedido de restrição do direito no caso concreto, devendo assegurar que se limite ao necessário e tão apenas isso.[3] Há um dever fiduciário de respeitar interesses e certo conjunto de razões jurídicas nessa tarefa. A partir daí, quando um agente estatal independente entende pela quebra de sigilo, ela seria juridicamente possível.

Tendo em vista esse papel, é possível dizer que se coloca até mesmo uma *preferência* por controle judicial prévio nos casos em que direitos e interesses que nossas práticas sustentam estão em risco de serem violados gratuitamente apenas sob a narrativa e o gosto policial/ministerial, sobretudo na ausência de emergências. Paul Ohm relaciona a tradição análoga da jurisprudência da Quarta Emenda no direito americano – de exigir *warrants* sempre que se concluir que a medida constitui uma *busca* sobre uma *expectativa legítima de privacidade* – a uma realização da separação de poderes: o juiz verifica se o agente de investigação, do braço executivo, atendeu aos requisitos para a quebra de sigilo enquanto um mecanismo de freio e contrapeso.[4] Diante das exigências materiais de fundamentação, para contenção do poder e proteção da autonomia, esse é um mecanismo potencialmente hábil desse controle, em respeito aos possíveis direitos em jogo.

Nesse cenário, essa não é apenas uma exigência formal, como se existisse discricionariedade judicial para se fazer o cálculo que se quiser para deferir quebras de sigilo. Ao contrário do que a jurisprudência do STF às vezes perde de vista (como no que vimos sobre sigilo telemático e do que uma leitura simples do texto de algumas leis brasileiras mais recentes faz parecer, como comentarei ao fim do capítulo), há pressupostos materiais de suspeita individualizada e pressupostos de proporcionalidade (adequação e necessidade, no caso) embutidos no nosso esquema de justificação de medidas de vigilância, para que se compatibilizem com a dignidade. De forma relevante, o papel do juiz é, frente a parâmetros da regulação, efetivamente prosseguir a *justificar* no caso concreto o modo como considerações sobre

[3] Thorburn, "Justifications, Power, and Authority", 1124.
[4] Paul Ohm, "The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause", in *The Cambridge Handbook of Surveillance Law*, org. David Gray e Stephen Henderson (Cambridge: Cambridge University Press, 2017), 500.

privacidade estão sendo levadas em conta a partir da importância que esse direito tem. Não é algo que se satisfaz apenas pela existência per se de uma decisão judicial nem apenas dizendo que privacidade não é direito absoluto ou que restrição para segurança é proporcional.

Isso não é matéria a ser deixada apenas a juízes fixarem caso a caso. Embora o trabalho judicial seja importantíssimo para interpretação contextual de categorias e para um esforço de consistência na sua aplicação frente a situações concretas, os parâmetros concretos de suspeita individualizada e de necessidade em diferentes cenários são elementos que merecem deliberação coletiva prévia legislativa. É o foro apto para calibrar e assentar o nível de risco que aceitamos incorrer de a medida de vigilância executada causar injustiça a depender dos critérios fixados e, ultimamente, o risco de ser condenado e/ou criminalizado mesmo se inocente, frente a outras prioridades que a comunidade possa ter. Como vimos, essa avaliação deve ser sensível ao nosso histórico de compromisso com princípios e consistente com ele, o que não afastaria a possibilidade de questionamento (controle de constitucionalidade) de leis que destoem de nossos paradigmas e levem a retrocessos. Isso também exige do juiz um esforço de integridade na sua aplicação concreta.

2.2 *Outras ferramentas regulatórias*

Como observação ainda mais geral, cabe notar que os instrumentos regulatórios possíveis de reconciliação do respeito a direitos à privacidade com o seu afastamento excepcional para promoção da segurança não se reduzem ao crivo judicial prévio. Em *The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause* (2017), Paul Ohm apresenta uma caixa com 16 ferramentas regulatórias divididas em 5 categorias: (1) justificação, (2) revisão substantiva; (3) limitações; (4) responsabilização; (5) transparência.[5]

Em termos de (1) justificação, o autor identifica a delimitação de (1.i) padrões de justificação, como níveis de suspeita, para permitir determinados tipos de medida, em linha com o que já apresentei, ao lado da delimitação de (1.ii) objetos com relação aos quais os padrões de justificação devem se referir – ex: causa provável de que no local em que será realizada uma busca se encontrará prova do crime ou de que o alvo da vigilância praticou determinado crime. Assim, os "padrões de justificação" podem variar segundo o grau de restrição, invasividade, contexto e

[5] Ohm, "The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause".

características da medida: o nível de suspeita que se exige e ao quê a causa provável deve se referir (o objeto da análise),[6] mas é característico da avaliação de legitimidade de toda medida de vigilância que respondem a propósitos de segurança e implicam a possibilidade de dano a direitos.

Para se garantir uma (2) "revisão criteriosa", Ohm aponta as possibilidades de (2.i) instituir a necessidade de revisão judicial ou (2.ii) de estabelecer uma revisão dentro da própria agência/órgão. Isso, a meu ver, certamente depende das características da medida em questão e do contexto em que se insere – para muitas emergências, o controle judicial prévio poderia ser insustentável, de modo que outros instrumentos de controle da fundamentação e de prestação de contas são pertinentes. Ohm indica ainda a possibilidade de (2.iii) estabelecer maiores exigências de detalhe com respeito aos fatos que devem ser articulados para que uma decisão de quebra de sigilo possa ser tomada. Já em termos de (3) limitações concretas, mapeia a possibilidade de estabelecer (3.i) limitações temporais para a vigilância, (3.ii) regras de minimização para filtragem e descarte de informações não-relevantes; (3.iii) condições de expiração da medida, assim que o objetivo é alcançado; (3.iv) predicados substantivos quanto aos tipos de crimes em que certas medidas podem ser utilizadas.

Ao lado desses atributos, também destaca (4) estratégias de responsabilização de agentes, como regras de (4.i) atuação sob juramento e (4.ii) exclusão de provas obtidas de forma ilícita. Por fim, outro mecanismo de regulação é por (5) transparência, para a qual se pode estabelecer regras de (5.i) notificação dos alvos da quebra de sigilo, uma vez que aquele que sequer fica sabendo da vigilância não pode se defender, (5.ii) limitação de ordens de silenciamento direcionadas a terceiros obrigados a participar de medidas de vigilância (como empresas intermediárias); (5.iii) divulgação de relatórios estatísticos sobre medidas de vigilância. Essas medidas ampliam a capacidade de controle social sobre as práticas.

Como se vê, é possível lançar mão de diversos elementos para garantir que a medida de vigilância respeitará direitos, controlará riscos de causar injustiça e será acompanhada de *accountability* e controle social. Isso depende da medida em questão, do contexto em que se insere e da maneira como coloca riscos ao exercício de direitos. A estratégia de proteção regulatória que funciona para uma interceptação telefônica pode não ser a mesma que funciona para abordagens policiais ou para uso de câmeras, mas isso não signica que esse segundo grupo não mereça tratamento regulatório se também pode ameaçar direitos e se também merece contenção do uso da

[6] Ohm, 498–99.

força. Também não é, por outro lado, culpa do STF o foco em estratégias de contenção a partir da perspectiva da necessidade de controle judicial prévio – um dos centrais, mas também não o único. Se é assim, é porque o Legislativo também se deixou a um papel tímido ou secundário nessa área, além de nossa tradição de direito administrativo dar margem para fios ficarem soltos. Ocorre que é cada vez mais insustentável que permaneça assim. Falo desses desafios a seguir.

2.3 *Coordenação e desafios institucionais*

O Poder Judiciário desenvolveu ao longo dos anos certas ferramentas (doutrinas) para lidar com a regulação de *quebras de sigilo* – seja bem ou seja mal, como já visto. Essa jurisprudência é focada no paradigma de um encontro transacional ocasional entre autoridade policial e o indivíduo em que a pergunta fundamental é se a autoridade policial tem autoridade para obter sobre certos elementos de prova que estavam fora de seu alcance.[7] Essa atuação se dá sobretudo por questionamentos da (i)licitude da prova, cuja repercussão é levar à sua anulação. Por outro lado, o Judiciário está cada vez mais inapto a atuar sozinho para conter novas ameaças a direitos e novos tipos de arbítrio: tanto porque as doutrinas antigas não "capturam" novos fenômenos, como porque não estão na melhor posição para fazer avaliações que são, em verdade, questões de política criminal que ainda não foram objeto de deliberação pública.

Nem todos os potenciais problemas com tratamento de dados pessoais se traduzem na linguagem da privacidade – e de que foi desrespeitada uma prerrogativa de manter um aspecto da vida longe do acesso de terceiros. O cenário é mais complexo do que isso e o desenvolvimento de um direito da proteção de dados pessoais – voltado justamente à mitigação de riscos e abusos no tratamento de informações pessoais, vista no capítulo 1 –, aponta para isso. A tendência, como vimos nos capítulos 2 e 3, é aumentar as iniciativas baseadas em uso de dados pessoais na área de segurança pública, em moldes que desafiam a viabilidade de contar apenas com crivo judicial.

Para começar, há um velho problema de "viés de amostra"[8]: juízes raramente apreciam casos em que as táticas policiais não deram certo – a análise sobre licitude ou não da prova em geral se dá em casos em que o elemento de prova foi, de alguma forma, relevante para a

[7] Falando da Quarta Emenda, ver Renan, "The Fourth Amendment as Administrative Governance", 1041;1051.
[8] Friedman, *Unwarranted: policing without permission*, 170-2 (e-book).

incriminação de alguém e por isso é questionado pela defesa. Juízes não julgam casos em que técnicas e medidas não funcionaram: não veem nem analisam, inclusive, inúmeras interações policiais que não resultaram em acusação e em que não lhes é suscitado questionamento sobre quebras de sigilo que, mesmo abusivas, não deram em nada, por isso não levaram a acusações formais e, portanto, não oportunizaram contraditório nem supervisão judicial posterior.[9] Nos casos que veem, por outro lado, é notório como há o elemento de que alguém pode sair impune: isso tanto cria, ainda que inadvertidamente, uma certa indisposição para anular a prova (cuja consequência seria deixar criminosos impunes), como acaba se tornando um precedente para a validação de certas medidas que podem ter sequer passado por discussão pública – sobre sua eficácia como um todo, muito menos sobre devidas salvaguardas aplicáveis.

Mas os problemas não param aí. As medidas de vigilância hoje em questão que cada vez mais se aproveitam do avanço tecnológico são problemas que não são aptos de serem enfrentados e tratados com a existência de controle judicial prévio, ou pelo menos não só com ele: são medidas que precisam de balizamento por medidas administrativas de uso (quando podem ser empregadas e rastreio de quando o são e por quem foram), de design das ferramentas tecnológicas (que limitem desde a estrutura usos inadmitidos), de prestação de contas. Como falei ainda na introdução, se a polícia passa a ter à sua disposição uma ferramenta que permite visualizar o que ocorre dentro de lares, não é só a exigência de um mandado judicial que vai funcionar: deve ser controlada a disponibilização dessa ferramenta a agentes, deve ser demonstrada sua eficácia, deve ser analisada sua acurácia e potencial discriminatório, devem ser gerados relatórios de uso, devem ser limitadas as instâncias e códigos de ativação para uso, deve haver transparência sobre hipóteses e quantidades de uso. O mesmo vale para ferramentas como uso de *drones*, de câmeras, de softwares

[9] Além de Friedman, também nesse sentido Gray, *The Fourth Amendment in an Age of Surveillance*, 285. Usa exemplo de abordagens policiais: "As it stands, then, officers effectively are at their discretion to stop or frisk anyone they like, for good reasons, for bad reasons, or for no reasons at all. In the vast majority of cases, they know that their decisions will not be subject to judicial review. That is because the vast majority of cases do not lead to arrest or prosecution and innocent citizens who are stopped, frisked, and released seldom have the means, motive, or opportunity to challenge their treatment in court." O mesmo raciocínio se estende para quebras de sigilo em geral: quando o afastamento abusivo da privacidade ocorre e, ainda assim, não se encontra elemento de prova de nenhum crime contra o atingido, a medida pode passar sem qualquer questionamento. No Brasil, em 2020, o Min. Rogério Schietti fez notar esse ponto em voto paradigmático sobre inviolabilidade do domicílio, que já mencionei: "Aliás, releva destacar que os tribunais, em regra, tomam conhecimento dessas ações policiais apenas quando delas resulta a prisão do suspeito, ou seja, quando atingem o fim a que visavam. O que dizer, então, das incontáveis situações em que agentes do Estado ingressam em domicílio, muitas vezes durante a noite ou a madrugada – com tudo o que isso representa para os moradores da residência – e nada encontram?" Superior Tribunal de Justiça, HC 598051, j. 02.03.2021, DJE 15.03.2021.

espiões. Diante da falta de familiariedade e sensibilidade, riscos incidentes ao uso massivo de dados pessoais podem ser menosprezados por não se encaixarem nos paradigmas tradicionais de privacidade: os direitos à privacidade em jogo poderiam ser suprimidos simplesmente porque "não existe privacidade em público" ou porque "são dados estáticos", na forma das doutrinas atuais comuns.

Os poderes Executivo, Legislativo e Judiciário devem trabalhar coordenadamente para fazer valer um esquema de proteção – necessário não só para que direitos de privacidade sejam respeitados, mas para que o exercício do poder policial seja contido e compatível com a dignidade de forma geral. O mesmo vale para os novos problemas mapeados pelo direito da proteção de dados pessoais, que podem extrapolar a linguagem de privacidade, mas ainda devem ser enfrentados com o objetivo de conter o poder do Estado.

O Legislativo é responsável por propor e editar as regras que nortearão prerrogativas de produção de prova no processo penal e de prevenção à criminalidade. A lei-modelo em matéria de quebra de sigilo – no caso do Brasil, como mencionei repetidamente – é a Lei de Interceptações. No mais, o que existe é válido de forma apenas setorial e ao fenômeno de quebras de sigilo como meios de obtenção de prova no processo penal – de acesso a dados protegidos por deveres de confidencialidade aplicáveis a empresas (e cuja intencionalidade é proteger a privacidade) e a outras medidas invasivas de interceptação e infiltração: como no Marco Civil da Internet, na Lei Complementar nº 105, na Lei das Organizações Criminosas, na Lei dos Crimes de Lavagem de Dinheiro e no Código de Processo Penal (cuja aplicação não deixa de ser objeto de diversas controversas na prática).[10]

Há um amplo espectro de regulação da atividade policial no contexto administrativo que não tem qualquer regulação específica: os poderes putativos são extraídos diretamente do texto da Constituição – algo que, na linha exposta, não poderia ser considerado específico suficiente. Paradoxalmente, uma das atividades estatais que mais precisa de regulação para *contenção de poder* contra abusos no uso da força é a que é menos regulada.[11] O próprio Legislativo está sujeito

[10] Ver Abreu e Antonialli, "Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais"; Jacqueline de Souza Abreu, "Infiltrações virtuais no direito brasileiro: mapeando o cenário", in *Direitos Fundamentais e Processo Penal na Era Digital: doutrina e prática em debate*, org. Francisco Brito Cruz e Nathalie Fragoso, vol. III (São Paulo: InternetLab, 2020), 222–33.
[11] Friedman, *Unwarranted: policing without permission*, 125 (e-book).

a amarras e incentivos que podem não lhes mobilizar a ter uma atuação ativa e espontânea na área de segurança pública: atuações que aparentem *dificultar* o combate ao crime não são populares.

Frente a déficit de "governança democrática", como Barry Friedman chama, o autor propõe que o Judiciário com mais frequência haja para *provocar* o legislativo a atuar em determinada área: pergunte-se se o que foi feito é autorizado por lei. Enquanto não houver legislação específica sobre certa matéria delicada, não poderia ser admitida.

Quanto à falta de vontade política, Friedman sustenta que "Para ser direto: se os tribunais disserem que a polícia não pode fazer algo, pelo menos na ausência de algum tipo de regulamentação legislativa, e se a polícia achar que é importante ter esse poder, ela virá ao legislativo e exigirá ação. Ataque o boi do estado, e ele se levantará e responderá. E então teremos o debate democrático que é tão necessário nesta área."[12] Quanto às ocasiões em que autorizações específicas são necessárias, propõe:

> A questão que os tribunais deveriam se perguntar em cada caso é se uma autorização geral existente é suficiente para cobrir o que a polícia fez. Para táticas de policiamento familiares com uma linhagem longa - como paradas de tráfego com base na causa provável - a resposta provavelmente é sim. Mas há uma série de situações, cada vez mais comuns, em que tais autorizações antigas encobrem duvidosamente o que aconteceu. Por exemplo, quando a polícia emprega tecnologias invasivas, como drones e sensores de calor, que estavam além da imaginação mais selvagem de qualquer pessoa, incluindo os legisladores, no momento em que a autoridade geral foi comunicada, parece inteiramente plausível exigir que o governo volte para legislativo e obtenha permissão específica.[13]

Um exemplo dessa possibilidade seria para as "government dragnets" (algo como 'redes de arrastão estatais') – "esforços programáticos do estado para investigar, detectar, deter ou prevenir o crime ou outro dano significativo submetendo um grupo de pessoas, a maioria das quais reconhecidamente inocentes de atos ilícitos ou de planos de cometê-los, a uma privação de liberdade ou outra intrusão significativa"[14]. Essa é a nova frente de medidas de vigilância

[12] Tradução livre. No original: "Stated directly: If the courts say the police cannot do something, at least absent some sort of legislative regulation, and if the police think it is important that they have this power, they will come to the legislature and demand action. Gore the government's ox, and it will rise and respond. And then we will have the democratic debate that is so desperately needed in this area."Friedman, 215 (e-book).

[13] Tradução livre. No original: "The question courts should be asking themselves in each case is whether an existing blanket authorization is sufficient to cover what the police did. For familiar policing tactics with a long pedigree—such as traffic stops based on probable cause—the answer likely is yes. But there are a number of situations, increasingly common, in which such age-old authorizations dubiously cover what has happened. For example, when police employ invasive technologies, such as drones and heat sensors, that were beyond the wildest imagination of anyone, including the legislators, at the time the general authority was conveyed, it seems entirely plausible to require the government to go back to the legislature and get specific permission."Friedman, 221 (e-book).

[14] Tradução livre. No original: "programmatic government efforts to investigate, detect, deter, or prevent crime or other significant harm by subjecting a group of people, most of whom are concededly innocent of wrongdoing or of

impulsionada pelas promessas do big data (e da lógica "atuarial"), como visto. Essas medidas são desafiadoras pois, se é que medidas como abordagens policiais e buscas domiciliares em tese podem deixar algum registro visível de que ocorreram e a partir dos quais é possível questionamento de sua validade, essa possibilidade não é a mesma para abusos, erros e excessos que sejam decorrência de uso de big data.[15]

Na linha de Friedman, Chistopher Slobogin defende deferência do judiciário apenas a "buscas e apreensões abrangentes que: (1) sejam autorizadas pela legislação (o critério da legislação); (2) resultam de deliberações que incluem representantes dos grupos que afeta (o critério de representação); e (3) evitam prejudicar grupos politicamente vulneráveis porque a legislação autorizativa limita a discricionariedade executiva e é implementada de forma imparcial (o critério de restrição executiva)"[16]. Tribunais têm a obrigação de verificar esses elementos, ainda que entendam que a Quarta Emenda não se aplica, diz – no caso brasileiro, eu diria, ainda que entendam que não há quebra de sigilo constitucional e mesmo que achem que não é o caso de exigir uma ordem judicial.

O pano de fundo legislativo é necessário inclusive para balizar a discricionariedade na atuação administrativa do Executivo no universo de uso de dados para atividades policiais. Para Daphna Renan, muitos desses novos problemas com uso de dados pessoais por autoridades policiais e em políticas públicas de segurança devem ser endereçados com *governança administrativa,* usando recursos dessa tradicional área do direito. Recursos de direito administrativo podem complementar regras de processo penal, infundindo procedimentos com requisitos de *accountability* política e jurídica para balizar a discricionariedade estatal.[17] Pode endereçar os novos tipos de vigilância logo no ponto de entrada: orientar a edição de políticas internas claras e transparentes sobre tratamento de dados e sobre as situações em que buscas podem ser feitas nos sistemas, que inclusive poderiam auxiliar tribunais posteriormente na apuração da

plans to engage in it, to a deprivation of liberty or other significant intrusion". Christopher Slobogin, "Government Dragnets", *Law and Contemporary Problems* 73, nº 3 (1º de julho de 2010): 110.

[15] Joh, "The New Surveillance Discretion", 37.

[16] Tradução livre. No original: "panvasive searches and seizures that: (1) are authorized by legislation (the legislation criterion); (2) result from deliberations that include representatives of the groups it affects (the representation criterion); and (3) avoid prejudicing politically vulnerable groups because the authorizing legislation limits executive discretion and is implemented in an evenhanded fashion (the executive-constraint criterion)".Christopher Slobogin, "Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine", *Georgetown Law Journal* 102 (2014 de 2013): 1742. Ver também Slobogin, "Government Dragnets".

[17] Renan, "The Fourth Amendment as Administrative Governance", 1077–90.

validade de certas buscas.[18] E, por fim, oferece estratégias para governança por desenho institucional, como pela criação/indicação de órgãos públicos melhor capacitados para fazer avaliações de "causa provável programática" – como propõe chamar a avaliação de eficácia da política/medida/programa em questão como um todo, que possa efetivamente amparar seu uso para a finalidade que se propõe. Esses órgãos estariam em posição mais confortável do que tribunais estão para tal avaliação (por não terem visão global de uso e papel de novas ferramentas de vigilância e temerem atrapalhar o uso de recursos indevidamente, sem todas as informações disponíveis).[19]

Na realidade brasileira, portanto, é imprescindível resgatar não só o sentido real do crivo judicial prévio, mas a importância do princípio da legalidade e sua racionalidade de contenção do poder do Estado em detrimento de uma crença cega de que o Estado atua a promover o bem quando faz o que quer que seja pela segurança das pessoas. Como coloca Mireille Hildebrandt,

> O princípio da legalidade está intimamente ligado a uma concepção substantiva do Estado de Direito, que vincula o governo às suas próprias leis, ao mesmo tempo que prevê um sistema de freios e contrapesos e um conjunto de direitos humanos efetivos. Sublinha que os governos são obrigados a restringir-se aos fins especificados e legítimos para os quais tenham uma competência explícita, atribuída por lei. Isso limita sua liberdade e fornece transparência, bem como responsabilidade. Embora os Estados possam descobrir que, no curto prazo, o princípio da legalidade obstrui a conveniência de seu trabalho, a limitação dos poderes estatais marca a diferença entre o governo de um déspota esclarecido e uma democracia constitucional. Obriga o Estado a deliberar sobre os fins que pretende atingir, sabendo que, uma vez definidas as competências em termos de finalidade, tem de se ater a elas. Isso tem sido chamado de princípio de vinculação da finalidade, que é um descendente direto do princípio da legalidade. Tanto no direito administrativo como no processo penal o uso de uma competência para outra finalidade que não a prevista na lei, tem efeitos jurídicos. [20]

Vimos no capítulo 2 como a legalidade tem papel fundamental para que nossas práticas de garantia de segurança estejam comprometidas com a dignidade, contenção de poder, e gestão de

[18] Renan, 1091–1107.
[19] Renan, 1108–28.
[20] Tradução livre. No original: "The legality principle is closely connected with a substantive conception of the Rule of Law, which binds the government to its own enactments, while providing for a system of checks and balances and a set of effective human rights. It underscores that governments are obliged to restrict themselves to the specified, legitimate purposes for which they have an explicit competence, attributed by law. This limits their freedom and provides transparency as well as accountability. Though governments might find that in the short term the legality principle obstructs the expediency of their work, the limitation of governmental powers marks the difference between the rule of an enlightened despot and a constitutional democracy. It forces government to deliberate on the purposes it wants to achieve, knowing that once the competences are defined in terms of purpose, it has to stick to them. This has been called the purpose binding principle, which is a direct descendant of the legality principle. In both administrative law and criminal procedure the use of a competence for another purpose than the one provided for by law, has legal effect." Hildebrandt, *Smart Technologies and the End(s) of Law*, 155.

riscos a que estamos dispostos a correr (ou não). A jurisprudência do STF ocasionalmente reconheceu a importância dessa legalidade para tratar de interceptações – e em diversos momentos destaca ou pelo menos usa o fato de que uma medida tem autorização legal para fundamentar porque poderia ser legítima em certo contexto. Esse compromisso, entretanto, não pode ser parcial: não pode ser uma exclusividade de interceptações já superado no passado nem destacado quando convenientemente exisita alguma previsão legal.

Há, nesse contexto, um papel a ser exercido tanto por novos esforços legislativos que lidem com novas medidas de vigilância que ameaçam direitos quanto por uma lei geral de proteção de dados pessoais de aplicação estruturante que se aplique às atividades de segurança pública e de investigações criminais e busque resgatar a importância da legalidade e da governança administrativa de políticas de uso de dados pessoais e conter riscos de danos decorrentes de certos tratamentos de dados pessoais.[21] Não são barreiras no combate ao crime, na "guerra" contra tráfico ou corrupção, mas instrumentos regulatórios canalizadores do exercício de poder comprometido com direitos.[22] Paralelamente, o Judiciário deve se despertar para o perigo de interpretações rasas, que colocam nossos compromissos a perder. Isto é: que não só não provocam o Legislativo a agir, como ainda maltratam a própria concepção de nossos direitos constitucionais e nos deixam despreparados para problemas da tecnologia do presente e do futuro. Trato mais disso a seguir.

3 A privacidade na era digital revistada

[21] Comentando esforços de elaboração de um Anteprojeto de Lei de Proteção de Dados Pessoais em Investigações Criminais e na Segurança Pública por uma Comissão de Juristas criada pela Câmara dos Deputados (do qual esta autora fez parte), ver Orlandino Gleizer, Lucas Montenegro, e Eduardo Viana, *O direito de proteção de dados no processo penal e na segurança pública* (Rio de Janeiro: Marcial Pons, 2021). Os autores criticam que uma tal lei seja aprovada antes da elaboração de leis que estabelecem "bases jurídicas" (normas autorizativas) para as atividades informacionais (tratamento de dados pessoais) – área em que o direito administrativo e processual penal brasileiro deixariam a desejar. O trabalho é feito sob as premissas da dogmática constitucional alemã e carregado no teste de proporcionalidade – premissas que não compartilhei neste trabalho, como falei, por abandonarem a exploração de uma noção de direito forte e deixarem de acomodar a dimensão interpretativa que invitavelmente inclui se fazer teoria do direito e teoria da justiça. De todo modo, nessa conclusão, e no que a abordagem aqui proposta também vê ameaça (riscos de injustiça) a *direitos morais fortes*, também penso que há necessidade de proteção regulatória tanto na frente de autorizações e balizamentos de medidas de vigilância, como potencialmente para um esforço estruturante como o do Anteprojeto.

[22] "Não há dúvida de que a tendência a se liberar de normas restritivas aumenta durante conjunturas sociais ou economicamente difíceis. Mas é também verdade que justamente nessas fases aumenta o risco de utilização autoritária das grandes coletâneas de informações e, logo, existe a necessidade de leis de garantia." Rodotà, *A vida na sociedade da vigilância – a privacidade hoje*, 56. Ver também, sobre estruturação do exercício de poder: de Hert e Gutwirth, "Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power".

3.1 *Desafios tecnológicos*

Doutrinas e "testes" tradicionais, criteriais e binários para verificação da existência de uma violação a direito à privacidade precisam ser revisitados diante do modo como a tecnologia pode afetar regras fixadas e truísmos extraídos de paradigmas tradicionais – como a de que "informações de atividades realizadas publicamente não são protegidas pelo direito à privacidade". Mais do que nunca, a tecnologia exige que revisitemos a teoria da privacidade que sustenta nossos paradigmas, para recuperar por que protegemos o que protegemos e assim oferecer respostas consistentes para novas circunstâncias fáticas, reconectadas com a intencionalidade de nossas práticas. Darei um exemplo do direito estadunidense de como a Suprema Corte de lá redirecionou a sua rota para lidar com desafios da era digital para depois retomar a discussão para o direito brasileiro.

Em 2018, no caso *Carpenter v. US,* a Suprema Corte dos Estados Unidos teve de decidir se a obtenção de registros históricos de localização de celulares constitui uma "busca" [*search*] no sentido protegido pela Quarta Emenda à Constituição norte-americana. Tal dispositivo constitucional, como visto, proíbe "buscas e apreensões irrazoáveis". O caso desafiou de modo frontal os limites da "*third-party doctrine*", estabelecida nos casos *US v. Miller* (1976) e *Smith v. Maryland* (1979), segundo a qual informações compartilhadas com terceiros perdem a "expectativa razoável de privacidade" e, portanto, não são mais protegidas pela Quarta Emenda[23]: no caso, tratava-se de informações geradas por usuários na utilização de celulares, compartilhadas com operadoras de serviço de telefonia celular, e que podem muito bem dizer respeito a registros de localização de trajetos realizados publicamente.

Por maioria[24], o tribunal não admitiu a aplicação dessa doutrina ao caso, em razão da natureza da intrusão e da extensão das informações passíveis de serem obtidas pela análise do histórico de localização e também pela ausência de uma "voluntariedade" afirmativa no compartilhamento de informações com operadoras. Recusaram, portanto, a aplicação binária criterial – que separa o mundo simplificadamente entre coisas que pertencem ao âmbito privado e coisas que não pertencem. Em um cenário de uso popular de celulares para as finalidades mais

[23] A consideração é fundamental porque um "teste" paradigmático da delineação do âmbito de proteção da Quarta Emenda é o fixado em *Katz* (389 U.S. 347 (1967)), em que a Suprema Corte desenvolveu o teste da "expectativa razoável de privacidade." Para que essa expectativa seja protegida pela Quarta Emenda, (i) a pessoa em questão deve exibir uma expectativa real (subjetiva) de privacidade e (ii) essa expectativa deve ser uma que a sociedade está preparada para reconhecer como 'razoável'. A *third party doctrine* aniquila qualquer chance de sobreviver a esse teste.
[24] O caso opôs os *justices* John Roberts Jr. (relator do voto da maioria), Ruth Bader Ginsburger, Stephen Breyer, Sonya Sotomayor e Elena Kagan aos *justices* Anthony Kennedy, Clarence Thomas, Samuel Alito e Neil Gorsuch.

cotidianas, bem como de cada vez mais empresas que oferecem serviços que envolvem compartilhamento de dados, decidir de outro modo seria admitir enorme exposição. A minoria entendeu, por outro lado, que a Quarta Emenda não deveria olhar para a existência ou não de uma "expectativa razoável de privacidade" nesses moldes, mas estar sempre vinculada a uma intromissão a um interesse de propriedade – existência de alguma forma de *trespass*, o que não existia nesse caso.

Apesar de apertada, a decisão avançou um ponto que, na decisão da Suprema Corte em *US v. Jones* (2012), havia ficado pendente: naquele caso, a questão era se a instalação, por parte de autoridades de investigação, de um aparelho de GPS no veículo de um investigado para monitorar os seus movimentos violava a Quarta Emenda. O voto que formou a maioria, o da ministra Sotomayor, já havia considerado que "o monitoramento de GPS gera um registro preciso e abrangente dos movimentos públicos de uma pessoa que reflete ricos detalhes sobre as suas associações familiares, políticas, profissionais, religiosas e sexuais.[...] Eu levaria esses atributos do monitoramento por GPS em conta ao considerar a existência de uma expectativa de privacidade razoável da sociedade no conjunto agregado dos movimentos públicos de alguém." Admitia, portanto, que, frente ao desenvolvimento tecnológico, é possível a violação da privacidade mesmo quando o acesso de autoridades é a informações *públicas* que, agregadas por um certo período, são muito capazes de revelar detalhes da vida de uma pessoa.[25] No entanto, para a maioria do tribunal, outro aspecto do caso já bastava para resolvê-lo: viram na instalação do GPS uma "busca" em razão da invasão à propriedade *carro* – sendo o teste da existência de *trespass* suficiente. *Carpenter* foi, portanto, fundamental, para impor limites à '*third party doctrine*' sob a perspectiva do teste da expectativa razoável de privacidade: diante dos avanços da tecnologia, informações "públicas" não podem encerrar discussões sobre o direito à privacidade.

Com isso quero assinalar, em reforço ao que já apresentei no capítulo 1, que, percebendo-se a privacidade e as avaliações de violação a esse direito estritamente relacionada a certos tipos de informações ou de espaços convencionais em si, sujeitos a uma análise criterial fixada por parâmetros antigos (houve intromissão em um espaço territorial ou em informações confidenciais tradicionalmente tidas como partes da privacidade?), rapidamente o direito constitucional vai permitir que a tecnologia fulmine qualquer direito à privacidade. Abstraindo-se das razões

[25] Leonardo G. P. Rosa, "GPS, privacidade e judiciário: breve análise de decisão da Suprema Corte dos EUA", *Revista Brasileira de Ciências Criminais* 105 (2013): 368.

normativas que sustentam e justificam essas proteções, isto é, da teoria da privacidade que sustenta esses paradigmas, das práticas e convicções que os informam e do seu papel para restringir a discricionariedade e o arbítrio do Estado no direito processual penal e no direito administrativo, serão descartados pleitos legítimos de privacidade antes mesmo de começar. Se os dispositivos que versam sobre privacidade na Constituição brasileira estiverem comprometidos com os princípios morais que tentei articular na primeira parte desse trabalho, impõe-se, no mínimo, um certo tipo de postura no enfrentamento de controvérsias e a reorientação de certas abordagens.

3.2 *Sigilo telemático: a necessidade de revisar parâmetros da jurisprudência*

Por novos rumos

Esse descolamento é o que vemos hoje nas discussões sobre *que tipos de dados* seriam protegidos por "sigilo" (art. 5º, XII, CF/88). Como mostrei, há anos prevalece no STF a noção de que apenas o "processo de comunicar" é protegido por esse inciso. Ocorre que, com a emergência de tecnologias digitais, em que todas as nossas atividades se tornam dados eletrônicos,[26] a implicação daí extraída é que a infinidade de "dados armazenados" – como toda a caixa de entrada de um e-mail – não estaria protegida: nossas atividades, características, pensamentos, obras e bens que se traduzem em dados "estáticos" não seriam protegidas. Para ser justa, quando muito, para *conteúdo* de comunicações *armazenadas,* é (resistentemente) reconhecida uma proteção constitucional pelo art. 5º, X, CF/88.[27]

Essa interpretação tem servido fundamentalmente para dispensar a necessidade não só de ordem judicial para acesso a diversos tipos de dados em uma era em que cada vez mais as interações e atividades de indivíduos deixam rastros eletrônicos e assim facilitar o trabalho da polícia na obtenção dessas informações, mas para dispensar até a exigência de observâncias aos requisitos materiais vistos e a parâmetros de proporcionalidade.[28] A afirmação de que "dados em

[26] Ferguson, "Structural Sensor Surveillance".

[27] Na doutrina, o descompasso que essa jurisprudência possui numa era com diversas comunicações *armazenadas* já vem sendo denunciada e criticada há um tempo. Ver Ricardo Sidi, "A interceptação de e-mails e a apreensão física de e-mails armazenados", *Revista Fórum de Ciências Criminais* 4 (julho de 2015): 112; João Fábio A. Azeredo, "Sigilo das Comunicações Eletrônicas Diante do Marco Civil da Internet", in *Direito & Internet III - Tomo II: Marco Civil da Internet (Lei n. 12.965/2014)* (São Paulo: Quartier Latin, 2015), 226–30.

[28] Essa colocação tem uma dimensão empírica mais abrangente não só sobre o que foi visto no STF, mas sobre o que se vê da jurisprudência do STJ e em tribunais estaduais ao redor do país que surge daí. Como muitos processos em que são proferidas ordens de quebra de sigilo tramitam em segredo de justiça e, as que são questionadas, são publicizadas muito excepcionalmente já a nível de discussão em tribunais superiores (quando o são), a realização de pesquisa empírica abrangente enfrenta desafios. Para uma visão do impacto dessa jurisprudência em casos de buscas

si" não são protegidos hoje apenas serve para facilitar o acesso de autoridades a essas informações. Recentemente, voto do Min. Gilmar Mendes no HC 168052 da 2ª Turma sinalizou que mudança de compreensão pode estar em curso, justamente em atenção aos novos hábitos de comunicação e às capacidades de celulares.[29] O caso foi, entretanto e como se viu, de resultado apertado (3x2) e, no Pleno, casos que recolocam o problema ainda estão em aberto (como o ARE 1042075), com risco de reafirmação desses critérios simplificadores antigos.[30]

A jurisprudência precisa ser redirecionada. A começar, ela é incoerente internamente à própria jurisprudência do STF. Como visto, o teste ainda hoje aplicado pelo STF e exportado para tribunais Brasil a fora surgiu a partir de um receio de que, não fosse assim, a proteção constitucional a dados teria de ser considerada absoluta na CF/88. Essa posição pressupõe que apenas o processo de comunicar de comunicações telefônicas pode ser quebrado por conta da linguagem de inviolabilidade e da exceção contida no próprio texto constitucional: "XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;".

Ocorre que, para que essa leitura e receio fossem minimamente plausíveis, o STF teria que admitir apenas quebra de sigilo de fluxo de interceptações telefônicas, por conta da exceção

---

de dispositivos eletrônicos em torno de prisões em flagrante, ver Antonialli et al., "Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes". Para um breve comentário sobre casos específicos que surgiram de questionamentos de ordens de quebras de dados de empresas de telefonia, ver Abreu, "Quebras de sigilo e privacidade". Para relatos de advogados que atuam na área, ver Azeredo, "Sigilo das Comunicações Eletrônicas Diante do Marco Civil da Internet", 227–28; Carina Quito, "Acesso a Comunicações Eletrônicas Armazenadas na Prática Judiciária", in *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*, org. Dennys Antonialli e Jacqueline de Souza Abreu, vol. I (São Paulo: InternetLab, 2018), 100–107.

[29] "STF: Suspenso julgamento sobre validade de provas obtidas no WhatsApp sem autorização", *Migalhas*, 12 de junho de 2019, https://www.migalhas.com.br/Quentes/17,MI304267,21048-STF+Suspenso+julgamento+sobre+validade+de+provas+obtidas+no+WhatsApp.

[30] Após voto do Min. Dias Toffoli mantendo as distinções entre dados em fluxo e dados estáticos, mas reformulando-a para uma distinção entre conteúdo de comunicações e outros dados e permitindo o acesso direto aos segundos (Tese proposta: É lícita a prova obtida pela autoridade policial, sem autorização judicial, mediante acesso a registro telefônico ou agenda de contatos de celular apreendido ato contínuo no local do crime atribuído ao acusado, não configurando esse acesso ofensa ao sigilo das comunicações, à intimidade ou à privacidade do indivíduo (CF, art. 5º, incisos X e XII), abriu a divergência o Min. Gilmar Mendes no ARE 1042075, já acompanhado do Min. Edson Fachin, com a tese ""O acesso a registro telefônico, agenda de contatos e demais dados contidos em aparelhos celulares apreendidos no local do crime atribuído ao acusado depende de prévia decisão judicial que justifique, 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)". O julgamento foi interrompido após pedido de vista do Min. Alexandre de Moraes.

contida no texto, restando os demais "fluxos" protegidos de forma absoluta.[31] Ao contrário disso, o STF admite tanto (i) interceptações de dados (interceptações telemáticas), tendo deixado de enfrentar definitivamente a discussão sobre a Lei nº 9.296/96 e deixando acumular uma prática de já 25 anos de interceptações do tipo, quanto (ii) interceptações mesmo de correspondências (quando há previsão legal ou ordem judicial), como visto no capítulo anterior. A suposição de que há algo completamente absoluto/inviolável aí simplesmente não se sustenta – esse também não pode ser o receio contra o reconhecimento da proteção a dados.

Uma perspectiva genealógica do problema deve reconhecer um tipo de vínculo entre a proteção do inciso XII e o "processo de comunicar-se". Como visto, olhando para casos anteriores a 1988 e pondo em perspectiva as origens internacionais históricas desse tipo de garantia de sigilo, temos que a proteção buscava garantir a possibilidade de se comunicar à distância ainda *em* privacidade, sem que canais de comunicação como os Correios fossem subvertidos e explorados por terceiros, pelas empresas e pelo próprio Estado para atravessar a privacidade dos comunicantes. Mesmo porque, fora desse contexto de fluxo, cartas trocadas estavam em geral "armazenadas" na *casa* de alguém (protegidas pelo domicílio) e, quando não à distância, pessoas conversam presencialmente umas com as outras, em que, então, também podia se pressupor haver privacidade, se não houvesse outras pessoas por perto ou se fossem, no máximo, estranhos desinteressados e com memória seletiva. A proteção de um processo de comunicação nunca quis dizer, portanto, que o que estava guardado junto a bens de alguém ou foi dito sob expectativas de privacidade inerentes a uma relação social não merecia proteção. Pelas mesmas razões, no equivalente eletrônico dessas experiências, nunca poderia significar que "dados estáticos" não seriam protegidos de modo algum, que a eles pode haver acesso facilitado ou mesmo livre. O próprio Min. Sepúlveda Pertence, em um dos julgados históricos que originaram essa distinção, usou essa leitura do art. 5º, XII apenas para afastar o argumento de que mídias eletrônicas, obtidas dentro de um lar junto e por conta de uma busca e apreensão domiciliar autorizada judicialmente, não poderiam nunca ser acessadas. E só.[32]

---

[31] Já aponto esse problema há algum tempo, em trabalhos com Dennys Antonialli: por exemplo, Abreu e Antonialli, "Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais". Essas leituras não apareceram do nada em votos no STF, mas foram também alimentadas por debates doutrinários, como apontamos no trabalho mencionado. Ver, mais recentemente, sobre a discussão em torno do que significa "em último caso" no art. 5º, XII da CF/88, ver Queiroz, "Privacidade, criptografia e dever de cumprimento de ordens judiciais por aplicativos de trocas de mensagens".

[32] Para uma desconstrução também da utilização que artigo do professor Tercio Sampaio Ferraz Jr. recebeu ao longo dos anos para suportar essa visão, ver Paula Pedigoni Ponce e Rafael Mafei Rabelo Queiroz, "Tércio Sampaio Ferraz

Ademais, dados bancários são dados estáticos – e "eletrônicos", insertos em sistemas eletrônicos que compõem o sistema financeiro como um todo e o sistema interno de bancos – e isso nunca foi desculpa para afastar discussões constitucionais sobre o tema. Pelo visto no capítulo anterior, o STF sempre trabalhou tanto com o inciso X como com o inciso XII ao deliberar sobre questões do tema. Mesmo quando alguns ministros quiseram rebaixar questões de sigilo bancário a uma matéria infraconstitucional, isso nunca prevaleceu – sempre que novas questões tocam o sigilo bancário, a questão é até hoje levada ao STF como matéria constitucional, nunca sendo deixada apenas ao STJ. De uma perspectiva básica de coerência, no mínimo, tudo isso deveria ensejar a mesma postura para dados telemáticos em geral: serem estáticos não é suficiente para encerrar qualquer questão nem os minimizar.

As necessidades de revisitar o problema não param aí. As considerações deste trabalho sugerem que um teste baseado no caráter "dinâmico" ou "estático" de um dado para identificar a proteção de direito constitucional à privacidade é, no mínimo, insuficiente e, no máximo, completamente equivocado. Se a razão de ser da proteção jurídica tradicional à confidencialidade de comunicações privadas é resguardar uma prerrogativa de privacidade que está enraizada em nossas práticas que prestigiam nossa autonomia sobre acessibilidade a outras pessoas de aspectos da vida de relevância pessoal sob certo contexto, devemos nos questionar se outros tipos de privacidades que valorizamos, igualmente enraizada em nossas práticas sociais, não necessitam de proteção em nossas práticas jurídicas. O teste hoje usado é arbitrário e vazio de qualquer convicção.[33] A que tipo de fundamento a exclusão de dados estáticos da proteção constitucional ou a redução a priori de sua importância poderia apelar? Não guardamos o que entendemos relevante guardar? Não fazemos isso com cartas e documentos e diversos outros bens que valorizamos e nossas práticas sociais não resguardam respeito a esse material pessoal? Como isso poderia contaminar pleitos de privacidade?

Diversos espaços virtuais se inserem em contextos sociais que informam nossas expectativas e refletem e alimentam práticas e regras sociais de privacidade. Emails armazenados e em fluxo são formas e registros de comunicações privadas que expressam nossos pensamentos e discursos com os respectivos interlocutores. Mensagens e arquivos armazenados em nuvens

Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado", *Internet & Sociedade* 1, nº 1 (18 de fevereiro de 2020): 64–90.

[33] Ver também Dworkin, *Law's Empire*, 253.

privadas mais se assemelham a diários e outros documentos pessoais físicos. Terceiros não acessam essas informações: já construímos esse sistema de comunicação para evitar tanto; as próprias empresas que fazem a hospedagem não podem espiá-las ou apenas o podem também na medida do nosso consentimento (ou alguma outra exceção que outro contexto governará). O mesmo vale para como nos comportamos com relação a celulares: não há nada em nossas práticas sociais que sugira que não nos importamos com tudo que está no celular e que não nos importamos com quem acessa o que está nele. Pelo contrário, nós damos essa deferência, tanto como damos a bens e a domicílios. Pessoas que desrespeitam isso são criticadas. Pessoas que tentam hackear o email alheio, também.

Nesse sentido, temos um direito à privacidade sobre o que é mantido no nosso celular e o que falamos em chats privados em face de terceiros. É mais que possível argumentar que proteções como as do domicílio e a de comunicações privadas – ou então intimidade e vida privada – alcançam prerrogativas de privacidade em novos recursos tecnológicos e que as percepções do que é "sagrado" (a conta de email ou a nuvem virtual como um domicílio e as mensagens privadas como comunicações telefônicas ou cartas) sejam levadas para essas novas experiências.[34] É mais que possível argumentar que merecem proteção contra acessos abusivos, excessivos, errados.

O fato de que hoje o teste binário aplicado pelo STF está longe da forma como pensamos e protegemos concepções de privacidade no domínio telemático até no direito penal é sintomático da necessidade de reconsideração. Que um hacker acessou dados *estáticos* de celulares de autoridades públicas nunca foi objeto suficiente para deixar de condenar a ação da perspectiva de violação à privacidade.[35] Suspeito ainda que se o hacker tivesse acessado não o conteúdo de

[34] Nessa linha, ver Katherine Strandburg, "Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change", *Maryland Law Review* 70, nº 3 (1º de janeiro de 2011): 614–80.

[35] O descompasso normativo – e até mesmo a incoerência/hipocrisia – dessa postura de que essas informações não são protegidas por um direito à privacidade veio a tona no Brasil quando autoridades de investigação foram alvo de ataque criminoso que envolveu acesso a comunicações armazenadas em celulares. Refiro-me a revelações do portal The Intercept Brasil, que supostamente recebeu de hacker histórico de mensagens trocadas entre membros da Lava Jato, notadamente o procurador da República Deltan Dallagnol, e ex-juiz e agora também ex-ministro da Justiça Sergio Moro. Ver Rafael Moro Martins, Alexandre de Santi, e Glenn Greenwald, "'Não é muito tempo sem operação?' Exclusivo: chats revelam colaboração proibida de Sergio Moro com Deltan Dallagnol na Lava Jato", *The Intercept Brasil*, 9 de junho de 2019, https://theintercept.com/2019/06/09/chat-moro-deltan-telegram-lava-jato/. Só é possível dizer que há violação da privacidade nesse caso se, em primeiro lugar, se admitir que dados constantes em celulares são protegidos por um tal direito, mesmo que sejam "estáticos". Comparar, por exemplo, manifestações da Procuradoria Geral da República diante de vazamento de mensagens de procuradores do MPF atuantes na Lava Jato em junho de 2019 ("Dodge questiona vazamento de mensagens e se manifesta contra Lula no Supremo", *Folha de S.Paulo*, 21 de junho de 2019, https://www1.folha.uol.com.br/poder/2019/06/dodge-questiona-vazamento-de-mensagens-e-se-manifesta-contra-lula-no-supremo.shtml.) e a posição que sustentou em recurso com repercussão

comunicações, mas todos os demais dados – metadados das comunicações, fotos, histórico de ligações, agenda de contatos, histórico de localização, histórico de websites acessados, também ainda teriam visto problema de privacidade em sua ação. Por quê? Porque precisamos de uma perspectiva mais honesta sobre como experimentamos privacidades na era tecnológica e as expectativas legítimas que carregamos nesses usos.

Outros tipos de testes binários tampouco ajudam. Uma interpretação concorrente poderia sustentar que, no lugar do teste binário dinâmico x estático, coloquemos um teste binário que distingua se é conteúdo ou se é informação cadastral e/ou metadados. Tampouco serviria. Os "metadados" podem estar atrelados a exercícios bastante valiosos de privacidade e reunir informações sobre pessoas que ninguém espera estarem disponíveis para análise de terceiros e sobre as quais legitimamente temos expectativas de privacidade enraizadas em nossas práticas sociais: ninguém sabe quais foram as últimas pessoas a quem eu telefonei e todos os sites que visitei na internet, senão eu mesma – é certo que temos expectativas de privacidade sobre essas informações, que não fazem parte do campo de conhecimento de nenhuma outra pessoa. Como já observava a Suprema Corte dos EUA e apareceu no meu exemplo de Elize Matsunaga ainda no capítulo 1, ainda que compartilhemos a quem ligamos e de onde ligamos com empresas de telefonia, fazemos isso no contexto de uma relação comercial. Esperar cuidado com relação ao que é feito com essas informações e não gratuitamente disponibilizadas a qualquer terceiro é um elemento comum dessas relações, que valorizamos e que pode muito bem receber proteção jurídica. Ademais, a própria arquitetura do serviço é uma em que o público em geral não fica sabendo – isso mantém a expectativa de privacidade em face de terceiros.

Outro teste binário a ser descartado é um que vincule a legalidade da conduta pelo tipo de matéria extraída do conteúdo obtido – que o teor da mensagem devesse ser de caráter íntimo para que se falasse em violação de direito à privacidade, por exemplo, o que não incluiria o que venha a se mostrar de "interesse público". Ainda que esses fatores possam vir a pesar no contexto do trabalho da imprensa na *divulgação* de furos jornalísticos, certamente não é razão que justifique o *acesso* não autorizado – seja de um hacker, seja da polícia, fora das premissas aqui estudadas. Esse fator contingencial pós-acesso não legitima a conduta. A prerrogativa de privacidade em questão contra terceiros não depende de fatores ulteriores sobre a sensibilidade do que foi obtido. É claro

geral sobre condições de acesso de autoridades policiais a celulares no STF em novembro de 2018 (ARE 1042075), afirmando que o sigilo das comunicações não se estende a dados armazenados.

que o impacto da violação e o tamanho do dano à dignidade pode ser muito maior em razão desse teor: o acesso a imagens íntimas em um caso como o de Carolina Dieckmann torna a violação ainda mais severa.[36] Por essa razão, esses fatores podem pesar como causas de aumento de pena e são relevantes em causas e pleitos de indenização cíveis. Mas já consideramos que existe dano no mero fato de que um terceiro praticou condutas que contradizem expectativas de privacidade contra *acessos* resguardadas em nossas práticas social e jurídica e cuja intencionalidade permite dizer que rejeitou valor a uma privacidade valiosa.

Além do abandono de testes binários, deve ser resgatada a noção de que o ônus de fundamentação para agir é do Estado, que precisa justificar que não está atuando arbitrariamente, descuidadamente, nem em excesso. Direitos específicos à privacidade não são os únicos que balizam a atuação do Estado, apenas reforçam limites de forma especial em certos momentos. A exigência de suspeita individualizada para meios de obtenção de prova em geral está imbricada com exigências de fundamentação de um tratamento desigual e seletivo do Estado sobre alguém e que envolve risco de dano moral, ainda que o nível dessa suspeita seja inserido em um espectro que leve em conta o risco de dano moral em jogo por trás de uma suspeita equivocada – uma decisão que deve ser tomada coletivamente em lei e ser coerente com nossas práticas jurídicas e sociais. As noções de justiça que vedam medidas inadequadas e desnecessárias estão também embutidas a toda atuação do Estado, como é paradigmático no direito administrativo. A interpretação jurídica não só dos dispositivos que versam sobre privacidade deve urgentemente se reconectar com os princípios morais e políticos subjacentes. Hoje, dizer que não se protege dados estáticos é só desculpa para deixar de enfrentar diversas outras questões difíceis.

No que segue, vou comentar as repercussões do que falei para três contextos – dois ainda dentro do tema de sigilo telemático e um terceiro no universo geral de dados pessoais.

Acesso a celulares

O primeiro é sobre acesso policial a celulares. O STJ, em 2016, no RHC 51.531[37], enxergou o descompasso normativo que a interpretação tradicional do STF acarreta: não havendo proteção constitucional para dados telemáticos estáticos, teriam de julgar que ninguém possui direito à

[36] Referência a "Polícia encontra hackers que roubaram fotos de Carolina Dieckmann", *Fantástico*, 13 de maio de 2012, http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html.
[37] Superior Tribunal de Justiça, RHC 51.531, Rel. Min. Néfi Cordeiro, Sexta Turma, j. 19.04.2016, DJe 09.05.2016.

privacidade sobre informações salvas em celulares. No caso, isso significaria que a polícia basicamente teria livre acesso a celulares: não haveria problema algum em que a autoridade policial acessasse celular de quem quisesse. Foi então afirmado que deveria ser reconhecida proteção a conteúdo de celulares, tornando necessária autorização judicial prévia e sendo ilícita a prova obtida sem essa ordem anterior. Mais recentemente, no entanto, o STJ começou a calibrar essa interpretação para autorizar acesso a "agenda de contatos e histórico de ligações" pela autoridade policial sem ordem judicial, reservando proteção apenas a conteúdo de comunicações.[38] Isto é, pondo no lugar da distinção entre dados em fluxo e dados estáticos uma distinção entre conteúdo de comunicações, de um lado, e outros tipos de dados, de outro. Vimos essa ambiguidade na jurisprudência do STF.

Não faz sentido raciocinar assim sobre privacidade. A proteção não é devida pela informação em si pura e simplesmente. Não há um balaio do que é protegido e outro balaio do que não é protegido e diversos tipos de dados a serem jogados em ou retirados de um ou outro que valha para todo caso. Também não há simplesmente gradação de maior para menor proteção. O que determina se é protegido é o contexto: dados cadastrais são considerados simples e recebem a menor proteção na legislação processual especial em termos de acesso, mas são esses os dados subjacentes à decisão que levou ao reconhecimento de um direito à proteção de dados e impossibilitou compartilhamento de dados, bem como são esses os dados que constituiam o dossiê antifascita do Ministério da Justiça que foi veementemente vetado pelo STF. O que importa é o contexto, se há uma prática de privacidade a se proteger e que se estende a eles, se há regulação para vedar abusos, erros e excessos, se há razão para obtê-los, se se limitam aos necessários.[39]

Como já tive a oportunidade de desenvolver, existem diversas práticas que sustentam um reconhecimento de direito à privacidade das pessoas sobre seus celulares por ser um espaço que diz respeito a si e não aos outros. É ainda um bem pessoal, sobre o qual não franqueamos disponibilidade a qualquer um. Em muitos aspectos, é extensão do nosso corpo e do nosso domicílio – e se há "partes" do nosso corpo e da nossa casa que consideramos mais "sensíveis" para a intimidade, isso não significa livre acessibilidade, sem respeito ao seu titular, em qualquer

[38] Abreu, "Comentário ao STJ – REsp 1.782.386/RJ: Acesso a Agenda de Contatos de Celular por Autoridade Policial sem Autorização Judicial".

[39] Para uma ilustração de como a interpretação que anula de pronto a proteção a dados cadastrais gera repercussões no sentido de permitir fornecimentos indicriminados de dados que fogem do escopo de uma investigação, ver o conjunto de casos sobre a determinação a que seja criada uma "senha" para acesso da autoridade policial a sistemas internos de empresas de telefonia: Abreu, "Quebras de sigilo e privacidade".

lugar e em relação a qualquer pessoa.

Ademais, informações sobre contatos e ligações dizem respeito às nossas associações sociais e às nossas atividades do dia a dia: quem possui agenda pública sobre o que fez durante o dia e, quando muito, a quem ligou, é tipicamente quem tem conta a prestar para alguém (políticos, magistrados), mas ninguém mais faz isso. Mantemos contatos e atividades que entendemos dizer respeito a nós e a mais ninguém de forma privada – dispomos sobre com quem compartilhamos se quisermos, não somos forçados a tanto. Quem desrespeita essa prerrogativa individual, acredito, seria criticado. Mesmo quem "compartilha" muito em redes sociais dispõe de sua privacidade: não é tudo de suas vidas que vai para lá para ser divulgado; em geral, seleciona-se muito bem a foto ou o vídeo que se postará e a audiência que a verá.[40] E, de todo modo, não é porque certas pessoas dispõem assim de aspectos de suas vidas que todo o resto que não faz deva perder direitos na mesma medida. Frente à insistência em um "rebaixamento" e considerando as exigências de integridade, há ainda de se reconhecer que tais informações são *dados pessoais*, em relação aos quais temos passado a reconhecer novos interesses: riscos de uso secundário, de vazamento, entre outros. A falta de discussão desses aspectos em preferência a uma distinção que se omite a desenvolver o assunto é uma tragédia não só conceitual, mas prática: frustra o objetivo de contenção de ações policiais contra abusos.

Ademais, esses encaminhamentos não poderiam ser mais sintomáticos de como há uma completa desconexão das discussões com o contexto em que se inserem. Se a polícia acessa celulares no meio de uma abordagem policial sem qualquer suspeita, se faz isso em resposta a uma urgência iminente, se faz isso no âmbito de obtenção de prova para investigação instaurada, se faz isso para colher corpo de delito – essas variações importam. Esses momentos colocam princípios específicos, como visto: sem suspeita já é controverso se a polícia pode identificar pessoas e revistar seu corpo – muito mais deveria ser se podem vasculhar seus celulares, qualquer parte que seja. Com suspeita individualizada, deve ser preferido que a demonstração de presença dos requisitos materiais seja posta a um juiz, como fórmula que busca limitar o arbítrio, como visto. Cenários de "urgência" – perigo concreto e iminente – que ensejariam uma busca em celular – se ensejam qualquer excepcionalidade que afastariam a opção regulatória por uma ordem judicial

[40] Para um relato etnográfico de como adolescentes dispõem sobre privacidade, ver: danah boyd, *It's Complicated: The Social Lives of Networked Teens* (New Haven: Yale University Press, 2014). Embora trate do cenário americano, acredito que muito se aplica também a adolescentes brasileiros.

prévia, precisam ser trazidos ao debate público. A possibilidade teórica de imaginar justificação para tanto não pode atropelar a deliberação coletiva sobre riscos de dano moral que essa exceção contém e a necessidade de ainda assim garantir proteção regulatória contra abusos, erros e excessos. Se o celular é, por outro lado, encontrado largado em uma cena de crime, pode em tese compor o material a ser periciado como outros que compõem a cena do crime – embora, da perspectiva regulatória, possamos de novo ainda reservar a exigência de autorização judicial prévia para também coibir abusos, considerando a quantidade de informações que carregam. O STF, o STJ e tribunais do Brasil a fora, passam ao largo dessas discussões e nuances ao simplesmente tratarem de "dados estáticos". E quando tomam decisões que valem para um contexto, não cuidam de bem delimitá-lo para que não provoquem avalanches em todos os demais. É um erro que permaneça assim.

Acesso a dados junto a controladores de dados – provedores de aplicações de internet

Como as razões do Min Francisco Rezek no caso MS 21729/DF[41] de 1995 deixam transparecer, 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.[42] Atualmente, compelir empresas a assistir investigações, quebrando-se sigilo, 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 viabilize comunicações não-interceptáveis – isto é, um formato em que a empresa não fosse capaz de acessar comunicações para entregar ao Estado, mesmo que o devido processo legal para o caso fosse observado e as condições de legitimidade estivessem presentes. É esse o debate contemporâneo sobre o uso de criptografia de ponta-a-ponta em aplicações de comunicações à distância como o WhatsApp, por exemplo.[43]

[41] 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.
[42] Ticom et al., "Histórico, implementação e uso do Sistema Guardião® de interceptação de dados de informática e telemática nas garantias do cidadão".
[43] Jacqueline de Souza Abreu, "Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação", *Revista Brasileira de Políticas Públicas* 7, nº 3 (6 de fevereiro de 2018): 24–42, https://doi.org/10.5102/rbpp.v7i3.4869; Carlos Augusto Liguori Filho e João Pedro Favaretto Salvador, "Crypto wars

Historicamente, como se viu, foram os bancos que primeiro levaram casos sobre seus deveres de guarda de sigilo com respeito a informações de clientes. Embora esses casos tenham reafirmado a necessidade de uma postura colaborativa para "habilitar a justiça", parecem ter sido importantes para se afirmar a necessidade de que esses acessos se deem mediante autorização judicial, não fossem excessivos e ocorressem na forma prevista em lei. Embora ainda não existam precedentes paradigmáticos no STF, por parte de empresas de telefonia, há ações diretas de inconstitucionalidade que já foram propostas por entidades representativas dessas empresas contra leis ambíguas e que estabeleceram prerrogativas a autoridades policiais de acesso a dados sem ordem judicial.[44] Algumas empresas também questionam pedidos específicos que lhes parecem abusivos e novas discussões vêm chegando ao STF.[45]

Nesse contexto, coloca-se mais uma perspectiva de análise (da fragilidade) do sigilo telemático. Comunicações privadas são documentadas em escala como nunca foram antes. Pessoas deixam vestígios, pegadas virtuais de suas atividades como nunca deixaram antes.[46] 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. Ao mesmo tempo em que grandes empresas 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"[47] do Estado. Nessa modalidade, como é para bancos e operadoras de telefonia, agentes de aplicação da lei não executam medidas diretamente, mas são *assistidos* por empresas.

---

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 (22 de dezembro de 2018): 135–61, https://doi.org/10.5380/rfdufpr.v63i3.59422.

[44] Por exemplo: é o caso da ADI 5063/DF, que questiona dispositivos da Lei das Organizações Criminosas (Lei nº 12.850/13), cuja leitura combinada seria usada para requerer registros telefônicos sem autorização judicial, e da ADI 5642, sobre os art. 13-A e 13-B incluídos no CPP pela Lei nº 13.344/16, que permitem acesso a dados cadastrais e, em certas circunstâncias, também a dados de geolocalização, sem ordem judicial, entre outros problemas da redação ambígua. Cf. Abreu e Antonialli, "Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais", 27 e 35.

[45] Por exemplo, casos em que se defere a criação de uma "senha" para acesso ao banco de dados da empresa de telefonia. Cf. Abreu, "Quebras de sigilo e privacidade". Também "STF decide que recurso do Google no caso Marielle será tema de repercussão geral", *CNN Brasil*, 28 de maio de 2021, https://www.cnnbrasil.com.br/nacional/stf-decide-que-recurso-do-google-no-caso-marielle-sera-tema-de-repercussao-geral/.

[46] Bruce Schneier, *Data and Goliath: The Hidden Battles to Collect Your Data and Control Your World* (New York: W. W. Norton & Company, 2015), 13–19.

[47] Alan Z. Rozenshtein, "Surveillance Intermediaries", *Stanford Law Review* 70 (janeiro de 2018): 102–89.

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. Se há alguma lição a ser extraída do art. 5º, XII e seu histórico é um interesse em não transformar estruturas de comunicação em máquinas de facilitação de vigilância que anulem a privacidade.

É de se esperar, portanto, a preservação desse compromisso básico, combinado com os dispositivos X e XI enquanto noções que preservam nossa soberania e conferem a atmosfera necessária à nossa autodeterminação pessoal e política, em uma sociedade caracterizada pelas novas "tecnologias de informações e comunicação" (TICs). 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". 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 porque descartar proteções de plano; pelo contrário.

Ademais, nós temos relações fiduciárias com muitas dessas empresas e esperamos delas tratamento que seja respeitoso de nossa privacidade e dos danos morais que o desrespeito pode provocar – 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.[48] Se no passado reconhecemos como relações profissionais com advogados, médicos, padres, contadores, banqueiros poderiam estar cobertas de uma expectativa de privacidade sobre o que é dito, inclusive a ponto de ser tutelado especialmente pelo direito, não há nenhum impedimento para reconhecer relações ou interesses análogos, ainda que não coincidentes. Se nossas relações com bancos até hoje pressupõem esses cuidados, não há porque afastar de partida essa possibilidade para empresas de tecnologia.

O Marco Civil da Internet (Lei nº 12.965/14) é um regime legal relevante a essa inovação tecnológica. 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,

[48] Para uma perspectiva nessa linha no direito americano, ver Kiel Brennan-Marquez, "Fourth Amendment Fiduciaries", *Fordham Law Review* 84, nº 2 (1º de novembro de 2015): 611.

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).

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).

Exceto ao que parecem ser referências pontuais à Lei nº 9.296/96, basicamente não se fala em requisitos materiais para a quebra de sigilo/fornecimento de dados. Para deixar claro: ordem judicial é importante e deve ser mesmo o instrumento regulatório *preferido* em respeito à privacidade nesse contexto, ainda que excepcionalmente, para certas intrusões e tipos de crime, se admita alguma exceção ou que outros mecanismos de tutela equivalentes sejam desenhados. Dito isso, considerando a cética jurisprudência sobre sigilo telemático, a fixação em só falar em autorização judicial cria o risco de que se esvazie dos parâmetros materiais de justa causa e de controles de necessidade – que, como se viu, são imprescindíveis ao respeito ao direito à privacidade em um Estado liberal igualitário e são também características centrais encontradas na jurisprudência do STF, embora balancem aqui ou se escondam acolá. Até aqui, entretanto, como visto no capítulo 4, alguns julgados mais recentes até parecem sugerir que só a Lei nº 9.296/96 impõe requisitos materiais e que eles não existem fora dela para o resto do mundo telemático. Considerando que esse ambiente é constituído por uma infinidade de dados que não são conteúdo

de comunicações privadas entre duas pessoas e por dados que não estão em fluxo, é muito a ficar de fora, como já tratei. (Isso tudo sem contar que o diploma deixa também de se engajar com outras ferramentas regulatórias disponíveis.)

O requisito formal da ordem judicial só foi explicitamente acompanhado de algum tipo de *padrão de justificação* do fornecimento para o fornecimento de registros de conexão e acesso a aplicações de internet (art. 22[49]): 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 de avançar investigações. O padrão de justificação desenhado pelo dispositivo leva em conta o propósito a que foi concebido em seu histórico legislativo[50]: permitir a obtenção de dados relativos a ilícitos praticados na internet como forma de identificar alguém junto aos únicos agentes capazes de auxiliar com o fornecimento de tais dados.

O que se tem assistido, por outro lado, é a uma utilização sobrecarregada de tal dispositivo para autorizar pedidos por quaisquer "dados estáticos" armazenados desde que algum ilícito tenha ocorrido – onde quer que seja, mesmo off-line – e bastando a indicação de um período temporal que se queira. Além de os requisitos materiais necessários à legitimidade da obtenção de informações pessoais pelo Estado serem fragilizados, essa ampliação do dispositivo sujeita pessoas ainda a uma "nova decisão" discricionária sobre danos colaterais a que devem tolerar em contextos não-regulados. Como visto no capítulo 2, se a definição da regra processual não existiu, ou se a decisão judicial desrespeita uma que foi fixada, o ajuste de pesos dos riscos de dano moral que a regra carrega é casuístico – desrespeita a responsabilidade pessoal e pode levar ao tratamento desigual; impõe-se um dano moral sobre um risco que não se assumiu quando as regras do jogo

[49] 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.

[50] Paulo Rená da Silva Santarém, "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), https://repositorio.unb.br/handle/10482/8828; Francisco Carvalho de Brito Cruz, "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.

foram fixadas. (Ironica e tragicamente, quando o art. 22 é corretamente afastado de aplicação em um caso que não envolve registros de IP, como se viu em julgados no STF que versavam sobre acesso a conteúdo de comunicações, é para afastar até suas garantias mínimas: a delimitação de um período para a quebra de sigilo – que, obviamente, também não pode ser definido a critério do freguês, mas apenas no que faça sentido à investigação).

Ao mesmo tempo em que promover categorias aleatórias de proteção que só olham para a qualidade dos dados vai produzir defesas superficiais contra arbítrio e discricionariedade estatal em investigações (se não as anular), o Marco Civil não pode ser interpretado de forma cega aos compromissos normativos que carrega de levar ao ambiente digital proteções e garantias básicas. Considerando os princípios subjacentes identificados e as demais ferramentas regulatórias indicadas por Ohm, é caso de maior atenção a uma revisão significativa (*meaningful review*), com mais regras do que precisa ser demonstrado, de limitação e ao necessário (regras de minimização, de expiração, de barreiras e balizamentos a encontro fortuito[51]). Em termos de transparência, cabe ainda levar a essa área a exigência 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. Tais mecanismos são cruciais para avaliar se as salvaguardas estão funcionando e para permitir debate público qualificado sobre tanto.

Por fim, cabe considerar que, como empresas de tecnologia controladoras de dados pessoais são cada vez mais acionadas para atuarem em investigações criminais em assistência ao Estado, e enquanto não houver uma instituição estatal de defesa que atue nesse estágio de investigações, elas também estão em posição única para questionar ordens de quebra de sigilo que sejam abusivas. Podem trazer questionamentos sobre o teor, natureza e amplitude das ordens antes que a violação irreversível à privacidade ocorra pela instrumentalização de seus serviços e ainda que o principal interessado sequer faça parte da relação ou a despeito de sua vontade. 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

[51] 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 e Machado, "Novos Paradigmas da Investigação Criminal", 30.

produtos e serviços, interesses de usuários (comuns ou corporativos).[52] Isso não impede a análise da cogência do argumento constitucional que suscitem, nem afasta o dever fiduciário que é exigível dessas empresas que possuem um relacionamento específico baseado no compartilhamento de dados pessoais com as pessoas atingidas. Porém mostra que é preocupante pelo que deixarem de questionar, tornando-se cúmplices de ordens abusivas, e que são necessárias outras salvaguardas[53].

Em um ambiente em que os usuários afetados por quebras de sigilo podem nunca nem ficar sabendo de que foram alvo de pedidos (por contra de determinações de silenciamento – *gag orders*) nem "verem" as devassas de que foram alvo, sem possibilidade de questionarem responsabilização pelos danos, e em que medidas são feitas sob segredo de justiça, de modo que não há instâncias de controle fora do ambiente direto das autoridades envolvidas na investigação concreta, devemos buscar mecanismos institucionais que façam as vezes do controle que esperamos em respeito à dignidade. Ao mesmo tempo, 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, quando é, *post facto*, quando alguém é acusado.

3.3 *Privacidade em público e igualdade: monitoramento de áreas públicas e reconhecimento facial*

O terceiro contexto de atuação policial a se comentar as repercussões deste trabalho é o monitoramento de áreas públicas e semi-públicas. O STF não tratou desse tema ainda, mas a contribuição é relevante, tendo em vista que essa é uma medida cada vez mais crescente e traz a oportunidade de já iniciar a história da jurisprudência brasileira nesse tema nos trilhos certos. Se dermos o tratamento genérico de que não há direito à privacidade em público, que a Constituição não ampara qualquer interesse relevante sobre o quando as pessoas fazem quando estão na rua, teremos repisado uma visão pobre do que é privacidade. Ao mesmo tempo, se nos contentarmos com uma solução de que é só uma matéria de calibração de interesses, também deixaremos passar limites duros relevantes que reafirmam *direitos*.

---

[52] "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): 1715–41.

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

Como já tratei, realmente não há um direito forte de não ser visto por outras pessoas em público: isso não tem qualquer correlação com nossas práticas sociais e jurídicas e seria insustentável. Quando esse "ser visto" extrapola capacidades humanas, por outro lado, a história começa a mudar.[54] Apesar de cedermos acesso momentâneo a informações pessoais quando estamos em espaços públicos, graças à memória limitada, desinteresse e outras normas sociais (não ficar "encarando" o outro), pessoas não registram características e tudo o que acontece com relação umas às outras em público – uma capacidade que sempre serviu a um estado de privacidade sobre nossa presença física, nossos deslocamentos e quais *terceiros* tem acesso a eles e por quando tempo.[55] Gerar registros sobre o que as pessoas fizeram em público e mantê-los pode, nesse sentido, criar riscos de causar danos morais a direitos à privacidade e a outros tutelados pelo direito da proteção de dados pessoais (como não-discriminação). Essa possibilidade está relacionada, sobretudo, ao modo *como* implementada e como gerida – já colocando também as questões de legalidade e "governança administrativa" que apresentei. Precisa, no entanto, também ser revista criticamente à luz do tipo de política de segurança pública que queremos avançar e o contexto em que é aplicada.[56]

Vou tratar particularmente de monitoramento público para segurança acoplado a mecanismos de reconhecimento facial: em linhas gerais, essa tecnologia detecta faces em vídeos e imagens, extrai delas uma identificação biométrica única por algoritmos e as compara com os resultados biométricos de uma outra base de dados – que pode ter diferentes amplitudes (pode ser de toda população, de apenas certos grupos de pessoas, ou de só uma pessoa) – com base em certa taxa de similaridade.[57] Nesse contexto, argumentos de privacidade – caso a Administração Pública e o Judiciário se importem em sofisticar suas considerações – podem até ajudar em parte a endereçar a regulação desse uso por autoridades estatais, mas estão longe de ser a única chave com a qual se pode e deve enfrentar o problema.

A começar, a ferramenta pode ser usada em diferentes cenários. Discutir uma (i) aplicação

[54] Nessa linha, ver também Nissenbaum, "Privacy as Contextual Integrity"; Selbst, "Contextual Expectations of Privacy"; Gray, *The Fourth Amendment in an Age of Surveillance*, 167.
[55] Hartzog e Selinger, "Why You Can No Longer Get Lost in the Crowd".
[56] Ver também Pablo Nunes, *Racismo algorítmico e segurança pública* (Nexo Políticas Públicas, 2022), https://pp.nexojornal.com.br/pergunte-a-um-pesquisador/2022/02/02/Pablo-Nunes-racismo-algor%C3%ADtmico-e-seguran%C3%A7a-p%C3%BAblica.
[57] Ver Thiago Guimarães Moraes, Eduarda Costa Almeida, e José Renato Laranjeira de Pereira, "Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces", *AI and Ethics* 1, nº 2 (1º de maio de 2021): 159–72, https://doi.org/10.1007/s43681-020-00014-3.

de reconhecimento facial que só faz autenticação de pessoas (isto é, confirma se uma pessoa é quem ela declara ser) é uma situação; discutir uma (ii) aplicação de reconhecimento facial que serve para identificar um rosto dentro de um conjunto de fotos é outra; (iii) discutir reconhecimento facial para um rastreamento generalizado de pessoas a partir de um banco de dados de identificação abrangente para catalogar por onde vão é outra. São atividades diferentes, são graus de riscos diferentes. Mais que isso: são também práticas que podem se inserir em contextos diferentes da atuação policial e acionar mecanismos de contenção e interesses, direitos e remédios distintos.[58]

O monitoramento público acompanhado de reconhecimento facial generalizado, feito sem suspeita alguma sobre os afetados por definição (situação iii), esbarra em direito forte à privacidade (no sentido de obscuridade) que trabalhei ainda no capítulo 1. Feita como política pública de segurança, buscando prevenção geral contra crimes, o direito trunfa. O Estado não pode, a partir de um interesse genérico de promover alguma segurança, catalogar todas as pessoas e seus trajetos, mesmo em vias públicas. Por mais que isso pudesse trazer ganhos para a segurança pública em geral, não é amparado em um *direito* à segurança e, na verdade, viola um direito à privacidade.

Agora imaginemos a situação ii: monitoramento público por CCTV, mas aplicação de reconhecimento facial implementada apenas para para identificar quem é certa pessoa que foi pega praticando crime e que não se sabe a identidade). A imagem específica dessa pessoa seria cruzada em uma base geral de dados. A princípio, em tese, do ponto de vista de um direito à privacidade, a diligência de desvendar quem é aquela pessoa usando um recurso como o de reconhecimento facial até poderia ser justificável já que seria individualizado a alguém envolvido em crime: existiriam razões especiais pelas quais a pessoa pode ser identificada). Apesar disso, a medida pode suscitar problemas com relação à liberdade de expressão e associação (por exemplo, no uso para identificar pessoas em protestos – um *abuso*) e/ou problemas de justiça graves na execução da procura: ferramentas de reconhecimento facial, no estágio atual da tecnologia, *erram* na identificação de pessoas, o que suscita problemas de criminalização indevida (falsos positivos) – pessoas presas incorretamente por problema na identificação.[59] Pode ainda criminalizar *mais* um grupo de pessoas do que outras, se o banco de dados usado para comparação é, nesse sentido,

[58] Ver essas distinções em Andrew Guthrie Ferguson, "Facial Recognition and the Fourth Amendment", *Minnesota Law Review* 105 (10 de fevereiro de 2021): 1105–1210.

[59] Ver, por exemplo, Bomfim, "'Disseram que eu era traficante', diz pedreiro preso injustamente". Diversos outros casos podem ser acompanhados no O Panóptico – Monitor do Reconhecimento Facial do Brasil < https://opanoptico.com.br/>, projeto do Centro de Estudo de Segurança e Cidadania.

enviesado sobre uma parcela só de pessoas. Tudo isso pode ser feito ainda de forma oculta, sem transparência necessária. Esses são problemas de injustiça que, ainda que não tratemos como um reflexo de um direito à privacidade nesse contexto, impediriam que a medida pudesse ser usada sem contenção de poder adequada contra riscos de abusos, excessos e erros e por mais que, do outro lado, haja uma pretensão legítima de garantir a responsabilização penal de alguém sobre uma ocorrência concreta.

O que dizer, por outro lado, de uma reversão da situação ii: sabe-se que alguém cometeu um crime em alguma ocasião e que essa pessoa possui um mandado de prisão, mas não se sabe onde está. É o caso de monitoramento público com reconhecimento facial para localização de pessoas mediante identificação de quem são. Nesse caso, todos os rostos captados por câmeras são "lidos" e cruzados com bases de dados contendo fotos (e parâmetros) de pessoas pré-selecionadas, gerando algum tipo de sinalização quando alguém procurado é identificado. Também nessa modalidade, da perspectiva do direito à privacidade, até parece que a busca poderia ser feita mediante suspeita individualizada contra tais pessoas procuradas. Ocorre que também nessa modalidade, no entanto, há possíveis erros que levam a criminalizações indevidas e provocam, portanto, questões de justiça por tratamento desigual e abusos. A adoção dessas ferramentas é reflexo de uma política criminal que amplia o poder de controle do Estado e, por essa razão em si mesma, deve ser debatida e, se admitida, contida. As bases de dados criadas e usadas para comparação, por sua vez, suscitam diversos problemas para os quais o direito da proteção de dados pessoais foi vocacionado: envolve por vezes *mission creep* (reutilização de dados criados para outro fim para o de buscar pessoas[60]), bases enviesadas,[61] bases desatualizadas[62]. Essas características também podem permitir questionamentos jurídicos, mesmo que o argumento direto

[60] Kashmir Hill, "The Secretive Company That Might End Privacy as We Know It", *The New York Times*, 18 de janeiro de 2020, seç. Technology, https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html. (contando a história da Clearview AI, empresa de tecnologia que 'raspou' todas as imagens faciais disponíveis na internet, inclusive de plataformas como Twitter, Instagram, para fornecer ferramenta de pesquisa para autoridades de investigação – que podem identificar alguém cujo nome ainda não possuem e encontrar mais traços seus deixados na internet).

[61] Joy Buolamwini e Timnit Gebru, "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification", in *Conference on Fairness, Accountability and Transparency* (Conference on Fairness, Accountability and Transparency, PMLR, 2018), 77–91, http://proceedings.mlr.press/v81/buolamwini18a.html. (identificando disparidades nas classificações de pessoas a partir de algoritmos de reconhecimento facial, com taxas maiores de erros para peles negras, sobretudo mulheres negras).

[62] Por exemplo, "Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano", *G1*, 11 de julho de 2019, https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml.

sobre violação à privacidade não esteja disponível. Para além de privacidade, outros direitos (trunfos) podem estar em questão – como o próprio direito a ser tratado como igual e não ter de suportar os ônus de uma medida de vigilância (correr o risco de ser preso indevidamente) apenas pela cor da pele ou do gênero.

Essas medidas são reflexo de políticas de segurança que preferem altos gastos na implementação e manutenção de tecnologias de contas, controladas sobretudo por agentes privados, aumentando o encarceramento e retroalimentando promessas auto-realizáveis de que crimes ocorrerão, em detrimento da adoção de outras políticas públicas de educação, trabalho, saúde, assistência social – que poderiam reduzir a incidência de jovens em crimes – e de melhoria de recursos e capacitação de policiais em investigações e de melhorias no sistema prisional, que diminuíssem o poder de facções criminosas. Não existe um direito à segurança que inclua um direito das pessoas de serem de algum modo "protegidas" por mecanismos de monitoramento público com reconhecimento facial. Por isso mesmo um direito à privacidade ou outros direitos morais são capazes de trunfar esse tipo de política pública se lhes causa ônus excessivo/dano sério. Nesse sentido, nenhuma dessas medidas poderia ser sequer cogitada sem ampla discussão pública, sem leis autorizadoras que contenham salvaguardas e reflitam decisões coletivas sobre os riscos de danos morais decorrentes desse tipo de medida. Caso definidos parâmetros que não são compatíveis com os princípios até aqui vistos, a própria lei poderá ser questionada.

Na Inglaterra, por exemplo, sistema de vigilância pública com reconhecimento facial para identificação de pessoas de uma "watchlist", e que chegava a ser regulado por um *Surveillance Camera Code of Practice*, foi considerado ilegal por ainda dar espaço a ampla discricionariedade policial quanto à sua forma de uso e a quem integrava a lista, por não oferecer uma análise de impacto de proteção de dados adequada, nem levar em consideração o impacto díspar por questões de raça e gênero por aspectos do próprio software.[63] Apesar de colocar limites, a decisão também não deixou de ser criticada por ter, na sua avaliação de proporcionalidade, passado ao largo das discussões políticas relevantes ao centro do debate sobre tendências de uso de reconhecimento facial[64] – sobre direitos que temos perante um Estado comprometido com a dignidade e que o

[63] Royal Court of Justice, Case No: C1/2019/2670, The Queen (on the application of Edward Bridges) (Appellant) v The Chief Constable of South Wales Police (Respondent) & others [2020] EWCA Civ 1058, j. 11/08/2020. Disponível em: https://www.judiciary.uk/judgments/r-bridges-v-cc-south-wales/ .

[64] Joe Purshouse e Liz Campbell, "Automated Facial Recognition and Policing: A Bridge Too Far?", *Legal Studies*, 2021, 16, https://doi.org/10.1017/lst.2021.22.

vincula mesmo na tarefa de segurança, nas palavras que avancei aqui.

Essas medidas colocam a questão de se queremos capacitar autoridades públicas com uma ferramenta que pode ser facilmente abusada e utilizada para fins escusos, impactar o dia-a-dia de diversas pessoas inocentes, se essa é a visão de política de segurança que efetivamente devemos avançar e se confiamos o suficiente nas instituições democráticas brasileiras responsáveis por fazer os freios e contrapesos. Se não quisermos correr esse risco autoritário, não é algo a se implementar. Não por outra razão, a posição de banimento dessa tecnologia tem sido seriamente discutida em diversos locais do mundo. Mas essa não é só uma questão política – e aqui o resgate da noção de direitos fortes, em detrimento de ver tudo como interesses ponderáveis, mostra onde mora sua força: enquanto a promoção genérica de segurança pública gera dano sério a pessoas inocentes, enquanto o ganho abstrato na segurança coletiva se apoia no ônus a pessoas negras sendo presas indevidamente, enquanto não houver salvaguardas técnicas e jurídicas, essas não são medidas que se compatibilizam com nossos direitos: não mostram respeito a eles. Nossos direitos trunfam essas iniciativas. De fato, não são nem compatíveis com a noção de segurança compatível com a dignidade.

Como visto, mesmo questões mais básicas e "não-tecnológicas" ainda enfrentam desafios para atenderem aos parâmetros de justiça: apenas em 2020 a jurisprudência do STJ reconheceu que o reconhecimento pessoal – que uma vítima faz de seu suposto algoz – pode ter problemas que levam a condenações indevidas de pessoas inocentes[65] e apenas em 2021 reconheceu a necessidade de fundadas razões prévias e preferência da autorização judicial para ingresso em domicílio[66]. Nesse contexto de fragilidades, diria que, além das razões de princípio, há uma inclinação em termos de política pública muito forte para que coisas do tipo não sejam autorizadas como parte de nossa política criminal. Do jeito que está, nossos tribunais demorarão décadas para notar a importância e o impacto desses problemas, a um custo muito grande de danos morais a pessoas inocentes até lá.

4 Conclusão parcial

[65] Superior Tribunal de Justiça, HC 598886, Rel. Min. Rogério Schietti Cruz, Sexta Turma, j. 27.10.2020, DJE 18.12.2020.
[66] Superior Tribunal de Justiça, HC 598051, Rel. Min. Rogério Schietti Cruz, Sexta Turma, j. 02.03.2021, DJE 15.03.2021.

Nesse capítulo, olhei para três aspectos da jurisprudência constitucional brasileira sobre privacidade e segurança: (i) a reverberação frequente ao truísmo de que privacidade não serve para acobertar ilícitos; (ii) o destaque à autorização judicial como mecanismo de controle de avanços sobre a privacidade pelo Estado; e (iii) o status da proteção do "sigilo telemático" – tema em que agrupei tudo o que tenha a ver com dados eletrônicos, digitais.

Se quisermos nos preparar para o futuro, e redirecionar os descaminhos do presente, precisaremos ter em mente que (i) o truísmo não encerra qualquer conversa; (ii) há muito mais ferramental regulatório necessário para lidar com as complexidades do direito à privacidade e da prática que hoje nomeamos de direito da proteção de dados pessoais; e (iii) a área de sigilo telemático coloca uma série de transformações que escancara os problemas de tratar direitos à privacidade a partir de uma fixação com testes binários acerca do que é ou não protegido; (b) uma redução direitos ao sentido de interesses e (c) uma desconexão com a intencionalidade de direitos à privacidade em face do Estado.

CONCLUSÃO

A relação entre os conceitos de privacidade e segurança é muito mais nuançada e imbricada do que a princípio pode parecer. Ao longo da primeira parte desse trabalho, procurei uma articulação atraente desses conceitos, que fosse tanto mais fiel ao sentido e ao valor que damos a cada um deles, como às maneiras como interagem entre si e como lidamos com essas ocasiões de interação em nossas práticas sociais e jurídicas. Na segunda parte, levei as conclusões para a análise do estado do direito constitucional sobre o tema no Brasil.

O caminho a tanto se deu da seguinte forma. No capítulo 1, sobre privacidade, apresentei três formas comuns de compreensão de direitos à privacidade: a partir da dicotomia entre público e privado, que separa as coisas do mundo, nossas atividades e relações entre o que seria protegido e o que não seria, usando testes binários que supõem um critério compartilhado para fazer a triagem; a partir de definição genérica do conceito, pelo qual privacidade se torna um interesse apto a passar por testes de proporcionalidade e exercícios de ponderação; a partir de uma simplificação pela qual a privacidade não protege atividades ilícitas. Defendi que essas compreensões anulam a relevância de contextos, o sentido de ter um direito e nossos interesses de contenção do poder do Estado em respeito à dignidade. Nesses termos, ofereci uma formulação pela qual temos direitos específicos a certas *privacidades* quando pudermos extrair de nossas práticas sociais regras intersubjetivamente compartilhadas que apoiem o reconhecimento de que alguém tem uma prerrogativa de manter certo aspecto de relevância pessoal para si e/ou fora de circulação ou contato do público geral em certo contexto. Essa é uma abordagem que protege a personalidade das pessoas e sua responsabilidade com relação às suas próprias vidas – está, assim, comprometida com a autonomia. Essa mesma autonomia precisa ser protegida em face do poder

do Estado, contra ações que interferem nessas nossas prerrogativas de forma abusiva, errada ou excessiva.

No capítulo 2, ofereci uma formulação do conceito da segurança que também reconhece seu caráter interpretativo e igualmente rejeita que seja compreendido como qualquer interesse – no caso, tornando-o um superprincípio. A concepção mais atraente de segurança, e do que tem de "direito", é a que a vê como um direito a uma regulação pública do Estado que se volte à proteção da vida, da integridade física e da propriedade contra danos de terceiros que comprometem a responsabilidade pessoal. Essa concepção é completamente compatível com a necessidade de se reconhecer direitos à privacidade e de dar a eles respeito em caso de qualquer restrição. A seguir, busquei sintetizar como os propósitos de áreas específicas do direito que giram em torno da noção de *segurança* podem ser justificados e o que revelam sobre suas premissas e compromissos normativos. O direito processual penal e o direito administrativo policial constituem campos da prática jurídica que manifestam a intencionalidade de nossas práticas jurídicas de forma tão central quanto saliente: justificar e conter a coerção estatal. Para que o Estado use a força sobre pessoas de forma legítima, nesses campos que são capazes de conduzir a intervenções graves do Estado na liberdade das pessoas e na igualdade entre elas, isso envolve certos compromissos com decisões políticas tomadas pela comunidade que denotam a importância que é dada a certos procedimentos e regras que balizem a coerção estatal de forma a ser capaz de justificá-la e seu compromisso de não ferir a dignidade. O Estado não pode agir arbitrariamente.

A seguir, e a partir dessas apresentações, sustentei no capítulo 3 que certas circunstâncias oferecem razões especiais para a atuação do Estado por meio de medidas de vigilância (de obtenção de informações). Elas podem ir na contramão de prerrogativas de privacidade que, não fosse por essas razões especiais, teríamos em face de terceiros nas circunstâncias em referência. Essas razões especiais são contextuais – isto é, não é apenas pelo teor da informação ou do canal em questão (se é público ou privado) que se resolve a pergunta sobre o que o Estado pode obter, nem simplesmente porque em algum lugar foi cometido ou pode ser cometido um crime. Não é assim porque não é assim que concebemos quais direitos à privacidade as pessoas têm nem como o Estado deve responder a seu chamado de promover a segurança das pessoas.

Quando diante de um evento criminoso, esperamos que autoridades de investigação do Estado sejam capazes de reunir informações e provas para responsabilizar a pessoa correta: para conter os riscos de violação a direitos fortes à privacidade e ao tratamento como igual incidentes

a essa atividade que seleciona certas pessoas a suportarem ônus específicos do poder estatal, decisões políticas coletivas devem fixar o nível de risco de injustiça aplicável, de forma compatível com nossas práticas na área em geral – algo que, no direito, compõe o processo penal. Diante de um perigo concreto e imediato de que um evento criminoso vá se concretizar, também esperamos de instituições policiais um certo esforço em contê-lo. Diante de políticas mais gerais de segurança pública, precaucionárias, o mesmo cuidado com riscos de que práticas do Estado se incompatibilizem com o respeito que o Estado deve à autenticidade e a responsabilidade das pessoas na condução de suas vidas é devido. Nelas, no entanto, não só exigimos que haja distribuição igualitária de ônus das políticas implementadas pelo Estado, como não admitimos que nossas prerrogativas de privacidade, que diante de qualquer outra pessoa teríamos, sejam afastadas.

Isto é, direitos fortes à privacidade (e à autodeterminação informacional e à igualdade, apesar de não terem sido meu foco) trunfam políticas públicas gerais de segurança. Quando há *suspeita individualizada* pós-evento criminoso, na fórmula clássica do direito processual penal, ou um *perigo concreto e iminente*, na forma específica do direito administrativo policial (subdesenvolvido no Brasil), a dinâmica é diferente: é possível mitigar tais direitos por tais razões especiais, baseadas em dano ou ameaça concreta de dano a direito alheio. Essas exceções devem obedecer aos procedimentos e regras fixados pela comunidade, levando em conta os riscos de danos morais que colocam em questão: o risco de que essas mitigações levem a dano moral – seja porque houve mitigação quando não havia justificativa disponível (abuso), seja porque a justificativa era equivocada (um alarme falso, uma restrição que se mostrou um erro), seja porque ela era excessiva.

Nesse sentido, há um amplo arsenal conceitual e poderosos compromissos morais que podemos encontrar nessa rede de articulação entre os conceitos de privacidade e segurança que se perderia se reduzíssemos tudo a análise de adequação, necessidade e proporcionalidade em sentido estrito. Parte dessa análise de proporcionalidade tem seu lugar em diversos pontos regulatórios e é inerente ao direito administrativo, mas ela não nos aponta e deixa de captar quando há direitos morais em jogo. Sem essa clareza, instalar câmeras nas casas de pessoas em nome de uma promoção genérica de segurança é só *desproporcional*. Com ela, é *errado* por negar prerrogativa moral a que temos direito e apelar a um ideal de segurança que não valorizamos.

Na segunda parte do trabalho, vimos como esses princípios e noções ajudam a explicar e justificar tanto nossos paradigmas sobre direitos a privacidades na Constituição Federal, quanto as

disputas emblemáticas da jurisprudência do STF. Muitos dos nossos direitos jurídicos à privacidade, consagrados já no texto da Constituição Federal, podem ser vistos como resultado do reconhecimento de práticas de respeito à privacidade e dignidade alheia que esperamos de terceiros nas mais frequentes e cotidianas circunstâncias – como não entrar na casa de alguém sem sua autorização. A polícia precisa de "razões especiais" para ser autorizada a deixar de observá-los, ou melhor, de razões por meio das quais mostra respeito à existência daquele direito pela observância de procedimentos e cumprimento de fundamentação suficiente.

A prática da jurisprudência revela esses compromissos: não identificamos uma autorização para que direitos de privacidade sejam violados pelo Estado de forma generalizada para políticas abstratas de segurança pública e, no lugar, vemos como operam as noções de suspeita individualizada e necessidade, muito embora muitas vezes isso se perca sob a alocação errônea de atenção ao elemento da autorização judicial, como se apenas um obstáculo formal fosse. Essa jurisprudência aparenta estar despreparada principalmente para enfrentar novas questões colocadas pela tecnologia – como o uso cada vez mais denso de dados pessoais – que estão nos obrigando a retornar aos fundamentos dos direitos à privacidade e aos princípios políticos que norteiam nossa política criminal de promoção da segurança, no processo penal e no direito administrativo. Esse trabalho, espero, é um resgate dessas premissas e dos compromissos, agora que a visão está turvando.

Nossos direitos à privacidade não se reduzem às interpretações do texto da Constituição Federal que hoje possuem. A inexistência prévia de reconhecimento de um direito moral e jurídico à privacidade em certo contexto (como a uma privacidade que podemos ter em público ou sobre dados estáticos) porque restrições sociais e tecnológicas dispensavam a necessidade de outras proteções e restrições jurídicas não significa que nos resta assistir sentados ao Estado fazer o que quer com novas ferramentas tecnológicas nem que não havia algo que valorizávamos ou que agora valorizamos naquela prática. A inexistência de um direito à privacidade também não significa que outros direitos morais não estão implicados, como a reputação e a igualdade. Cabe-nos averiguar como os princípios que já reconhecemos e protegemos em nossos paradigmas também não amparam o reconhecimento de novas proteções e cobrá-las das instituições do Estado – um esforço com o qual este trabalho quis contribuir.

Em diversos pontos penso que esse trabalho soa como reverberação de ideias já conhecidas: vejo isso como virtude, pois é um esforço de enunciar características centrais do nosso pensamento

comum sobre a articulação da privacidade em face do Estado que devem soar intuitivas para quem é praticante do direito, mas também a qualquer um que pare para refletir sobre como o direito é mobilizado para permitir, autorizar ou proibir a conduta estatal interessada em promover a segurança e em como encontra limites na privacidade. Em cima desse terreno comum, várias controvérsias existem e acredito que essa pesquisa mapeou diversas delas, ofereceu direcionamentos para a doutrina, o debate público e a jurisprudência em alguma delas e abriu agenda de pesquisa sobre diversos pontos.

Por exemplo, embora tenha falado da importância da suspeita individualizada, não me aprofundei sobre a forma como pode e deve ser calibrada e como é também contextual. Também não aprofundei o impacto que algoritmos de inteligência artificial poderiam ter sobre ela, nem sobre seu impacto em policiamento preditivo, embora tenha alertado sobre os avanços de uma noção de segurança *atuarial* que se afasta dos fundamentos de princípio com a dignidade. Ainda, embora tenha falado do direito da proteção de dados pessoais ao longo desse trabalho, não mergulhei na área. Apenas me limitei a sugerir que a concepção mais atraente de direito à autodeterminação informacional é a que combina a implementação de uma política social para justiça no uso de dados pessoais frente a relações assimétricas de poder inerentes a operações de tratamento de dados ainda com o reconhecimento de direitos específicos contra operações que causem danos morais à dignidade de uma perspectiva bem mais abrangente que a linguagem de privacidade oferece. Não deixa direitos se ofuscarem nem esmorecerem sob a linguagem de interesses e pressupostos apenas de proporcionalidade, mas fortalece-os frente a novos problemas decorrentes do uso de dados, deixando trunfos trabalharem em pleno efeito. Há muito a avançar e esse foi um esforço inicial de recuperar as razões que justificam práticas que, até algumas disrupções tecnológicas as chacoalharem, eram consideradas paradigmas. Lidei com o que me pareceu mais urgente no momento – como a área de sigilo telemático e os erros conceituais e práticos de trabalhar com distinções sobre natureza de dados.

Falei na introdução que este era um projeto de pesquisa na intersecção entre teoria do direito, direito constitucional, direito administrativo policial, direito processual penal e direito e tecnologia. Estar nessa intersecção significou em muitos aspectos não descer às profundezas de todas essas áreas. Mas a pesquisa iluminou essa rede e coloca uma agenda de pesquisa para todos esses campos. Para a teoria do direito, acredito que esse trabalho contribui com um esboço de articulação de direitos à privacidade no Dworkin, uma visão de como funcionam "razões

especiais" que autorizam interferências em *trunfos*, e uma demonstração da relevância de sua abordagem interpretativa sobre o direito para questões práticas que enfrentamos dia a dia. Para o direito constitucional brasileiro, mostra fundamentos de racionalidades, furos em interpretações da Constituição Federal que precisam ser revistos e o que escapa ao teste de proporcionalidade. Para o direito da proteção de dados pessoais, mostra o perigo de uma leitura genérica e traiçoeiramente "generosa" do direito da autodeterminação informacional, se abandonarmos a compreensão do que torna um direito um direito e quando estamos diante de danos que configuram injustiças. Recoloca a urgência do desenvolvimento e amadurecimento do direito administrativo policial e de um olhar crítico sobre o valor da segurança que estamos promovendo. Mostra como o direito processual penal deve resgatar e aprofundar suas próprias premissas sobre suspeita individualizada. Para o campo de direito e tecnologia, mostra as repercussões do avanço tecnológico em doutrinas de todas essas outras áreas do direito. Em qualquer lado, espero que essa seja uma contribuição para uma nova rodada de reflexões.

Bibliografia

Livros, artigos, revistas e notícias

Abreu, Jacqueline de Souza. "Comentário ao STJ – REsp 1.782.386/RJ: Acesso a Agenda de Contatos de Celular por Autoridade Policial sem Autorização Judicial". *Revista dos Tribunais* 1026 (2021): 371–406.

———. "Guarda obrigatória de registros de telecomunicações no Brasil: sobre as origens da retenção de dados e as perspectivas para direitos fundamentais". In *¿Nuevos paradigmas de vigilancia? miradas desde América Latina : Memorias del IV Simposio Internacional Lavits, Buenos Aires, 2016*, organizado por Camilo Rios Rozo, 1º ed, 295–306. Buenos Aires: Fundación Vía Libre, 2017.

———. "Infiltrações virtuais no direito brasileiro: mapeando o cenário". In *Direitos Fundamentais e Processo Penal na Era Digital: doutrina e prática em debate*, organizado por Francisco Brito Cruz e Nathalie Fragoso, III:222–33. São Paulo: InternetLab, 2020.

———. "Passado, presente e futuro da criptografia forte: desenvolvimento tecnológico e regulação". *Revista Brasileira de Políticas Públicas* 7, nº 3 (6 de fevereiro de 2018): 24–42. https://doi.org/10.5102/rbpp.v7i3.4869.

———. "Privacidade, proteção de dados pessoais e crises epidemiológicas: racionalidades e lições da pandemia". *Internet & Sociedade* 3 (1º de julho de 2021): 5–26.

———. "Quebras de sigilo e privacidade: três casos idênticos, três resultados diversos". *Gazeta do Povo*, 6 de dezembro de 2017. https://www.gazetadopovo.com.br/opiniao/artigos/quebras-de-sigilo-e-privacidade-tres-casos-identicos-tres-resultados-diversos-1zo7q26et3qh31cd42u88k6sh/.

Abreu, Jacqueline de Souza, e Dennys Antonialli. "Vigilância sobre as comunicações no Brasil: interceptações, quebras de sigilo, infiltrações e seus limites constitucionais". São Paulo: InternetLab, 2017. http://www.internetlab.org.br/wp-content/uploads/2017/05/Vigilancia_sobre_as_comunicacoes_no_Brasil_2017_InternetLab.pdf.

Afonso da Silva, José. *Curso de Direito Constitucional Positivo*. São Paulo: Malheiros, 2009.

Afonso da Silva, Virgilio. *Direito Constitucional Brasileiro*. São Paulo: Edusp, 2021.

———. "O Proporcional e o Razoável". *Revista dos Tribunais*, nº 798 (2002): 23–50.

Aleinikoff, Alexander. "Constitutional Law in the Age of Balancing". *Yale Law Journal* 96, nº 5 (1987): 943.

Alencastro, Luiz Felipe de. "Vida privada e ordem privada no Império". In *História da Vida Privada no Brasil: Império e a modernidade nacional*, organizado por Luiz Felipe de Alencastro, 1ª edição., 2:12–72. São Paulo: Companhia de Bolso, 2019.

Alexander, Larry. "The Philosophy of Criminal Law". In *The Oxford Handbook of Jurisprudence & Philosophy of Law*, organizado por Jules Coleman e Scott Shapiro, 815–67. Oxford: Oxford University Press, 2002.

Alexy, Robert. "Constitutional Rights and Proportionality". *Revus - Journal for Constitutional Theory and Philosophy of Law* 22 (2014): 51–65.

———. *Teoria dos direitos fundamentais*. Traduzido por Virgilio Afonso da Silva. Segunda Edição. São Paulo: Malheiros Editores, 2015.

Algranti, Leila Mezan. “Famílias e vida doméstica”. In *História da Vida Privada no Brasil: Cotidiano e vida privada na América portuguesa*, organizado por Laura de Mello e Souza, 1ª edição., 1:62–119. São Paulo: Companhia de Bolso, 2018.

Allen, Anita L. *Uneasy Access: Privacy for Women in a Free Society*. Rowman & Littlefield, 1988.

Antonialli, Dennys, Jacqueline de Souza Abreu, Heloísa Massaro, e Maria Luciano. “Acesso de Autoridades Policiais a Celulares Em Abordagens e Flagrantes: Retrato e Análise Da Jurisprudência de Tribunais Estaduais”. *Revista Brasileira de Ciências Criminais* 154 (2019): 177–214.

Antonialli, Dennys, Nathalie Fragoso, e Heloísa Massaro. “Da investigação ao encarceramento: as propostas de incremento do uso da tecnologia no Projeto de Lei Anticrime |”. *Boletim IBCCRIM* 318 (maio de 2019). https://www.ibccrim.org.br/boletim_artigo/6337-Da-investigacao-ao-encarceramento-as-propostas-de-incremento-do-uso-da-tecnologia-no-Projeto-de-Lei-Anticrime.

G1. “Após quase três anos preso por crimes que não cometeu, jovem é solto com ajuda do Projeto Inocência”. Acessado 23 de julho de 2021. https://g1.globo.com/fantastico/noticia/2021/07/04/apos-quase-tres-anos-preso-por-crimes-que-nao-cometeu-jovem-e-solto-com-ajuda-do-projeto-inocencia.ghtml.

Ashworth, Andrew, e Lucia Zedner. “Prevention and Criminalization: Justifications and Limits”. *New Criminal Law Review: An International and Interdisciplinary Journal* 15, nº 4 (1º de outubro de 2012): 542–71. https://doi.org/10.1525/nclr.2012.15.4.542.

Assembleia Nacional Constituinte. “Diário da Assembléia Nacional Constituinte (Suplemento ‘B’)”. Brasília, 1988. http://imagem.camara.gov.br/Imagem/d/pdf/307anc23set1988SUPB.pdf.

———. “Diário da Assembléia Nacional Constituinte (Suplemento ‘C’)”. Brasília, 1987. https://www.senado.leg.br/publicacoes/anais/constituinte/9b_Sistematizacao.pdf.

Austin, Lisa M. “Enough About Me: Why Privacy Is About Power, Not Consent (or Harm)”. In *A World without Privacy: What Law Can and Should Do?*, organizado por Austin Sarat, 131–89. Cambridge: Cambridge University Press, 2014.

———. “Re-Reading Westin”. *Theoretical Inquiries in Law* 20, nº 1 (1º de janeiro de 2019): 53–81. https://doi.org/10.1515/til-2019-0003.

Azeredo, João Fábio A. “Sigilo das Comunicações Eletrônicas Diante do Marco Civil da Internet”. In *Direito & Internet III - Tomo II: Marco Civil da Internet (Lei n. 12.965/2014)*, 211–32. São Paulo: Quartier Latin, 2015.

Badaró, Gustavo Henrique. *Direito Processual Penal*. 2º ed. Vol. Tomo I. Rio de Janeiro: Elsevier, 2008.

Barak, Aharon. “Proportionality (2)”. In *The Oxford Handbook of Comparative Constitutional Law*, organizado por Michael Rosenfeld e András Sajo. Oxford: Oxford University Press, 2012.

Barbon, Júlia, e João Pedro Pitombo. “Casos de abusos de policiais em abordagem são rotina no Brasil”. *Folha de S. Paulo*. 18 de julho de 2020. https://www1.folha.uol.com.br/cotidiano/2020/07/casos-de-abusos-de-policiais-em-abordagem-sao-rotina-no-brasil.shtml.

Bennett, Mark, e Petra Butler. “A Dworkinian Right to Privacy in New Zealand”. In *Dignity in the Legal and Political Philosophy of Ronald Dworkin*, organizado por Salman Khurshid,

Lokendra Malik, e Veronica Rodriguez-Blanco, 433–65. Oxford: Oxford University Press, 2018.
Berg, Chris. *The Classical Liberal Case for Privacy in a World of Surveillance and Technological Change*. London: Palgrave Macmillan, 2018. https://www.palgrave.com/gp/book/9783319965826.
Berman, Emily. "Individualized Suspicion in the Age of Big Data". *Iowa Law Review* 105 (2020): 463–506.
———. "When Database Queries Are Fourth Amendment Searches". *Minnesota Law Review* 102 (2017): 577–638.
Bioni, Bruno, e Daniel Dias. "Responsabilidade civil na proteção de dados pessoais: construindo pontes entre a Lei Geral de Proteção de Dados Pessoais e o Código de Defesa do Consumidor". *civilistica.com* 9, nº 3 (22 de dezembro de 2020): 1–23.
Bioni, Bruno R. *Proteção de dados pessoais: a função e os limites do consentimento*. 1º ed. Rio de Janeiro: Forense, 2019.
Bitencourt, Cezar Roberto. *Tratado de Direito Penal – Parte Geral 1*. 14ª Edição. São Paulo: Saraiva, 2009.
Bloustein, Edward J. "Privacy as an Aspect of Human Dignity: An Answer to Dean Prosser". *New York University Law Review* 39 (1964): 962–1007.
Bomfim, Fabiano. "'Disseram que eu era traficante', diz pedreiro preso injustamente". *R7.com*, 15 de dezembro de 2021, seç. Brasília. http://noticias.r7.com/brasilia/disseram-que-eu-era-traficante-diz-pedreiro-preso-injustamente-16122021.
Electronic Frontier Foundation. "Border Searches". Acessado 27 de janeiro de 2022. https://www.eff.org/issues/border-searches.
boyd, danah. *It's Complicated: The Social Lives of Networked Teens*. New Haven: Yale University Press, 2014.
Brayne, Sarah. *Predict and Surveil: Data, Discretion, and the Future of Policing*. Oxford: Oxford University Press, 2020.
———. "The Criminal Law and Law Enforcement Implications of Big Data". *Annual Review of Law and Social Science* 14, nº 1 (2018): 293–308. https://doi.org/10.1146/annurev-lawsocsci-101317-030839.
Brennan-Marquez, Kiel. "Fourth Amendment Fiduciaries". *Fordham Law Review* 84, nº 2 (1º de novembro de 2015): 611.
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.
Bueno, Samira, Renato Sérgio de Lima, e Teixeira, Marco Antonio C. "Limites do uso da força policial no Estado de São Paulo". *Cadernos EBAPE.BR* 17, nº Edição Especial (2019): 783–99.
Buolamwini, Joy, e Timnit Gebru. "Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification". In *Conference on Fairness, Accountability and Transparency*, 77–91. PMLR, 2018. http://proceedings.mlr.press/v81/buolamwini18a.html.
Burkert, Herbert. "Privacy-Data Protection: a German/European Perspective", 1999. http://www.coll.mpg.de/sites/www/files/text/burkert.pdf.

Câmara dos Deputados. *A construção do artigo 5º da Constituição de 1988*. Brasília: Câmara dos Deputados, Edições Câmara, 2013.
Cardoso, Bruno. *Todos os olhos: videovigilâncias, voyeurismos e (re)produção imagética*. Rio de Janeiro: Editora UFRJ; Faperj, 2014.
Castro, Gustavo A. Paolinelli. "Direito à segurança pública no Estado Democrático de Direito: uma releitura à luz da teoria discursiva". *Revista Direito, Estado e Sociedade* 33 (2008): 70–84. https://doi.org/10.17808/des.33.239.
Cate, Fred. "Principles of Internet Privacy". *Connecticut Law Review* 32 (1º de janeiro de 2000): 877–96.
Centro de Análise da Liberdade e do Autoritarismo e Data Privacy Brasil. "Retrospectiva Tecnoautoritarismo 2020 | Laut e Data Privacy Brasil". LAUT, 26 de janeiro de 2021. https://laut.org.br/retrospectiva-tecnoautoritarismo-2020/.
Chaves, Antônio. "Os direitos fundamentais da personalidade moral (à integridade psíquica, à segurança, à honra, ao nome, à imagem, à intimidade)". *Revista de Informação Legislativa* 15, nº 58 (abril de 1978): 157–80.
Coaf – Conselho de Controle de Atividades Financeiras. "Relatório de Atividades 2020". Brasília, 2021. https://www.gov.br/coaf/pt-br/centrais-de-conteudo/publicacoes/publicacoes-do-coaf-1/relatorio-de-atividades-2020-publicado-20210303.pdf.
Cohen, Julie E. "How (Not) to Write a Privacy Law". Knight First Amendment Institute, 23 de março de 2021. https://knightcolumbia.org/content/how-not-to-write-a-privacy-law.
———. "What privacy is for". *Harvard Law Review* 126 (2013): 1904–33.
Costa, Arthur Trindade. "Como as democracias controlam as polícias: os mecanismos institucionais de controle da atividade policial". *Novos Estudos CEBRAP* 70, nº 3 (2004): 65–78.
Costa Júnior, Paulo José da. *O direito de estar só: tutela penal da intimidade*. 4ª ed. rev. atual. São Paulo: Revista dos Tribunais, 2007.
Costa, Luiz. "Privacy and the Precautionary Principle". *Computer Law & Security Review* 28, nº 1 (1º de fevereiro de 2012): 14–24. https://doi.org/10.1016/j.clsr.2011.11.004.
Crespo, Andrew Manuel. "Probable Cause Pluralism". *Yale Law Journal* 129, nº 5 (2020): 1276–1391.
Cretella Júnior, José. "Polícia e poder de polícia". *Revista de Direito Administrativo* 162 (1985): 10–34.
"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): 1715–41.
Dieter, Maurício Stegemann. "O programa de política criminal brasileiro: funções declaradas e reais contribuições de Claus Offe para fundamentação da crítica criminológica à teoria jurídica das penas". *Revista Eletrônica do CEJUR* 1, nº 2 (2007). https://doi.org/10.5380/cejur.v1i2.16744.
———. "Política Criminal Atuarial: A Criminologia do fim da história". Tese de Doutorado, Universidade Federal do Paraná, 2012.
Notícias STJ. "Divulgação de mensagens do WhatsApp pode gerar indenização", 2 de setembro de 2021. https://www.stj.jus.br/sites/portalp/Paginas/Comunicacao/Noticias/02092021-Divulgacao-de-mensagens-do-WhatsApp-sem-autorizacao-pode-gerar-obrigacao-de-indenizar-.aspx.

Folha de S.Paulo. “Dodge questiona vazamento de mensagens e se manifesta contra Lula no Supremo”, 21 de junho de 2019. https://www1.folha.uol.com.br/poder/2019/06/dodge-questiona-vazamento-de-mensagens-e-se-manifesta-contra-lula-no-supremo.shtml.
Doneda, Danilo. *Da Privacidade à Proteção de Dados Pessoais*. Rio de Janeiro: Renovar, 2006.
———. *Da Privacidade à Proteção de Dados Pessoais*. 2º ed. São Paulo: Revista dos Tribunais, 2019.
Donohue, Laura. “The Original Fourth Amendment”. *University of Chicago Law Review* 83 (2016): 1181–1328.
Dotti, René Ariel. “A liberdade e o direito à intimidade”. *Revista de Informação Legislativa* 16, nº 66 (1980): 125–52.
Dworkin, Ronald. *A Matter of Principle*. Clarendon Press, 1985.
———. “Do Values Conflict? A hedgehog’s approach”. *Arizona Law Review* 43 (2001): 251–59.
———. *Domínio da Vida*. São Paulo: Martins Fontes, 2009.
———. *Freedom’s Law: The Moral Reading of the American Constitution*. Oxford: Oxford University Press, 1996.
———. “Hart’s Postscript and the Character of Political Philosophy”. *Oxford Journal of Legal Studies* 24, nº 1 (1º de março de 2004): 1–37. https://doi.org/10.1093/ojls/24.1.1.
———. *Is democracy possible here?* Princeton and Oxford: Princeton University Press, 2006.
———. *Justice for Hedgehogs*. Cambridge, MA: Harvard University Press, 2011.
———. *Law’s Empire*. Harvard University Press, 1986.
———. *Taking Rights Seriously*. Cambridge: Harvard University Press, 1977.
———. “Terror & the Attack on Civil Liberties”. *The New York Review of Books*, 6 de novembro de 2003. http://www.nybooks.com/articles/2003/11/06/terror-the-attack-on-civil-liberties/.
———. *Uma questão de princípio*. 2º ed. São Paulo: Martins Fontes, 2005.
Elize Matsunaga: Era Uma Vez Um Crime. Documentário. Netflix, 2021. https://www.netflix.com/br/title/81043160.
Fabretti, Humberto Barrionuevo. *Segurança pública: fundamentos jurídicos para uma abordagem constitucional*. São Paulo: Atlas, 2013.
Ferguson, Andrew Guthrie. “Facial Recognition and the Fourth Amendment”. *Minnesota Law Review* 105 (10 de fevereiro de 2021): 1105–1210.
———. “Predictive Policing and Reasonable Suspicion”. *Emory Law Journal* 62, nº 2 (2012): 259–325.
———. “Structural Sensor Surveillance”. *Iowa Law Review* 106 (2021): 47–112.
———. *The Rise of Big Data Policing. Surveillance, Race, and the Future of Law Enforcement*. New York: New York Univeristy Press, 2017.
Fernandes, Milton. *Proteção civil da intimidade*. São Paulo: Saraiva, 1977.
Ferraz Junior, Tercio Sampaio. “Sigilo de Dados: o direito à privacidade and os limites da função fiscalizadora do Estado”. *Revista da Faculdade de Direito da Universidade de São Paulo* 88 (1993): 439–59.
Ferreira Filho, Manoel Gonçalves. *Curso de Direito Constitucional*. 35º ed. São Paulo: Saraiva, 2009.
Filho, Carlos Augusto Liguori, e João Pedro Favaretto Salvador. “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 (22 de dezembro de 2018): 135–61. https://doi.org/10.5380/rfdufpr.v63i3.59422.
Filocre, Lincoln D'Aquino. *Direito Policial Moderno*. São Paulo: Almedina, 2017.
Fragoso, Nathalie, e Gabriel Brezinski Rodrigues. "Protodefesa à Brasileira: Contraditório e Ampla Defesa em Investigações Sigilosas". *Direito Público* 18, nº 100 (2021): 581–605.
Fried, Charles. "Privacy". *Yale Law Journal* 77, nº 3 (1968): 475–93.
Friedman, Barry. *Unwarranted: policing without permission*. New York: Farrar, Straus, Giroux, 2017.
Gallie, W. B. "Essentially Contested Concepts". *Proceedings of the Aristotelian Society* 56 (1955): 167–98.
Gavison, Ruth. "Privacy and the Limits of Law". *Yale Law Journal* 89, nº 3 (1980): 421–71.
Gellert, Raphaël. "Data Protection: A Risk Regulation? Between the Risk Management of Everything and the Precautionary Alternative". *International Data Privacy Law* 5, nº 1 (1º de fevereiro de 2015): 3–19. https://doi.org/10.1093/idpl/ipu035.
Gellert, Raphael. "We Have Always Managed Risks in Data Protection Law: Understanding the Similarities and Differences between the Rights-Based and the Risk-Based Approaches to Data Protection". *European Data Protection Law Review (EDPL)* 2 (2016): 481.
Gellert, Raphaël, e Serge Gutwirth. "The legal construction of privacy and data protection". *Computer Law & Security Review* 29, nº 5 (1º de outubro de 2013): 522–30. https://doi.org/10.1016/j.clsr.2013.07.005.
Gielow, Igor. "Dificuldade de rastreamento afeta metade do arsenal de armas no Brasil". Folha de S.Paulo, 29 de julho de 2021. https://www1.folha.uol.com.br/cotidiano/2021/07/dificuldade-de-rastreamento-afeta-metade-do-arsenal-de-armas-no-brasil.shtml.
Gleizer, Orlandino, Lucas Montenegro, e Eduardo Viana. *O direito de proteção de dados no processo penal e na segurança pública*. Rio de Janeiro: Marcial Pons, 2021.
Gray, David. *The Fourth Amendment in an Age of Surveillance*. Cambridge: Cambridge University Press, 2017.
Greco, Luís. "Introdução – 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 *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*, por Jürgen Wolter, 21–82. organizado por Luís Greco. São Paulo: Marcial Pons, 2018.
Greco, Luís, e Orlandino Gleizer. "A infiltração online no processo penal – Notícia sobre a experiência alemã". *Revista Brasileira de Direito Processual Penal* 5, nº 3 (31 de outubro de 2019): 1483–1518. https://doi.org/10.22197/rbdpp.v5i3.278.
Grinover, Ada Pellegrini. *Liberdades públicas e processo penal: as interceptações telefônicas*. São Paulo: Saraiva, 1976.
Gross, Clarissa Piterman. "Pode dizer ou não? Discurso de ódio, liberdade de expressão e a democracia liberal igualitária". Tese de Doutorado, Faculdade de Direito da Universidade de São Paulo, 2017.
Guerra, Maria Pia, e Roberto Dalledone Machado Filho. "O regime constitucional da segurança pública: dos silêncios da Constituinte às deliberações do Supremo Tribunal Federal". *Revista de Informação Legislativa* 55, nº 219 (2018): 155–81.

Guindani, Miriam. “Sistemas de Política Criminal no Brasil: retórica garantista, intervenções simbólicas e controle social punitivo”. In *Series Cadernos CEDES/IUPERJ n. 2*, 1–20. Rio de Janeiro, 2005.

Hadjimatheou, Katerina. “Surveillance Technologies, Wrongful Criminalisation, and the Presumption of Innocence”. *Philosophy & Technology* 30, nº 1 (1º de março de 2017): 39–54.

———. “The Relative Moral Risks of Untargeted and Targeted Surveillance”. *Ethical Theory and Moral Practice* 17, nº 2 (2014): 187–207.

Hart, H. L. A. *Punishment and Responsibility: Essays in the Philosophy of Law*. 2º ed. Oxford: Oxford University Press, 2008.

Hartzog, Woodrow, e Evan Selinger. “Why You Can No Longer Get Lost in the Crowd”. *New York Times*, 17 de abril de 2019. https://www.nytimes.com/2019/04/17/opinion/data-privacy.html?smid=tw-nytopinion&smtyp=cur.

Hert, Paul de, e Serge Gutwirth. “Privacy, Data Protection and Law Enforcement: Opacity of the Individual and Transparency of the Power”. In *Privacy and the Criminal law*, organizado por Erik Claes, Antony Duff, e Serge Gutwirth, 61–104. Antwep/Oxford: Intersentia, 2006.

Hildebrandt, Mireille. “Privacy and Identity”. In *Privacy and the criminal law*, organizado por Erik Claes, Antony Duff, e Serge Gutwirth, 43–57. Oxford: Intersentia, 2006.

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

Hill, Kashmir. “The Secretive Company That Might End Privacy as We Know It”. *The New York Times*, 18 de janeiro de 2020, seç. Technology. https://www.nytimes.com/2020/01/18/technology/clearview-privacy-facial-recognition.html.

Hirsch, Dennis, e Jonathan King. “Big Data Sustainability: An Environmental Management Systems Analogy”. *Washington and Lee Law Review Online* 72, nº 3 (31 de março de 2016): 406.

Hoffmann-Riem, Wolfgang. “Der grundrechtliche Schutz der Vertraulichkeit und Integrität eigengenutzter informationstechnischer Systeme”. *JuristenZeitung* 21 (2008): 1009–22.

Hubmann, Heinrich. “Der zivilrechtliche Schutz der Persönlichkeit gegen Indiskretion”. *JuristenZeitung* 12, nº 17 (1957): 521–28.

Igo, Sarah E. *The Known Citizen*. Cambridge, MA: Harvard University Press, 2018.

Jancsó, István. “A sedução da liberdade: cotidiano e contestação política no final do século XVIII”. In *História da Vida Privada no Brasil: Cotidiano e vida privada na América portuguesa*, organizado por Laura de Mello e Souza, 1ª edição., 1:304–50. São Paulo: Companhia de Bolso, 2018.

Joh, Elizabeth E. “The New Surveillance Discretion: Automated Suspicion, Big Data, and Policing”. *Harvard Law & Policy Review* 10 (2016): 15–42.

Júnior, Ronaldo Porto Macedo. “Liberdade de expressão: que lições devemos aprender da experiência americana?” *Revista Direito GV* 13, nº 1 (30 de maio de 2017): 274–302.

Justen Filho, Marçal. *Curso de direito administrativo [livro eletrônico]*. 5º ed. São Paulo: Thomson Reuters Brasil, 2018.

Folha de S.Paulo. “Justiça de SP autoriza uso de bala de borracha pela PM em manifestações”, 8 de novembro de 2016. http://www1.folha.uol.com.br/cotidiano/2016/11/1830368-justica-de-sp-libera-uso-de-bala-de-borracha-pela-pm-em-manifestacoes.shtml.

Kanashiro, Marta Mourão. “Biometria no Brasil e o registro de identidade civil: novos rumos para a identificação”. Tese de Doutorado, Faculdade de Filosofia, Letras e Ciências Humanas da Universidade de São Paulo, 2011.
Kemeny, Richard. “Brazil Is Sliding into Techno-Authoritarianism”. MIT Technology Review, 19 de agosto de 2020. https://www.technologyreview.com/2020/08/19/1007094/brazil-bolsonaro-data-privacy-cadastro-base/.
Klatt, Matthias, e Moritz Meister. *The Constitutional Structure of Proportionality*. Oxford: Oxford University Press, 2012.
Knijnik, Danilo. “A trilogia Olmstead-Katz-Kyllo: o art. 5o da Constituição Federal do século XXI”. *Revista da Escola da Magistratura do TRF da 4a Região* 4 (2016): 77–96.
Lazarus, Liora. “Mapping The Right to Security”. In *Security and Human Rights*, organizado por Liora Lazarus e Benjamin Goold, 325–46. Oxford; Portland: Hart Publishing, 2007.
———. “The Right to Security”. In *Philosophical Foundations of Human Rights*, organizado por Rowan Cruft, S. Matthew Liao, e Massimo Renzo, 423–41. Oxford: Oxford University Press, 2015.
———. “The Right to Security: Securing Rights or Securitizing Rights?” In *Examining Critical Perspectives on Human Rights*, organizado por Rob Dickinson, 87–106. Cambridge: Cambridge University Press, 2012.
Lazzarini, Álvaro. “A ordem constitucional de 1988 e a ordem pública”. *Revista de Informação Legislativa* 115 (1992): 275–94.
Lessig, Lawrence. “Reading the Constitution in Cyberspace”. *Emory Law Journal* 45, nº 3 (1996): 869–910.
Lever, Annabelle. “Privacy rights and democracy: a contradiction in terms?” *Contemporary Political Theory* 5 (2006): 142–62.
Lima, Renato Sérgio de, Samira Bueno, e Guaracy Mingardi. “Estado, polícias e segurança pública no Brasil”. *Revista Direito GV* 12, nº 1 (abril de 2016): 49–85. https://doi.org/10.1590/2317-6172201603.
Lipsky, Michael. *Street-Level Bureaucracy: The Dilemmas of the Individual in Public Service*. Russell Sage Foundation, 1983.
Louzada, Luiza. “Princípios da LGPD e os bancos de perfis genéticos: instrumentalizando a garantia de direitos no processo penal”. *Revista do Advogado* 144 (novembro de 2019): 90–98.
Luz, Yuri Corrêa da. “O combate à corrupção entre direito penal e direito administrativo sancionador”. *Revista Brasileira de Ciências Criminais* 89 (2011): 429–70.
Lynskey, Orla. *The Foundations of EU Data Protection Law*. Oxford: Oxford University Press, 2015.
Macedo Junior, Ronaldo Porto. *Contratos Relacionais e Defesa do Consumidor*. 2º ed. São Paulo: Editora Revista dos Tribunais, 2007.
———. *Do xadrez à cortesia: Dworkin e a teoria do direito contemporânea*. São Paulo: Saraiva, 2013.
———. “Temos direito a uma justiça penal que não seja completamente ineficaz?” *Fumus boni iuris - O Globo*, 19 de março de 2021. https://blogs.oglobo.globo.com/fumus-boni-iuris/post/ronaldo-porto-macedo-junior-temos-direito-uma-justica-penal-que-nao-seja-completamente-ineficaz.html.
Machado, Marta Rodriguez de Assis. *Sociedade do risco e direito penal: uma avaliação de novas tendências político-criminais*. São Paulo: IBCCRIM, 2005.

MacKinnon, Catharine A. *Toward a Feminist Theory of the State*. Harvard University Press, 1989.
Macnish, Kevin. "Government Surveillance and Why Defining Privacy Matters in a Post-Snowden World". *Journal of Applied Philosophy* 35, nº 2 (2018): 417–32. https://doi.org/10.1111/japp.12219.
———. "Just Surveillance? Towards a Normative Theory of Surveillance". *Surveillance & Society* 12, nº 1 (2014): 142–53.
Manso, Bruno Paes, e Camila Nunes Dias. *A guerra: a ascensão do PCC e o mundo do crime no Brasil*. São Paulo: Todavia, 2018.
Manunta, Giovanni. "What Is Security?" *Security Journal* 12, nº 3 (1º de julho de 1999): 57–66. https://doi.org/10.1057/palgrave.sj.8340030.
Marmor, Andrei. "What Is the Right to Privacy?" *Philosophy and Public Affairs* 43, nº 1 (Winter de 2015): 3–26.
Mata, Jéssica da. *A política do enquadro*. São Paulo: Revista dos Tribunais, 2021.
Mathews, Jud, e Alec Sweet. "Proportionality Balancing and Global Constitutionalism". *Columbia Journal of Transnational Law* 47 (1º de janeiro de 2009): 72–164.
Matida, Janaína, e Antonio Vieira. "Para além do BARD: uma crítica à crescente adoção do standard de prova 'para além de toda a dúvida razoável' no processo penal brasileiro". *Revista Brasileira de Ciências Criminais* 156 (2019): 221–48.
Mattiuzzo, Marcela. "'Let the Algorithm Decide': Is Human Dignity at Stake?" *Revista Brasileira de Políticas Públicas* 11, nº 1 (2 de abril de 2021). https://www.publicacoes.uniceub.br/RBPP/article/view/6784.
Mayer-Schönberger, Viktor. "Generational Development of Data Protection in Europe". In *Technology and Privacy: The New Landscape*, organizado por Philip E. Agre e Marc Rotenberg, 219–41. Cambridge, MA: The MIT Press, 1997.
McClain, Linda. "Inviolability and Privacy: The Castle, the Sanctuary, and the Body". *Yale Journal of Law & the Humanities* 7, nº 1 (8 de maio de 2013): 195–241.
Meirelles, Hely Lopes. *Direito Administrativo Brasileiro*. 22º ed. São Paulo: Malheiros, 1997.
Mendes, Conrado Hubner. "Direito à segurança e a sensação de segurança". Época, 25 de janeiro de 2019. https://oglobo.globo.com/epoca/direito-seguranca-a-sensacao-de-seguranca-23397881.
Mendes, Laura Schertel. "Autodeterminação informacional: origem e desenvolvimento conceitual na jurisprudência da Corte Constitucional alemã". In *Lei Geral de Proteção de Dados (Lei nº 13.709/2018): a caminho da efetividade: contribuições para a implementação da LGPD*, organizado por Danilo Doneda, Laura Schertel Mendes, e Ricardo Villas Bôas Cueva, 211–42. São Paulo, 2020.
———. *Privacidade, proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental*. São Paulo: Saraiva, 2014.
Miranda, Pontes de. *Tratado de Direito Privado: Parte Especial – Tomo VII: Direito de personalidade, Direito de Família*. Atualizada. São Paulo: Revista dos Tribunais, 2012.
Möller, Kai. "Proportionality and Rights Inflation". In *Proportionality and the Rule of Law: Rights, Justification, Reasoning*, organizado por Bradley W. Miller, Grant Huscroft, e Grégoire Webber, 155–72. Cambridge: Cambridge University Press, 2014. https://doi.org/10.1017/CBO9781107565272.010.

Monteiro, Artur Pericles Lima. “Online anonymity in Brazil: identification and the dignity in wearing a mask”. Dissertação de Mestrado, Faculdade de Direito da Universidade de São Paulo, 2017.
Moore, Adam D. *Privacy Rights: Moral and Legal Foundations*. University Park, PA: Penn State University Press, 2010.
Moraes, Thiago Guimarães, Eduarda Costa Almeida, e José Renato Laranjeira de Pereira. “Smile, You Are Being Identified! Risks and Measures for the Use of Facial Recognition in (Semi-)Public Spaces”. *AI and Ethics* 1, nº 2 (1º de maio de 2021): 159–72. https://doi.org/10.1007/s43681-020-00014-3.
Moro Martins, Rafael, Alexandre de Santi, e Glenn Greenwald. “‘Não é muito tempo sem operação?’ Exclusivo: chats revelam colaboração proibida de Sergio Moro com Deltan Dallagnol na Lava Jato”. *The Intercept Brasil*, 9 de junho de 2019. https://theintercept.com/2019/06/09/chat-moro-deltan-telegram-lava-jato/.
Mulligan, Deirdre K., Colin Koopman, e Nick Doty. “Privacy is an essentially contested concept: a multi-dimensional analytic for mapping privacy”. *Philosophical Transactions of the Royal Society A: Mathematical, Physical and Engineering Sciences* 374: 20160118, nº 2083 (28 de dezembro de 2016): 1–15. https://doi.org/10.1098/rsta.2016.0118.
Nagel, Thomas. “Concealment and Exposure”. *Philosophy and Public Affairs* 27, nº 1 (janeiro de 1998): 3–30.
———. “The Value of Inviolability”. In *Morality and Self-Interest*, organizado por Paul Bloomfield, 102–13. Oxford: Oxford University Press, 2007.
Nery, Rosa Maria de Andrade, e Nelson Nery Junior. *Instituições de Direito Civil: volume I [livro eletrônico]: parte geral do Código Civil e direitos da personalidade*. 2º ed. São Paulo: Thomson Reuters, 2019.
Nigri, Tânia. *O Sigilo Bancário e a Jurisprudência do Supremo Tribunal Federal*. São Paulo: IASP, 2016.
Nissenbaum, Helen. “Privacy as Contextual Integrity”. *Washington Law Review* 79 (2004): 119–58.
———. *Privacy in Context: Technology, Policy, and the Integrity of Social Life*. Stanford, CA: Stanford University Press, 2010.
Nunes, Diego. “As iniciativas de reforma à Lei de Segurança Nacional na consolidação da atual democracia brasileira: da inércia legislativa na defesa do Estado Democrático de Direito à ascensão do terrorismo”. *Revista Brasileira de Ciências Criminais* 107 (2014): 265–305.
———. “‘Garantia da Lei e da Ordem’, ‘comoção intestina’ e outras vaguezas constitucionais na história dos regimes jurídicos da exceção”. In *Estudos de direito público: aspectos penais e processuais*, organizado por Leonardo Schmitt de Bem, D’Plácido., 633–38. Belo Horizonte, 2018.
Nunes, Pablo. *Racismo algorítmico e segurança pública*. Nexo Políticas Públicas, 2022. https://pp.nexojornal.com.br/pergunte-a-um-pesquisador/2022/02/02/Pablo-Nunes-racismo-algor%C3%ADtmico-e-seguran%C3%A7a-p%C3%BAblica.
Odon, Tiago Ivo. “Segurança pública e análise econômica do crime: o desenho de uma estratégia para a redução da criminalidade no Brasil”. *Revista de Informação Legislativa* 55, nº 218 (2018): 33–61.
Ohm, Paul. “The Surveillance Regulation Toolkit: Thinking Beyond Probable Cause”. In *The Cambridge Handbook of Surveillance Law*, organizado por David Gray e Stephen Henderson, 491–508. Cambridge: Cambridge University Press, 2017.

Oliveira, Nina Ribeiro Nery de. “O Conselho de Controle de Atividades Financeiras – COAF e a Nulidade das Provas”. Monografia (Especialização), Instituto Brasiliense de Direito Público - IDP, 2016.

Peron, Alcides Eduardo dos Reis, e Marcos César Alvarez. “Governing the City: The Detecta Surveillance System in São Paulo and the Role of Private Vigilantism in the Public Security”. *Sciences Actions Sociales* N° 12, nº 2 (2019): 33–68.

Piccolo, Carla Henriete Bevilacqua. “A moral e o conceito de direito em H.L.A. Hart”. Mestrado, Faculdade de Direito da Universidade de São Paulo, 2011. https://www.teses.usp.br/teses/disponiveis/2/2139/tde-06062012-091850/publico/Carla_Henriete_Bevilacqua_Piccolo_ME.pdf.

Pieroth, Bodo, e Bernhard Schlink. *Grundrechte, Staatsrecht II*. 28. Auflage. Heidelberg: C.F. Müller, 2012.

Pimenta, Victor Martins, Izabella Lacerda Pimenta, e Danilo Cesar Maganhoto Doneda. “‘Onde eles estavam na hora do crime?’: Ilegalidades no tratamento de dados pessoais na monitoração eletrônica”. *Revista Brasileira de Segurança Pública* 13, nº 1 (20 de setembro de 2019): 59–75.

Fantástico. “Polícia encontra hackers que roubaram fotos de Carolina Dieckmann”, 13 de maio de 2012. http://g1.globo.com/fantastico/noticia/2012/05/policia-encontra-hackers-que-roubaram-fotos-de-carolina-dieckmann.html.

Pombo, Bárbara. “Consumidores buscam danos morais por vazamento de dados”. *Valor Econômico* (blog), 18 de julho de 2021. https://valor.globo.com/legislacao/noticia/2021/07/18/consumidores-buscam-danos-morais-por-vazamento-de-dados.ghtml.

Ponce, Paula Pedigoni, e Rafael Mafei Rabelo Queiroz. “Tércio Sampaio Ferraz Júnior e Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado: o que permanece e o que deve ser reconsiderado”. *Internet & Sociedade* 1, nº 1 (18 de fevereiro de 2020): 64–90.

Powell, Rhonda. *Rights as Security: The Theoretical Basis of Security of Person*. Oxford, New York: Oxford University Press, 2019.

Prado, Daniel Nicory do. “Prisão em flagrante em domicílio: um olhar empírico”. *Revista Direito GV* 16, nº 2 (2020): e1962. https://doi.org/10.1590/2317-6172201962.

Prosser, William. “Privacy”. *California Law Review* 48, nº 3 (31 de agosto de 1960): 383. https://doi.org/10.15779/Z383J3C.

Purshouse, Joe, e Liz Campbell. “Automated Facial Recognition and Policing: A Bridge Too Far?” *Legal Studies*, 2021, 1–19. https://doi.org/10.1017/lst.2021.22.

Queiroz, Rafael Mafei Rabelo. *O Direito a Ações Imorais: Paul Johann Anselm von Feuerbach e a construção do moderno direito penal*. São Paulo: Almedina, 2012.

———. “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.

Queiroz, Rafael Mafei Rabelo, e Natalia Neris. “Revoar - Servir a quem, proteger o quê?” Temporada 1. Acessado 6 de agosto de 2020. https://open.spotify.com/episode/6UnkIg44OkZdwifCB5uULL?si=oaHHYracRrOow1ZpkcrxQA.

Quito, Carina. “Acesso a Comunicações Eletrônicas Armazenadas na Prática Judiciária”. In *Direitos Fundamentais e Processo Penal na Era Digital: Doutrina e Prática em Debate*, organizado por Dennys Antonialli e Jacqueline de Souza Abreu, I:100–107. São Paulo: InternetLab, 2018.

Reiman, Jeffrey H. “Privacy, Intimacy, and Personhood”. *Philosophy & Public Affairs* 6, nº 1 (1976): 26–44.

Renan, Daphna. “The Fourth Amendment as Administrative Governance”. *Stanford Law Review* 68, nº 5 (2016): 1039–1129.

Report of the Advisory Committee on Automated Data Systems. “Records, Computers, and The Rights of Citizens”. U.S. Department of Health, Education & Welfare, julho de 1973. https://www.justice.gov/opcl/docs/rec-com-rights.pdf.

Ribeiro, Caio Gentil. “Para além da subsunção e do sopesamento: uma crítica à teoria da proporcionalidade a partir do caso da liberdade de expressão”. *Revista Publicum* 5, nº 1 (5 de novembro de 2019): 221–37. https://doi.org/10.12957/publicum.2019.30353.

Richards, Neil. *Intellectual Privacy: Rethinking Civil Liberties in the Digital Age*. 1st edition. Oxford, UK; New York, NY: Oxford University Press, 2015.

Richards, Neil M. “The Dangers of Surveillance”. *Harvard Law Review* 126 (2013): 1934–65.

Richards, Neil M., e Woodrow Hartzog. “A Duty of Loyalty for Privacy Law”. SSRN Scholarly Paper. Rochester, NY: Social Science Research Network, 3 de julho de 2020. https://doi.org/10.2139/ssrn.3642217.

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.

Rosa, Leonardo G. P. “GPS, privacidade e judiciário: breve análise de decisão da Suprema Corte dos EUA”. *Revista Brasileira de Ciências Criminais* 105 (2013): 363–74.

———. “O liberalismo igualitário de Ronald Dworkin: o caso da liberdade de expressão”. Dissertação de Mestrado, Faculdade de Direito da Universidade de São Paulo, 2014.

Rosenthal, Lawrence. “The Case for Surveillance”. In *The Cambridge Handbook of Surveillance Law*, organizado por David Gray e Stephen Henderson, 308–29. Cambridge: Cambridge University Press, 2017.

Rozenshtein, Alan Z. “Surveillance Intermediaries”. *Stanford Law Review* 70 (janeiro de 2018): 102–89.

Santarém, Paulo Rená 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. 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.

Schreiber, Anderson. *Direitos de personalidade*. 2º ed. São Paulo: Atlas, 2013.

Schwartz, Paul M. “The Computer in German and American Constitutional Law: Towards an American Right of Informational Self-Determination”. *American Journal of Comparative Law* 37 (1989): 675–705.

Selbst, Andrew D. “Contextual Expectations of Privacy”. *Cardozo Law Review* 35 (2014 de 2013): 643–709.

Sennett, Richard. *The Fall of Public Man*. Penguin UK, 2003.

Shapiro, Stuart. “Places and Spaces: The Historical Interaction of Technology, Home, and Privacy”. *The Information Society* 14, nº 4 (1º de novembro de 1998): 275–84. https://doi.org/10.1080/019722498128728.
Shecaira, Sérgio Salomão. *Criminologia*. 4º ed. São Paulo: Editora Revista dos Tribunais, 2012.
Sidi, Ricardo. “A interceptação de e-mails e a apreensão física de e-mails armazenados”. *Revista Fórum de Ciências Criminais* 4 (julho de 2015): 101–21.
Siegel, Reva B. “‘The Rule of Love’: Wife Beating as Prerogative and Privacy”. *The Yale Law Journal* 105, nº 8 (1996): 2117–2207. https://doi.org/10.2307/797286.
Simitis, Spiros, Gerrit Hornung, e Indra Spiecker gen. Döhmann, orgs. *Datenschutzrecht*. Baden-Baden: Nomos, 2019.
G1. “Sistema de reconhecimento facial da PM do RJ falha, e mulher é detida por engano”, 11 de julho de 2019. https://g1.globo.com/rj/rio-de-janeiro/noticia/2019/07/11/sistema-de-reconhecimento-facial-da-pm-do-rj-falha-e-mulher-e-detida-por-engano.ghtml.
Slobogin, Christopher. “Government Dragnets”. *Law and Contemporary Problems* 73, nº 3 (1º de julho de 2010): 107–43.
———. “Panvasive Surveillance, Political Process Theory, and the Nondelegation Doctrine”. *Georgetown Law Journal* 102 (2014 de 2013): 1721.
———. “Subpoenas and Privacy”. *DePaul Law Review* 54 (2005): 805–45.
Smith, Hillel R. “Do Warrantless Searches of Electronic Devices at the Border Violate the Fourth Amendment?” Congressional Research Service, 17 de março de 2021.
Solove, Daniel. “A Brief History of Information Privacy Law”. In *Proskauer on Privacy: A Guide to Privacy and Data Security Law in the Information Age*, organizado por Christopher Wolf, 1–46. Practising Law Institute, 2006.
———. “‘I’ve Got Nothing to Hide’ and Other Misunderstandings of Privacy”. *San Diego Law Review* 44, nº 4 (2007): 745–72.
Solove, Daniel J. “Digital Dossiers and the Dissipation of Fourth Amendment Privacy”. *Southern California Law Review* 75 (2002 de 2001): 1083–1168.
———. *Understanding Privacy*. Cambridge, MA: Harvard University Press, 2008.
Solove, Daniel J., e Paul M. Schwartz. *Information Privacy Law*. 5º ed. New York: Wolters Kluwer, 2015.
Solove, Daniel, e Neil Richards. “Privacy’s Other Path: Recovering the Law of Confidentiality”. *The Geogetown Law Journal* 96 (2007): 123–82.
Soprana, Paula. “PF compra sistema que cruzará dados biométricos de 50 milhões de brasileiros”. *Folha de S.Paulo*, 7 de julho de 2021, seç. Tec. https://www1.folha.uol.com.br/tec/2021/07/pf-compra-sistema-que-cruzara-dados-biometricos-de-50-milhoes-de-brasileiros.shtml.
Souza, Adilson Paes de. “PM aposentado conta assalto e sequestro que sofreu e critica políticas de segurança”. *Folha de S.Paulo*, 22 de janeiro de 2022. https://www1.folha.uol.com.br/ilustrissima/2022/01/pm-aposentado-conta-assalto-e-sequestro-que-sofreu-e-critica-politicas-de-seguranca.shtml.
Souza, Luís Antônio Francisco. “Polícia, direito e poder de polícia. A polícia brasileira entre a ordem pública e a lei.” *Revista Brasileira de Ciências Criminais* 43 (2003): 295–321.
Stewart, Hamish. “Concern and Respect in Procedural Law”. In *The Legacy of Ronald Dworkin*, organizado por Will Waluchow e Stefan Sciaraffa, 373–89. Oxford: Oxford University Press, 2016.

CNN Brasil. “STF decide que recurso do Google no caso Marielle será tema de repercussão geral”, 28 de maio de 2021. https://www.cnnbrasil.com.br/nacional/stf-decide-que-recurso-do-google-no-caso-marielle-sera-tema-de-repercussao-geral/.

Migalhas. “STF: Suspenso julgamento sobre validade de provas obtidas no WhatsApp sem autorização”, 12 de junho de 2019. https://www.migalhas.com.br/Quentes/17,MI304267,21048-STF+Suspenso+julgamento+sobre+validade+de+provas+obtidas+no+WhatsApp.

Strandburg, Katherine. “Home, Home on the Web and Other Fourth Amendment Implications of Technosocial Change”. *Maryland Law Review* 70, nº 3 (1º de janeiro de 2011): 614–80.

Sunstein, Cass R., e Adrian Vermeule. “The Morality of Administrative Law”. *Harvard Law Review* 131, nº 7 (2018): 1924–77.

Tácito, Caio. “O poder de polícia e seus limites”. *Revista de Direito Administrativo* 27 (1952): 1–11.

———. “Poder de polícia e polícia do poder”. *Revista de Direito Administrativo* 162 (1985): 1–9.

Tadros, Victor. “Crimes and Security”. *The Modern Law Review* 71, nº 6 (1º de novembro de 2008): 940–70. https://doi.org/10.1111/j.1468-2230.2008.00730.x.

———. “Power and the value of privacy”. In *Privacy and the Criminal Law*, organizado por Erik Claes, Serge Gutwirth, e Antony Duff, 105–20. Antwerp/Oxford: Intersentia, 2006.

Thorburn, Malcolm. “Criminal Law as Public Law”. In *Philosophical Foundations of Criminal Law*, organizado por RA Duff e Stuart P. Green, 21–43. Oxford: Oxford University Press, 2011.

———. “Identification, Surveillance, and Profiling: On the Use and Abuse of Citizen Data”. In *Seeking Security: Pre-empting the Comission of Criminal Harms*, organizado por G R Sullivan e Ian Dennis, 15–35. Oxford: Hart Publishing, 2012.

———. “Justifications, Power, and Authority”. *Yale Law Journal* 117, nº 6 (2008): 1170–1130.

Ticom, Miguel Ângelo Duarte, Wanderson de Freitas Pereira Neto, Silde Monteiro de Albuquerque, Israel Carbone de Carvalho, e Arnaldo Rosa Silva Jr. “Histórico, implementação e uso do Sistema Guardião® de interceptação de dados de informática e telemática nas garantias do cidadão”. *Cadernos de Segurança Pública* 12 (setembro de 2020).

Tsakyrakis, Stavros. “Proportionality: An assault on human rights?” *International Journal of Constitutional Law* 7 (2009): 468–93.

Tribunal Superior Eleitoral. “TSE e Polícia Federal vão compartilhar banco de dados biométricos”. Tribunal Superior Eleitoral, 16 de novembro de 2017. https://www.tse.jus.br/imprensa/noticias-tse/2017/Novembro/tse-e-policia-federal-vao-compartilhar-banco-de-dados-biometricos.

“Vídeo mostra diretor da Yoki com amante, na véspera do assassinato”. *Bom Dia Brasil*. Globo, 11 de junho de 2012. http://g1.globo.com/bom-dia-brasil/noticia/2012/06/video-mostra-diretor-da-yoki-com-amante-na-vespera-do-assassinato.html.

Vilalta, Luís Antônio, e Talles Amaral Machado. “Novos Paradigmas da Investigação Criminal”. *Revista Brasileira de Ciências Policiais* 9, nº 1 (8 de novembro de 2018): 13–41. https://doi.org/10.31412/rbcp.v9i1.542.

Volkszählung (BVerfGE 65, 1 15 de dezembro de 1983).

Wachter, Sandra, e Brent Mittelstadt. “A Right to Reasonable Inferences: Re-Thinking Data Protection Law in the Age of Big Data and AI”. *Columbia Business Law Review* 2019 (2019): 494–620.
Waldron, Jeremy. “Accountability and Insolence”. In *Political Political Theory: Essays on Institutions*, 167–94. Cambridge, MA: Harvard University Press, 2016.
———. “Safety and Security”. *Nebraska Law Review* 85, nº 2 (2011): 454–507.
———. *The Harm in Hate Speech*. Reprint edição. Cambridge: Harvard University Press, 2014.
———. *Torture, Terror, and Trade-Offs: Philosophy for the White House*. Oxford: Oxford University Press, 2010.
Wanderley, Gisela Aguiar. “A busca pessoal no direito brasileiro: medida processual probatória ou medida de polícia preventiva?” *Revista Brasileira de Direito Processual Penal* 3, nº 3 (set.-dez de 2017): 1117–54.
———. “A Quarta Emenda e o controle judicial da atividade policial: busca e apreensão e stop and frisk na jurisprudência da Suprema Corte estadunidense”. *Revista de Direito Brasileira* 24, nº 9 (1º de dezembro de 2019): 341–64. https://doi.org/10.26668/IndexLawJournals/2358-1352/2019.v24i9.3259.
———. “Comentário ao STF - RE 603.616/RO: Busca domiciliar sem mandado judicial em situação de flagrante de crime permanente”. *Revista dos Tribunais* 966 (2016): 337–59.
———. “Entre a lei processual e a praxe policial: Características e consequências da desconcentração e do descontrole da busca pessoal”. *Revista Brasileira de Ciências Criminais*, nº 128 (2017): 115–49.
———. “Privacidade e Cidadania: os limites jurídicos da atividade investigativa e a legalidade do acesso policial a aparelhos celulares”. In *Direitos Fundamentais e Processo Penal na Era Digital*, organizado por Dennys Antonialli e Nathalie Fragoso, 2:108–31. São Paulo: InternetLab, 2019.
Warren, Samuel, e Louis Brandeis. “The Right to Privacy”. *Harvard Law Review* 4, nº 5 (1890): 193–220.
Wermuth, Maiquel Ângelo Dezordi. “Política criminal atuarial: contornos biopolíticos da exclusão penal”. *Revista Direito e Práxis* 8 (setembro de 2017): 2043–73. https://doi.org/10.1590/2179-8966/2017/22314.
Westin, Alan F. *Privacy and Freedom*. Organizado por Daniel J. Solove. New York: Ig Publishing, 2015.
VEJA. “Wilson Witzel: ‘A polícia vai mirar na cabecinha e… fogo’”, 1º de novembro de 2018. https://veja.abril.com.br/politica/wilson-witzel-a-policia-vai-mirar-na-cabecinha-e-fogo/.
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*. Organizado por Luís Greco. São Paulo: Marcial Pons, 2018.
Zanatta, Rafael. “Proteção de dados pessoais como regulação do risco: uma nova moldura teórica?”, 30 de janeiro de 2018. https://doi.org/10.13140/RG.2.2.16815.43684.
Zedner, Lucia. *Security*. 1 edition. London; New York: Routledge, 2009.
———. “Too much security?” *International Journal of the Sociology of Law* 31, nº 3 (1º de setembro de 2003): 155–84. https://doi.org/10.1016/j.ijsl.2003.09.002.

Jurisprudência nacional

(*Por tribunal, por ordem cronológica de julgamento)*

Superior Tribunal de Justiça, RHC 51.531, Rel. Min. Néfi Cordeiro, Sexta Turma, j. 19.04.2016, DJe 09.05.2016.
Superior Tribunal de Justiça, RHC 53.541/RJ, Rel. Min. Jorge Mussi, Quinta Turma, j. 12.09.2017, DJe 20.09.2017.
Superior Tribunal de Justiça, AgRg no REsp 1760815/PR, Rel. Min. Laurita Vaz, Sexta Turma, j. 23.10.2018, DJe 13.11.2018.
Superior Tribunal de Justiça, HC 514.617/SP, Rel. Min. Ribeiro Dantas, Quinta Turma, j. 10.09.2019, DJe 16.09.2019.
Superior Tribunal de Justiça, HC 598.051/SP, Rel. Min. Rogério Schietti Cruz, Sexta Turma, j. 02.03.2021, DJE 15.03.2021.
Superior Tribunal de Justiça, HC 598.886, Rel. Min. Rogério Schietti Cruz, Sexta Turma, j. 27.10.2020, DJE 18.12.2020.
Superior Tribunal de Justiça, REsp 1903273, Rel. Min. Nancy Andrighi, j. 24.08.2021, DJE 30.08.2021.

Supremo Tribunal Federal, MS 1047, Rel. Min. Ribeiro da Costa, Tribunal Pleno, j. 06.09.1949.
Supremo Tribunal Federal, RE 22175-MG, Rel. Min. conv. Afrânio Costa, Segunda Turma, j. 9.01.1953.
Supremo Tribunal Federal, RE 22255, Rel. Min. Afrânio Costa, Segunda Turma, j. 24.04.1953.
Supremo Tribunal Federal, RE 2172, Rel. Min. Nelson Hungria, Tribunal Pleno, j. 10.07.1953.
Supremo Tribunal Federal, RMS 2574, Rel. Min. Antonio Villas Boas, Tribunal Pleno, j. 08.07.1957, DJ 08.08.1957.
Supremo Tribunal Federal, RE 27596 EI, Rel. Min. Barros Barreto, Tribunal Pleno, j. 17.10.1958.
Supremo Tribunal Federal, RHC 38039, Rel. Min. Nelson Hungria, Tribunal Pleno, j. 12.10.1960.
Supremo Tribunal Federal, RMS 9057, Rel. Min. Gonçalves de Oliveira, Tribunal Pleno, j. 13.09.1961.
Supremo Tribunal Federal, HC 39.308, Rel. Min. Ary Franco, Min. p. acórdão Pedro Chaves (voto vencedor), Tribunal Pleno, j. 19.09.1962.
Supremo Tribunal Federal, RMS 11274-PE, Rel. Min. Evandro Lins Silva, Tribunal Pleno, j. 27.11.1963.
Supremo Tribunal Federal, RMS 9057, Rel. Min. Gonçalves de Oliveira, Tribunal Pleno, j. 20.05.1966, DJ 26.10.1961.
Supremo Tribuna Federal, RE 60.176, Rel. Min. Luiz Gallotti, Terceira Turma, j. 17.06.1966, DJ 9.11.1966.
Supremo Tribunal Federal, AI 40883, Rel. Min. Hermes Lima, Terceira Turma, j. 10.11.1967, DJ 08.03.1968.
Supremo Tribunal Federal, AI 40812, Rel. Min. Djaci Falcão, Primeira Turma, j. 21.08.1967.
Suprema Tribunal Federal, HC 48934, Rel. Min. Raphael de Barros Monteiro, Primeira Turma, j. 19.11.1971.
Supremo Tribunal Federal, RE 86.926 PR, Rel. Min. Cordeiro Guerra, Segunda Turma, j. 21.10.1977.
Supremo Tribunal Federal, RE 85.439, Rel. Min. Xavier de Albuquerque, Segunda Turma, j. 11.11.1977.

Supremo Tribunal Federal, RE 86420-RS, Rel. Min. Xavier de Albuquerque, Primeira Turma, j. 16.05.1978, DJ 02.06.1978.
Supremo Tribunal Federal, HC 56563-SP, Rel. Min. Cordeiro Guerra, rel. p/ acórdão Min. Decio Miranda, Segunda Turma, j. 20.10.1978, DJ 28.12.1978.
Supremo Tribunal Federal, RE 100.094-PR, Rel. Min. Rafael Mayer, Segunda Turma, j. 28.06.1984.
Supremo Tribunal Federal, RHC 63834-SP, Min. Aldir Passarinho, Segunda Turma, j. 18.12.1986.
Supremo Tribunal Federal, RHC 66278-PR, Rel. Min. Aldir Passarinho, Segunda Turma, j. 17.05.1988, DJ 17.06.1988.
Supremo Tribunal Federal, RHC 67058-RS, Rel. Min. Francisco Rezek, Segunda Turma, j. 03.03.1989.
Supremo Tribunal Federal, Pet 557 QO, Rel. Min. Carlos Velloso, Tribunal Pleno, j. 25.03.1992.
Supremo Tribunal Federal, RHC 69818-SP, Rel. Min. Sepúlveda Pertence, Primeira Turma, j. 03.11.1992.
Supremo Tribunal Federal, RHC 69912-RS, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, j. 30.06.1993.
Supremo Tribunal Federal, Inq 657, Rel. Min. Carlos Velloso, Tribunal Pleno, j. 30.09.1993.
Supremo Tribunal Federal, HC 70814, Rel. Min. Celso de Mello, Primeira Turma, j. 01.03.1994.
Supremo Tribunal Federal, HC 70909, Rel. Min. Paulo Brossard, Segunda Turma, j. 11.10.1994.Supremo Tribunal Federal, HC 71736, Rel. Min. Francisco Rezek, Rel. p/ acórdão Min. Marco Aurélio, Tribunal Pleno, j. 10.11.1994, DJE 22.11.1996.
Supremo Tribunal Federal, AP 307, Rel. Min. Ilmar Galvão, Tribunal Pleno, j. 13.12.1994.
Supremo Tribunal Federal, MS 21729/DF, Rel Min. Marco Aurélio. Redator p/ acórdão Min. Néri da Silveira, Tribunal Pleno, j. 05.10.1995, DJE 19.10.2001.
Supremo Tribunal Federal, MC na ADI 1488, Rel. Min. Néri da Silveira, Tribunal Pleno, j. 07.11.1996.
Supremo Tribunal Federal, HC 74963, Rel. Min. Ilmar Galvão, Primeira Turma, j. 25.03.1997.
Supremo Tribunal Federal, HC 74127-4 RJ, Rel. Min. Carlos Velloso, Segunda Turma, j. 15.04.1997.
Supremo Tribunal Federal, HC 75232-2-RJ, Rel. Min. Carlos Velloso, Tribunal Pleno, j. 05.07.1997.
Supremo Tribunal Federal, HC 75338, Rel. Min. Nelson Jobim, Tribunal Pleno, j. 11.03.1998.
Supremo Tribunal Federal, HC 76.760, Rel. Min. Sepúlveda Pertence, Primeira Turma, j. 31.03.1998, DJE 15.05.1998.
Supremo Tribunal Federal, RE 215301/CE, Rel Min. Carlos Velloso, Segunda Turma, j. 13.04.1999, DJE 28.05.1999.
Supremo Tribunal Federal, MS 23452, Rel. Min. Celso de Mello, Tribunal Pleno, j. 16.09.1999.
Supremo Tribunal Federal, HC 79512, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, j. 16.12.1999.
Supremo Tribunal Federal, RE 251.445-GO, Rel. Min. Celso de Mello, j. 21.06.2000, DJE 03.08.2000.
Supremo Tribunal Federal, HC 80724, Rel. Min. Ellen Gracie, Primeira Turma, j. 20.03.2001.
Supremo Tribunal Federal, MS 23.879, Rel. Min. Maurício Correa, Tribunal Pleno, j. 03.10.2001.

Supremo Tribunal Federal, Rcl 2.040-QO, Rel. Min. Néri da Silveira, Tribunal Pleno, j. 21.02.2002, DJE 27.06.2003.
Supremo Tribunal Federal, RE 327717 AgR-ED, Rel. Min. Ellen Gracie, j. 04.11.2003.
Supremo Tribunal Federal, RE 331303 AgR, Rel. Min. Sepúlveda Pertence, Primeira Turma, j. 10.02.2004. Supremo Tribunal Federal, RE 230020, Rel. Min. Sepúlveda Pertence, Primeira Turma, j. 06.04.2004.
Supremo Tribunal Federal, HC 83515, Rel. Min. Nelson Jobim, Tribunal Pleno, j. 16.09.2004
Supremo Tribunal Federal, HC 85455, Rel. Min. Marco Aurélio, Primeira Turma, j. 8.03.2005.
Supremo Tribunal Federal, HC 82788, Rel. Min. Celso de Mello, Segunda Turma, j. 12.04.2005.
Supremo Tribunal Federal, RE 418.416-SC, Rel. Min. Sepúlveda Pertence, Tribunal Pleno, j. 10.05.2006; DJe 02.02.2007.
Supremo Tribunal Federal, HC 84.758-7 GO, Rel. Min. Celso de Mello, Tribunal Pleno, j. 25.05.2006.
Supremo Tribunal Federal, Inq 2206 AgR, Rel. Min. Joaquim Barbosa, Tribunal Pleno, j. 29.11.2006.
Supremo Tribunal Federal, RHC 90376, Rel. Min. Celso de Mello, Segunda Turma, j. 03.04.2007.
Supremo Tribunal Federal, Inq 2424 QO-QO, Rel. Min. Cezar Peluso, Tribunal Pleno, j. 20.06.2007.
Supremo Tribunal Federal, HC nº 84.827/TO, Rel. Min. Marco Aurélio, Primeira Turma, j. 07.08.2007, DJ de 23.11.2007.
Supremo Tribunal Federal, HC 94.028, Rel. Min. Cármen Lucia, Primeira Turma, j. 22.04.2008.
Supremo Tribunal Federal, HC 93050, Rel. Min. Celso de Mello, j. 10.06.2008.
Supremo Tribunal Federal, HC 93050, Rel. Min. Celso de Mello, Segunda Turma, j. 10.06.2008;
Supremo Tribunal Federal, HC 89083-MS, Rel. Min. Marco Aurélio, Primeira Turma, j. 19.08.2008.
Supremo Tribunal Federal, AP 470 QO-QO, Rel. Min. Joaquim Barbosa, Tribunal Pleno, j. 22.10.2008, DJ 30.04.2009.
Supremo Tribunal Federal, Inq 2424, Rel. Min Cezar Peluso, Tribunal Pleno, j. 26.11.2008, DJ 26.03.2010.
Supremo Tribunal Federal, RE 583937 QO-RG, Rel. Min. Cezar Peluso, Tribunal Pleno, j. 19.11.2009.
Supremo Tribunal Federal, Inq 2424, Rel. Min. Cezar Peluso, Tribunal Pleno, j. 26.11.2008, DJ 26.03.2010.
Supremo Tribunal Federal, HC 95244, Rel. Min. Dias Toffoli, Primeira Turma, j. 23.03.2010, DJe 30.04.2010.
Supremo Tribuna Federal, ADI 1127, Rel. Min. Marco Aurélio, Tribunal Pleno, j. 17.05.2006, DJ 11.06.2010.
Supremo Tribunal Federal, RE 389.808/PR, Rel. Min. Marco Aurélio, Tribunal Pleno, j. 15.12.2010.
Supremo Tribunal Federal, HC 99490, Rel. Min. Joaquim Barbosa, Segunda Turma, j. 23.11.2010, DJe 01.02.2011.
Supremo Tribunal Federal, RE 559646 AgR, Rel. Min. Ellen Gracie, Segunda Turma, j. 07.06.2011, DJE 24.06.2011
Supremo Tribunal Federal, RHC 108.156/SP, Rel. Min. Luiz Fux, Primeira Turma, j. 28.06.2011.

Supremo Tribunal Federal, SS 3902 AgRg-segundo, Rel. Min. Ayres Britto, Tribunal Pleno, j. 03.10.2011.
Supremo Tribunal Federal, HC 103325, Rel. Min. Celso de Mello, Segunda Turma, j. 03.04.2012.
Supremo Tribunal Federal, HC 91.867, Rel. Min. Gilmar Mendes, Segunda Turma, j. 24.04.2012, DJe 20.09.2012.
Supremo Tribunal Federal, HC 103425, Rel. Min. Rosa Weber, Primeira Turma, j. 26.06.2012.
Supremo Tribunal Federal, Inq 3014 AgR, Rel. Min. Marco Aurelio, Tribunal Pleno, j. 13.12.2012.
Supremo Tribunal Federal, RHC 115983, Rel. Min. Ricardo Lewandowski, Segunda Turma, j. 16.04.2013.
Supremo Tribunal Federal, HC 121271 AgR, Rel. Min. Celso de Mello, Segunda Turma, j. 13.05.2014.
Supremo Tribunal Federal, RE 767180 AgR, Rel. Min. Dias Toffoli, Primeira Turma, j. 19.08.2014.
Supremo Tribunal Federal, ARE 657.777-SP RG, Rel. Min. Teoria Zavascki, Tribunal Pleno, j. 23.04.2015.
Supremo Tribunal Federal, RE 603616, Rel. Min. Gilmar Mendes, Tribunal Pleno, j. 05.11.2015.
Supremo Tribunal Federal, RE 601.314-SP, Rel. Min. Edson Fachin, Tribunal Pleno, j. 24.02.2016.
Supremo Tribunal Federal, ADI 2859/DF, Rel. Min. Dias Toffoli, Tribunal Pleno, j. 24.02.2016.
Supremo Tribunal Federal, HC 124322 AgR, Rel. Min. Luis Roberto Barroso, Primeira Turma, j. 12.09.2016.
Supremo Tribunal Federal, RHC 132062, Rel. Min. Marco Aurélio, Primeira Turma, j. 22.11.2017.
Supremo Tribunal Federal, ADI 5.494, Rel. Min. Alexandre de Moraes, Tribunal Pleno, j. 22.03.2018.
Supremo Tribunal Federal, AP 1003, Rel. Min. Edson Fachin, Segunda Turma, j. 19.06.2018.
Supremo Tribunal Federal, HC 152836 AgR, Rel. Min. Gilmar Mendes, Segunda Turma, j. 22.06.2018.
Supremo Tribunal Federal, AP 1030 Ag-Rg, Rel. Min. Edson Fachin, Segunda Turma, j. 25.09.2018.
Supremo Tribunal Federal, RE 1.055.941/SP, Rel. Min. Dias Toffoli, Tribunal Pleno, j. 04.12.2019.
Supremo Tribunal Federal, RHC 169682 AgR, Rel. Min. Luiz Fux, Primeira Turma, j. 03.04.2020.
Supremo Tribunal Federal, HC 176766, Rel. Min. Marco Aurélio, Primeira Turma, j. 04.05.2020.
Supremo Tribunal Federal, Referendo da MC nas ADIs nº 6387, 6388, 6389, 6390 e 6393, Rel. Min. Rosa Weber, Tribunal Pleno, j. 07.05.2020, DJE 12.11.2020.
Supremo Tribunal Federal, HC 170376 AgR, Rel. Min. Rosa Weber, Primeira Turma, j. 08.06.2020.
Supremo Tribunal Federal, ADI 6529 MC, Rel. Min. Cármen Lúcia, Tribunal Pleno, 13.08.2020, DJE 15.10.2020.
Supremo Tribunal Federal, HC 139749 MG, Rel. Min. Marco Aurélio, Primeira Turma, j. 16.06.2020.
Supremo Tribunal Federal, RE 1116949, Rel. Min. Marco Aurélio, Redator p/ acórdão Min. Edson Fachin, Tribunal Pleno, j. 18.08.2020.

Supremo Tribunal Federal, ADPF 722 MC, Rel. Min. Cármen Lúcia, Tribunal Pleno, j. 20.08.2020, DJE 22.10.2020.
Supremo Tribunal Federal, MC na ADI 6561 TO, Rel. Min. Edson Fachin, Tribunal Pleno, j. 13.10.2020.
Supremo Tribunal Federal, HC 168052, Rel. Min. Gilmar Mendes, Segunda Turma, j. 20.10.2020.
Supremo Tribunal Federal, Rcl 19464 AgR, Rel. Min. Dias Toffoli, Segunda Turma, j. 10.10.2020, DJe 14.12.2020.

Tribunal de Justiça de São Paulo, HC 0280822-12.2011.8.26.0000, rel. des. Sérgio Ribas, 5ª Câmara de Direito Criminal, j. 02.02.2012, DJE 09.02.2012.
Tribunal de Justiça de São Paulo, Apelação Cível 1103117-25.2016.8.26.0100, Rel. Des. José Wagner de Oliveira Melatto Peixoto, 15ª Câmara de Direito Privado, j.13.09.2017, DJE 18.09.2017.