1. Introdução

Em *A vida dos outros*[1], Florian Henckel von Donnersmarck permite que o espectador acompanhe a rotina de um agente da Stasi, a polícia política da República Democrática Alemã ou Alemanha Oriental. Dentre os valores estéticos e narrativos desta obra cinematográfica, é adequado mencionar o retrato de um regime político que não media esforços para invadir a privacidade de todos os cidadãos que poderiam vir a figurar como dissidentes. Evidencia-se o insaciável afã de perscrutar a vida privada em seus mínimos detalhes. É claro, por se tratar de um regime político de feições autoritárias, essa representação de uma sistemática e orquestrada violação da vida privada talvez não provoque escândalo. Entretanto, o verdadeiro impacto ocorre quando se percebe que o nível de invasão da intimidade nas contemporâneas sociedades democráticas é ainda mais elevado do que aquele que caracterizou a Alemanha Oriental. Está cada vez mais evidente que a vida nas atuais sociedades interconectadas em rede está à mercê de invasões ainda mais ferozes do que aquelas que perpetradas por regimes não democráticos.

É precisamente com o intuito de denunciar e enfrentar a conjuntura de uma democracia flanqueada por dispositivos de captura e tratamento de dados que surgiu o projeto do WikiLeaks.[2] Capitaneado por Julian Assange e alimentado por informações vazadas pelo soldado americano Bradley Manning, em 2010 o WikiLeaks se tornou um fenômeno de envergadura planetária ao revelar milhares de documentos diplomáticos e militares dos Estados Unidos. Tais documentos comprovaram o recolhimento sistemático de informações implantado, sobretudo, depois dos ataques às Torres Gêmeas em 11 se setembro de 2001, abarcando de cidadãos comuns a chefes de Estado. Sabe-se, por exemplo, que até mesmo a infraestrutura física da internet da América do Sul está constituída em torno de cabos de fibra ótica que adentram as fronteiras dos Estados Unidos.[3] Nesse sentido, Assange não poupa esforços ao alertar que já se iniciou a consolidação de uma distopia em âmbito internacional, declarando enfaticamente que "a internet, nossa maior ferramenta de emancipação, está sendo

[1] *A vida dos outros* ou *Das Leben der Anderen*, no título original, é um filme alemão de 2006 dirigido por Florian Henckel von Donnersmarck. Muito aclamado pela crítica, foi agraciado com o Oscar na categoria de melhor filme de língua estrangeira.

[2] Fundado em 2006, o WikiLeaks tem o objetivo de constituir uma plataforma criptografada de dados em rede com a finalidade de receber denúncias anônimas de violação de direitos humanos.

[3] Assange denuncia que "todos os dias, centenas de milhões de mensagens vindas de todo o continente latino-americano são devoradas por órgãos de espionagem norte-americanos e armazenadas para sempre em depósitos do tamanho de cidades" (ASSANGE, 2013, p. 21).

transformada no mais perigoso facilitador do totalitarismo que já vimos". Arrematando com a gravosa sentença: "a internet é uma ameaça à civilização humana" (ASSANGE, 2013, p. 25).

Pode-se dizer, portanto, que o horizonte distópico propugnado por obras de ficção científica do século XX, tais como *Admirável mundo novo* (HUXLEY, 2009) e *1984* (ORWELL, 2009), veio a ser factível no século XXI e, para muitos, tal como para Assange, esta distopia já em fase de consumação. Desde o acontecimento WikiLeaks evidenciou-se que o temor hiperbólico veiculado em narrativas de ficção científica poderia estar mais próximo da realidade do se supunha. Consumou-se uma preocupação real com a privacidade de cidadãos comuns mesmo em países de democracias consolidadas, isso porque se tomou indubitável consciência de que a sociedade da informação, muitas vezes esposada em tons utópicos de uma democracia comunicacional global, possui uma faceta periclitante: a da vigilância total. Um dos paradoxos inerentes à sociedade da informação parece residir precisamente na coexistência entre maior liberdade de comunicação e a proliferação de meios de vigilância.

Certamente a internet fornece as condições para que se estabeleçam comunicações mais livres, mormente quando se compara a arquitetura em rede – na qual cada pessoa pode atuar tanto como receptor quanto como produtor de conteúdo – com a estrutura das mídias convencionais, que produzem um espectador inerte. Com o advento da internet, os meios de comunicação se multiplicaram e diversificaram, de sorte que hoje a produção e a circulação de informação ultrapassou qualquer precedente histórico.[4] Contudo, é exatamente a intensificação dos fluxos comunicacionais que forneceu o material e estimulou a proliferação de dispositivos de vigilância. Basicamente, a sociedade da informação convive com o dilema de opor e conjugar maior comunicação e maior vigilância (ASSANGE, 2013, p. 43).

Inclusive o perfil anímico que se impregna nas subjetividades contemporâneas corrobora as referidas circunstâncias político-sociais, pois constata-se o quanto mudou a sensibilidade a respeito do que deve ser público e do que deve permanecer privado. Ser visto, ser conhecido, tornou-se uma condição social desejável. Estar em posição de visibilidade, atualmente, confere sentido à existência (BAUMAN, LYON, 2013, p. 28-30). Diante de tal conjuntura, evidencia-se a passagem do modelo de controle racional-burocrático, típico das disciplinas e condizente com modelo do panóptico, originalmente descrito por Bentham e mais

[4] Exemplo de uma postura mais otimista em relação às possibilidades intrínsecas à internet é a de Pierre Lévy (2014, p. 30) que, dentre outras, sustenta a ideia de que o ciberespaço opera como uma inteligência coletiva: "o ideal da inteligência coletiva implica a valorização técnica, econômica, jurídica e humana de uma inteligência distribuída por toda parte, a fim de desencadear uma dinâmica positiva de reconhecimento e mobilização das competências".

tarde apropriado por Foucault (2013, p. 88), ao modelo de vigilância terceirizada, em que quem efetua a vigilância é o próprio vigiado. Os dispositivos tecnológicos de uso pessoal, especialmente os *smartphones*, facilitam uma vigilância do tipo "faça você mesmo" (BAUMAN, LYON, 2013, p. 60-61).

A vigilância burocrática, operando segundo a exigência de cumprimento de rotinas, exigia extensos planejamentos sociais, burocracias destinadas à vigilância, correção e punição. Esse modelo centralizado de vigilância tolhia a autonomia dos controlados (e até mesmo dos controladores), generalizando a sensação de enfado e criando uma situação instável, constantemente na iminência de eclodir e produzir uma reviravolta em decorrência do ressentimento latente. Houve uma reorientação paradigmática no campo da vigilância, eis que os mecanismos que vigiam passam a assimilar a participação dos controlados com a finalidade de extorquir informações de forma suave, alimentando bancos de dados (BAUMAN, LYON, 2013, p. 70-74). Por essas razões, impende verificar quais instrumentos jurídicos encontram-se aptos a conferir proteção aos dados pessoais, de modo a conter a tendência persecutória instalada nos dispositivos de vigilância que coexistem com as sociedades da informação.

2. Cidadania digital e privacidade em rede

Mediante a proliferação de dispositivos de captura de dados, bem com o desenvolvimento do aparato técnico-informático destinado ao armazenamento de informações, constata-se que os desdobramentos da técnica ensejaram transformações paralelas no que tange aos direitos. Almejando estudar a condição *sui generis* dos direitos da personalidade ante a ascensão do ciberespaço, o presente artigo propõe enfocar a salvaguarda da privacidade como o centro irradiador para a tutela de outros direitos da personalidade. Na esteira do que ressalta Stefano Rodotà (2014, p. 15), a implantação da infraestrutura da rede mundial de computadores ensejou o ciberespaço, uma nova e verdadeira dimensão da realidade onde são produzidos conhecimentos e veiculadas informações que são de interesse comum a todas as pessoas. Por esse motivo, em virtude da constituição de um espaço de comum interesse, é viável postular um direito universal de acesso à internet. Logo, delineia-se o advento de uma "cidadania digital", que nada mais é que a adequação da cidadania ao horizonte tecnológico que se sedimenta nas primeiras décadas do século XXI. Assim, a noção de cidadania passa a albergar um direito fundamental de acesso à rede (RODOTÀ, 2014, p. 17).

Ao embasar-se sobre a constatação de que a internet se tornou um espaço de produção e circulação de conhecimentos que devem ser de desfrute comum a todos os interessados, para ser efetiva, a cidadania digital exige a *neutralidade da rede*. Esta expressão sintetiza a aplicação do preceito constitucional de isonomia de tratamento ao âmbito dos fluxos de informação nas redes de computador. Sem dúvida, a neutralidade configura-se como princípio indispensável para afastar a discriminação do tráfego de dados na internet. Esse preceito é de suma importância para evitar que os conteúdos divulgados *on-line* sejam discriminados, bem como se mostra indispensável para assegurar que as características e a origem da pessoa usuária sejam levadas em conta no momento de alocar banda de internet disponível. Eventualmente, um tema como a velocidade de tráfego de dados pode parecer mais técnico do que propriamente jurídico, porém tal conclusão seria precipitada. Destarte, a velocidade da distribuição dos pacotes de *bytes*, um assunto aparentemente técnico, apresenta-se como indispensável para assegurar a não discriminação na rede. Do contrário, ou seja, no caso de uma rede desprovida de neutralidade, o direito de acesso à internet esvaziar-se-ia, visto que não basta acessar a rede sem que se possa livremente navegar nela. Não é admissível que certos assuntos ou certas pessoas sejam beneficiados no trato da transmissão de dados. Pode-se constatar, em face de tais circunstâncias, a importância de que direito ao acesso e a neutralidade da rede caminhem de mãos dadas, pois sem neutralidade de rede o direito de acesso à internet se esvazia de seu conteúdo de cidadania (RODOTÀ, 2014, p. 21-22).

Tanto o reconhecimento de um direito fundamental e universal de acesso à internet quanto a constatação de que a rede não pode declinar um funcionamento balizado pelo princípio da neutralidade são indispensáveis para consagrar a chamada cidadania digital, porém não são suficientes. Além do direito de acesso à internet e da neutralidade da rede, revela-se cada vez mais importante garantir a aplicação de instrumentos jurídicos à salvaguarda da privacidade no meio ambiente digital. Não restam dúvidas de que a disseminação de dispositivos de captura e tratamento de informações digitalizadas, quando não amparada por um arcabouço de preceitos jurídicos de contrapeso, tem o condão de acarretar violações aos direitos da personalidade mediante a invasão da vida privada dos cidadãos. Por isso, é plenamente viável depreender que as sociedades da informação encetaram seus próprios mecanismos de controle social, contrariando as utopias libertárias, que propugnavam um horizonte informático autorregulado, que prescindiria em absoluto da presença reguladora dos ordenamentos jurídicos.[5]

[5] John Perry Barlow, por exemplo, notabilizou-se por ter redigido uma *Declaração de Independência do Ciberespaço*. Nela, logo no primeiro parágrafo, lê-se: "Governos do Mundo Industrial, vocês gigantes aborrecidos

Danilo Doneda (2006, p. 10-12), remetendo à ascensão histórica do conceito, ensina que a noção de privacidade emerge no horizonte jurídico em meados do século XIX, sob a égide do liberalismo jurídico. Inicialmente de base eminentemente individualista, a privacidade representou uma reivindicação de isolamento e tranquilidade. Pode-se admitir que essa concepção da privacidade perdurou até meados dos anos 1960, momento decisivo em que, na conjuntura do *welfare state*, as relações entre cidadãos e Estado se alteraram substancialmente. Não menos importante para provocar as inflexões do conceito jurídico de privacidade foi o exponencial crescimento do fluxo de informações, acarretado pelo desenvolvimento tecnológico. No contexto de aludida conjuntura, além de um direito a certo isolamento, a privacidade passa a abarcar a proteção de dados pessoais como um pressuposto da autodeterminação privada da própria personalidade.

Nesse sentido, percebe-se que a privacidade se insinua no horizonte dos direitos da personalidade no período subsequente à Segunda Guerra Mundial, consubstanciada na *Declaração Americana de Direitos e Deveres do Homem* e na *Declaração Universal dos Direitos Humanos*, ambas de 1948. É imediatamente evidente que a chamada "virada cibernética" só viria a lume décadas mais tarde, circunstância de relevo para compreender porque a privacidade foi tradicionalmente formulada como o direito de construir uma vida privada independente das injunções da sociedade ou de outros cidadãos; o direito de privacidade consubstanciava um direito a edificar uma esfera de vida intangível pelos demais membros da sociedade. Stefano Rodotà (2014, p. 28-29) ressalta que a privacidade comungava a estrutura jurídica tradicionalmente atribuída ao direito de propriedade; caracterizava-se por circunscrever uma área que pertenceria exclusivamente ao sujeito, tal como se fosse proprietário. A privacidade era concebida em moldes espaciais, sugerindo a existência de uma esfera incólume às injunções do mundo exterior, um refúgio imune às investidas da sociedade e do Estado.

Nos dias de hoje, em meados da segunda década do século XXI, está claro que os desafios que se impõem à tutela do direito à privacidade não são idênticos àqueles do pós-Guerra, eis que as circunstâncias que rodeiam o desenvolvimento das tecnologias da informação empurram o direito na direção do reconhecimento que a vida está mais digitalizada do que nunca. E diante da crescente digitalização dos mais variados aspectos da vida cotidiana, os dilemas atinentes à tutela da privacidade transportam-se para o ciberespaço, compelindo a

---

de carne e aço, eu venho do espaço cibernético, o novo lar da Mente. Em nome do futuro, eu peço a vocês do passado que nos deixem em paz. Vocês não são benvindos entre nós. Vocês não têm a independência que nos une". O texto de Barlow pode ser lido na íntegra em: <http://www.dhnet.org.br/ciber/textos/barlow.htm>. Acessado em 09 de setembro de 2016.

cultura jurídica a reconhecer a importância de proteger os dados pessoais que circulam em rede, se se pretende salvaguardar o direito à privacidade na sociedade da informação. Essa conjuntura não implica o apagamento do tradicional direito à privacidade, mas exige que se supere o antigo paradigma mediante a incorporação da perspectiva segundo a qual é imprescindível estender a tutela jurídica também aos dados pessoais. Em face dessas circunstâncias, a cultura jurídica se vê compelida a reconhecer que uma tutela centrada na pessoa já não é suficiente; impende adaptar os mecanismos jurídicos de forma a garantir uma tutela dinâmica da privacidade, por meio do acompanhamento do fluxo de dados atinente ao indivíduo (DONEDA, 2006, p. 168).

É nesse sentido que a *Carta dos Direitos Fundamentais da União Europeia*, editada no preâmbulo do presente século, incorpora as duas acepções do direito à privacidade, isto é, tanto admite a concepção da privacidade como uma esfera inviolável quanto reconhece os limites de tal noção ao incorporar a perspectiva da proteção de dados. Destarte, no art. 7º da referida Carta consagra-se o respeito pela vida privada e familiar, ao domicílio e às suas comunicações, ao passo que a redação do art. 8º almeja concretizar a proteção de dados pessoais, determinando o direito a acessar e a retificar os dados coligidos, tanto quanto propõe a existência de uma autoridade independente destinada à fiscalização desses direitos atinentes aos dados pessoais. A posição de Stefano Rodotà (2014, p. 31-32) parece estar em consonância com a supramencionada norma, eis que o jurista italiano declara a insuficiência do momento individualista da tutela da privacidade e, com base nisso, pugna pela existência de um momento público e transindividual de salvaguarda da vida privada por intermédio de uma autoridade pública independente com atribuições concernentes à proteção da vida privada.

Danilo Doneda (2006, p. 27-30) registra preocupações em idêntico sentido. Defende que o primeiro destes artigos denota o momento individualista da proteção da privacidade, ao passo que o segundo alude à chamada *funcionalização da proteção da privacidade*, exercida mediante a tutela dinâmica dos dados pessoais. Tanto no âmbito da legislação internacional quanto no que se refere à cultura jurídica, registra-se que a tutela da privacidade de índole patrimonialista vem a ser suplantada por novos mecanismos e institutos. Destarte, a superação do viés patrimonialista também atesta o incentivo ao reconhecimento da dimensão coletiva da privacidade, incluindo a percepção de que a privacidade está interconectada com o livre desenvolvimento da personalidade. Por isso, Doneda (2006, p. 30) ressalta a importância de reconhecer a dimensão coletiva da privacidade, abarcando a identificação de sujeitos coletivos que venham a ser prejudicados pela invasão de privacidade exercida por meio da apropriação desarrazoada de dados pessoais.

Vê-se claramente, portanto, que a tutela da privacidade na sociedade da informação envolve a garantia de condições que viabilizem a *autodeterminação informativa*, pois é imprescindível que o interessado tenha o controle dos dados que se lhe referem. Um dos meios para dar consequência ao princípio da autodeterminação informativa é colocar à disposição do usuário da internet recursos técnicos de navegação anônima. Tal é o caso da opção "*do not track*"[6], que coloca nas mãos do usuário a opção de bloquear o rastreamento de dados. A fragilidade de tal recurso reside no fato de que, dado o nível de habitualidade que cerca a navegação na internet, há um sem números de atos executados *on-line* já naturalizados no comportamento cotidiano, de forma que o usuário nem cogita que está sendo vigiado ou sequer lembra de ativar a função de não ser seguido. Ademais, esta é uma resposta demasiado individualista ao problema, vez que sobrecarrega o usuário, depositando sobre suas costas o permanente dever de precaver-se contra os procedimentos automáticos de recolha de dados sempre em seu encalço. O limite de tal abordagem está em exigir do usuário toda a precaução, assegurando aos grandes armazenadores de informação a posição cômoda, sem sérios deveres de precaução e prevenção para com os dados pessoais alheios. É uma aproximação válida à questão da recolha de dados, porém insuficiente, vez que exime da responsabilidade órgãos públicos e empresas, que poderiam agir segundo padrões jurídicos predeterminados de proteção da privacidade. Tendo em vista a complexidade inerente às sociedades de intensa produção e circulação de informação, torna-se imperativo a extensão dos *princípios de prevenção e precaução* para abarcar a proteção aos dados pessoais na internet (RODOTÀ, 2014, p. 34-36).

O fenômeno da coleta quantitativa e qualitativa de dados focaliza uma questão fulgurante nos dias de hoje: a existência de procedimentos automatizados de recolha de informações. É equivocado imaginar que a coleta de dados pessoais ocorre prioritariamente mediante organizações repletas de pessoas lendo *e-mails* e escutando ligações telefônicas. A perspectiva de uma sociedade da vigilância torna-se especialmente temerária porque surgiram dispositivos de tratamento automatizado da informação, ou seja, dispositivos que prescindem da figura censória de um ser humano que domina nossas vidas. A automatização computacional da sociedade da informação inaugura uma nova perspectiva de controle social: o governo dos algoritmos.[7] As operações automáticas desfrutam da vantagem de serem céleres e de não

[6] Mais informações sobre esse dispositivo de não rastreamento podem ser localizadas em: <http://donottrack.us/>. Acessado em 09 de setembro de 2016.

[7] Dominique Cardon (2015, p. 7) apresenta uma elucidativa definição de algoritmo: "Este termo da informática tem uma significação bem maior do que podemos crer. Tal como uma receita de cozinha, um algoritmo é uma série de instruções que permitem obter um resultado. Em velocidade muito grande, ele opera um conjunto de cálculos a partir de gigantescas massas de dados (os "*big data*"). Ele hierarquiza a informação, torna-se o que nos

sofrerem interferências humanas que poderiam turvar a coleta de dados. Em alguns casos, as deliberações humanas têm sido deixadas de lado para dar azo aos procedimentos automatizados; isso tem ocorrido em um sem número de esferas que tocam a vida de cada pessoa. No caso das violações à privacidade, os algoritmos são centrais, visto que sem esse tipo de procedimento seria inviável processar um montante tão elevado de dados, mormente se se considera que tais dados são atinentes ao "perfil" singular de cada pessoa (RODOTÀ, 2014, p. 37).

As consequências da adoção exponencialmente progressiva dos algoritmos em substituição a decisões humanas ainda estão em aberto. Há importantes alertas asseverando os perigos de que a sociedade esteja prestes a sucumbir à uma ditadura dos algoritmos, colocando em questão direitos fundamentais e liberdades cívicas a partir do temor de que, na relação entre seres humanos e máquinas, as últimas levem a melhor. Por outro lado, seguramente há quem sustente que a complexidade da rede mundial de computadores, e sua correspectiva frenética circulação de informações, simplesmente não poderia funcionar sem o auxílio dos cálculos automatizados levados a cabo por algoritmos inteligentes. Provavelmente há um bom tanto de verdade em cada uma das posições, porém um balanço dos extremos ainda está por se fazer.

A despeito da interrogação fundamental concernente à positividade ou à negatividade dos presentes fenômenos, o que se manifesta como realidade consumada é o funcionamento da rede mundial de computadores por intermédio de algoritmos. Assim sendo, se a sociedade atual é uma sociedade da informação e se os algoritmos são centrais no processamento de dados, começa-se a assistir transformações na economia do poder, sobretudo com a ascensão de novos sujeitos da maior importância política (dentre os quais o mais comentado é o Google). Rodotà (2014, p. 38-40) ressalta que a sociedade dos algoritmos, ao colocar em jogo novas relações de poder entre humanos e máquinas, tem o potencial de violar garantias consolidadas. Da mesma forma que outrora o desenvolvimento tecnológico impulsionou o direito na direção da proteção de dados pessoais, nos dias de hoje os procedimentos automatizados de tratamento de dados (algoritmos) estimulam uma inflexão adicional, demandando do ordenamento jurídico um olhar especial. De fato, na medida em que os dispositivos de produção e de captura de dados se disseminaram, o montante de dados circulando em rede multiplicou-se em escala astronômica. O fato é que os dados recolhidos só possuem valor na medida em que possam ser interpretados e manejados. Logo, para tornar empregáveis os dados recolhidos, revelou-se necessário o

interessa, seleciona os bens que nós preferimos e se esforça para nos auxiliar em numerosas tarefas. Nós fabricamos esses calculadores, mas em resposta eles nos constroem" (tradução nossa).

desenvolvimento de procedimentos automatizados hábeis no tratamento de dados – trata-se dos famigerados algoritmos.

Aos poucos, a importância de aplicar aos algoritmos uma regulação vem sendo reconhecida. No âmbito da União Europeia, a Diretiva 95/46 do Parlamento Europeu e do Conselho, relativa à proteção do tratamento e da circulação de dados pessoais, já reconhece o direito de qualquer pessoa a não ser submetida ao tratamento automatizado de dados que provoque alterações em sua esfera jurídica. Esta Diretiva consigna que o tratamento de dados deve respeitar direitos e liberdades fundamentais, e consagra um importante artigo às "decisões individuais automatizadas". Em síntese, o art. 15º da referida Diretiva assegura ser direito pessoal não ter a própria esfera jurídica atingida de modo significativo pelo tratamento automatizado de informações, fazendo referência expressa ao recolhimento de dados atinentes à personalidade, tais como os referentes à capacidade profissional, ao crédito, à confiança de que a pessoa seja merecedora e ao seu comportamento. Destarte, vê-se que já começa a se esboçar na comunidade jurídica o reconhecimento de que procedimentos automatizados mediante algoritmos podem afetar decisivamente a vida das pessoas. Mais ainda, reconhece-se o direito a não ser submetido a estes mecanismos já que, conforme destaca Rodotà (2014, p. 40), o tratamento de dados pessoais por meio de algoritmos tem o condão de transformar as pessoas em abstrações numéricas, meras compilações de dados ou armazenamento de *bytes*.

Do acimo exposto é adequado inferir que a contemporânea sociedade da informação ameaça a privacidade em virtude do montante de informações pessoais em circulação e do armazenamento potencialmente infinito desses dados. Tendo em vista o substrato técnico de circulação e armazenamento de informações, Gediel e Corrêa (2008, p. 149-150) destacam o risco vislumbrável de que todo esse acúmulo de dados corrobore a hipótese de uma sociedade de controle, tal como aventada por Gilles Deleuze em texto seminal.[8] Amiúde evoca-se, inclusive nos países reconhecidamente democráticos, os imperativos da segurança pública com o intuito de açambarcar os dados pessoais e utilizá-los de maneira atentatória à privacidade. Noutro extremo, os agentes do mercado estão igualmente interessados na coleta e na manipulação de dados pessoais com o intuito de calibrar o marketing, de forma a adequar as

[8] Sem sombra de dúvidas, Gilles Deleuze (2010, p. 222) foi muito preciso ao antever a ascensão de uma sociedade movida a algoritmos computacionais que se infiltram nos mais recônditos aspectos da vida privada: "Nas sociedades de controle, ao contrário, o essencial não é mais uma assinatura e nem um número, mas uma cifra: a cifra é uma senha, ao passo que as sociedades disciplinares são reguladas por palavras de ordem (tanto do ponto de vista da integração como da resistência). A linguagem numérica do controle é feita de cifras, que marcam o acesso à informação, ou a rejeição".

estratégias de venda a cada indivíduo tomado em sua singularidade. Vê-se, pois, o quanto as razões de Estado e as iniciativas mercadológicas interseccionam-se no intuito de armazenar e empregar os dados pessoais. Por isso a relevância de elucidar as mutações jurídicas no âmbito do conceito de privacidade, vez que as transformações no contexto tecnológico e social acarretam inelutáveis consequências no âmago da cultura jurídica. Persiste ainda a tarefa de examinar as contribuições do importante Marco Civil da Internet, o que se fará a seguir.

3. O meio ambiente digital e o Marco Civil da Internet

Em território pátrio, a grande referência na regulação da rede mundial de computadores veio a lume em 2014, graças ao advento da Lei nº 12.965, mais conhecida pela alcunha de Marco Civil da Internet. Nutrido de significativa participação da sociedade, o Marco Civil consolidou fundamentos, princípios e objetivos da disciplina da internet no Brasil. A despeito de envolta em muitos debates e polêmicas, a aprovação do Marco Civil tem sido considerada muito positiva por ativistas dos direitos fundamentais na era digital – dentre os quais está Tim Berners-Lee, considerado o criador da *World Wide Web* e reconhecido militante pela preservação de direitos e liberdades na rede. O tema da regulação da rede mundial de computadores está presente nos debates jurídicos internacionais, tanto quanto está incandescente em território nacional, sobretudo porque a aprovação do Marco Civil da Internet conferiu centralidade às discussões em torno da cidadania digital e dos direitos na era da internet. Logo, a disciplina jurídica da internet no Brasil passa por um momento de suma relevância para garantir que os direitos fundamentais prevalecerão sobre a desmedida obsessão por segurança, vigilância e controle.

A interconexão mundial de computadores, consubstanciada na digitalização da informação, permitiu a ascensão do chamado ciberespaço, que nada mais é que a constituição de elos cooperativos estabelecidos entre computadores espalhados por todo o globo planetário. Essa infraestrutura viabilizou o desdobramento de um espaço de produção e difusão dos mais variados saberes, avalizando que cada pessoa esteja em condições de adicionar à rede sua própria contribuição. Assim, o ciberespaço emerge da possibilidade de produzir e acessar o conhecimento produzido em qualquer ponto da rede mundial de computadores (LÉVY, 2010, p. 96). Em sentido semelhante, com base nos arts. 215 e 216 da Constituição da República, Celso Antonio Pacheco Fiorillo (2015a, p. 90) sustenta que o ciberespaço pode ser classificado como bem ambiental. Isso porque, dada a natureza jurídica do bem ambiental, o ciberespaço figuraria perante o ordenamento jurídico na qualidade de bem difuso.

De fato, nesse sentido, o art. 215, *caput*, da Constituição assevera que o Estado tem o dever de garantir o acesso às fontes da cultura nacional, assim como tem a missão de apoiar e incentivar a valorização e a difusão de manifestações culturais. Ademais, o mesmo artigo, em seu §3º e respectivos incisos, fixa diretrizes para o Plano Nacional de Cultura. Dentre tais diretrizes, são especialmente aplicáveis à tutela do meio ambiente digital a exigência de criar as condições favoráveis à "produção, promoção e difusão de bens culturais" (§3º, II), tanto quanto o mandamento rumo à "democratização do acesso aos bens da cultura" (§3º, IV). Além disso, o art. 216 parece corroborar a leitura do ciberespaço como bem ambiental ao salientar que o patrimônio cultural brasileiro engloba bens materiais e imateriais. Assim sendo, é adequado destacar que a internet se encaixa na categoria de patrimônio cultural, eis que o referido artigo assinala que "as formas de expressão" (I), "os modos de criar, fazer e viver" (II) e "as criações artísticas, científicas e tecnológicas" (III) são merecedores de tutela por parte do Estado em parceria com a sociedade civil (§ 1º). Neste ponto a Constituição elucida que a relação jurídica ambiental é nitidamente multilateral, visto que a tutela do bem ambiental congrega agentes públicos e privados, tal como evidencia a exegese dos arts. 215, 216 e 216-A da Constituição.

A Lei nº 12.965/2014, ou simplesmente Marco Civil da Internet, vem a lume para estabelecer princípios, garantias, diretrizes, direitos e deveres para o uso da internet no Brasil, tal como assenta seu art. 1º. Destarte, o Marco Civil da Internet regulamenta e especifica, em plano infraconstitucional, tanto os princípios e garantias constitucionais fundamentais quanto estende e aplica ao âmbito da internet brasileira a disciplina da comunicação social, fixada nos arts. 220 a 224 da Constituição Federal. Porém, a Lei nº 12.965/2014 não se adstringe à comunicação social, visto que a internet alberga um verdadeiro meio ambiente cultural na esfera digital, atraindo para si também os artigos da Constituição da República que abordam a valorização do patrimônio cultural material e imaterial, pois cada vez mais se reconhece a relevância do ciberespaço como uma dimensão de criação e profusão cultural. Ademais, é inegável que na atualidade a internet tenha se tornado um espaço de profusão comercial, o que faz com que os princípios gerais da atividade econômica também impactem na regulamentação infraconstitucional da internet (FIORILLO, 2015b, p. 16-17).

Na atualidade, um dos temas mais sensíveis no que concerne ao uso da internet é o da preservação da privacidade, justamente porque a sociedade da informação tem como força motriz a produção e a circulação de informações ou, noutros termos, pode-se dizer que a sociedade contemporânea leva a cabo a digitalização da vida cotidiana. Nesse contexto, a

internet incentiva o acúmulo de dados pessoais, o que suscita uma série de situações ameaçadoras à vida privada. Não é por outro motivo que o art. 7º do Marco Civil da Internet, além de destacar outros direitos do usuário da internet, insiste no tema da proteção da personalidade defronte da realidade digital. Por essa razão este artigo consagra a inviolabilidade da vida privada e da intimidade, tal como já o fizera o inciso X do art. 5º da Constituição Federal, incluindo a possibilidade de indenização por dano moral ou material em caso de violação, seguindo um rumo já pavimentado pela cultura jurídica.

Além disso, em consonância com o inciso XII do art. 5º da Constituição, o Marco Civil garante a inviolabilidade e o sigilo do fluxo e do armazenamento de comunicações pela internet. A distância temporal entre a Constituição Federal, promulgada em 1988, e a Lei 12.965, oriunda de 2014, demonstra que, embora a preocupação com a inviolabilidade e com o sigilo se mantenham, os substratos concretos por meio dos quais a comunicação de opera são deveras distintos. A Constituição volta-se à correspondência física, às comunicações telegráficas e às comunicações telefônicas, ao passo que o Marco Civil ambienta-se na sociedade da informação, o que o impele a salientar o caráter inviolável e sigiloso dos fluxos de comunicação em rede e do armazenamento de dados. Entretanto, a despeito da notável dissonância tecnológica que particulariza cada momento histórico, é perfeitamente adequado assumir que a razão jurídica subjacente a ambas as normas é bastante semelhante, eis que se trata de tutelar a vida privada, um dos requisitos da dignidade humana, não importando qual seja a tecnologia informacional empregada na comunicação.

Depois de transportar a proteção constitucional conferida às comunicações à era da informação digital, o mesmo artigo contemporiza a disciplina de acordo com as especificidades da internet. Por esse motivo, destaca-se o direito a não fornecer a terceiros dados referentes aos comportamentos pessoais no domínio da internet, o que inclui registros de conexão e de acesso a aplicações, a não ser em caso de consentimento livre, expresso e informado. Assim, para assegurar que o consentimento não seja meramente de fachada, exige-se que a cláusula contratual que exprime o consentimento esteja destacada das demais cláusulas contratuais. Já para os casos em que há coleta de dados, o Marco Civil estabelece o direito de receber informações sobre coleta, uso, armazenamento, tratamento e proteção dos dados pessoais. Além disso, o artigo em comento adianta-se e elucida balizas para a recolha de dados, visto que o recolhimento de informações só pode ser realizado na medida em que guarde pertinência com finalidades que justifiquem sua coleta e que estejam especificadas em contratos de prestação de serviços ou termos de uso de aplicações, bem como salienta-se a ilegalidade da recolha de dados

com finalidades vedadas pela legislação. É também viável requerer a exclusão dos dados pessoais fornecidos ao término da relação entre as partes, exceção feita aos dados de guarda obrigatória, prevista no próprio Marco Civil da Internet.

Dada a relevância do tema da privacidade para preservação da vida privada nas atuais sociedades da informação digital, o Marco Civil da Internet fornece mais elementos para a disciplina da privacidade nas comunicações. O art. 8º, em primeiro lugar, assevera que o exercício do direito de acesso à internet envolve duas garantias elementares: o direito à privacidade e à liberdade de expressão. Merece destaque o fato de ambos – direito à privacidade e liberdade de expressão – serem colocados lado a lado no mesmo artigo, visto que esta é uma das equações determinantes nas sociedades da informação. Aqui, o problema envolve equilibrar a existência de um direito que constitui uma esfera de informações cuja divulgação é interditada a outro direito que promove o oposto, um direito a disseminar informações ao público. A problemática do chamado direito ao esquecimento é bem representativa do desafio em questão, eis que o direito ao esquecimento surge com o intuito de remediar situações em que informações atinentes à vida privada foram transladadas para o domínio público, engendrando contundentes males existenciais aos indivíduos atingidos. Ciente dessas circunstâncias, há no artigo em comento a determinação da nulidade de cláusulas contratuais que contrariem a inviolabilidade e o sigilo das comunicações.

Nesse ínterim, Stefano Rodotà (2014, p. 41-44) sustenta que as tecnologias da informação introduzem novas relações entre os seres e a memória social. Hoje, a memória social já não é apenas recrutada pelos meios tradicionais, isto é, por intermédio da oralidade e da escrita; na atualidade, a memória social está minuciosamente açambarcada em rede, disponível *on-line*. Se se constata que o armazenamento e tratamento de informações é, atualmente, uma forma de exercitar um poder decisivo, a partir do momento em que se nota que afeta a vida de populações inteiras, não é precipitado afirmar a necessidade de erigir mecanismos institucionais oponíveis a tais poderes. É com esse propósito que emerge no horizonte jurídico o chamado direito ao esquecimento. Não deixa de soar incômodo levantar a bandeira do esquecimento numa sociedade acostumada a informar de maneira incessante, mas é precisamente na qualidade de um contrapoder que o direito ao esquecimento se insinua no cenário jurídico. É assaz relevante assegurar à pessoa o direito de desvencilhar-se de seu passado – quando este não está eivado de fatos de importância pública. A possibilidade de recomeçar integra o direito à autodeterminação existencial, uma faceta indispensável da liberdade.

Nos casos em que haja guarda de registros de conexão, de dados pessoais ou de comunicações privadas, assegura o art. 10 do Marco Civil que se preserve a intimidade, a vida privada, a honra e a imagem das pessoas envolvidas direta ou indiretamente nas informações armazenadas. O mesmo artigo determina que registros de conexão, dados pessoais ou quaisquer outras informações que possam levar à identificação do usuário ou do terminal de acesso à internet só serão disponibilizados mediante decisão judicial. A mesma disposição é válida para o acesso ao conteúdo de comunicações privadas armazenadas, que só pode acontecer por intermédio de intervenção judicial. Acrescenta-se ainda que o provedor dos serviços de guarda tem o dever de explanar as medidas e os procedimentos de segurança e sigilo adotados.

Além disso, nos termos do art. 11, o Marco Civil oferece uma disciplina referente à coleta, ao armazenamento, à guarda e ao tratamento de dados pessoais ou comunicações aplicável sempre que pelo menos um dos terminais interconectados esteja no Brasil, inclusive quando o prestador do serviço é pessoa jurídica sediada no exterior, bastando que haja prestação de serviços em território nacional. Tal disposição é de suma relevância, tendo em vista que depois da globalização o princípio da territorialidade, indispensável para os Estados-nação soberanos, foi colocado em xeque. Assim, com o advento da interconexão global e, especialmente, com a ascensão definitiva do ciberespaço, a própria noção de soberania passa por profundas reformas. Mesmo que seja necessário admitir que a internet não é uma realidade homogênea, apresentando-se de maneira diferente de acordo com as interferências sociais que a conformam, é igualmente imperativo reconhecer que no ciberespaço as fronteiras dos Estados nacionais não se replicam pura e simplesmente. Destarte, no ciberespaço, a territorialidade cede em face da localização da informação na rede (FIORRILO, 2015b, p. 98). Ainda que desprovido de grandiloquência, o art. 11 do Marco Civil aponta para a revisão desse horizonte territorial ao indicar que, para a aplicação da disciplina jurídica brasileira de proteção de dados, é suficiente que a prestação de serviço envolva pelo menos um terminal localizado no país.

Para encerrar esse breve e parcial resumo dos dispositivos jurídicos de salvaguarda da vida privada contidos no Marco Civil da Internet, é adequado mencionar alguns princípios referentes à proteção de dados que têm sido esposados pela doutrina e devem orientar a interpretação das normas contidas no marco regulatório. Primeiramente, o *princípio da publicidade* consigna que os bancos de dados devem ser de conhecimento público, eis que o armazenamento secreto de dados não se afigura compatível com o Estado democrático de direito. Em seguida, formula-se o *princípio da exatidão*, que determina que os dados recolhidos devem ser fieis à realidade. Tal disposição compele os gestores de bancos de dados a realizar a

constante atualização dos dados sob guarda. Tendo em vista que amiúde a recolha de dados é excessiva, a doutrina sedimentou o *princípio da finalidade*, cujo objetivo é evitar a recolha desmedida de dados, compelindo os bancos de dados a demonstrar que os dados coletados cumprem com uma finalidade razoável. O *princípio do livre acesso* almeja facilitar o acesso da pessoa aos seus próprios dados armazenados, incluindo a possibilidade de retificá-los, bem como de adicionar as informações que se façam necessárias. É perceptível o comprometimento deste princípio com a formatação conferida ao *habeas data*, previsto no inciso LXXII do art. 5º da Constituição. Por fim, o *princípio da segurança física e logística* atribui ao ente que efetua a guarda o dever de assegurar a integridade dos dados coligidos, o que implica que os dados não sejam extraviados, destruídos, modificados, transmitidos ou acessados por pessoas desautorizadas (DONEDA, 2006, p. 216-217).

Em suma, procurou-se trazer a lume e elucidar aquela que, em território pátrio, é a grande referência legislativa na regulação da rede, o Marco Civil da Internet. A aprovação do Marco Civil conferiu centralidade ao debate em torno da cidadania digital e dos direitos na era da internet também em território nacional. Assim sendo, parece plausível depreender que a disciplina jurídica da internet no Brasil passa por um momento decisivo e que, por conseguinte, está-se diante de uma conjuntura de suma relevância para garantir que os direitos fundamentais prevalecerão sobre a vigilância persecutória. Na medida em que a privacidade, elemento indispensável da dignidade humana, mudou de figura na sociedade da informação, demonstrou-se que a tutela jurídica da vida privada se volta cada mais para o controle do fluxo de dados pessoais. Soa coerente imaginar que o direito exercerá um papel indispensável na regulação dos bancos de dados, sobretudo, como acontece atualmente, quando a privacidade é digitalizada tanto voluntária ou quanto sub-repticiamente.

4. Conclusão

Em síntese, o presente artigo almejou delinear a candência do tema proposto para análise. Evidencia-se que tanto no plano internacional quanto em território nacional a proteção jurídica dispensada aos dados pessoais goza de atualidade e relevância. Ademais, é razoável imaginar que as dificuldades atreladas a proteção de dados pessoais tende a se agravar, visto que hoje já se sabe que o horizonte tecnológico aponta na direção de uma interconexão ainda mais profunda, sobretudo mediante o desenvolvimento da chamada internet das coisas, que nada mais é que o ingresso nos domínios da internet dos mais ordinários objetos da vida cotidiana. Essa conjuntura indubitavelmente ensejará um acréscimo quantitativo de dados

recolhidos e, principalmente, uma mudança qualitativa no tipo de dados açambarcados, eis que a tendência é que esses dados sejam cada vez mais sensíveis ou íntimos.

Destarte, procurou-se compreender em que medida a sociedade da informação, com seus desenfreados mecanismos de recolha de informações, traz riscos eminentes de violação de direitos fundamentais, mormente de direitos da personalidade. Buscou-se elucidar, assim, o perigo intrínseco a uma sociedade da informação, quando destituída de regras jurídicas claras a respeito da proteção de dados pessoais, converter-se em sociedade de vigilância. Assim, colocou-se o objetivo de evidenciar as transformações que a sociedade da informação provocou na ideia de privacidade vez que, além de demarcar uma esfera inviolável de intimidade, a privacidade atualmente assinala o direito de acessar e retificar dados pessoais e, sobretudo, o direito de saber quais informações sobre si estão sendo recolhidas, bem como para qual finalidade estão sendo armazenadas e manipuladas. Visou-se, por fim, a esclarecer a relevância de formular instrumentos jurídicos aptos a enfrentar a recolha abusiva de dados pessoais; instrumentos oponíveis tanto a agências estatais quanto a entidades privadas que detêm e manipulam informações atinentes aos cidadãos e, assim, garantir as condições para o exercício democrático da chamada cidadania digital.

5. Referências bibliográficas

ASSANGE, Julian et al. *Cypherpunks*: liberdade e o futuro da internet. Trad. de Cristina Yamagami. São Paulo: Boitempo, 2013.

BARLOW, John Perry. *Declaração de Independência do Ciberespaço*. Disponível em: <http://www.dhnet.org.br/ciber/textos/barlow.htm>. Acessado em: 09 de setembro de 2016.

BAUMAN, Zygmunt; LYON, David. *Vigilância líquida*. Trad. de Carlos Alberto Medeiros. Rio de Janeiro: Zahar, 2013.

CARDON, Dominique. *À quoi rêvent les algorithmes*: nos vies a l'heure des big data. Paris: Seuil/La République des Idées, 2015.

DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

FIORILLO, Celso Antonio Pacheco. *O Marco Civil da Internet e o meio ambiente digital na sociedade da informação*: comentários à Lei n. 12.965/2014. São Paulo: Saraiva, 2015b.

FIORILLO, Celso Antonio Pacheco. *Princípios constitucionais do direito da sociedade da informação*: a tutela jurídica do meio ambiente digital. São Paulo: Saraiva, 2015a.

FOUCAULT, Michel. *A verdade e as formas jurídicas*. 4. ed. Trad. de Eduardo Jardim e Roberto Machado. Rio de Janeiro: Nau, 2013.

GEDIEL, José Antônio Peres; CÔRREA, Adriana Espíndola. Proteção jurídica de dados pessoais: a intimidade sitiada entre o Estado e o mercado. *Revista da Faculdade de Direito – UFPR*, Curitiba, n. 47, p. 141-153, 2008.

HUXLEY, Aldous. *Admirável mundo novo*. Trad. de Lino Vallandro e Vidal Serrano. São Paulo: Globo, 2009.

LÉVY, Pierre. *A inteligência coletiva*: por uma antropologia do ciberespaço. Trad. de Luiz Paulo Rouanet. 9. ed. São Paulo: Loyola, 2014.

LÉVY, Pierre. *Cibercultura*. 3. ed. Trad. de Carlos Irineu da Costa. São Paulo: Editora 34, 2010.

ORWELL, George. *1984*. Trad. de Alexandre Hubner e Heloisa Jahn. São Paulo: Companhia das Letras, 2009.

RODOTÀ, Stefano. *Il mondo nella rete*: quali i diritti, quali i vincoli. Roma: Laterza, 2014.