DOI: 10.33242/rbdc.2020.04.002

A PRIVACIDADE NO PENSAMENTO DE AMITAI ETZIONI

PRIVACY IN THE THOUGHT OF AMITAI ETZIONI

Luiz Augusto Castello Branco de Lacerda Marca da Rocha

Professor de Direito Civil da Unisuam. Mestre em Direito pela UCP. Especialista em Direito Civil/Processo Civil pela Unesa. Bacharel em Direito pela UFRJ. Advogado.

Resumo: O artigo tem por objetivo examinar o direito à privacidade em contexto americano, de acordo com a análise do pensador comunitarista Amitai Etzioni. Para tanto, será traçado um breve recorte histórico da caminhada da *privacy* nos tribunais daquele país (em especial, na jurisprudência da Suprema Corte), bem como dos critérios adotados pelos sistemas americano e europeu para a proteção de dados pessoais. O pensamento do autor busca estabelecer uma definição adequada para o mencionado direito, bem como parâmetros que permitam equilibrar sua proteção aos ditames do bem comum e a ameaças proporcionadas por agentes públicos e privados.

Palavras-chave: Privacidade. Constituição. Informações pessoais. Bem comum.

Abstract: The article aims to examine the right to privacy in the American context, according to the analysis of communitarian thinker Amitai Etzioni. In order to do so, a brief historical review of the privacy path will be drawn up in that country's courts (in particular, in Supreme Court jurisprudence), as well as the criteria adopted by the American and European systems for the protection of personal data. The author's intention is to establish an adequate definition for the aforementioned right, as well as parameters that allow to balance its protection to the dictates of the common good and the threats provided by public and private agents.

Keywords: Privacy. Constitution. Personal information. Common good.

1 Considerações iniciais

Os tempos atuais, marcados pela significativa presença da tecnologia em virtualmente todos os campos da vida humana – fenômeno denominado por

Lipovetsky[1] "hipertecnicização" –, impõem a necessidade de uma releitura de diversos institutos jurídicos, como forma de conferir-lhes adequada tutela.

Entre tais direitos, encontra-se a privacidade. Muito embora sua noção possa ser algo intuitiva, não poucas são as dificuldades em alcançar um conceito que compreenda seus variados aspectos.[2] Tais entraves transcendem a doutrina pátria, conforme leciona Doneda, para quem a falta de uma definição "âncora" seria um problema por igual enfrentado na doutrina dos EUA.[3]

O presente trabalho tem como objetivo estudar a privacidade no pensamento de Amitai Etzioni. O autor, expoente do comunitarismo liberal, apresenta a necessidade de se estabelecer uma noção de *privacy* que equilibre as tensões existentes entre os interesses individuais e a necessidade de salvaguardar o bem comum. Tal definição deve se mostrar apta a lidar com os desafios apresentados pela pós-modernidade, considerando que seu eixo de proteção se desloca de uma associação à propriedade privada para o controle efetivo das informações pessoais, disponibilizadas em uma sociedade em rede, passando sua tutela a ser estruturada na relevância dada à informação.[4] Naturalmente que este relacionamento entre privacidade e tecnologia não pode ser encarado sob uma perspectiva ludista,[5] mas sob o prisma da necessária harmonização entre ambos.

Para tanto, o trabalho traça inicialmente um panorama histórico da privacidade centrado numa análise dos tribunais americanos, em especial na Suprema Corte. Muito embora o tratamento dado à *privacy* nos EUA seja fragmentado[6] e

1 LIPOVETSKY, Gilles; SERROY, Jean. *A cultura-mundo*. Resposta a uma sociedade desorientada. Tradução de Maria Lúcia Machado. São Paulo: Companhia das Letras, 2011. p. 32.

2 Tatiana Malta Vieira classifica a vida privada em quatro categorias, a saber: "física (protegendo o corpo do titular do direito contra procedimentos invasivos não autorizados), domiciliar (cujo objetivo é preservar o domicílio ou local de trabalho do titular ameaçado), de comunicações (evitando sua interceptação, violação e propagação indevida de conteúdo por terceiros), decisional (ligada à ideia de autodeterminação, que pode ser considerada em relação aos próprios dados ou mesmos a valores íntimos do titular, correspondentes a seu projeto existencial) e informacional (que busca proteger os dados que traçam o perfil identitário do titular e sejam correlatos à sua intimidade, ou suas relações pessoais)" (VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sérgio Antônio Fabris. 2007. p. 31-34).

3 "A verdade é que a falta de uma definição 'âncora', que reflita uma consolidação do seu tratamento semântico, não é um problema localizado da doutrina brasileira: tome-se, por exemplo, a doutrina norte-americana, que conta com um vocábulo consolidado (privacy) e que faz referência a um vasto número de situações, muitas das quais a tradição da civil law não relacionaria com a privacidade" (DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. *Âmbito Jurídico*, Rio Grande, n. 51, 31 mar. 2008. p. 1. Disponível em: http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460. Acesso em: 7 out. 2017).

4 CASTELLS, Manuel. *A sociedade em rede*. Tradução de Roneide Venâncio Majer. 17. ed. São Paulo: Paz &Terra, 2016. p. 124.

5 ETZIONI, Amitai. Are new technologies the enemy of privacy? *Knowledge, Technology & Policy*, n. 20, 2007. p. 115. Disponível em: http://www.amitaietzioni.org/art_magazines/. Acesso em: 7 out. 2017.

6 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 301.

marcado por uma pluralidade de fontes, entre as quais o *Privacy Act* (1974) e o altamente controverso *Patriot Act* (2001), é inegável o papel desempenhado pela jurisprudência daquele país no esforço de alcançar parâmetros para tratamento.

A seguir, é feita uma breve análise de como a privacidade vê algo de desafios impostos pelo Poder Público e por agentes privados, sendo este último aspecto tradicionalmente negligenciado na cultura americana.

Posteriormente, é realizada uma comparação entre os sistemas de proteção de dados dos Estados Unidos (a doutrina conhecida como *third-party*) e da Europa (com esteio especialmente na Diretiva 95/46 da União Europeia e no Regulamento 2016.679, que a revogou recentemente), sendo ambos os sistemas criticáveis e tidos como insuficientes na opinião de Etzioni.

No momento seguinte, é apresentado um critério defendido pelo autor, com base no pensamento comunitarista liberal, que busca harmonizar as necessidades de salvaguardar a privacidade individual e as expectativas concernentes ao bem comum.

Por fim, é apresentada uma tentativa conceitual realizada pelo autor que, inicialmente entendendo a privacidade como a possibilidade legítima de evadir-se ao escrutínio alheio, passa a associá-la à figura de um cubo, composto por três dimensões: a sensibilidade, o volume e a "cybernacionalização".

Desta forma, o estudo pretende contribuir com a demonstração da alteração da percepção do direito à privacidade, produto das profundas modificações trazidas ao contexto social em virtude especialmente do avanço tecnológico, e a apresentação do conceito formulado pelo autor. Uma maior precisão conceitual tende a fornecer critérios mais sólidos para a proteção e aplicação do referido direito, seu alcance e limites, permitindo sua efetivação diante das ameaças que o cercam.

2 A tutela jurídica da privacidade na jurisprudência dos EUA em uma perspectiva histórica

Danilo Doneda,[7] ao analisar o papel da privacidade na cultura dos EUA, afirma que esta é "um componente fundamental da própria identidade do direito norte-americano e reflete uma concepção generalizada desta sociedade a seu próprio respeito, segundo a qual a privacidade é valorizada e prezada pelo cidadão".

[7] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 261.

Em que pese esta importância fortemente enraizada na cultura daquele país, não há uma unidade quanto ao seu tratamento.[8]

O desenvolvimento da ideia de *privacy* em solo americano apresenta, segundo Etzioni, um processo histórico dividido em algumas etapas.

Inicialmente, na fase pré-1890, a noção de privacidade não se encontrava, ainda, sedimentada conceitualmente – embora sobre ela já houvesse uma percepção empírica e fluida, desprovida de autonomia –, derivando do direito de propriedade privada, sendo extraída de princípios dele derivados. A noção de propriedade, dotada de elevada densidade no pensamento liberal daquele país (muito em virtude da influência das ideias de John Locke), era tida como um reflexo do direito natural, dotado de caráter "semissacramental", inalienável e irredutível, ou, quando ao menos, como um bem fortemente privilegiado.[9] O uso do domínio privado, embora encontrasse limitações no exercício do mesmo direito por outros indivíduos, era, *a priori*, livre, cabendo a prova de sua violação àqueles que desejavam restringi-lo diante de uma situação concreta. Assim, *e.g.*, ao tutelar-se a privacidade de um indivíduo, ameaçada pela divulgação de sua correspondência pessoal, o que efetivamente era objeto de guarida jurídica era seu domínio sobre algo que lhe pertencia, *in casu*, sua reputação, sendo sua privacidade salvaguardada apenas de forma oblíqua e residual.[10]

O segundo (e mais reconhecido) marco histórico foi o multirreferenciado ensaio de Samuel Warren e Louis Brandeis, intitulado *The right to privacy*, publicado na *Harvard Law Review*, em 1890. Neste trabalho – considerado por muitos autores o momento em que a privacidade passa a ser efetivamente considerada um

[8] "O right to privacy foi ou é evocado para regular a tranquilidade no próprio lar, o controle sobre informações pessoais, o controle sobre o próprio corpo, a liberdade de pensamento, o controle sobre a vigilância, a proteção da reputação, a proteção contra averiguações e interrogatórios abusivos, o planejamento familiar, a educação dos próprios filhos, o aborto, a eutanásia, entre outros" (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 264).

[9] ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 189.

[10] "Antes de 1890, a Sociedade Americana, como muitos outras, tinha um vago conceito social de privacidade, mesmo que não estivesse incorporado em uma doutrina jurídica distinta, ou direito constitucional. Embora houvesse vários casos legais defendendo algum aspecto do que mais tarde viria ser chamado de privacidade, estes geralmente dependiam do bem estabelecido direito à propriedade privada. Por exemplo, prejudicar a reputação de uma pessoa através da revelação de detalhes privados foi considerado legalmente passível de reparação porque se pensava que causava danos a algo que possuía (ou seja, a reputação deste alguém), em vez de ser visto como uma invasão de privacidade" (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 189, tradução nossa). No original: "Before 1890 American Society, like many others, had a vague social concept of privacy, albeit one that was not embedded in a distinct legal doctrine or constitutional right. Although there were several legal cases defending some aspect of what later would be called privacy, these typically relied on the well-established right to private property. For example, harming a person's reputation through the revelation of private details was deemed legally redressable because it was thought to do damage to something one owned (i.e., one's reputation), rather than because it was viewed as an invasion of privacy".

direito autônomo, conceitualmente desvinculado de outros direitos e liberdades, como a propriedade privada (embora seu exercício fosse intimamente associado a esta) –, o *right to be left alone* passa a significar um direito de exclusão, afastando intrusões indevidas na vida privada de uma pessoa, especialmente aquelas proporcionadas pelos novos meios tecnológicos.[11]

Tal possibilidade de evadir-se a olhares alheios seria presumidamente conferida a qualquer indivíduo, de forma ampla, especialmente no interior domiciliar.[12]

Este direito, considerado pelos autores como autoevidente, passa a representar aspecto crucial da autonomia e liberdade individuais, valores extremamente relevantes na sociedade americana.[13]

Em que pese o prestígio obtido, o *right to be left alone* não encontrou imediata ressonância nos tribunais, tendo sido sua existência negada pela Corte de

[11] "As invenções recentes e os métodos de negócios chamam a atenção para o próximo passo que deve ser tomado para a proteção da pessoa e para garantir ao indivíduo o que o juiz Cooley chama de 'ser deixado sozinho'. Fotografias instantâneas e empresas jornalísticas invadiram os recintos sagrados da vida privada e doméstica; e numerosos dispositivos mecânicos ameaçam fazer bem a previsão de que 'o que é sussurrado no armário deve ser proclamado desde o topo da casa'. Durante anos tem tido a sensação de que a lei deve oferecer algum remédio para a circulação não autorizada de retratos de pessoas privadas; e o mal da invasão da privacidade pelos jornais, há muito sentido, já foi discutido recentemente por uma escrita capaz" (BRANDEIS, Louis Dembitz; WARREN, Samuel Dennis. The right to privacy. *Harvard Law Review*, Cambridge, v. IV, n. 5, 15 dez. 1890. p. 2. Disponível em: http://readingnewengland.org/app/books/right toprivacy/?l=righttoprivacy. Acesso em: 6 out. 2017, tradução nossa). No original: "Recent inventions and business methods call attention to the next step which must be taken for the protection of the person, and for securing to the individual what Judge Cooley calls the right 'to be let alone'. Instantaneous photographs and newspaper enterprise have invaded the sacred precincts of private and domestic life; and numerous mechanical devices threaten to make good the prediction that 'what is whispered in the closet shall be proclaimed from the house-tops.' For years there has been a feeling that the law must afford some remedy for the unauthorized circulation of portraits of private persons; and the evil of invasion of privacy by the newspapers, long keenly felt, has been but recently discussed by an able write".

[12] "Conforme invocado, o direito de ficar sozinho é supremo e separado de outras considerações; presume que todas as pessoas podem ficar sozinhas tanto quanto desejem – completamente, se preferirem – sem restringir as habilidades de outras pessoas para exercer seu próprio reconhecimento de que, se os membros de uma comunidade exercerem esta liberdade na íntegra, o bem comum será permutado" (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 190, tradução nossa). No original: "As invoked, the right to be left alone stands supreme and apart from other considerations; it presumes that all people can be left alone as much as they desire – completely if they so prefer – without restricting other persons' abilities to exercise their own recognition that if the members of a community exercise this liberty in full, the common good will be shortchanged".

[13] "Outros alegaram que a privacidade está intimamente associada aos nossos valores mais profundos, a nossa compreensão do que significa ser um agente moral autônomo capaz de autorreflexão e escolha, e que sua violação é 'degradante para a individualidade [e] uma afronta à dignidade pessoal', ou seja, sua violação ofende o núcleo dos valores ocidentais. Jean Cohen acrescenta que 'um direito constitucionalmente protegido à privacidade pessoal é indispensável para qualquer concepção moderna da liberdade'" (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 191, tradução nossa). No original: "Others have claimed that privacy is intimately associated with our most profound values, our understanding of what it means to be an autonomous moral agent capable of self-reflection and choice, and that its violation is 'demeaning to individuality [and] an affront to personal dignity' that is, its violation offends the core of Western values. Jean Cohen adds that 'a constitutionally protected right to personal privacy is indispensable to any modern conception of freedom".

Apelos de Nova Iorque, no caso *Robertson* (1902), para poucos anos mais tarde ser acolhido pela Suprema Corte do estado da Geórgia no caso *Pavesich v. New England Life Insurance Co* (1905).[14]

A Suprema Corte teve sua primeira oportunidade de manifestar-se a respeito do tema no caso *Olmstead v. United States* (1928), no qual se discutiu a validade da interceptação de "grampos" telefônicos, realizados pelo governo federal sem um mandado em aparelhos de comerciantes de bebidas alcoólicas (então proibidas no país), à luz da Quarta Emenda. A decisão foi pelo sentido da não aplicabilidade da tutela constitucional, tendo sido adotada uma interpretação de que esta estaria vinculada à propriedade. Nota-se nesta fase uma preocupação vinculada a uma dimensão procedimental da privacidade.[15]

O terceiro estágio de desenvolvimento apontado pelo autor foi marcado por uma série de decisões da Suprema Corte que conduziu aos fundamentos legais do aludido direito. Destacam-se aqui *Griswold v. Connecticut* (1965), *Eisenstadt v. Baird* (1972) e *Roe v. Wade* (1973). Tais precedentes representaram uma virada interpretativa, rompendo com a tendência, verificada na década de sessenta, de proferir decisões que privilegiassem amplamente alguma concepção de bem comum, em detrimento de uma noção individual de privacidade. Os casos em comento tiveram como elemento comum o questionamento acerca de direitos reprodutivos, suscitando a autonomia individual quanto a tais questões como sendo prevalente em relação a uma suposta moralidade/interesse públicos. Doneda ressalva que tais decisões abordariam na verdade um outro aspecto da privacidade, distinto do convencional, consistente na *fundamental decision privacy*.[16]

[14] A controvérsia neste período é descrita por Doneda: "A causa, em ambas as situações, era praticamente a mesma: uma pessoa teve sua foto (no segundo caso, também o seu nome) utilizada por terceiros para fins publicitários sem seu consentimento. Nos anos seguintes, a disputa sobre a existência ou não do direito à privacidade continuou, com as cortes norte-americanas oscilando entre a decisão do caso Robertson ou do caso Pavesich, embora na década de 1930 a balança tenha passado a pender fortemente no sentido da existência de um right to privacy, com sua menção no Restatement of Torts – muito embora fora do contexto constitucional. Porém, o fato de que os casos que balizaram o reconhecimento deste direito se relacionavam com questões que, para o jurista que os examina de fora do common law, não se assemelham ao universo da privacidade, já nos dá uma primeira indicação da diversidade de concepções deste direito, que vai marca-lo, notadamente, na evolução jurisprudencial norte-americana" (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 274-275).

[15] Na ocasião, o *Justice* Brandeis apresentou *dissent* no qual sustentava que: "A interpretação da Constituição deveria levar em conta o impacto dos progressos técnicos, que exigiam uma leitura mais atenta da real intenção dos frames, como condição para que ela própria pudesse se modernizar. Essa modernização consistiria em reconhecer que a intenção da quarta emenda vai muito além da proteção da propriedade, dos bens materiais que poderiam ser vasculhados: seria uma proteção efetiva contra a intrusão na vida privada pelo governo, algo que, à época da reunião dos constituintes norte-americanos na Virgínia, somente poderia ser realizado pelo acesso físico à casa, às cartas ou a outros objetos de uma pessoa – isto é, a 'tecnologia' de investigação da época foi levada em consideração. Para Brandeis, o papel da Corte seria a interpretação da quarta emenda de forma a preservar seu sentido" (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 278-279).

[16] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 289.

Em *Griswold*, a Suprema Corte entendeu pela inconstitucionalidade de uma norma editada pelo estado de Connecticut, que proibia o uso de contraceptivos entre pessoas casadas, por violar a privacidade do casal. Tal decisão teve seu alcance ampliado para pessoas não casadas pelas decisões *Eisenstadt* – que invalidou lei que proibia a distribuição de contraceptivos – e *Carey v. Population Services International* (1977) – que anulou a lei que limitava tal venda, quando feita a menores. Tais julgados (em especial, o caso *Eisenstadt*) produziram uma "nova e muito alargada" concepção de privacidade individual, que poderia ser exercida onde quer que seu titular se encontrasse, não mais se limitando a seu domicílio.[17]

O polêmico caso *Roe v. Wade*, no qual a Corte se posicionou a respeito do aborto – tema extremamente sensível à sociedade americana – igualmente envolveu o direito à privacidade. Ao estabelecer níveis diferenciados para a intervenção estatal legítima no tocante ao direito da mulher de suspender sua gestação (dividindo o processo gravídico em trimestres, e considerando a esfera de liberdade decisional quanto à interrupção do processo gravídico mais ampla no primeiro e mais sujeita a regulamentações estatais no último), o tribunal, ao mesmo tempo em que estabelece um raciocínio de ponderação entre o interesse público em restringir a liberdade reprodutiva em alguns casos e o interesse individual de decidir quanto à interrupção da gestação, toma em consideração a privacidade (no sentido de privacidade decisional), permitindo que, em certas circunstâncias, "a behavior that had previously been controlled by the state was freed to be subject to personal choice".[18]

Outro marco relevante para o estudo da privacidade na jurisprudência americana foi o caso *Katz v. United States* (1967), que derrubou o precedente estabelecido em *Olmstead*. Nele, a Corte se valeu de uma interpretação da Quarta Emenda para afirmar que a privacidade está ligada a seu titular, e não propriamente a um local.[19]

Contudo, o critério utilizado (o da "expectativa razoável de privacidade") manteve o grau de distinção entre os espaços público e privado, conferindo a este último um maior nível de proteção.[20]

---

[17] ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 193.

[18] ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 193.

[19] Escrevendo sobre o tema, Doneda destaca a *concurrent opinion* do *Justice* Harlan: "Ainda no caso Katz, uma concurrent opinion do juiz Harlan tornou-se famosa por conter um teste, que foi posteriormente aceito e padronizado pela Corte, que serviria para verificar a existência de uma 'razoável expectativa de privacidade' em um determinado caso Esta é uma noção capital para a atuação da quarta emenda, pois a Corte somente reconheceria esta violação da privacidade quando julgasse que uma pessoa não poderia razoavelmente esperar ter sua privacidade garantida em uma determinada situação" (DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 282).

[20] "Em Katz, a maioria decidiu que 'a Quarta Emenda protege as pessoas, não os lugares', rejeitando a doutrina de 'transgressão' enunciada em Olmstead. No entanto, mesmo depois disso, a casa permaneceu

Posteriormente, a Suprema Corte viria a enfraquecer o precedente estabelecido em *Katz*, no caso *Smith v. Maryland* (1979), em que entendeu inexistirem expectativas razoáveis de privacidade daquele que usasse os serviços de uma linha telefônica, dado que assumiria o risco de a companhia telefônica revelá-los para a polícia,[21] adotando a doutrina *third-party* (*infra*).

A decisão *Katz*, em que pese ter tido o aludido mérito de romper com uma necessária associação entre privacidade e propriedade, manteve a ideia de que os mais elevados parâmetros de privacidade se dão no *locus* privado.[22] Tal posicionamento suscita inúmeras críticas apontadas por Etzioni.[23] Particularmente no que se refere aos desafios impostos pela sociedade atual, não é mais razoável estabelecer um espaço físico particular como reduto no qual a proteção à vida privada goza de maior densidade, na medida em que sensíveis e substanciais violações podem ser realizadas independentemente do lugar em que o titular do referido direito se encontre. Em suas palavras: "All of this shows that the most important consideration when it comes to protecting privacy in an age of exponential technological growth is not where a person is, but rather what kind of information is collected".[24]

praticamente inviolável aos olhos dos tribunais. Parece que Katz não separou as salvaguardas da Quarta Emenda da casa, mas ampliou a esfera da privacidade além dela para outros espaços protegidos. A informação coletada sobre eventos em casa própria ainda é considerada uma violação a priori de privacidade, enquanto muito mais licença é concedida ao estado quando ele coleta informações sobre conduta em espaços públicos e comerciais" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 3, tradução nossa). No original: "In Katz the majority ruled that 'the Fourth Amendment protects people, not places', rejecting the 'trespass' doctrine enunciated in Olmstead. However, even after this, the home remained largely inviolable in the eyes of the courts. It seems Katz did not detach Fourth Amendment safeguards from the home but rather extended the sphere of privacy beyond it to other protected spaces. Information collected about events in one's home is still often considered a priori a violation of privacy, while much more license is granted to the state when it collects information about conduct in public and commercial spaces".

21 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 284.

22 "Várias decisões da Corte que se seguiram sustentaram que se poderia ter uma expectativa razoável de privacidade fora do lar – por exemplo, em contêineres fechados e portáteis e em veículos. A discussão de alguns desses exemplos segue. Deve-se notar, no entanto, que essas decisões geralmente dependem da ideia de que a área protegida é de alguma forma semelhante ou uma extensão artificial da casa 68 e, portanto, Katz e as decisões que seguiram em vigor continuaram a basear-se na lógica de excepcionalismo da habitação" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 69, tradução nossa). No original: "Several Court rulings that followed held that one could have a reasonable expectation of privacy outside of the home – for example in closed, portable containers and in vehicles. Discussion of a few such examples follows. One should note, though, that these rulings often rely on the idea that the protected area is in some way similar to or an artificial extension of the home 68 and thus Katz and the rulings that followed in effect continued to draw on the rationale of housing exceptionalism".

23 ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 49-61.

24 ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 68.

De fato, o substancial incremento das tecnologias de comunicação em rede, onipresentes na vida cotidiana, naquilo que se convencionou chamar era digital,[25] impôs uma releitura da ideia de *privacy*.[26]

Esta capacidade da tecnologia de "encolher o reino da privacidade" foi reconhecida em *Kyllo v. United States* (2001), quando a Corte reconheceu que a utilização de dispositivos capazes de medir a quantidade de calor emanada do interior de uma casa caracteriza uma busca e, como tal, é abrangida pela Quarta Emenda, necessitando de um mandado, sob pena de considerar-se ilegal. Em abordagem mais recente, Etzioni propõe uma nova interpretação possível de *Kyllo*, que rompe com o critério das "expectativas razoáveis" de privacidade.[27]

[25] No original, *cyber age* é a expressão adotada pelo autor para referir-se aos tempos atuais, nos quais a tecnologia em rede produziu significativas alterações no modo de viver individual e coletivo, bem como no tratamento jurídico dado ao direito à privacidade, foco central deste estudo.

[26] "Na verdade, quando Warren e Brandeis publicaram seu artigo pioneiro de 1890 na Harvard Law Review, considerado a 'gênese do direito à privacidade', eles não estavam preocupados com a fofoca per se (uma violação de privacidade de primeira ordem), mas sobre a distribuição mais ampla de detalhes íntimos através da mídia (um uso secundário). No entanto, a digitalização da informação, o uso generalizado da Internet e dos computadores e a introdução de sistemas de inteligência artificial para analisar grandes quantidades de dados aumentaram a extensão, o volume, o escopo, e tipos de usos secundários por tantas ordens de grandeza que é difícil encontrar uma expressão adequada para capturar a importância desta transformação. O ponto principal não é que as informações agora possam ser processadas a uma pequena fração do custo e em velocidades incomparavelmente mais rápidas do que quando estavam vinculadas a papel, o que é certamente o caso, mas que esses modos de análise que prognosticam novas informações pessoais a partir de dados pessoais previamente coletados são comuns hoje, mas eram inconcebíveis quando a maioria das informações pessoais estava vinculada a papel" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 69, tradução nossa). No original: "Indeed, when Warren and Brandeis published their groundbreaking 1890 article in the Harvard Law Review, considered the 'genesis of the right of privacy,' they were not concerned about gossip per se (a first order privacy violation), but about the wider distribution of intimate details through the media (a secondary usage). However, the digitization of information, the widespread use of the Internet and computers, and the introduction of artificial intelligence systems to analyze vast amounts of data have increased the extent, volume, scope, and kinds of secondary usages by so many orders of magnitude that it is difficult to find a proper expression to capture the importance of this transformation. The main point is not that information can now be processed at a tiny fraction of the cost and at incomparably faster speeds than when it was paper bound, which is certainly the case, but that modes of analysis that divine new personal information out of personal data previously collected are common today, but were inconceivable when most personal information was paper bound".

[27] "Se alguém guiar-se por Katz, a legalidade da realização de imagens térmicas de fora da casa depende do que se presumam ser as expectativas pessoais e sociais. Pelo menos nos subúrbios americanos da classe média, as pessoas podem considerar essa leitura de calor como uma violação de suas expectativas. Se alguém se apega à ideia de que 'minha casa é meu castelo', medir o calor dentro da casa é de fato uma grande violação da privacidade. No entanto, se alguém segue a doutrina de privacidade da Era Digital aqui delineada, essas leituras possuem muito baixo grau de sensibilidade, porque não revelam nada sobre as preferências médicas, financeiras ou políticas do residente, e muito menos seus pensamentos. Com efeito, elas detectam uma banda extremamente baixa de informações (o termo 'largura de banda' refere-se a uma medida do número de diferentes tipos de informações coletadas). A informação revelada é menos consequente do que tipo de cereal ou qual marca de café que a pessoa comprou" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 8, tradução nossa). No original: "If one goes by Katz, the legality of conducting thermal imaging from outside the home depends on what one presumes personal and societal expectations to be. At least in middle class American suburbs, people may consider such a heat reading to be a violation of their expectations. If one clings to the idea that 'my

Há um outro aspecto problemático em *Katz* e em outras decisões até então alicerçadas na Quarta Emenda, consistente no fato de que esta não protege (ao menos não diretamente) a privacidade sob o aspecto decisional (ângulo enfocado nas decisões supramencionadas que tratavam de direitos reprodutivos), mas tão somente fornece alguns critérios quanto ao que seja uma expectativa legítima de ocultamento do interesse público (o que, como se verá, é parte componente do conceito de privacidade proposto pelo autor em um primeiro momento, embora atualmente carecedor de complementação).[28]

Esta análise do tratamento dispensado à privacidade na jurisprudência da Suprema Corte americana torna evidente a mudança histórica do conteúdo deste direito, impondo uma atualização de seu conceito, seja para alcançar uma interpretação da norma constitucional adequada ao contexto atual – reconhecendo-a como um "documento vivo", cujo sentido deve ser adaptado às necessidades cambiantes de cada tempo –,[29] em que os avanços tecnológicos demandam uma superação da doutrina da expectativa legítima associada a um local físico não mais indevassável, seja para buscar outros fundamentos que, reconhecendo a existência de ameaças provenientes dos setores público e privado – conforme se pretende demonstrar a seguir – proporcionem proteção satisfatória diante das demandas e riscos que se multiplicam diariamente.

3 A violação da vida privada praticada por agentes públicos e privados

O tratamento jurídico dado pelo ordenamento dos EUA aos direitos e liberdades fundamentais tende a concebê-los sob um ângulo estritamente *vertical*, ou

home is my castle,' measuring the heat inside the home is indeed a major violation of privacy. However, if one goes by the cyber age privacy doctrine here outlined, such readings rank very low on sensitivity because they reveal nothing about the resident's medical, financial, or political preferences, let alone their thoughts. In effect, they detect an extremely low bandwidth of information (the term 'bandwidth' here refers to a measurement of the number of different types of information collected). The information revealed is less consequential than what kind of cereal or which brand of coffee the person purchased".

[28] "Uma interpretação literal da Quarta Emenda não teria levado à livre escolha – o direito de uma pessoa controlar seus direitos reprodutivos que o Tribunal estava evoluindo em Griswold, Eisenstadt e Roe. Na Quarta Emenda, a privacidade é concebida como o direito de evitar legitimamente estar sujeito a escrutínio público, ser 'assistido' pelo governo – não o direito de controlar as ações em jogo, tomar decisões que conduzam os rumos de tal direito. Buscas tornam público o que foi mantido privado, no sentido de estar protegido contra a divulgação" (ETZIONI, Amitai. *The limits of privacy.* Nova York: Basic Books, 1999. p. 205, tradução nossa). No original: "A straightforward reliance on the Fourth Amendment would not have led to free choice – the right of a person to control her reproductive life that the Court was evolving in *Griswold, Eisenstadt* and Roe. In the Forth Amendment, privacy is conceived as the right legitimately to avoid being subject to public *scrutiny*, to being 'watched' by the government – not the right to *control* the action at stake, to make the driving decisions. Searchs make public what had been kept private, in the sense of being protected from disclosure".

[29] ETZIONI, Amitai. *How patriotic is the Patriot Act?* Nova York: Routledge, 2005. p. 5.

seja, como pretensões de defesa formuladas ante o Estado, tido como seu principal violador em potencial e não fornecendo resposta adequada para sua violação por parte de agentes privados.[30] Este posicionamento jurídico/doutrinário parte de uma mentalidade fortemente enraizada na cultura americana que encara com suspeitas o governo e enxerga no setor privado mais um promotor das liberdades que uma eventual ameaça a elas,[31] desta maneira negligenciando o papel desempenhado pelos agentes privados enquanto agressores efetivos de tais direitos. Tal equívoco é constatado na percepção do governo como o principal invasor da vida privada.[32]

Muito embora inegavelmente os governos possam violar os direitos individuais de privacidade de seus jurisdicionados e dos cidadãos de outros países (e frequentemente o façam, conforme se tornou notório com a exposição das práticas realizadas pelo governo americano, denunciadas por Eduard Snowden), valendo-se, para isso, do argumento da necessidade de salvaguardar a segurança nacional dos próprios jurisdicionados, é não menos verdade que a utilização de informações obtidas por agentes privados – muitas das vezes sem o conhecimento das pessoas a quem tais dados se referem – constitui um importantíssimo ativo econômico, capaz de estabelecer um perfil acerca de seus titulares, que pode ser utilizado para diversas finalidades, as quais incluem, até mesmo, sua alienação para entes governamentais, desejosos de instrumentos que permitam uma otimização de mecanismos de vigilância e controle comportamental.[33] Ademais,

[30] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 276.

[31] ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 162.

[32] "Embora nossa cultura cívica, políticas públicas e doutrinas legais estejam atentas à privacidade quando esta é violada pelo Estado, quando a privacidade é ameaçada pelo setor privado, nossa cultura, políticas e doutrinas oferecem uma defesa surpreendentemente fraca. Consumidores, funcionários, mesmo pacientes e crianças têm pouca proteção contra comerciantes, companhias de seguros, banqueiros e vigilância corporativa. Se a privacidade deve ser protegida contra intrusões comerciais, é necessário desenvolver uma nova abordagem" (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 10, tradução nossa). No original: "Although our civic culture, public policies and legal doctrines are attentive to privacy when it is violated by the state, when privacy is threatened by the private sector our culture, policies and doctrines provide a surprisingly weak defense. Consumers, employees, even patients and children have little protection from marketeers, insurance companies, bankers and corporate surveillance. If privacy is to be protected from commercial intrusions, a new approach needs to be developed".

[33] "No entanto, o governo pode e usa dados já acumulados pelos 'mercadores da privacidade' por sua própria iniciativa. Nem as leis prevalecentes impedem as empresas privadas de analisar a atividade online com o objetivo de atender às necessidades do governo e moldar suas violações de dados privados de forma a torná-los mais atraentes para os compradores do governo de seus serviços. Na verdade, porque o governo é um cliente tão grande e confiável, os bancos de dados corporativos têm um forte interesse financeiro em antecipar suas necessidades" (ETZIONI, Amitai. The privacy merchants: what's to be done? *U. Pa. J. Const. L.*, n. 14, 2011-2012. p. 935. Disponível em: http://heinonline.org/HOL/LandingPage?handle=hein.journals/upjcl14&div=30&id=&page=. Acesso em: 7 out. 2017, tradução nossa). No original: "However, the government can and does use data already amassed by Privacy Merchants for their own sake. Nor do prevailing laws prevent private corporations from analyzing online activity with an eye towards the government's needs and shaping their privacy-violating data in ways to

mesmo a utilização de tais dados para transações estritamente particulares é capaz de produzir consequências graves e discriminatórias.[34]

Tal quadro se agrava na medida em que os significativos avanços tecnológicos permitem, a um custo cada vez mais reduzido, coleta, armazenamento e processamento dos dados e metadados obtidos acerca de indivíduos, ou mesmo de populações inteiras (naquilo que se convencionou denominar "vigilância de massa"). Técnicas como *profiling*, *data shadowing* e *data mining* se tornaram eficientes mecanismos para a obtenção de perfis e dados.[35]

make them more attractive to government purchasers of their services. Indeed, because the government is such a large and reliable client, corporate databanks have a strong financial interest in anticipating its needs".

[34] "No entanto, deve-se notar que a violação da privacidade por agentes privados tem alguns efeitos semelhantes às violações cometidas por agentes do governo, efeitos que levam a discriminação e 'arrepio' da expressão e dissensão. Assim, quando as pessoas gays que procuram manter sua orientação sexual privada são 'expostas' pela mídia, ou quando bancos recusam empréstimos daqueles que descobrem câncer, ou os empregadores se recusam a contratar pessoas porque aprendem sobre suas opiniões políticas ou religiosas, a privacidade é violada de uma forma tão severa como se as mesmas violações tivessem sido realizadas por uma agência governamental" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 78-79, tradução nossa). No original: "However, one must note that the violation of privacy by private agents has some similar effects to violations committed by government agents, effects that lead to discrimination and 'chilling' of expression and dissent. Thus, when gay people who seek to keep their sexual orientation private are 'outed' by the media, or banks call in loans of those they find out have cancer, or employers refuse to hire people because they learn about their political or religious views, privacy is violated in a manner about as consequential as if the same violations had been carried out by a government agency".

[35] Esta verdadeira revolução, marcada pela transição "do papel para a nuvem" e pela ubiquidade da internet no cotidiano dos indivíduos é retratada nas palavras de Bruce Schneier: "Nem sempre foi assim. Na era dos jornais, do rádio, da televisão, recebíamos informações, mas nenhuma gravação do evento era criada. Agora, recebemos nossas novidades e entretenimento pela Internet. Costumávamos falar com as pessoas cara a cara e depois por telefone; agora temos conversas através de mensagens de texto ou e-mail. Costumávamos comprar coisas com dinheiro em uma loja; agora usamos cartões de crédito pela internet. Nós costumávamos pagar com moedas em um pedágio, metrô ou um medidor de estacionamento. Agora, usamos o sistema de pagamento automático, como o EZPass, que estão conectados ao número da nossa placa de carro, ou cartão de crédito. Os táxis costumavam ser pagos apenas em dinheiro. Em seguida, começamos a pagar com cartão de crédito. Agora, estamos usando nossos smartphones para acessar sistemas de taxi em rede como Uber e Lyft, que produzem registros de dados da transação, além de nossa localização. Com algumas exceções específicas, os computadores estão agora em todos os lugares que nos envolvemos no comércio e na maioria dos lugares nos envolvemos com nossos amigos" (SCHNEIER, Bruce. *Data and the Goliath*. The hidden battles to collect your data and control your world. Nova York: W. M. Norton, 2015. p. 15, tradução nossa). No original: "It wasn't always like this. In the era of newspapers, radio, television, we received information, but no record of the event was created. Now we get our news and entertainment over the Internet. We used to speak to people face-to-face and then by telephone; we now have conversations over text or e-mail. We used to buy things with cash at a store; now we use credit cards over the Internet. We used to pay with coins at a tollbooth, subway turnstile, or parking meter. Now we use automatic payment system, such as EZPass, that are connected to our license plate number or credit card. Taxis used to be cash only. Then we started paying by credit card. Now we're using our smartphones to access networked taxi systems like Uber and Lyft, which produce data records of the transaction, plus our pickup and drop-off locations. With a few specific exceptions, computers are now everywhere we engage in commerce and most places we engage with our friends".

Esta mudança implica igualmente uma variação dos danos causados pelos usos primários e secundários da informação, com um incremento substancial destes últimos.[36]

Em que pese esta constatação, a maioria dos casos relevantes submetidos ao crivo da Suprema Corte ainda lida em essência com o uso primário da informação, recaindo sobre aquilo que o autor denomina "coleta pontual".[37]

Um "efeito colateral" gerado pela prática de violações praticadas por empresas privadas é uma tentativa de minimizar a relevância da privacidade individual, ou entendê-la como um fato superado. Tal comportamento é fortemente estimulado por uma "cultura de exibicionismo", de "celebridades conhecidas por nada"[38] e hiperexposição, disseminada pelo maciço uso das denominadas redes sociais.[39]

[36] "O advento da era cibernética – também conhecida como a revolução digital – exige uma nova doutrina de privacidade. O motivo principal – embora não o único – para este requisito é que a proporção de violações de privacidade que resultam de usos secundários de informações pessoais em comparação com as que resultaram da coleção primária mudou radicalmente. A maioria das violações da privacidade na era do papel resultou da utilização primária. A maioria das violações na Era Digital resulta de usos secundários de informações legalmente coletadas. Se uma obtenção fosse considerada legal na era do papel, havia limites muito acentuados, pelo menos na prática, sobre os seus usos adicionais. Assim, o perigo de que a permissão sofresse um uso abusivo fosse relativamente limitado. Na era cibernética, os limites funcionais referentes ao abuso de dados são menores e os usos secundários proliferam" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 19, tradução nossa). No original: "The advent of the cyber age – also referred to as the digital revolution – requires a new privacy doctrine. The main – although not the only – reason for this requirement is that the proportion of privacy violations that result from secondary usages of personal information compared to those that result from primary collection has radically changed. Most privacy violations in the paper age resulted from primary collection; most violations in the cyber age result from secondary usages of information that has been legally collected. If a collection was deemed legal in the paper age, there were very sharp limits, at least in practice, on the additional uses of the information. Thus, the danger that permission would be abused was relatively limited. In the cyber age, functional limits on data abuse are fewer and secondary usages proliferate".

[37] No original, o autor utiliza o termo *spot collection*, para referir-se à obtenção de uma pequena quantidade de informação, referente a aspectos pontuais da conduta de uma pessoa, que não são armazenados, tampouco propagados para outras finalidades (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 20).

[38] LIPOVETSKY, Gilles; SERROY, Jean. *A cultura-mundo*. Resposta a uma sociedade desorientada. Tradução de Maria Lúcia Machado. São Paulo: Companhia das Letras, 2011. p. 85-86.

[39] "Do modo como eu vejo, é verdade que as normas de privacidade estão corroídas devido a fatores outros além do impulso corporativo em usar informações privadas para fins lucrativos, evidenciados por pessoas que participam de *talk shows* para revelar muito sobre si mesmas, o que é uma forma de exibicionismo. No entanto, não há dúvida de que as corporações, especialmente as novas mídias sociais, lideradas pelo Facebook, estão ajudando e incentivando e buscando legitimar a erosão da privacidade" (ETZIONI, Amitai. The privacy merchants: what's to be done? *U. Pa. J. Const. L.*, n. 14, 2011-2012. p. 938. Disponível em: http://heinonline.org/HOL/LandingPage?handle=hein.journals/upjcl14&div=30&id=&page=. Acesso em: 7 out. 2017, tradução nossa). No original: "As I see it, it is true that the privacy norms are eroding due to factors other than the corporate drive to use private information for profit-making, evidenced by people going on talk shows to reveal much about themselves, a form of exhibitionism. However, there can be little doubt that corporations, especially the new social media, led by Facebook, are aiding and abetting and seeking to legitimize the erosion of privacy".

Este padrão de comportamento generalizado e a forte massificação de uma cultura em rede apresentam-se como uma barganha injusta, na medida em que, em que pese a não obrigatoriedade de acesso à internet, esta se tornou onipresente no cotidiano das pessoas, de modo que evitar o acesso às suas facilidades e benefícios como forma de preservação da privacidade implicaria verdadeira marginalização.[40]

O que se percebe é que a privacidade se equilibra diante de duas ameaças constantes: de um lado, o Estado, cuja alegada necessidade de ampliação dos níveis de segurança tem servido como justificativa para inúmeros atentados à privacidade, com base "no discurso falacioso de que maior segurança exige menor privacidade".[41] [42] Esta advertência quanto aos riscos da adoção de um discurso potencialmente totalitário em nome de assegurar a segurança nacional/internacional está presente na obra de Stefano Rodotà.[43]

[40] Em sentido similar, Schneier: "Não é razoável dizer às pessoas que se elas não gostam da coleta de dados, não deveriam enviar *e-mail*, comprar *on-line*, usar o Facebook ou ter um telefone celular. Não consigo mais imaginar estudantes passando pela escola sem pesquisa na Internet na Wikipédia, muito menos encontrando um emprego depois. Estas são as ferramentas da vida moderna. Elas são necessárias para uma carreira e uma vida social. Excluir-se não é uma opção viável para a maioria de nós, na maioria das vezes; isso viola o que se tornaram normas muito reais da vida contemporânea" (SCHNEIER, Bruce. *Data and the Goliath*. The hidden battles to collect your data and control your world. Nova York: W. M. Norton, 2015. p. 60, tradução nossa). No original: "It's not reasonable to tell people that if they don't like the data collection, they shouldn't e-mail, shop online, use Facebook or have a cell phone. I can't imagine students getting through school anymore without Internet search on Wikipedia, much less finding a job afterwards. These are the tools of modern life. They're necessary to a career and a social life. Opting out just isn't a viable choice for most of us, most of the time; it violates what have become very real norms of contemporary life".

[41] SCHREIBER, Anderson. *Direitos da personalidade*. 3. ed. São Paulo: Atlas, 2014. p. 142.

[42] Esta falácia é reforçada por Maria Celina Bodin de Moraes, na apresentação da tradução brasileira da obra de Rodotà: "Menos privacidade, mais segurança" é uma receita falsa, avisa Stefano Rodotà. A propósito, ele recorre com frequência à metáfora do homem de vidro, de matriz nazista. A ideia do homem de vidro é totalitária porque sobre ela se baseia a pretensão do Estado de conhecer tudo, até os aspectos mais íntimos da vida dos cidadãos, transformando automaticamente em "suspeito" todo aquele que quiser salvaguardar sua vida privada. Ao argumento de que "quem não tem nada a esconder, nada deve temer", o autor não se cansa de admoestar que o emprego das tecnologias da informação coloca justamente o cidadão que nada tem a temer em uma situação de risco, de discriminação. "Menos cidadãos, mais suspeitos" é a expressão estigmatizante do momento (RODOTÀ, Stefano. *A vida na sociedade da vigilância*. Organização de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p. 8).

[43] "É justamente a necessidade de um uso social das tecnologias a exigir que sejam projetadas novas intuições da liberdade, capazes de evitar uma poluição totalitária da sociedade e de garantir a defesa dos direitos fundamentais em um ambiente caracterizado pelo recurso maciço às coletâneas de informações. Realmente, é preciso suspeitar do argumento de quem ressalta que o cidadão honesto nada tem a temer com a disseminação das informações que lhe dizem respeito: o 'homem de vidro' é uma metáfora totalitária, pois é nela que se baseia a pretensão do Estado de tudo saber, até mesmo os aspectos mais íntimos da vida do cidadão. É preciso também não se deixar fascinar por simplificações como a que surge nas primeiras páginas do livro 'The Transparent Society', onde se parte da descrição de uma comunidade urbana na qual cada espaço público é submetido ao controle de câmeras de vídeo, e ali se contrapõem dois modelos de organização social. O primeiro é fundado sobre o poder de um grupo restrito (por exemplo, a polícia) de usar essa tecnologia, tornando-se assim depositário exclusivo do controle sobre uma

Por outro ângulo, os agentes privados, conforme já ressaltado, apresentam-se como perpetradores de gravíssimas violações, quer à própria *privacy* em si, quer a outros direitos que possam ser afetados uma vez superada a proteção que esta lhes confere. Etzioni enxerga aí um paradoxo: ao mesmo tempo em que a cultura americana receie mais a ameaça proporcionada pelo governo que pelo mercado, é aquele que pode proporcionar algum nível de proteção contra os abusos deste.[44]

4 Os critérios da proteção de dados pessoais adotados pelos Estados Unidos em comparação com a sistemática da União Europeia

Existem substanciais diferenças entre os modelos adotados pelos Estados Unidos e pela União Europeia, no tocante ao tratamento de dados pessoais.

O modelo estadunidense é pautado na doutrina *third-party*, que essencialmente significa que, uma vez que um indivíduo tenha voluntariamente revelado alguma informação a seu respeito para outra pessoa, esta pessoa poderia comunicá-la ao agente público, sem que tal fato caracterizasse uma busca, nos moldes previstos pela Quarta Emenda, o que acarretaria a consequência prática (e particularmente grave) da desnecessidade de obtenção, por tal agente, de um mandado judicial que autorizasse tal busca. Etzioni aponta que esta doutrina foi adotada pela Suprema Corte em alguns casos envolvendo documentos financeiros, contatos telefônicos, ou mesmo conversas entre suspeitos de atos criminosos e informantes.[45]

comunidade inteira. No segundo grupo, no entanto, todos podem controlar todos, inclusive os agentes de polícia, operadores do sistema: a todos seria assim atribuído um idêntico poder de controle. Mas, à parte outras considerações, essa transparência total e generalizada conduzirá realmente a uma maior democracia ou, pelo contrário, não terá condições de eliminar o risco maior, ligado à possibilidade de conservar, cruzar e elaborar as diversas informações, e que permanece evidentemente reservada a um grupo restrito?" (RODOTÀ, Stefano. *A vida na sociedade da vigilância*. Organização de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p. 147-148).

[44] ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 10.

[45] "A Suprema Corte decidiu em Estados Unidos *v.* Miller e Smith *v.* Maryland que os registros comerciais, como documentos financeiros e registros de números de telefone discados, não estão protegidos contra a coleta não autorizada por agências policiais sob certas circunstâncias. O Tribunal também considerou que a execução legal da coleta do conteúdo das conversas entre suspeitos e terceiros informantes não é presumidamente inconstitucional, porque esses terceiros poderiam transmitir a informação à polícia, mesmo sem assistência tecnológica. Richard A. Epstein resume a doutrina de terceiros da seguinte forma: 'A sabedoria judicial recebida é que qualquer pessoa que opte por revelar informações a uma terceira pessoa perde necessariamente qualquer proteção que a Quarta Emenda lhe forneça'" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 21, tradução nossa). No original: "The Supreme Court ruled in United States v. Miller and Smith v. Maryland that business records such as financial documents and records of phone numbers dialed are not protected from warrantless collection

A adoção deste critério é potencialmente lesiva às liberdades individuais, especialmente tomando em consideração as modernas formas de interação, amplamente difundidas pelo uso de transações eletrônicas e pela quase onipresente utilização das denominadas "redes sociais" como ferramentas de comunicação e do armazenamento de dados em "nuvem", guardado por *third-parties*.[46] [47] Em tal contexto, o consenso implícito e presumido tende a debilitar sobremaneira a tutela da *privacy*.

Modelo alternativo à doutrina *third-party* é encontrado na União Europeia. O sistema europeu, estabelecido especialmente a partir da Diretiva 95/46, atrela a privacidade à tutela da personalidade humana, sendo concebida como um de seus atributos e, deste modo, implicando a necessidade de autorização expressa de seu titular para a divulgação de dados particulares a ele referentes. O documento

by law enforcement agencies under certain circumstances. The Court also held that law enforcement's collection of the content of conversations between suspects and third-party informants is not presumptively unconstitutional, because those third parties could pass along the information to the police even without technological assistance. Richard A. Epstein summarizes the third-party doctrine as follows: "The received judicial wisdom is that any person who chooses to reveal information to a third person necessarily forfeits whatever protection the Fourth Amendment provides him".

[46] SCHNEIER, Bruce. *Data and the Goliath*. The hidden battles to collect your data and control your world. Nova York: W. M. Norton, 2015. p. 68.

[47] "A doutrina *third-party* é particularmente problemática em uma era da tecnologia cibernética, porque terceiros podem compartilhar informações com outras pessoas e combiná-las com ainda mais informações, resultando em dossiês detalhados e íntimos de pessoas inocentes insuspeitas de crimes. Dado que cada vez mais informações sobre as pessoas estão nas mãos de terceiros, devido ao extenso número e alcance das transações e comunicações realizadas no ciberespaço e armazenadas na nuvem, se a doutrina externa for permitida, muito pouco impedirá o governo de invadir a privacidade dos cidadãos americanos. Os indivíduos constantemente deixam para trás um rastro de dados com cada clique de um mouse; 'Escape de dados' semelhante aos vapores deixados atrás de um carro. Will Thomas DeVries aponta que uma das principais características da 'revolução digital' para a privacidade é que 'toda interação com a Internet, todas as transações com cartão de crédito, cada retirada do banco, cada assinatura de revista é gravada digitalmente e ligada a indivíduos específicos. [...] [O] impacto da era digital é tão profundo e generalizado que a expansão de uma única área do direito à privacidade não é susceptível de resolver adequadamente os problemas. Uma vez que a Era Digital afeta todos os aspectos da privacidade, requer uma evolução não apenas no quadro existente, mas no status muito conceitual e legal da privacidade" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 21-22, tradução nossa). No original: "The third-party doctrine is particularly problematic in an age of cybernation, because third parties can share information with others and combine it with still more information, resulting in detailed and intimate dossiers of innocent people unsuspected of crimes. Given that more and more information about people is in the hands of third parties due to the extensive number and scope of transactions and communications carried out in cyberspace and stored in the cloud, if the third-party doctrine is allowed to stand, precious little will prevent the government from intruding on the privacy of American Citizens. Individuals constantly leave behind them a trail of data with every click of a mouse; 'data exhaust' akin to the vapors left behind a car. Will Thomas DeVries points out that one of the key characteristics of the 'digital revolution' for privacy is that 'every interaction with the Internet, every credit card transaction, every bank withdrawal, every magazine subscription is recorded digitally and linked to specific individuals. [...] [The] impact of the digital age is so deep and pervasive that expansion of a single area of privacy law is unlikely to adequately address the problems. Since the digital age affects every aspect of privacy, it requires an evolution not just in the existing framework, but in the very conceptual and legal status of privacy".

é o produto de uma tradição iniciada pela Convenção Europeia para os Direitos do Homem (1950) e pela Convenção para a Proteção de Indivíduos com Respeito ao Processamento Automatizado de Dados Pessoais, também conhecida como Convenção de Estrasburgo (1981). Doneda analisa que a diretiva se estrutura em torno de dois eixos centrais – a proteção da pessoa humana e a necessidade de livre circulação de pessoas, mercadorias e capitais –, ambos envolvendo o uso de dados e informações e usando a referência ao homem e seus direitos fundamentais como critério de equilíbrio.[48] Esta doutrina presume que a informação pessoal seja de titularidade da pessoa a quem se aplica, que tem o direito de mantê-la em reservado.[49]

A crítica apresentada por Etzioni à doutrina europeia reside no fato de que seu uso em termos estritos tornaria muito difícil a obtenção do consenso necessário para o uso da informação, o que poderia acarretar óbices ao bem comum. O autor constata que a existência de inúmeras exceções legais à necessidade de consenso do titular dos dados termina por mitigar sua proposta original, afetando sua aplicação. Outra dificuldade prática apontada refere-se à pouca compreensão dos termos jurídicos envolvidos, o que compromete a existência de um consenso real acerca do uso dos dados pessoais.[50]

[48] DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 237.

[49] "Presume que a informação pessoal pertence à pessoa a quem se aplica, que o indivíduo tem o direito de manter essa informação privada que se estende além da obtenção primária, e que somente a pessoa pode concordar com usos secundários da informação – mesmo quando já tenham concordou com a coleta primária. (Alguns se referem a esta doutrina como a abordagem dos direitos fundamentais, outros referem-se a ela como a informação como abordagem proprietária). Os europeus citam frequentemente esta doutrina, que está na base da Diretiva Europeia de Proteção de Dados e do Regulamento Geral de Proteção de Dados Europeu" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 22, tradução nossa). No original: "It assumes that personal information belongs to the person to whom it applies, that the individual has a right to keep this information private that extends beyond primary collection, and that only the person can agree to secondary usages of the information – even when they have already consented to primary collection. (Some refer to this doctrine as the fundamental rights approach; others refer to it as the information as property approach.) Europeans often cite this doctrine, which is at the foundation of the European Data Protection Directive and the European General Data Protection Regulation".

[50] "Os redatores da abordagem europeia, no entanto, perceberam que, se a União Europeia seguisse suas limitações em usos secundários, muitos bens comuns sofreriam em demasia. Eles, portanto, introduziram uma grande quantidade de áreas nas quais os usos secundários de informações pessoais não requerem o consentimento. De acordo com a abordagem europeia, o governo não precisa pedir o consentimento de pessoas cuja informação pessoal coleta e usa se a obtenção for para uma lista considerável de finalidades públicas, como saúde pública ou segurança. Assim, a Diretiva de Proteção de Dados exclui da exigência de que os 'controladores' adquiram o consentimento pessoal para registrar e processar informações pessoais em qualquer instância em que 'o processamento seja realizado no âmbito de um contrato ou no contexto de uma relação de confiança quase-contratual com a pessoa em causa e é necessário para a sua descarga, 'quando' os dados provêm de fontes geralmente disponíveis para o público e seu processamento é destinado exclusivamente para fins de correspondência, 'e quando' o controlador do arquivo está buscando um interesse legítimo, na condição de o interesse do titular dos dados não prevaleça'. De acordo com Joris van Hoboken 'as exceções se tornaram a regra, o que significa que o significado do direito fundamental,

Recentemente, a Diretiva 95/46 foi revogada pelo Regulamento 2016/679.[51] Este, considerando a insuficiência da diretiva para a proteção concreta dos dados pessoais,[52] reconhece sua proteção como um direito fundamental da pessoa,[53] devendo, contudo, ser ponderado quando em colisão com outros direitos fundamentais.[54] O tratamento dos dados pessoais segue tendo como base de validade

mesmo que alguém deseje proteger mais categoricamente determinado núcleo interesses, é corroído'. Além disso, a abordagem europeia sobrevive apenas porque é aplicada com pouca frequência. E as declarações de privacidade fornecidas por empresas e outros agentes que dependem da coleta de dados do consumidor são frequentemente extensas e se baseiam na terminologia jurídica, tornando-os incompreensíveis para a maioria dos usuários. O consentimento significa pouco se aqueles que o dão não podem entender o que estão permitindo. Em suma, a abordagem europeia parece não fornecer uma base sólida para lidar com usos secundários. Em outras palavras, dificilmente soa como uma abordagem plausível" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 22-23, tradução nossa). No original: "The drafters of the European approach, however, realized that if the European Union were to follow its limitations on secondary usages, many common goods would suffer greatly. They hence introduced a large number of areas in which secondary usages of personal information do not require consent. According to the European approach, the government need not ask the consent of those whose personal information it collects and uses if the collection is for a considerable list of public purposes, such as public health or security. Thus, the Data Protection Directive excludes from its requirement that 'controllers' gain personal consent to record and process personal information in any instance in which 'the processing is carried out under a contract, or in the context of a quasi-contractual relationship of trust, with the data subject and is necessary for its discharge,' when 'the data come from sources generally available to the public and their processing is intended solely for correspondence purposes,' and when 'the controller of the file is pursuing a legitimate interest, on condition that the interest of the data subject does not prevail.' According to Joris van Hoboken, 'The exceptions have to become the rule, which means that the meaning of the fundamental right, even if one would want to more categorically protect certain core interests, is eroded.' Moreover, the European approach survives only because it is infrequently enforced. And privacy statements provided by businesses and other agents that rely on the collection of consumer data are frequently extensive and draw on legal terminology, making them incomprehensible to most users. Consent means little if those who give it cannot possibly understand what they are allowing. In short, the European approach seems not to provide a sound foundation for dealing with secondary usages. In other words, it is hardly a sound approach".

[51] Art. 94º, 1. "A Diretiva 95/46/CE é revogada com efeitos a partir de 25 de maio de 2018".

[52] Considerando (9): "Os objetivos e os princípios da Diretiva 95/46/CE continuam a ser válidos, mas não evitaram a fragmentação da aplicação da proteção dos dados ao nível da União, nem a insegurança jurídica ou o sentimento generalizado da opinião pública de que subsistem riscos significativos para a proteção das pessoas singulares, nomeadamente no que diz respeito às atividades por via eletrónica. As diferenças no nível de proteção dos direitos e das pessoas singulares, nomeadamente do direito à proteção dos dados pessoais no contexto do tratamento desses dados nos Estados-Membros, podem impedir a livre circulação de dados pessoais na União. Essas diferenças podem, por conseguinte, constituir um obstáculo ao exercício das atividades económicas a nível da União, distorcer a concorrência e impedir as autoridades de cumprirem as obrigações que lhes incumbem por força do direito da União. Essas diferenças entre os níveis de proteção devem-se à existência de disparidades na execução e aplicação da Diretiva 95/46/CE".

[53] Considerando (1): "A proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental. O artigo 8º, nº 1, da Carta dos Direitos Fundamentais da União Europeia («Carta») e o artigo 16º, nº 1, do Tratado sobre o Funcionamento da União Europeia (TFUE) estabelecem que todas as pessoas têm direito à proteção dos dados de caráter pessoal que lhes digam respeito".

[54] Considerando (4): "O tratamento dos dados pessoais deverá ser concebido para servir as pessoas. O direito à proteção de dados pessoais não é absoluto; deve ser considerado em relação à sua função na sociedade e ser equilibrado com outros direitos fundamentais, em conformidade com o princípio da proporcionalidade. O presente regulamento respeita todos os direitos fundamentais e observa as liberdades e os princípios reconhecidos na Carta, consagrados nos Tratados, nomeadamente o respeito pela vida privada e familiar, pelo domicílio e pelas comunicações, a proteção dos dados pessoais, a liberdade de pensamento, de consciência e de religião, a liberdade de expressão e de informação, a liberdade de empresa, o direito à ação e a um tribunal imparcial, e a diversidade cultural, religiosa e linguística".

o consentimento de seu titular,[55] sendo pautado pelos princípios da transparência, licitude e lealdade,[56] admitidas exceções legalmente previstas.[57] [58]

Ambas as abordagens são criticáveis na visão de Etzioni, na medida em que a primeira "deixa pouco espaço para a privacidade", ao passo que a segunda compromete o bem comum.[59] Desta forma, o autor propõe um critério que será discutido a seguir.

5 O balanceamento entre os interesses individuais e o bem comum no pensamento comunitarista liberal

A vertente comunitarista sustentada por Etzioni é representativa daquilo que se convencionou denominar comunitarismo liberal, ou comunitarismo responsivo.

[55] Art. 7º: "1. Quando o tratamento for realizado com base no consentimento, o responsável pelo tratamento deve poder demonstrar que o titular dos dados deu o seu consentimento para o tratamento dos seus dados pessoais. 2. Se o consentimento do titular dos dados for dado no contexto de uma declaração escrita que diga também respeito a outros assuntos, o pedido de consentimento deve ser apresentado de uma forma que o distinga claramente desses outros assuntos de modo inteligível e de fácil acesso e numa linguagem clara e simples. Não é vinculativa qualquer parte dessa declaração que constitua violação do presente regulamento. 3. O titular dos dados tem o direito de retirar o seu consentimento a qualquer momento. A retirada do consentimento não compromete a licitude do tratamento efetuado com base no consentimento previamente dado. Antes de dar o seu consentimento, o titular dos dados é informado desse facto. O consentimento deve ser tão fácil de retirar quanto de dar. 4. Ao avaliar se o consentimento é dado livremente, há que verificar com a máxima atenção se, designadamente, a execução de um contrato, inclusive a prestação de um serviço, está subordinada ao consentimento para o tratamento de dados pessoais que não é necessário para a execução desse contrato".

[56] Art. 5º, 1. a).

[57] Considerando (40): "Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento da titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro 4.5.2016 PT Jornal Oficial da União Europeia L 119/7 ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar".

[58] Art. 6º: "1. O tratamento só é lícito se e na medida em que se verifique pelo menos uma das seguintes situações: a) O titular dos dados tiver dado o seu consentimento para o tratamento dos seus dados pessoais para uma ou mais finalidades específicas; b) O tratamento for necessário para a execução de um contrato no qual o titular dos dados é parte, ou para diligências pré-contratuais a pedido do titular dos dados; c) O tratamento for necessário para o cumprimento de uma obrigação jurídica a que o responsável pelo tratamento esteja sujeito; d) O tratamento for necessário para a defesa de interesses vitais do titular dos dados ou de outra pessoa singular; e) O tratamento for necessário ao exercício de funções de interesse público ou ao exercício da autoridade pública de que está investido o responsável pelo tratamento; f) O tratamento for necessário para efeito dos interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros, exceto se prevalecerem os interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for uma criança. O primeiro parágrafo, alínea f), não se aplica ao tratamento de dados efetuado por autoridades públicas na prossecução das suas atribuições por via eletrônica".

[59] ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 23. Em que pese a crítica do autor, no tocante ao sistema europeu de proteção de dados, ser pautada na Diretiva 95/46, então vigente, parece aplicável ao regulamento atualmente em vigor.

A base deste pensamento reside na necessidade de se estabelecer mecanismos equilibradores das tensões existentes entre direitos individuais e responsabilidades sociais, entre as liberdades de cada pessoa e o bem comum.[60] Por "bem comum" se entendem as preocupações compartilhadas de dada sociedade em dado tempo acerca de assuntos de interesse global (ou, ao menos, de amplo alcance). Naturalmente, a noção de bem comum é cambiante no tempo e suscetível a particularidades regionais. Contudo, sua ideia é algo intuitiva (embora o que efetivamente a represente em um contexto específico possa não o ser). O autor aponta que, em função da ausência de mecanismos espontâneos, há uma tendência de as sociedades oscilarem entre estabelecer maiores restrições em nome do interesse público ou o flexibilizarem em demasia, de modo a ampliar a tutela dos direitos individuais. Tais oscilações, contudo, podem ser contornadas e reequilibradas mediante o recurso a mecanismos democráticos.[61] O comunitarismo liberal surge então como uma vertente alternativa ao pensamento liberal puro e ao comunitarismo oriental.[62]

Partindo desta premissa, e considerando que o direito à privacidade se encontra frequentemente em colisão com interesses associados ao bem comum (como segurança nacional ou saúde pública), o autor propõe quatro critérios que, em uma análise combinada, permitem avaliar se eventual restrição ao referido direito em nome de um alegado interesse público se encontraria justificada.

O primeiro destes critérios afirma que qualquer restrição à privacidade deva fundar-se em uma ameaça bem documentada[63] e que constitua num risco em

[60] ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 5.

[61] ETZIONI, Amitai. *How patriotic is the Patriot Act?* Nova York: Routledge, 2005. p. 5.

[62] "Em contraste com a aplicação desta abordagem de equilíbrio, os libertários, libertários civis e um número razoável de liberais contemporâneos tendem a enfatizar os direitos individuais e a autonomia sobre as considerações do bem comum. No extremo oposto do espectro estão os comunitaristas autoritários (principalmente na Ásia Oriental) que privilegiam o bem comum *a priori* e somente dão atenção aos direitos na medida em que sirvam aos objetivos dos governantes. Nesse sentido, o comunitarismo liberal ocupa o meio do espectro entre o liberalismo e o autoritarismo e se pauta principalmente em pressões sociais mais do que em coerção estatal" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 124, tradução nossa). No original: "In contrast to applying this balancing approach, libertarians, civil libertarians, and a fair number of contemporary liberals tend to emphasize individual rights and autonomy over considerations of the common good. At the opposite end of the spectrum are authoritarian communitarians (mainly in East Asia) who privilege the common good a priori and pay mind to rights mainly to the extent that they serve the rulers' aims. In this sense, liberal communitarianism occupies the middle of the spectrum between libertarianism and authoritarianism, and draws mainly on social pressures rather than state coercion".

[63] "Os formuladores de políticas e o público em geral são bombardeados com terríveis advertências de que a sociedade está prestes a enfrentar esse ou aquele perigo tão grave (por exemplo, bactérias carnívoras, supergripe aviária, doenças cerebrais cortesia de vacas loucas, buracos abertos na camada de ozônio, El Niño, a extinção do peixe-espada) que proporciona um fundamento para a redução da privacidade e outros direitos individuais. Se uma sociedade devesse responder a cada advertência por meio da limitação dos direitos, eles iriam se erodir rapidamente, muitas vezes sem servir nenhum verdadeiro bem comum" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 124, tradução nossa). No original: Policymakers and the general public are bombarded with dire warnings that society is about to

larga escala ao bem comum – não apenas uma situação puramente hipotética, ou que represente risco a uma coletividade pouco expressiva.[64] [65]

O segundo critério propõe que a reação a um perigo significativo e tangível deve priorizar mecanismos que alcancem tal finalidade sem implicar novas – ou maiores – restrições à privacidade.[66]

Em terceiro lugar, caso se façam necessárias medidas restritivas do direito à privacidade, estas devem ser tão minimamente intrusivas quanto possível.[67] [68]

face this or that danger that is so grave (e.g., flesh-eating bacteria, chicken-derived super-flu, brain disease courtesy of mad cows, gaping holes in the ozone layer, El Niño, the extinction of swordfish) that it provides ground for curtailment of privacy and other individual rights. If a society were to respond to every such warning by curbing rights, they would erode rapidly, often without serving any true common-good".

64 "Antes de limitar a privacidade, uma sociedade comunitária bem equilibrada primeiro determina o quão bem documentados são os vários perigos relatados para o bem comum e quão abrangentes serão suas consequências esperadas. Quando milhares de vidas são perdidas e muitos milhões de outras estão em risco, como com o HIV, enfrentamos uma ameaça clara e importante. Os efeitos de abusar da maconha são reais, mas de uma magnitude muito menor, e, portanto, não justificam o mesmo tipo de resposta. Ainda outros perigos são altamente hipotéticos e, portanto, geralmente não merecem ação pública" (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 12, tradução nossa). No original: "Before limiting privacy, a well-balanced, communitarian Society first determines how well documented various reported dangers to the common good are and how encompassing their expected consequences will be. When many thousands of lives are lost and many millions more are at risk, as with HIV, we face a clear and major threat. The effects of abusing marijuana are real but of a much lower magnitude, and hence do not justify the same kind of response. Still other dangers are highly hypothetical and hence usually do not merit public action".

65 De destacar-se, contudo, que o próprio autor sustenta que algumas situações pouco prováveis, porém que – uma vez eventualmente consumadas – acarretariam danos de larga escala (como um ataque terrorista utilizando resíduos nucleares) justificariam a adoção de algumas medidas restritivas da privacidade (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 12).

66 "Por exemplo, isso pode ser alcançado removendo informações de identificação pessoal (tais como nomes, endereços e números da Segurança Social) quando os pesquisadores precisam de registros médicos, o que possibilitaria o acesso a dados anteriormente inacessíveis (por exemplo, banco de dados do Medicare). Várias dificuldades técnicas surgem para assegurar o anonimato dos dados. Várias sugestões ingênuas foram feitas para lidar com esse desafio. Por outro lado, se a necessidade de privacidade for premente, deve-se buscar formas de proceder, como a introdução de trilhas de auditoria, que não imponham 'perdas' ao bem comum" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 6-7, tradução nossa). No original: "For instance, this can be achieved by removing personally identifying information (e.g., names, addresses and Social Security numbers) when researchers need medical records, which would make it possible to allow access to previously inaccessible data (e.g., Medicare databanks). Various technical difficulties arise in securing the anonymity of the data. Several ingenious suggestions have been made to cope with this challenge. Conversely, if privacy needs shoring up, one should look for ways to proceed, such as introducing audit trails, that impose no 'losses' to the common good".

67 "Por exemplo, muitos concordam que os testes de drogas devem ser realizados sobre aqueles, como motoristas de ônibus escolares, diretamente responsáveis pela vida de outros. Alguns empregadores, no entanto, recorrem a uma vigilância visual altamente intrusiva para garantir que a amostra seja retirada da pessoa que a entrega. Em vez disso, pode-se confiar no procedimento muito menos intrusivo de medir a temperatura da amostra imediatamente após a entrega" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 7, tradução nossa). No original: "For example, many agree that drug tests should be conducted on those, such as school bus drivers, directly responsible for the lives of others. Some employers, however, resort to highly intrusive visual surveillance to ensure that the sample is taken from the person who delivers it. Instead, one can rely on the much less intrusive procedure of measuring the temperature of the sample immediately upon delivery".

68 Em outra passagem, o autor refere-se ainda ao caso do uso de arquivos que contenham dados acerca de má conduta médica para a contratação de profissionais por outros hospitais: "O princípio de limitar o

Por fim, devem ser preferíveis medidas que minimizem – ou, se possível, revertam – efeitos colaterais indesejados.[69]

A adoção de tais critérios permitiria fornecer parâmetros seguros que indicassem quais medidas restritivas seriam adequadas e razoáveis a alcançar a finalidade de ponderação, e quais se demonstrariam insuficientes ou excessivas.

6 Uma proposta conceitual de privacidade e alguns desafios impostos pela era digital

As complexidades produzidas pela era digital tornam insuficiente a concepção de *privacy* adotada pelo clássico estudo de Warren e Brandeis. O *right to be left alone* passa a não mais responder de forma plena às demandas atuais. Embora advirta para a inexistência de um conceito de privacidade amplamente aceito pelo pensamento comunitarista, Etzioni sugere que essa seja encarada

uso de medidas intrusivas de restrição da privacidade é ilustrado pelo exemplo de um banco de dados nacional que contenha os nomes dos médicos que foram processados, sancionados ou penalizados por crimes, má conduta ou incompetência. O *National Practitioner Data Bank* permite que os hospitais que estejam considerando se concedem 'privilégios' (o direito de atuar no hospital) a um médico que realizem verificações limitadas de antecedentes sobre ele ou ela. No entanto, o banco de dados revela apenas que um médico foi sujeito a um litígio de negligência ou parte de um acordo extrajudicial ou ação adversa (o que pode incluir revogação de licença para praticar ou remoção de privilégios, por atos como abuso de substâncias), mas deixa de fornecer detalhes da violação. Porque é sabido que, em regra, os médicos são desfilhados apenas por violações graves, sendo esta informação suficiente para hospitais que procuram proteger o público" (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 13, tradução nossa). No original: "The principle of limiting the intrusiveness of privacy-curbing measures is further illustrated by the example of a national database that contains the names of medical practitioners who have been sued, sanctioned, or otherwise penalized for crimes, misconduct, or incompetence. The National Practitioner Data Bank allow hospitals that are considering whether to grant 'privileges' (the right to practice in the hospital) to a physician to conduct limited background checks on him or her. However, the data bank discloses only that a physician has been subject to malpractice litigation or has been a party to an out-of-court settlement or adverse action (which might include revocation of license to practice or removal of privileges, for acts such as substance abuse), but it stops short of providing details of the violation. Because it is known that, as a rule, physicians are disaffiliated only for major violations, this information suffices for hospitals who seek to protect the public".

[69] "Assim, se o rastreamento de contatos for considerado necessário para combater a disseminação de doenças infecciosas, a fim de proteger a saúde pública, devem ser feitos esforços para proteger o anonimato dos envolvidos. Um terceiro pode informar aqueles que estavam em contato com um indivíduo infectado e as medidas terapêuticas e de proteção que deveriam ser tomadas depois sem divulgar a identidade da pessoa diagnosticada" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 7, tradução nossa). No original: "Thus, if contact tracing is deemed necessary to fight the spread of infectious diseases in order to protect public health, efforts must be made to protect the anonymity of those involved. A third party may inform those who were in contact with an affected individual about such exposure and the therapeutic and protective measures they ought to next undertake without disclosing the identity of the diagnosed person".

como uma "licença social", que permite a seu titular evadir-se legitimamente da curiosidade pública e do escrutínio governamental.[70]

A era digital, contudo, impõe que uma definição de privacidade envolva critérios para o tratamento de dados e informações coletados acerca de uma pessoa, considerando aspectos de sua vida *off-line* (termo preferível à expressão "vida real", que desconsidera o crescente – e quase onipresente – papel desempenhado pela internet na vida contemporânea) e virtual.[71]

Neste sentido, em trabalho mais recente, Etzioni descreve a privacidade como um cubo tridimensional, cujas dimensões envolveriam os dados sensíveis, o volume de dados coletados e a "cybernacionalização".[72]

O primeiro aspecto desta figura seria a sensibilidade dos dados obtidos. Stefano Rodotà assim denomina aqueles referentes a informações as quais, uma vez reveladas, possuiriam significativo potencial discriminatório.[73] Doneda observa que a proteção a tais dados extrapola os aspectos tradicionais de proteção à privacidade, para tomar em conta a necessidade de garantir igualdade material.[74] A inclusão de determinados dados em uma categoria de "sensíveis" – a justificar uma maior cautela em sua coleta e tratamento em relação a outros dados excluídos desta classificação – envolve uma análise valorativa, que suscita algumas dificuldades. Inicialmente, há que se indagar se tais dados devem ser tomados em conta com base na ótica do titular do direito, ou sob o prisma de valores culturais dominantes em dado contexto social e histórico.[75] Neste sentido, o autor menciona a regulamentação existente no ordenamento dos Estados Unidos, estabelecendo algumas categorias de dados como particularmente merecedoras de tratamento mais zeloso.[76]

---

70 "Eu sugiro que um tratamento comunitário sólido da vida privada é o domínio em que um agente (uma pessoa ou grupo, como um casal) pode legitimamente agir sem divulgação e responsabilidade para com os outros. A privacidade, portanto, é uma licença social que isenta uma categoria de atos (incluindo pensamentos e emoções) do escrutínio comunal, público e governamental" (ETZIONI, Amitai. *The limits of privacy*. Nova York: Basic Books, 1999. p. 196, tradução nossa). No original: "I suggest that a sound communitarian treatment of privacy views it as the realm in which an actor (either a person or group, such as a couple) can legitimately act without disclosure and accountability to others. Privacy thus is a societal license that exempts a category of acts (including thoughts and emotions) from communal, public and governmental scrutiny".

71 ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 40.

72 O termo usado pelo autor no texto original é o neologismo *cybernation*.

73 RODOTÀ, Stefano. *A vida na sociedade da vigilância*. Organização de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p. 119.

74 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 161.

75 ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 7-8.

76 "Os especialistas em matéria de privacidade e os legisladores muitas vezes articularam e operacionalizaram a observação de que alguns tipos de informações são mais sensíveis do que outros, embora usando uma variedade de termos, que incluem 'informações íntimas' e 'informações reveladoras'. Nos Estados Unidos, o Congresso classificou muitos tipos de informação de acordo com a sensibilidade. As informações

Rodotà acrescenta aí alguns dados tradicionalmente reputados como sensíveis, outros como as opções política e religiosa os quais, em que pese se destinarem ao conhecimento da comunidade e à própria formação de uma identidade política, podem, uma vez armazenados e utilizados indevidamente, produzir efeitos nocivos à pessoa a quem se referem. Esta perspectiva algo difere da noção americana na medida em que implica o reconhecimento de que mesmo algumas informações destinadas a se tornarem públicas necessitam receber tratamento diferenciado.[77]

A ideia de adjetivar determinados dados como "sensíveis" remete à teoria das esferas, de origem germânica, que estabelece distintos níveis de proteção à vida privada.[78]

médicas de um indivíduo recebem um alto nível de proteção. A informação financeira não é considerada sensível, embora próxima disto. Os tipos adicionais de informações com direito a um nível relativamente alto de proteção incluem registros de educação (Direitos de Educação Familiar e Lei de Privacidade), informações genéticas (vinte e sete legislaturas estaduais regulamentaram a divulgação de informações genéticas identificáveis de alguma forma a partir de 2008) e fontes jornalísticas (*Privacy Protection Act* de 1980). A FTC classificou cinco categorias de informações, nomeadamente informações financeiras, informações de saúde, números de segurança social, informações coletadas de crianças e informações de geolocalização, como dados confidenciais. O resultado dessa consideração fragmentada é uma louca colcha de retalhos. No entanto, dado que muitos tipos de informação já foram classificados, não levaria uma grande quantidade de leis para classificar sistematicamente o nível de sensibilidade de todos os principais tipos de informação" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 71, tradução nossa). No original: "Privacy scholars and lawmakers have often articulated and operationalized the observation that some kinds of information are more sensitive than others, albeit using a variety of terms including 'intimate information' and 'revealing information.' In the United States, Congress has ranked many types of information according to sensitivity. An individual's medical information is granted a high level of protection; financial information is not regarded as sensitive but nearly so. Additional types of information entitled to a relatively high level of protection include education records (Family Educational Rights and Privacy Act), genetic information (twenty-seven state legislatures had regulated the disclosure of identifiable genetic information in some way as of 2008), and journalistic sources (Privacy Protection Act of 1980). The FTC has classified five categories of information, namely financial information, health information, social security numbers, information collected from children, and geo-location information, as sensitive data. The result of this piecemeal consideration is a crazy patchwork quilt. However, given that many kinds of information have already been ranked, it would not take a great deal of legislation to systematically rank the level of sensitivity of all the major kinds of information".

77 "A necessidade de intimidade dilatou-se para muito além das informações relacionadas à esfera íntima da pessoa, constituída esta pelos dados que o indivíduo quer ver excluídos de qualquer tipo de circulação. Do exame dos textos relevantes nessa matéria, percebe-se claramente que o 'núcleo duro' da privacidade é ainda hoje constituído por informações que refletem a tradicional necessidade de sigilo (por exemplo, aquelas relacionadas à saúde ou aos hábitos sexuais): internamente, porém, assumiram cada vez maior relevância outras categorias de informações, protegidas sobretudo para evitar que pela sua circulação possam nascer situações de discriminação com danos os interessados. Trata-se, em especial, de informações relacionadas às opiniões políticas e sindicais, além daquelas relativas ao credo religioso. Ora, a particularidade dessa situação decorre do fato de que as opiniões políticas e sindicais não podem ser confinadas somente na esfera 'privada': pelo menos nos estados democráticos elas são destinadas a caracterizar a esfera 'pública', fazem parte das convicções que o indivíduo deve poder manifestar 'em público', contribuem a determinar a sua identidade 'pública'" (RODOTÀ, Stefano. *A vida na sociedade da vigilância*. Organização de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008. p. 95-96).

78 "O primeiro círculo, de maior amplitude, representa a esfera privada – Privatsphäre ou sphere of privacy dos norte-americanos – excluindo-se do conhecimento de terceiros aspectos específicos da vida da pessoa. O

Contudo, o prestígio desta teoria pode restar algo comprometido na medida em que mesmo pequenos fragmentos de informação, quando obtidos em volume substancial de fontes distintas podem, uma vez cruzados, causar lesões substanciais à privacidade.[79] Desta forma, o perigo não teria origem numa qualificação do dado em si, mas do uso que se faz dele.[80] Daí o surgimento de uma concepção da privacidade como um mosaico, em que os dados e metadados são tomados em consideração pelo potencial lesivo que representam quando analisados de forma global. Esta nuance cresce em importância na medida em que os avanços tecnológicos permitem a captura, o processamento e a utilização dos dados (para fins públicos e privados) em níveis até então inimagináveis. Bruce Schneier[81] chama a atenção para a questão da *correlação* dos dados, permitindo inferências produzidas a partir da combinação deles, e mesmo a possibilidade de predição de determinados comportamentos futuros.[82]

A segunda dimensão da privacidade vislumbrada por Etzioni refere-se ao volume de dados obtidos.[83] Trata-se de uma preocupação *a priori* quantitativa, mas

segundo – Intimsphäre – compreende os valores atinentes ao âmbito da intimidade ou esfera confidencial, cujo acesso é mais restrito, somente permitindo àqueles indivíduos com os quais a relação pessoal se desenvolve de forma mais intensa. O terceiro e mais fechado dos círculos – Geheimsphäre – abrange a reserva, o sigilo, o segredo, as mais profundas manifestações espirituais da pessoa, caracterizadoras da vida íntima stricto sensu" (VIEIRA, Tatiana Malta. *O direito à privacidade na sociedade da informação*: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. Porto Alegre: Sérgio Antônio Fabris. 2007. p. 37).

79 DANTAS, Fernanda Lages Alves. *O paradoxo do direito à privacidade e sua operacionalização*. Rio de Janeiro: Lumen Juris, 2016. p. 33.

80 DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 162.

81 SCHNEIER, Bruce. *Data and the Goliath*. The hidden battles to collect your data and control your world. Nova York: W. M. Norton, 2015. p. 40.

82 "Uma vez que você possa correlacionar diferentes conjuntos de dados, há muito o que você pode fazer com eles. Imagine construir uma imagem da saúde de alguém sem nunca olhar para seus registros de paciente. Os registros de cartões de crédito e os cartões de afinidade dos supermercados revelam o alimento e o álcool que ele compra, os restaurantes em que ele come, se ele frequenta uma academia e quais itens sem receita que ele compra em uma farmácia. Seus telefones revelam com que frequência ele vai àquela academia, e seu rastreador de atividades revela seu nível de atividade quando ele está lá. Os dados dos sites revelam quais termos médicos ele pesquisou. É assim que uma empresa como a ExactData pode vender listas de pessoas que namoram online, apostadores e pessoas que sofrem de ansiedade, incontinência ou disfunção erétil" (SCHNEIER, Bruce. *Data and the Goliath*. The hidden battles to collect your data and control your world. Nova York: W. M. Norton, 2015. p. 72-73, tradução nossa). No original: "Once you can correlate different data sets, there is a lot you can do with them. Imagine building up a picture of someone's health without ever looking at his patient records. Credit card records and supermarket affinity cards reveal what food and alcohol he buys, which restaurants he eats at, whether he has a gym membership, and what nonprescription items he buys at a pharmacy. His phones reveals how often he goes to that gym, and his activity tracker reveals his activity level when he' there. Data from websites reveals what medical terms he's searched on. This is how a company like ExactData can sell lists of people who date online, people who gamble, and people who suffers from anxiety, incontinence, or erectile disfunction".

83 "'Volume' refere-se à quantidade total de informações coletadas sobre uma pessoa por uma agência ou ator privado. O volume reflete a extensão em que o tempo de vigilância é aplicado (a questão levantada em Jones), a quantidade de informações coletadas em cada ponto (por exemplo, apenas os e-mails enviados

que se revela substancialmente perigosa na medida em que a capacidade de captação/armazenamento de dados tem crescido substancialmente, a um custo tendencialmente decrescente,[84] o que estimula a obtenção do máximo volume de informações, para uma análise *a posteriori*.[85] A junção desta capacidade de coleta/armazenamento permite a já mencionada correlação de dados, o que torna possível vaticinar que esta dimensão da privacidade possa mesmo superar em importância o aspecto qualitativo da sensibilidade dos dados.

A terceira e última dimensão da privacidade (à qual o autor atribui especial relevância) foi denominada *cybernacionalização*. O neologismo opõe-se à coleta pontual de dados,[86] utilizados de forma específica e limitada. A *cybernacionalização*, por sua vez, envolve um amplo espectro de coleta, armazenamento, análise e difusão.[87]

O autor refere-se ainda a um quarto fator que, sem representar efetivamente uma dimensão da privacidade, estaria ligado à *cybernacionalização*, atuando como seu componente limitador. Trata-se do que denominou *responsabilização*.[88] [89]

para uma pessoa específica ou todos os e-mails armazenados em um disco rígido?), e a largura de banda da informação coletada em qualquer momento (por exemplo, apenas os endereços de *e-mail* enviados ou também o conteúdo deles?). Uma única parcela de dados merece menor proteção e um alto volume de informações deve receber o máximo" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 10, tradução nossa). No original: "'Volume' refers to the total amount of information collected about one person by one agency or actor. Volume reflects the extent of time surveillance is applied (the issue raised in Jones), the amount of information collected at each point in time (e.g., only e-mails sent to a specific person or all e-mails stored on a hard drive?), and the bandwidth of information collected at any one point in time (e.g., only the addresses of e-mail sent or also their content?). A single piece of data deserves the least protection and a high volume of information should receive the most".

84 SCHNEIER, Bruce. *Data and the Goliath*. The hidden battles to collect your data and control your world. Nova York: W. M. Norton, 2015. p. 18.

85 SCHNEIER, Bruce. *Data and the Goliath*. The hidden battles to collect your data and control your world. Nova York: W. M. Norton, 2015. p. 56.

86 No original: *spot collection*.

87 "Ambos os sistemas são baseados na coleta pontual, ou seja, na coleta de informações que pertencem a um evento ou a um ponto específico muito limitado e que tipicamente são de pouca importância em si mesmas – como no caso do primeiro estado. No entanto, se essa informação é armazenada, combinada com outras informações, analisada e distribuída – ou seja, se essa informação for cibernacionalizada – conforme descrito no segundo cenário, fornece um perfil muito abrangente e revelador de sua vida pessoal. Em suma, as violações mais graves da privacidade são muitas vezes perpetuadas não por coleta de vigilância ou informação por si só, mas por combinação, manipulação e compartilhamento de dados – pela cibernética. Quanto mais informações for cibernacionalizada, mais intrusiva se torna" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 12, tradução nossa). No original: "Both systems are based on spot collection, that is, the collection of pieces of information that pertain to a very limited, specific event or point in time and that typically are of little significance in and of themselves – as in the case in the first state. However, if such information is stored, combined with other information, analyzed, and distributed – that is, if such information is cybernated – as depicted in the second scenario, it provides a very comprehensive and revealing profile of one's personal life. In short, the most serious violations of privacy are often perpetuated not by surveillance or information collection per se, but by combination, manipulation, and data sharing – by cybernation. The more information is cybernated, the more intrusive it becomes".

88 No original: *accountability*.

89 A relevância da responsabilização é explicitada na seguinte passagem: "Todas as medidas de responsabilização limitam um elemento ou outro de cybernacionalização. Algumas afetam os limites de compartilhamento,

A presença destas três dimensões comporia um conceito adequado a amoldar-se às necessidades atuais, além do que sua combinação é capaz de fornecer critérios mais seguros para atender à necessidade de preservar a privacidade e harmonizá-la com as exigências de mercado, ou do bem comum. Assim, um menor volume de dados coletados (com uma duração de armazenamento temporalmente mais limitada), ou um maior controle e responsabilização da *cybernacionalização* – especialmente dos dados sensíveis – poderia consistir em uma prática mais tolerável.[90] Por outro lado, a coleta em grande volume de dados, ainda que não considerados sensíveis, somente poderia ser aceitável quando houvesse baixo ou nenhum grau de *cybernacionalização*.[91] Para o caso de dados particularmente sensíveis, a coleta somente pode ser admitida quando haja um inegável e premente interesse público em fazê-lo,[92] e em caso de baixa (ou nenhuma) *cybernacionalização*.

7 Considerações finais

A era digital se apresenta como desafiadora para inúmeras instituições sociais e particularmente para o direito. A necessidade de rever os institutos jurídicos

como tornar os dados do Medicare inacessíveis; outras limitam o armazenamento garantindo que os dados armazenados por um lapso maior que um determinado período sejam apagados; outras limitam a análise, como por desidentificação da informação. Quanto mais extensas e efetivas são as medidas de responsabilização, menos cybernacionalização ocorre e melhor proteção é obtida. Daqui resulta que, quanto mais fortes forem as medidas de responsabilização associadas a um determinado banco de dados, menos violações da privacidade ocorrerão mesmo que o volume de informações seja alto, a sensibilidade da informação considerável e um grau significativo de intercâmbio e análise ocorra. Por outro lado, se a responsabilidade for deficiente, mais violações da privacidade ocorrerão mesmo que o volume seja relativamente baixo, a informação relativamente insensível e a coleta e análise não sejam particularmente extensas. Isso demonstra mais uma vez que a coleta é menos importante na Era Digital do que o alcance – ou limites – dos usos secundários, uma proporção que deverá continuar a crescer significativamente devido a melhorias na inteligência artificial" (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 34, tradução nossa). No original: "All accountability measures limit one element of cybernation or another. Some limit sharing, such as making Medicare data inaccessible; others limit storage by ensuring that data stored for longer than a given period is erased; others limit analysis, such as by de-identifying the information. The more extensive and effective accountability measures are, the less cybernation occurs and the better privacy is protected. It follows that the stronger the accountability measures associated with a given database, the fewer privacy violations will occur even if the volume of information is high, the information's sensitivity is considerable, and a significant degree of collation and analysis takes place. Conversely, if accountability is deficient, more violations of privacy will occur even if volume is relatively low, information is relatively insensitive, and collation and analysis are not particularly extensive. This demonstrates once again that collection is less important in the cyber age than the scope of – or limits on – secondary usages, a ratio that is expected to continue to grow significantly due to improvements in artificial intelligence".

90 O autor utiliza o termo "tolerável" no sentido de um permissivo de coleta de dados *a priori*, que pode ceder diante de objeções específicas (ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 37).

91 ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 45.

92 ETZIONI, Amitai. *Privacy in a cyber age*. Nova York: Palgrave Macmillan, 2015. p. 46; DONEDA, Danilo. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006. p. 163.

põe em xeque conceitos até então profundamente sedimentados no pensamento do estudioso do direito. Neste sentido, os direitos da personalidade sofrem inúmeras ameaças e riscos, quer pelas potencialidades da técnica, quer pela massificação despersonificadora.

Este artigo se propôs a analisar um destes direitos. A privacidade tem sido objeto de inúmeros questionamentos e dúvidas quanto a sua extensão e limites. Limitando um recorte histórico que vai dos fins do século XIX até os dias atuais – desde seu surgimento como um direito autônomo a ser deixado só, passando por sua gradual desvinculação da propriedade privada até sua associação à proteção de dados e informações pessoais –, turbulenta tem sido sua caminhada. A própria noção de privacidade é conceitualmente imprecisa, abrangendo, sob um mesmo vocábulo, uma miríade de situações que abrangem da proteção do domicílio e das informações pessoais à integridade corporal e a possibilidade de tomar decisões que repercutam sobre a esfera de seu titular. De um direito supervalorizado em seus contornos liberais-burgueses, passa a ser banalizado – e até a ter sua "morte" vaticinada – em uma sociedade caracterizada pela ubiquidade da vigilância, seja por governos interessados em aumentar o nível de controle sobre seus jurisdicionados (sob a justificativa da necessidade de proporcionar segurança), seja por agentes privados interessados em potencializar suas atividades lucrativas, seja até mesmo por seus próprios titulares, inseridos em uma cultura de hiperexposição voluntária.

Amitai Etzioni, representante do pensamento comunitarista liberal, sustenta que a privacidade é um entre outros bens sociais, e que seu superdimensionamento ou banalização constituem posturas equivocadas. Como qualquer outro interesse ou direito individual, seu exercício deve ser balanceado com os reclames do bem comum. Desta forma, o autor, após promover uma breve análise histórica do tratamento dispensado pela Suprema Corte americana ao referido direito, e de uma comparação dos sistemas americanos – da doutrina *third-party* – e europeu – galgado especialmente na Diretiva 95/46 da CE –, ambos apontados como insuficientes, e de desmistificar a ideia (fortemente inserida na cultura americana) de que o Poder Público seria a principal – se não a única – ameaça às liberdades individuais (e à vida privada em particular), passa a estabelecer um conceito atualizado e critérios (re)equilibradores de sua tensão com o bem comum, critérios estes que, num plano concreto, podem estabelecer uma adequada ponderação com interesses públicos e privados igualmente relevantes.

O pensamento de Etzioni referente à vida privada é produto de uma reflexão amadurecida ao longo das últimas décadas, que envolve não só a compreensão da Constituição como um "documento vivo", de sentido mutável e em permanente diálogo com os ditames sociais, como ainda a reoxigenação necessária ante

as complexidades da contemporaneidade pós-moderna. O estudo de suas ideias se prova de grande valia, não somente ao estudioso de direito comparado, mas aos juristas como um todo, na medida em que, em uma sociedade em rede, as ameaças a este direito ultrapassam os limites de fronteiras geográficas. Ademais, suas reflexões podem auxiliar a busca por um conceito que – se não dotado de pretensão de universalidade inequívoca – possa ao menos estabelecer contornos mais bem definidos que conduzam a mecanismos de proteção mais eficazes, bem como de critérios mais seguros que – reduzindo ao máximo a carga de subjetivismo em sua apreciação –, permitam garantir sua máxima potencialidade no contexto atual.

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

ROCHA, Luiz Augusto Castello Branco de Lacerda Marca da. A privacidade no pensamento de Amitai Etzioni. *Revista Brasileira de Direito Civil – RBDCivil*, Belo Horizonte, v. 26, p. 19-47, out./dez. 2020.

Recebido em: 12.10.2018
1º parecer em: 14.01.2019
2º parecer em: 14.07.2019