

A VIGILÂNCIA NO MARCO CIVIL DA INTERNET: UMA ANÁLISE LIBERAL-IGUALITÁRIA DO ARMAZENAMENTO GERAL DE DADOS

SURVEILLANCE IN THE MARCO CIVIL DA INTERNET: A LIBERAL-EGALITARIAN ANALYSIS OF DATA RETENTION

Pedro Nobuyuki Carvalho Urashima*

RESUMO

O presente trabalho propõe uma análise das implicações da retenção de metadados no exercício das liberdades civis no Brasil. Esta empreitada analítica é desenvolvida aqui como uma busca por categorias filosóficas capazes de identificar qual tipo de dano uma política desta natureza pode causar. Assim sendo, as principais referências são as contribuições teóricas de Ronald Dworkin. Também é objetivo deste trabalho dialogar com os argumentos daqueles que defendem restrições a direitos civis para garantir a segurança. Esse tipo de interação argumentativa parece capaz de mostrar como a defesa da vigilância pode se estruturar e, principalmente, de explicar os valores perdidos em decorrência dos danos à privacidade. Por fim, aborda-se a incompatibilidade dessa espécie de retenção de dados com o Marco Civil da Internet.

PALAVRAS-CHAVE

Ética. Dignidade. Liberdades civis. Metadados.

SUMÁRIO

Introdução. 1. O que está em jogo? 2. Privacidade como uma questão de dignidade. 3. Concepções de privacidade. 4. Desafios contemporâneos da privacidade. 5. Dificuldades práticas. 6. Uma possível resposta. 7. De volta ao Marco Civil da Internet. Conclusão. Referências.

REFERÊNCIA: URASHIMA, P. N. C. A vigilância no Marco Civil da Internet: uma análise liberal-igualitária do armazenamento geral de dados. *Res Severa Verum Gaudium*, Porto Alegre, v. 3, n. 2, p. 179-196, abr. 2018.

ABSTRACT

The object of this study is to analyze the implications of metadata retention in the exercise of civil liberties in Brazil. It aims at identifying the philosophical categories capable of indicating which kind of damages a policy of this nature may cause. Thus, the main references are the theoretical works of Ronald Dworkin. This study also aims to engage in dialogue with the arguments of those who defend restrictions to civil rights in order to promote security. This kind of argumentative interaction appears to be capable of indicating how the defense of surveillance may be structured and to explain the loss of values due privacy damages. Finally, this article addresses the incompatibility between this kind of data retention and the Marco Civil da Internet.

KEYWORDS

Ethics. Dignity. Civil liberties. Metadata.

INTRODUÇÃO

O espaço cibernético e as tecnologias que nos conectam a ele se mostram cada vez mais centrais na sociabilidade contemporânea. Assim sendo, mostrou-se necessária a garantia de que os internautas brasileiros também estariam resguardados e vinculados aos fundamentos de seu ordenamento. O Marco Civil da Internet surge nesse contexto. Além disso, a Lei 12.965/2014 também regulamenta o papel dos provedores enquanto agentes construtores e participantes dessa nova realidade. Sobre este último ponto, creio ser necessária análise mais aprofundada.

Pretendo analisar neste trabalho as implicações da retenção de dados de registros de conexão e de acesso a aplicações de internet no exercício de liberdades civis no Brasil. Para tanto, toma-se como

* Graduando em Direito (Universidade Federal de Lavras – UFLA). Pesquisador de iniciação científica voluntária na área de Filosofia do Direito e membro do Núcleo de estudos “Direito, argumentação e justiça”.

ponto de partida os artigos 13 e 15 da referida Lei, que estabelecem:

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento (BRASIL, 2014).

Chamo atenção para o fato de o legislador, assim, demonstrar falta de sensibilidade ao caráter particular dos chamados metadados. Essa categoria define-se enquanto conjunto de dados que permite a ocorrência da comunicação e diz respeito às partes envolvidas. Exemplos de metadados são: nas comunicações telefônicas, o número de origem e de destino; na internet, endereço da página acessada (URL) e endereço de IP; nos *smartphones*, horário e posição geográfica de uma foto. Especificamente, o Marco Civil da Internet estabelece que:

Art. 5º Para os efeitos desta Lei, considera-se:

[...]

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

[...]

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (BRASIL, 2014).

A relevância desse tipo de informação é significativa, pois se cruzando os diversos bancos de metadados é possível realizar um amplo mapeamento do cotidiano e intimidade das pessoas.¹

Cabe destacar que o problema identificado não é a utilização de tais informações em investigações. O ponto merecedor de crítica é a abrangência de uma política de armazenamento geral, isto é, que incide em todos os usuários de comunicação indiscriminadamente. Importante também pontuar que os metadados armazenados por determinação do referido texto legal podem ser aproveitados para a formação de conjunto probatório em processo judicial cível ou penal (vide o art. 22, *caput*, da Lei 12.965). Contudo, o foco deste artigo é apenas as implicações de sua utilização na esfera penal.

Uma vez exposto o objeto de análise, parto para a compreensão dos direitos ameaçados com a manutenção dessa prática de coleta de dados.

¹ Para uma melhor compreensão das possibilidades de vigilância a partir de metadados recomenda-se: HENSCHKE, 2015. Disponível em: < <https://theconversation.com/whistleblowers-may-bypass-the-media-thanks-to-new-data-laws-39877> >. Ver também: PEARSON, 2015. Disponível em: <<https://theconversation.com/how-surveillance-is-wrecking-journalist-source-confidentiality-43228>>.

1 O QUE ESTÁ EM JOGO?

Primeiramente, acredito ser necessário identificar uma compreensão do direito à privacidade suficientemente elaborada para integrar os seus variados sentidos. Assim, torna-se possível ter ampla dimensão do porquê de ele dever ser preservado. Adoto as categorias formuladas por Dworkin em sua obra *Domínio da vida* (2003b, p. 74) para abarcar essa variedade. Dessa forma, temos que a privacidade pode ter um sentido territorial, quando se refere à ideia de que as pessoas possuem a prerrogativa de fazer o que quiserem em certo espaço delimitado. Privacidade também pode significar uma questão de confidencialidade, isto é, as pessoas podem não revelar amplamente convicções que lhes são próprias. Ademais, segundo Dworkin, na jurisprudência norte-americana, pode-se compreender outro sentido com base nas discussões do caso *Griswold vs Connecticut*, que asseguraram o direito a contraceptivos. Por privacidade, entendeu-se “soberania sobre decisões pessoais”. Em outras palavras:

[...] a um Estado não compete prescrever o que as pessoas deveriam pensar sobre o significado [ultimate point] e valor últimos de uma vida humana, sobre por que uma vida tem importância intrínseca, e sobre como este valor é respeitado ou desonrado em diferentes circunstâncias. (DWORKIN, 2003b, p. 230).

O referido sentido de privacidade é uma afirmação do ideal do individualismo ético. Trata-se de conceito apresentado por Dworkin no capítulo 11 de sua obra *Freedom's Law* (1996). Esse ideal afirma o seguinte:

[...] cada um de nós possui responsabilidade de fazer o tanto de sucesso de nossas vidas o quanto pudermos, e [...] esta responsabilidade é pessoal, no sentido de que cada um de nós deve formular sua própria ideia, enquanto questão de convicção pessoal, o que se trata uma boa vida. (DWORKIN, 1996, p. 250, tradução nossa).

Com base nessa ideia *dworkiniana*, identifica-se que, ao se falar de privacidade, em qualquer de suas espécies, há uma derivação e/ou afirmação da ideia de soberania sobre decisões pessoais. Vê-se que, a partir da concepção de “boa vida” estabelecida como referência, nós adotamos convicções, desenvolvemos gostos, priorizamos atividades, cultivamos relações. As convicções desejáveis de serem mantidas confidenciais são nada mais do que valores que refletem nossa perspectiva de mundo. Visão essa que é estruturada a partir do que entendemos por enriquecedor para nossa personalidade, ou seja, nossa ideia de “boa vida”.

Exploro agora como a territorialidade está conectada com a independência sobre decisões pessoais. Sem a proteção de uma esfera de comunicação íntima na qual se exploram e testam ideias, os indivíduos não são capazes de alcançar maturidade intelectual e espiritual (WESTIN, 1967 *apud* KLINEFELTER, 2007). Há uma íntima relação entre a ideia de confidencialidade e esta agora apresentada.

Uma vez que desenvolvemos um juízo ético de qual ideia de “boa vida” nos serve de referência,

aderimos a visões de mundo, expressas em correntes e em intuições políticas, religiosas, filosóficas, as quais reafirmam o projeto de vida almejado e estimulam práticas para alcançá-lo. Tais práticas vão se expressar nos atos cotidianos dos indivíduos, na construção de seus laços de convivência, na dinâmica de seu lar, na sua constituição familiar; em razão disso, esses espaços devem ser resguardados de intervenções.

2 PRIVACIDADE COMO UMA QUESTÃO DE DIGNIDADE

A compreensão dos prejuízos às garantias fundamentais dos cidadãos, contudo, somente se torna completa com a articulação do direito à privacidade com a ideia de dignidade. Esse exercício é feito na busca por resposta à seguinte objeção: a vigilância do Estado nas comunicações dos internautas aumenta a segurança. A máxima liberal de que políticas públicas não podem justificar-se com base em argumentos éticos, ou seja, escolhendo determinados estilos de vida como inapropriados e detestáveis, aqui não se aplica. Isso se dá em razão da justificativa apontada pautar-se por uma ideia de justiça.

Apresento o porquê de esta ideia ser frágil, buscando aprofundar-me no seguinte argumento apresentado por Dworkin em *Levando os direitos a sério* (2002, p. 294): direitos a liberdades básicas não estão propensos a ser modificados pela simples avaliação de melhoria do bem-estar geral. Isto se justifica, na medida em que sua restrição gera um impacto que vai além do próprio constrangimento da liberdade; há outros valores fundamentais em jogo – a dignidade humana e a igualdade política (DWORKIN, 2002, p. 304-307).

O valor da dignidade será tratado em um sentido específico, isto é, enquanto critério ético que guiará a interpretação de conceitos morais (DWORKIN, 2011, p. 203). Há de se destacar que essa identificação tem como fundamento a ideia de Dworkin de que padrões morais estabelecem como devemos tratar os outros; padrões éticos, por sua vez, estabelecem como devemos viver nós mesmos (DWORKIN, 2011, p. 13). Nesse sentido, seu conteúdo (o da dignidade) é composto por dois valores: 1) o do autorrespeito, e 2) o da autenticidade. O primeiro não se trata de uma declaração moral em si mesma, mas sim descreve uma atitude que as pessoas deveriam ter ao longo de suas vidas. Temos uma responsabilidade de "viver bem", e a sua importância é levada em conta na afirmação do valor de se ter uma vida criticamente boa. Em outras palavras: "Este princípio afirma que eu devo reconhecer o valor objetivo do meu viver bem. Eu devo aceitar, portanto, que seria um erro não me importar como eu vivo." (DWORKIN, 2011, p. 205, tradução nossa).

O valor de "viver bem" é mais bem compreendido a partir de uma analogia com a arte (DWORKIN, 2011, p. 196). A comparação é pertinente, pois o valor estético e o valor de "viver bem" podem ambos ser explicados a partir da relação entre o valor criado e os atos de criação desse valor. Para

compreender essa relação, é necessário, primeiramente, fazer uma consideração: o valor de produto é aquele reconhecível em uma coisa independentemente do processo de sua criação, isto é, essa coisa apenas possui valor como um objeto. A arte pode ser avaliada com referência a este último tipo de valor. Pode-se, assim, constatar que uma obra possui valor de produto subjetivo, pois agrada seus apreciadores; e, possui valor de produto objetivo, pois seus aspectos formais são belos. Mas, então, o que diferencia o valor estético de uma réplica exata daquele de uma obra original? O valor de produto objetivo será o mesmo. Por sua vez, o valor de produto subjetivo vai depender do conhecimento pelos apreciadores de que se trata de uma réplica. O fundamental é compreender que há algo na obra original ausente na réplica: o ato criativo de um artista. A beleza da obra original, portanto, é diferente porque essa é resultado de uma *performance*. Ou seja, a arte produzida é a resposta ao desafio de se criar algo belo.

Da mesma forma, valorizamos uma vida humana bem vivida, porque ela incorpora uma *performance* de uma resposta ao desafio de se ter uma vida a ser conduzida. O valor de nossas vidas é, portanto, adverbial (DWORKIN, 2011, p. 196-197). Pode-se avaliar, contudo, que o valor de “viver bem” reside na melhoria que a vida agrega ao mundo. Nessa ótica, uma vida “bem vivida” é aquela que possui impacto positivo. Logo, o valor de “viver bem” é pensado como um valor de produto. Contudo, os juízos sobre quais escolhas *devemos* adotar para termos uma “boa vida” não têm o impacto como critério fundamental (DWORKIN, 2011, p. 198). Nós possuímos ideias sobre como viver a vida da melhor forma possível e tentamos, com ajustes e recomeços, viver estas ideias. O que se está afirmando é que temos um poderoso e inarticulado senso de o que torna nossa vida mais valiosa enquanto *performance* (DWORKIN, 2011, p. 206).

O segundo é nada mais do que outra faceta do primeiro. Vê-se que, uma vez que um indivíduo leva a sério ele mesmo, ele julga que “viver bem” significa expressar a si mesmo em sua vida, procurando alguma forma de viver que seja a certa para ele e para as suas circunstâncias (DWORKIN, 2011, p. 2009). Isso significa uma forma de viver que se adéque à situação, e não uma formulada irrefletidamente a partir de convenções, tradições ou expectativas de outros. Deve-se, portanto, almejar independência. Isso não significa evitar influências. As pessoas não conseguem inventar formas completamente novas de viver; todos vivemos em uma cultura ética que nos fornece, em qualquer época, a paleta de valores éticos reconhecíveis dos quais possibilidades podem ser desenvolvidas (DWORKIN, 2011, p. 211).

Se por um lado não escapamos de influência, por outro, devemos combater a dominação. A autenticidade de alguém não é restringida por limitações de circunstância ou natureza (impostos e habilidades esportivas são, respectivamente, exemplos). Não há tantas cores em sua paleta nesses casos, mas a vida que se elabora com as cores disponíveis pode ser uma vida tão autêntica quanto a que ele

gostaria (DWORKIN, 2011, p. 212).

Contudo, não se vive de forma autêntica se são negadas opções que estariam disponíveis se não fossem vistas como menos valiosas. Importante destacar que autenticidade não se confunde com autonomia. A última aqui entendida como a faculdade de escolher diante das opções disponíveis. Essa diferenciação é importante, pois esta se mantém intacta se o governo manipula a cultura de uma comunidade com o fim de remover ou tornar menos elegível certas formas de vida tidas como inferiores, desde que ainda haja margem para escolha de outras opções de vida. A autenticidade, contudo, é ferida. Com base nela, afirma-se que "viver bem" significa não só elaborar um projeto de vida, como se qualquer um fosse válido, mas elaborá-lo enquanto exercício de julgamento de valor ético (DWORKIN, 2011, p. 212). Assim, abandonar determinado projeto de vida por medo de reprovação social ou política viola a autenticidade.

Percebe-se a íntima relação entre se importar com como se vive (autorrespeito) e, em razão disso, querer conduzir uma vida autêntica (autenticidade), com a ideia de ser livre na identificação do valor da vida (soberania sobre decisões pessoais). A dignidade, assim, é o elemento estruturante da ideia de privacidade.

3 CONCEPÇÕES DE PRIVACIDADE

Neste momento, faz-se necessária uma breve apresentação das mudanças na compreensão do que é o direito à privacidade, pois, assim, é possível identificar aproximações e distanciamentos da concepção acima exposta em relação à literatura especializada na temática.

O marco inicial das discussões sobre a privacidade é o pioneiro artigo de Warren e Brandeis, publicado na *Harvard Legal Review*, e intitulado "The Right to Privacy", no qual os autores denunciavam como a fotografia, os jornais e demais aparatos tecnológicos dificultavam a preservação da vida privada e doméstica (SCHERTEL MENDES, 2008, p. 14). Os autores, diante desse cenário, defendem o respeito ao chamado *right to be let alone* (direito a ser deixado só), direito cujo fundamento era a inviolabilidade da personalidade. Ao defenderem tal posição, os autores romperam com o entendimento, predominante à sua época, de que o domínio privado deveria ser resguardado em razão do direito à propriedade. Há de se destacar que, para Warren e Brandeis, domínio privado significava o espaço da vida doméstica e das relações sexuais, apenas. Essa definição limitada caracteriza o "direito a ser deixado só" como uma prerrogativa fortemente individualista (SCHERTEL MENDES, 2008, p. 15-16).

No decorrer do século XX, há uma significativa transformação da função do Estado, e alinhado a esse processo inicia-se a revolução tecnológica. Nesse contexto,

A evolução do direito à privacidade prosseguiu para se adaptar às novas transformações sociais ocasionadas pela revolução da tecnologia da informação, que possibilitou a coleta e o processamento dos dados pessoais dos cidadãos de forma pioneira. [...] A partir do momento em que a tecnologia passa a permitir o armazenamento e o processamento rápido e eficiente de dados pessoais, dá-se a associação entre proteção à privacidade e informações pessoais. Nesse contexto, percebe-se, uma alteração não apenas do conteúdo do direito à privacidade, mas também do seu léxico, passando a ser denominado “privacidade informacional”, “proteção de dados pessoais”, “autodeterminação informativa”, entre outros (SCHERTEL MENDES, 2008, p. 17-18).

Laura Schertel Mendes, em sua obra *Transparência e Privacidade: Violação e Proteção da Informação Pessoal na Sociedade de Consumo* (2008), após fazer esse resgate histórico, aponta qual é a sua compreensão do direito em questão. Para a autora,

[...] não obstante os diversos conceitos de privacidade, entende-se que a definição mais adequada é a que faz prevalecer a ideia de controle do indivíduo sobre as suas informações, em detrimento da ideia de isolamento do indivíduo. Conceituada dessa forma, a privacidade reflete claramente a existência de uma autonomia do seu titular na conformação desse direito. Isso significa que o titular tem a faculdade de conformar as fronteiras e os limites do exercício de seu direito à privacidade (SCHERTEL MENDES, 2008, p. 21).

Essa posição vai ao encontro do que foi desenvolvido nas duas seções anteriores, na medida em que mantém o indivíduo como elemento central na definição da privacidade, sem, contudo, desconsiderar que esse vive em sociedade. A última, inclusive, não é aqui vista como oposta à privacidade, mas como o espaço no qual o indivíduo atua e é reconhecido com base nas informações que deseja divulgar. Em outras palavras, se privacidade significa o controle do indivíduo sobre suas informações, quando há o respeito a tal direito, o espaço público não é o oposto do exercício da privacidade, mas sim, em certa medida, resultado desse usufruto.

Pensar privacidade nesses termos é vantajoso, pois as dificuldades que o armazenamento e o processamento rápido e eficiente de dados pessoais trazem ainda podem ser pensadas teoricamente com referência a tal direito. Eventualmente, haverá a preferência pelo uso do termo proteção de dados pessoais, sob o argumento de que esse abrange a complexidade dos problemas de forma mais satisfatória (SCHERTEL MENDES, 2008 p. 27 e DONEDA, 2011 p. 95). Esse outro termo engloba um setor de política pública autônomo, dotado de instrumentos legais próprios e de organismos regulatórios específicos, trazendo à tona, portanto, elementos que vão além da caracterização de direito fundamental (SCHERTEL MENDES, 2008 p. 43). Entretanto, quando se fala da proteção de dados pessoais como um direito, a privacidade ainda se apresenta como fundamento último.

Nesse sentido, é possível dizer que a busca por limitações à manipulação de dados pessoais é uma demanda concreta da privacidade, o que fica claro neste trecho:

Tendo em vista que as informações pessoais constituem-se em intermediários entre a pessoa e a sociedade, a personalidade de um indivíduo pode ser gravemente violada com a inadequada

divulgação e utilização de informações armazenadas a seu respeito. Nessa hipótese, tem-se a violação também da autodeterminação e da liberdade do indivíduo, na medida em que ele deixa de ter controle sobre as suas próprias informações, ficando eventualmente sujeito ao poder de organismos privados ou públicos.

Nesse sentido, a proteção de dados pessoais tem como uma das suas finalidades principais prover o indivíduo de poder para controlar livremente a revelação e a utilização dos seus dados pessoais na sociedade, preservando, assim, a sua capacidade de autodeterminação e de livre desenvolvimento de sua personalidade.

Por se constituir como um direito sobre as informações pessoais, a proteção de dados pessoais tem um forte componente de autodeterminação e de autoconformação, tendo em vista que somente o indivíduo pode determinar o âmbito da própria privacidade, isto é, em que medida as suas informações pessoais podem ou não ser coletadas e transmitidas e até que ponto isso não viola a sua personalidade. Nesse aspecto, nota-se que a proteção de dados pessoais, à semelhança do direito que lhe deu origem, o direito à privacidade, é marcado por esse acentuado viés de autocontrole e de liberdade do seu titular (SCHERTEL MENDES, 2008 p. 41).

4 DESAFIOS CONTEMPORÂNEOS DA PRIVACIDADE

A partir de tais considerações, é possível pensar de forma mais completa na estrutura da privacidade. Ao se enfatizar a ideia de proteção de dados pessoais, explicita-se como contemporaneamente a formulação abstrata desse direito (privacidade) tem seus pressupostos desafiados de uma nova maneira. Fundamental também é a percepção de que refletir sobre a privacidade e seus horizontes contemporâneos implica, necessariamente, repensar o que é a vigilância.

O cenário de revolução tecnológica, que se inicia no século XX, acentua-se de tal forma que o processamento em tempo real e o armazenamento ilimitado de dados tornam-se corriqueiros. Como consequência, a vigilância não apenas se qualifica, mas adquire nova natureza, merecendo uma denominação específica: *surveillance* (JACOB NETO, 2014 p. 164). Um dos pontos que marca a distinção entre o modelo teórico da vigilância e este último, portanto, é o contexto social que lhes serve de pano de fundo. Assim, percebe-se que nessa nova ótica:

A tecnologia, antes de causa, é instrumento para coletar, armazenar, processar, classificar e transmitir informações. Ao invés de ser um aspecto externo – como nos remete a ideia de “vigilância” –, a tecnologia é parte da textura que compõe a vida nas sociedades contemporâneas. Nesse sentido, o que se busca é diferenciar a vigilância no sentido tradicional – ou seja, como espionagem e investigação sigilosa de atividades individuais – das técnicas facilitadas pela tecnologia da informação que, por sua natureza, são endêmicas nas sociedades contemporâneas. Tais técnicas têm como objetivo a sistemática coleta, armazenamento, processamento, individualização e classificação das informações sobre as pessoas em determinados grupos (JACOB NETO, 2014 p. 165).

A diferenciação, contudo, não se limita a esse aspecto. Primeiramente, é valioso o esforço de conceituação do que é *surveillance*. Deve-se entender que:

Ela é a atenção concentrada, sistematizada e rotineira aos dados pessoais cujo objetivo é influenciar, gerenciar, proteger ou dirigir. Concentrada, pois seus alvos finais são, via de regra, os indivíduos. Sistematizada, uma vez que essa atenção não é aleatória ou ocasional: é deliberada e depende de determinados protocolos e técnicas. Rotineira, porque “normalizada”, ou seja, compreendida como parte inescapável do cotidiano em todas as sociedades atuais, uma vez que

dependem da associação crescente entre a tecnologia da informação e a administração burocrática (JACOB NETO, 2014 p. 166).

Outras características marcantes desse novo arranjo são a ênfase na prevenção e a descentralização. Há ampla coleta de informações, sendo que variados são os espaços de retenção. Em razão da ampla capacidade de armazenamento dos bancos informacionais, o que acaba por ocorrer é o recolhimento de variados dados para o aproveitamento posterior (JACOB NETO, 2014 p. 170). Também se deve destacar que a natureza rotineira desse novo fenômeno faz com que ele incida nos mais diversos grupos sociais, ou seja, seu alcance não se limita aos grupos desfavorecidos ou politicamente indesejados (JACOB NETO, 2014 p. 171). Esse cenário se mostra evidente quando da análise da manipulação de informações pessoais para fins comerciais. Contudo, busca-se demonstrar que, em razão do potencial revelador dos metadados, o armazenamento geral de dados de registros de conexão e de acesso a aplicações de internet também pode ser criticado como medida típica de *surveillance*.

Jonathan Mayer e Patrick Mutchler, em seu estudo *MetaPhone: The Sensitivity of Telephone Metadata* (2014), dedicaram-se a demonstrar empiricamente o quão reveladores os metadados podem ser. O estudo em questão iniciou-se com o *download* do aplicativo *MetaPhone* por voluntários em seus *smartphones Androids*. No aplicativo, *logs* dos dispositivos e informações de redes sociais são submetidos à análise. Uma vez submetidas as informações de cada participante, cruzam-se os contatos telefônicos com os diretórios dos aplicativos *Yelp* e *Google Places*. Em seguida, destacam-se os contatos que parecem se relacionar com uma atividade sensível, isto é, reveladora das convicções e associações cultivadas ou buscadas pelas pessoas. Dois resultados foram buscados: coletar os contatos e ligações relacionados a atividades sensíveis, e demonstrar como é possível, a partir de padrões nas ligações, identificar o quão reveladores são os metadados.

Os pesquisadores bem destacam que muitas organizações possuem propósitos limitados. Ou seja, a realização de ligações constantes pode servir de base para inferências sensíveis sobre os indivíduos. Um simples exemplo pode ilustrar melhor tal conclusão: se uma pessoa está frequentemente envolvida com uma instituição religiosa, ela, provavelmente, compartilha aquela fé ou valoriza a instituição. Outra possibilidade de revelação da vida das pessoas dá-se nas ligações destinadas à realização ou obtenção de serviços e/ou produtos específicos. Torna-se possível, por exemplo, saber que alguém está lidando com uma doença grave a partir do cruzamento de dados de busca por produtos e serviços médicos com a ligação para o advogado de planejamento sucessório.

Diante do exposto acima, é perceptível que os metadados podem ser materiais para a elaboração de padrões reveladores, e, portanto, seu armazenamento cotidiano é medida típica de *surveillance*. O artigo 5º do Marco Civil da Internet conceitua quais serão as informações a serem armazenadas pelos provedores:

Art. 5º Para os efeitos desta Lei, considera-se:

[...]

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

[...]

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP (BRASIL, 2014).

A leitura desse dispositivo, se conjugada com a consciência de que metadados podem ser cruzados, deixa claro que essa política representa efetiva ameaça à privacidade e à proteção de dados pessoais. Novamente, a privacidade deve ser compreendida como um desdobramento da ideal do individualismo ético, isto é, cabe ao sujeito buscar sucesso em sua vida, e a definição do que é uma “boa vida” é sua responsabilidade pessoal. Nessa perspectiva, o direito em questão é lido como o controle do indivíduo sobre as suas informações. Assim, o respeito a essa garantia envolve a faculdade de conformar as fronteiras e os limites do seu exercício. Em um contexto de ampla complexificação e difusão das tecnologias da informação, isso se traduz na ideia de proteção de dados pessoais. Em outras palavras, o indivíduo é quem define em que medida as suas informações pessoais podem ou não ser coletadas e transmitidas e até que ponto isso não viola a sua personalidade. Os artigos 13 e 15 da Lei 12.965/2014, ao estipularem a coleta indiscriminada das informações destacadas, impossibilitam o pleno exercício dessa faculdade, impedindo que os internautas possam delimitar como seu uso da internet será processado como informação. Vê-se, então, que a compreensão teórica de privacidade exposta se reafirma como a mais adequada, pois é a formulação que melhor acompanha a mudança conceitual de vigilância para *surveillance*.

Contudo, restam as dúvidas: o Estado pode indiscriminadamente restringir a privacidade de seus cidadãos por razões de conveniência política? Ou, uma vez conhecida a potencialidade sensível dos metadados, é fundamental a limitação de sua obtenção por autoridades com base nos direitos processuais já existentes?

5 DIFICULDADES PRÁTICAS

Nesta seção, discutirei de forma breve a legitimidade do Estado para manter uma política desta natureza a partir de elementos concretos. Para tanto, mostrou-se valioso o relato do Prof. Hans Jörg Albrecht, em entrevista ao grupo de estudos Internet Lab (2016), sobre as características da retenção geral de dados implementada na Alemanha.

O autor aponta com precisão que a utilização de dados de tráfego de telecomunicações para investigações é prática por vezes necessária para a resolução das controvérsias criminais. Contudo, esse

aproveitamento justifica-se somente na hipótese em que há uma suspeita sobre um indivíduo ou grupo. Diferencia-se, portanto, da retenção geral. Nessa última, há algo de diferente porque, nesse caso, não se trata apenas de dados individuais que são transferidos dos provedores a uma agência de segurança ou à polícia – o procedimento é uma retenção de todos os dados de tráfego relacionados a celulares ou à internet, sem qualquer causa (BRITO CRUZ; KIRA, 2016, p. 12-13).

Albrecht mostra-se crítico também da ideia de que o armazenamento geral é necessário por permitir a utilização de informações para casos futuros (BRITO CRUZ; KIRA, 2016, p. 13). A fraqueza desse argumento decorre do fato de que não se pode, por um ganho futuro incerto, sacrificarem-se direitos essenciais dos indivíduos, como a privacidade e a liberdade de expressão. Em outras palavras, os potenciais ganhos, identificados por um raciocínio de custo-benefício, na implementação de uma política de vigilância não podem ser entendidos como justificativas legítimas quando garantias desta natureza estão em jogo. Estes direitos são especiais, porque não são somente prerrogativas em face de outros indivíduos, mas contra o próprio governo. Isso se deve, pois se tratam de direitos morais cuja proteção expressa o compromisso de se respeitar a igual importância das vidas dos cidadãos e a soberania pessoal desses em identificar e criar valor em suas vidas (DWORKIN, 2006, p. 32). Compromisso, esse, que, em razão de sua natureza, por vezes, contraria os interesses políticos mais imediatos ao limitar as possibilidades de agir dos governantes.

Vê-se, portanto, que sua violação compromete não só a liberdade, mas, também, valores fundamentais, como a dignidade e a igualdade. Ou seja, ao se falar destas liberdades básicas, tem-se em vista uma compreensão normativa de liberdade. O dano a esse valor político, assim, implica a desconsideração do *status* de membros da comunidade humana de certos indivíduos, e do fato de que os membros mais frágeis da comunidade política têm direito à mesma consideração e ao mesmo respeito que o governo concede aos seus membros mais poderosos. Dessa forma, qualquer que seja o efeito sobre o bem estar geral, o mesmo grau de liberdade deve ser concedido a todos os indivíduos (DWORKIN, 2002, p. 303). Em síntese:

O governo deve, sem dúvida, tentar reduzir a devastação violenta de vidas e propriedades, mas deve reconhecer que qualquer tentativa de localizar e eliminar uma causa de distúrbios que deixe de lado uma reorganização da sociedade haverá de ser um exercício de especulação, tentativa e erro. O governo deve tomar suas decisões sobre condições de extrema incerteza, e a instituição dos direitos, quando levados a sério, limita sua liberdade de experimentar sobre tais condições. (DWORKIN, 2002, p. 310)

A incerteza quanto aos possíveis ganhos com a vigilância torna-se ainda maior quando se analisa como a experiência funciona em outros países. Na Alemanha, país onde, segundo Albrecht, há cerca de 120 milhões de celulares ativos, e um número parecido de computadores, *smartphones*, etc., a média anual alemã de uso de dados é, contudo, de aproximadamente 2 mil. O que chama atenção, para além

desse ponto quantitativo, é a natureza dos crimes solucionados: roubo de celular e *download* de pornografia infantil (na Alemanha, a posse de material desse tipo é considerada “crime leve”). Em outras palavras, os principais alvos pretendidos (terroristas, por exemplo) são pouco alcançados pela norma, segundo análise do professor alemão (BRITO CRUZ; KIRA, 2016 p. 27).

6 UMA POSSÍVEL RESPOSTA

Penso que ainda resta um ponto para que minha exposição teórica seja completa. A discussão sobre liberdades civis e políticas de segurança não costuma ser apresentada pelos liberais como uma disputa argumentativa. Com isso, considero que a defesa de direitos em face da ampliação de medidas de vigilância, restrição de certas liberdades ou prejuízo a garantias processuais, por vezes, deixa de ser uma conclusão em contraste com uma defesa articulada dessas políticas. Em outras palavras, ataca-se as políticas sem se ter a iniciativa de avaliar que, ao se posicionarem priorizando as garantias individuais, os liberais estão se engajando em um confronto entre percepções distintas de justiça, direito e democracia (DWORKIN, 2006, p. 6-9). Em razão disso, procuro agora identificar os elementos nucleares desta perspectiva “pró-segurança”, no intuito de esclarecer quais argumentos contrários no presente trabalho.

A forma mais atraente de apresentar uma “teoria da segurança” é pensá-la como uma concepção do *plateau*² aqui adotado, isto é, como uma interpretação da dignidade. Assim, uma defesa da segurança torna-se possível a partir do seguinte argumento: as pessoas têm direito a toda proteção necessária para se afirmar a igual importância de suas vidas e sua responsabilidade soberana em identificar e criar valor em suas próprias vidas (RODRIGUES, L. B. P. S. A.; MAXIMO, E, 2016, p. 20-21). Nessa perspectiva, o Estado pode estabelecer mecanismos de vigilância se estes se mostrarem efetivos no combate a violências (RODRIGUES, L. B. P. S. A.; MAXIMO, E, 2016, p. 23).

Pensando-se no combate de crimes em geral, a defesa da retenção de metadados não parece ajustar-se a esse argumento. Uma vez que não houve crime, não fica claro como uma coleta prévia de informações promoverá o respeito à ideia de que as vidas de todos possuem igual importância e que, portanto, importa que aquela seja uma expressão de autenticidade. Porém, quando está em discussão o rastreamento e punição de crimes cibernéticos e digitais, o cenário muda. A natureza desses crimes, diria o teórico da segurança, é específica, pois a plataforma em que se manifestam permite aos agentes dispersarem-se e ocultarem-se. Quanto mais imediata é a ação da autoridade investigativa, mais efetivo é o combate a tais condutas (RODRIGUES, L. B. P. S. A.; MAXIMO, E, 2016, p. 23-24).

Vê-se então que, para os defensores da segurança, a guarda geral é uma das possibilidades mais

² A categoria “concepção” aqui explorada pode ser mais bem compreendida em: DWORKIN, 1986, cap. 2.p. 71.

adequadas de se aproveitar os meios tecnológicos com a finalidade de combater a criminalidade digital (RODRIGUES, L. B. P. S. A.; MAXIMO, E, 2016, p. 25). A retenção posterior, por sua vez, poderia se mostrar incapaz de combater as principais condutas que afligem os internautas, mostrando o desrespeito às suas vidas.

Essa abordagem, contudo, tem o ônus argumentativo de responder ao seguinte: implementar mecanismos de vigilância com a finalidade de agilizar a persecução penal é moralmente errado, uma vez que, por um ganho incerto, sacrifica-se direitos fundamentais. Com base na teoria aqui desenvolvida, a resposta de um defensor da segurança possivelmente seria a de que o ganho pode até ser incerto, mas a possibilidade de haver perdas significativas na ausência de vigilância dessa natureza já basta para se reter metadados. Ou seja, a invasão à privacidade dos cidadãos, em geral, é tolerável enquanto uma consequência, pois não agir dessa forma permite que crimes sejam facilitados. E a perpetuação dessas condutas criminosas no meio cibernético, e no uso das tecnologias de informação e comunicação (destaque para os *smartphones*), faz com que a própria autodeterminação dos indivíduos se fragilize.

A interpretação nesse sentido, apesar da centralidade que concede à dignidade, não afirma consequências práticas compatíveis com o melhor entendimento dessa categoria. Com isso, quer-se dizer o seguinte: é mais convincente a ideia de que respeitar a dignidade significa, necessariamente, comprometimento com um generoso arranjo de garantias processuais. Isso se justifica, pois a intervenção imperativa do Estado que uma condenação gera nas vidas dos indivíduos é sempre incisiva. Assim sendo, o governo responsável com sua obrigação de tratar a vida de cada pessoa como de distinta, objetiva e igual importância, deve buscar evitar ao máximo que erros sejam cometidos, e para tanto, delimitar as possibilidades investigativas é fundamental (DWORKIN, 2011, p. 372).

O sucesso nessa empreitada permite que a condenação de um indivíduo signifique que “[n]ão escolhemos o prejudicar para o benefício do resto de nós; ele é que escolheu para ele mesmo essa situação a partir de sua decisão deliberada de prejudicar outros para o seu próprio benefício e interesses” (DWORKIN, 2006, p. 44, tradução nossa). Nessa perspectiva, a guarda geral de dados não pode ser mantida. Nota-se que não há, primeiramente, limitação de seu escopo subjetivo, uma vez que todos são abrangidos. Também sua abrangência objetiva é problemática, pois mesmo quando a utilização dos dados se dá motivada por uma suspeita, uma vez que há a retenção geral de informações, não é possível discriminar previamente ao acesso quais informações são adequadas como provas ao caso concreto e quais dizem respeito ao foro íntimo do sujeito.

Dessa forma, a busca pela afirmação do direito processual penal brasileiro e sua conformação às novas tecnologias há de passar por esta discussão. Chama atenção o fortalecimento de debates nacionais acerca da apreensão de celulares e investigação de seus dados. Penso que o próximo passo a ser tomado é o de se repensar de forma mais aprofundada os artigos 13 e 15 do Marco Civil da Internet.

7 DE VOLTA AO MARCO CIVIL DA INTERNET

Os próximos argumentos buscam explicitar a inadequação do que preveem os artigos 13 e 15 do Marco Civil da Internet com o seu “espírito”.

Primeiramente, é necessário compreender quais são as principais categorias consagradas pelas discussões e produções jurídicas e legislativas sobre proteção de informações pessoais. A literatura reconhece que nas legislações que tratam da temática é possível identificar um “núcleo comum” (DONEDA, 2011 p. 100). Assim, busca-se destacar esses elementos característicos:

Para que o indivíduo possa exercer o seu poder de autodeterminação informativa, existem importantes princípios que devem nortear a atividade de tratamento de dados pessoais. Esses princípios têm como finalidade impor limitações ao tratamento de dados, bem como atribuir poder ao indivíduo para que esse possa controlar o fluxo de seus dados (SCHERTEL MENDES, 2008, p. 56).

O primeiro princípio a ser destacado é o da publicidade. Esse princípio exige que a existência de um banco de dados pessoais seja de conhecimento público (SCHERTEL MENDES, 2008, p. 56). O Marco Civil endossa esse princípio em diversos pontos, sendo exemplos claros disso os incisos VI, VIII e XI de seu artigo 7º. O segundo princípio merecedor de destaque é o da exatidão, o qual estabelece que os dados coletados devem ser fiéis à realidade, o que torna necessária a atualização periódica e tratamento com cuidado e correção (DONEDA, 2011, p. 100). O terceiro princípio é o do livre acesso. Este demanda que:

[...] um banco de dados pessoais esteja sempre disponível ao interessado que possui seus dados ali armazenados. Além de garantir a obtenção de cópias dos registros dos bancos de dados, este princípio também assegura o direito do interessado em retificar as informações incorretas ou atrasadas (SCHERTEL MENDES, 2008, p. 57).

O quarto é o princípio da segurança, o qual dispõe ser “[...] exigência básica de que qualquer banco de dados pessoais esteja protegido contra extravios, destruições, modificações e desvios não autorizados pelos interessados” (SCHERTEL MENDES, 2008, p. 57). Por fim, tem-se o princípio da finalidade, o qual estabelece que:

[...] qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. [...] a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade) (DONEDA, 2011, p. 100).

Esse princípio é trazido pela Lei 12.965/2014, que prevê:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

[...]

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet. (BRASIL, 2014)

A crítica ao armazenamento geral pode ser feita a partir desse princípio. Vê-se que a legislação estipula tal obrigação aos administradores de sistemas autônomos e aos provedores de aplicações de internet, com o fim de formar conjunto probatório para processos judiciais (artigo 22, *caput*, da Lei 12.965). Contudo, por ser de caráter geral e indiscriminado, essa política extrapola seus fins, atentando contra a privacidade e proteção de dados pessoais dos cidadãos. Assim sendo, constata-se o que já foi dito anteriormente: a finalidade proposta (uso para fins probatórios) justifica a utilização dessas informações, porém o método utilizado é inadequado. Logo, não se atende ao critério de justificativa da coleta.

Quanto à vedação pela legislação, argumenta-se que uma leitura atenta permite concluir que há incompatibilidade da retenção geral dos registros de conexão e registros de acesso a aplicações de internet com os princípios e objetivos do Marco Civil. Em suas disposições preliminares, o texto legal destaca que os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais são fundamentos do uso da internet do Brasil (artigo 2º, II). Em seguida, estipula como princípios desse uso a proteção da privacidade e a proteção dos dados pessoais, na forma da lei (artigo 3º, incisos II e III, respectivamente). Os argumentos desenvolvidos nas seções anteriores têm por finalidade justamente defender que não há como conciliar a retenção de metadados com o respeito à privacidade e, por consequência, com o desenvolvimento da personalidade e com a proteção de informações pessoais.

CONCLUSÃO

Buscou-se no presente trabalho identificar a importância da proteção da privacidade. As razões substantivas apresentadas são fruto da articulação das principais espécies desse direito com o ideal do individualismo ético, desenvolvido por Ronald Dworkin – ideia esta que está intimamente conectada ao significado de dignidade. Portanto, violar a privacidade é violar a dignidade. Uma vez exposto o núcleo normativo da privacidade, buscou-se identificar o respaldo da concepção defendida na literatura especializada do tema. Ao final desse esforço, a ideia da proteção de informações pessoais foi destacada. Essa passa a ser de suma importância, pois é o desdobramento do direito à privacidade em um contexto social no qual a tecnologia da informação integra a vida social. A partir dessas considerações, espera-

se ter esclarecido que este modelo de coleta de dados é incompatível com os objetivos estruturantes do Marco Civil da Internet.

Vê-se, contudo, que nesse cenário tecnológico são variados os problemas a serem enfrentados pelos defensores da privacidade. Dessa forma, o fim do armazenamento geral de metadados isoladamente não basta, pois os principais problemas (como, por exemplo, o uso de técnicas de *surveillance* pela iniciativa privada com a finalidade de controlar e incentivar o consumo) ainda geram grandes dificuldades.

REFERÊNCIAS

BRASIL. Câmara dos deputados. Lei nº 12.965. Brasília/DF, 23 abr. 2014.

BRITO CRUZ, Francisco; KIRA, Beatriz. *Direito a Privacidade e a Guarda Obrigatória de Dados para Investigações*: entrevista com Prof. Dr. Dr. h.c. Hans-Jörg Albrecht. Internet Lab, 2016. Disponível em: <<http://www.internetlab.org.br/pt/noticias/entrevista-albrecht/>>. Acesso em: 29 mar. 2017

Câmara dos Deputados. *Combate aos crimes cibernéticos deve ser mais ostensivo, defende especialista*. 23 set. 2015. Disponível em: <<http://www2.camara.leg.br/camaranoticias/noticias/CIENCIA-E-TECNOLOGIA/496738-COMBATE-AOS-CRIMES-CIBERNETICOS-DEVE-SER-MAIS-OSTENSIVO,-DEFENDE-ESPECIALISTA.html>>. Acesso em: 29 mar. 2017

Câmara dos Deputados. *CPI constata dificuldade em rastrear e punir crimes de internet*. 20 ago. 2015. Disponível em: <<http://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/494363-CPI-CONSTATA-DIFICULDADE-EM-RASTREAR-E-PUNIR-CRIMES-DE-INTERNET.html>>. Acesso em: 29 mar. 2017

DONEDA, Danilo. *A Proteção dos dados pessoais como um direito fundamental*. Joaçaba: Espaço Jurídico, v. 12, nº 2, p. 91-108, jul./dez. 2011

DWORKIN, Ronald. *Domínio da vida: aborto, eutanásia e liberdades individuais*. São Paulo: Martins Fontes, 2003.

DWORKIN, Ronald. *Freedom's Law: the moral reading of the American Constitution*. Cambridge (Mass): Harvard University Press, 1996.

DWORKIN, Ronald. *Is Democracy Possible Here? Principles for a new political Debate*. Princeton/Oxford: Princeton University Press, 2008.

DWORKIN, Ronald. *Justice for Hedgehogs*. London/Cambridge: The Belknap of Harvard University Press, 2011.

DWORKIN, Ronald. *Levando os Direitos a Sério*. Tradução Nelson Boeira. Revisão da tradução Silvana Vieira. São Paulo: Martins Fontes, 2002.

JACOB NETO, Elias. *Vigilância ou surveillance? Proposta para começar a compreender corretamente este fenômeno*. São Paulo: Revista dos Tribunais, v. 939, p. 159-182, 2014.

KLINEFELTER, A. Privacy and library public services: or, I know what you read last summer. *Legal Reference Service Quarterly*, v. 26, n. 1/2, set. 2007.

MACEDO Jr., Ronaldo Porto. O Método de Leitura Estrutural. *Cadernos Direito GV*, v. 4, n. 2, mar. 2007.

MAYER, Jonathan. MUTCHELER, Patrick. *MetaPhone*: the sensitivity of telephone metadata. Web-Policy, 12 mar. 2014. Disponível em: <<http://webpolicy.org/2014/03/12/metaphone-the-sensitivity-of-telephone-metadata/>>. Acesso em: 29 mar. 2017

MENDES, Laura Schertel. *Transparência e privacidade: violação e proteção da informação pessoal na sociedade de consumo*. 2008. 156 f. Dissertação (Mestrado em Direito)—Universidade de Brasília, Brasília, 2008.

RODRIGUES, L. B. P. S. A.; MAXIMO, E. A criminalidade aliada a tecnologia: uma abordagem acerca dos meios insuficientes para prevenção e repressão no ciberespaço. *Juris Rationes*, v. 8, n. 2, p. 17-28, 2016.

