

OS DESAFIOS DA COMPREENSÃO DO DIREITO À PRIVACIDADE NO SISTEMA JURÍDICO BRASILEIRO EM FACE DAS NOVAS TECNOLOGIAS¹

Erick Lucena Campos Peixoto²

Marcos Ehrhardt Júnior³

Resumo: O nascimento da privacidade na contemporaneidade tem por base o desenvolvimento de tecnologias que, a seu tempo, representaram mudanças paradigmáticas, como o foi com a fotografia no final do século XIX e a criação dos primeiros computadores em meados do século XX. A privacidade é composta por três dimensões: a espacial, que se refere a uma privacidade física; a decisional, que coloca o indivíduo no controle de quem tem acesso ou não à sua vida de modo a influenciar suas decisões; e a informacional, trazendo a importância da proteção dos dados pessoais, inclusive através de técnicas de

¹ Versão revista, atualizada e modificada do artigo intitulado “Breves notas sobre a ressignificação da privacidade”, publicado na Revista Brasileira de Direito Civil – RBDCivil, v. 16, p. 35-56, 2018.

² Advogado. Mestre em Direito pela Universidade Federal de Alagoas (UFAL). Professor de Direito Civil e de Direito Digital na Faculdade de Tecnologia de Alagoas (FAT-AL). Pesquisador no grupo de pesquisa Direito Privado e Contemporaneidade, da Universidade Federal de Alagoas. Membro da Comissão de Inovação e Tecnologia da OAB Alagoas.

³ Advogado. Doutor em Direito pela Universidade Federal de Pernambuco (UFPE) e Mestre pela Universidade Federal de Alagoas (UFAL). Professor de Direito Civil dos cursos de mestrado e graduação da Universidade Federal de Alagoas. Professor de Direito Civil e Direito do Consumidor do Centro Universitário CESMAC. Pesquisador Visitante do Instituto Max-Planck de Direito Privado Comparado e Internacional (Hamburgo - Alemanha). Líder do Grupo de Pesquisa Direito Privado e Contemporaneidade (UFAL). Editor da Revista Fórum de Direito Civil (RFDC). Diretor Regional Nordeste do Instituto Brasileiro de Direito Civil (IBDCIVIL). Membro do Instituto Brasileiro de Direito de Família (IBDFAM).

anonimização.

Palavras-Chave: Privacidade. Tridimensionalidade da Privacidade. Direitos da Personalidade. Privacidade Informacional. Anonimização.

Abstract: The birth of contemporary privacy is based on the development of technologies that, at the same time, represented paradigmatic changes, as was the case with photography in the late nineteenth century and the creation of the first computers in the mid-twentieth century. Privacy is composed of three dimensions: the spatial dimension, which refers to a physical privacy; the decisional dimension, that puts the individual in control of who has access or not to their life in order to influence their decisions; and the informational dimension, bringing the importance of the protection of personal data, including through anonymization techniques.

Keywords: Privacy. Three-dimensionality of Privacy. Personality Rights. Informational Privacy. Anonymization.

Sumário: 1. Introdução – 2. Nascimento da Privacidade Contemporânea – 2.1. A Privacidade Segundo Warren e Brandeis – 2.2. O Desenvolvimento da Privacidade na Europa – 3. As Três Dimensões da Privacidade – 3.1. A Estrutura Tridimensional da Privacidade – 3.2. Dimensão Decisional da Privacidade – 3.3. Dimensão Espacial da Privacidade – 3.4. Dimensão Informacional da Privacidade – 3.4.1. Pessoas Identificadas, Identificáveis e Não-Identificáveis – 3.4.2. Problemas com a Anonimização e o Risco da Reidentificação – 4. Conclusão – 5. Referências.

1. INTRODUÇÃO



preocupação com a privacidade, durante muito tempo, foi algo restrito a uma pequena parcela da humanidade. Muitos nunca tiveram e outros ainda não tem uma noção, ainda que mínima, daquilo que se pode tratar por privacidade nos dias de hoje. Ao longo da história, nas diferentes sociedades e em seus mais diferentes meios, a noção de privacidade foi sentida de uma maneira muito própria em cada círculo social. Daí a razão de se dizer que a privacidade é algo plástico, que varia conforme a época e o local. É adaptável, valorada de um jeito por uma cultura, e até dispensável para outra.

Desde que o homem resolveu demarcar limites, estabelecendo um espaço para sua convivência apartada dos demais, surge a noção que mais tarde se consubstanciaria no que denominamos privacidade. Desse modo, é possível afirmar que a privacidade começa no sentido físico.

A partir do século XIX, com o desenvolvimento da fotografia, a facilidade em se reproduzir qualquer imagem, aliada ao poder de disseminação da informação através da mídia impressa, pode ser considerada a antessala dos problemas da privacidade que enfrentamos hoje.

No pós-guerra do século XX, a invenção dos computadores fez desenvolver a tecnologia da informação de um modo impactante. Em pouco tempo, a capacidade de processamento de dados crescia em progressão geométrica, e os problemas trazidos com as novas tecnologias começaram a afetar de um modo novo a privacidade. A preocupação passou a ser em relação aos dados informáticos (principalmente os dados pessoais), a partir os censos promovidos pelos governos. Este momento histórico redesenhou o modo como a privacidade era vista, incorporando uma dimensão que nos dias de hoje passou a ter mais destaque que o tratamento dado à privacidade tradicionalmente.

Ao lado da privacidade espacial e a privacidade sobre as decisões e ações tomadas em decorrência do modo pessoal de

vida, a privacidade informacional encontra fundamento nos direitos à intimidade, vida privada, sigilo, imagem, honra, inviolabilidade da casa e inviolabilidade dos dados estão inseridos no texto constitucional.

Este trabalho, empregando a metodologia civil-constitucional, pretende dar uma nova significação à privacidade enquanto direito, estabelecendo-a como categoria de direitos reunidos em torno de semelhanças familiares, cuja característica comum é o controle de acesso. Este controle de acesso fará correspondência com cada uma das dimensões da privacidade, sendo de dois tipos: o que diz respeito ao acesso físico, tangível, que corresponderá à dimensão espacial da privacidade; e o que diz respeito a um acesso intangível, virtual, que corresponderá à dimensão decisional e à dimensão informacional da privacidade.

2. NASCIMENTO DA PRIVACIDADE CONTEMPORÂNEA

2.1. A PRIVACIDADE SEGUNDO WARREN E BRANDEIS

No ano de 1890, a Sra. Warren, uma jovem dona de casa de Boston, Massachusetts, realizava em sua casa uma série de eventos sociais. Filha de um senador de Delaware e mulher de um jovem e bem-sucedido fabricante de papel que tinha desistido da prática jurídica para tomar de conta do negócio que herdara, Samuel Dennis Warren. A Sra. Warren circulava entre a elite da sociedade e os jornais da época, mais precisamente o *Saturday Evening Gazette*, especializado em temas de “sangue azul”, cobria suas festas em detalhes altamente pessoais e embaçados.

Naquela era onde o *yellow journalism* (imprensa marrom é o equivalente em português) a florava, a imprensa, na busca de ampliar suas vendas, começou com os excessos que são tão

comuns hoje. A cidade de Boston, no dizer de Prosser, talvez fosse, de todas as cidades americanas, aquela em que uma dama e um cavalheiro mantinham seus nomes e seus assuntos pessoais longe dos jornais.

O assunto sobre a casa dos Warren veio à tona com um furo jornalístico, na ocasião do casamento de uma filha dos Warren, o que aborreceu muito os seus pais. Nas palavras de William L. Prosser, foi um aborrecimento pelo qual a imprensa, os anunciantes e a indústria do entretenimento dos Estados Unidos tiveram que pagar caro pelos próximos setenta anos⁴.

O Sr. Warren se voltou para o seu sócio na advocacia, Louis Dembitz Brandeis. Juntos, reuniram decisões antigas cujas soluções tenham se dado com base em difamação, violação de algum direito de propriedade, violação de confiança ou contrato implícito⁵. O resultado foi o artigo “*The right to privacy*” publicado em 1890 na *Harvard Law Review*⁶.

O artigo concluía que tais casos eram baseados em um princípio mais amplo, o qual merecia reconhecimento em separado. A esse princípio Warren e Brandeis chamaram de direito à privacidade (*right to privacy*), o remédio para os crescentes abusos da imprensa através de um nível mais profundo de proteção do indivíduo contra a imposição de sofrimento mental.

Warren e Brandeis trouxeram a ideia de que a privacidade seria o direito de ser deixado em paz – *the right to be let alone* – expressão que utilizaram de Thomas McIntyre Cooley, da sua obra de 1879, “*A Treatise on the Law of Torts: Or the*

⁴ PROSSER, William L. *Privacy*. In: *California Law Review*, n. 3, vol 48, agosto de 1960, p. 383.

⁵ PROSSER, William L. *Privacy*, cit., p. 384. Envolviam publicação de correspondências privadas (*Woolsey v. Judd*), exposição de gravuras e publicação de catálogo (*Prince Albert v. Strange*), publicação de receitas obtidas sorrateiramente por funcionário (*Yovatt v. Winyard*), publicação de palestras para sala de aula cujo demandado era um membro (*Abernethy v. Hutchinson*), publicação da imagem do autor feita pelo demandado (*Pollard v. Photographic Co.*).

⁶ BRANDEIS, Louis D. WARREN, Samuel D. *The right to privacy*. In: *Harvard Law Review*, vol. 4, n. 5, dec. 15, 1890.

Wrongs Which Arise Independently of Contract". Cooley, define imunidade pessoal assim, em tradução livre⁷:

Imunidade Pessoal: o direito à personalidade pode ser considerado como sendo um direito de completa imunidade: o direito de ser deixado em paz. O dever correspondente é, não para infligir uma lesão, nem, dentro de tal proximidade que possa torná-lo bem-sucedido, tentar infligir uma lesão. Neste particular, o dever vai além do que é exigido na maioria dos casos; geralmente uma finalidade não executada ou uma tentativa malsucedida não é considerada. Mas a tentativa de cometer uma *battery*⁸ envolve vários elementos da lesão que nem sempre estão presentes nas violações do dever; envolve geralmente um insulto, uma situação que cause medo, um chamado repentino sobre as energias para pronta e efetiva resistência. Há uma grande possibilidade de um choque nos nervos, e a paz e quietude da pessoa é perturbada por um período de maior ou menor duração. Há, conseqüentemente, razão suficiente para que o estado de direito faça do *assault* um *legal wrong*, mesmo sem ter havido *battery*. Assim, neste caso, a lei vai ainda mais longe e faz com que o dano tentado seja uma ofensa criminal também⁹.

⁷ COOLEY, Thomas McIntyre. A treatise on the law of torts, or the wrongs which arise independent of contract. Chicago: Callaghan and company, 1879. In: *HathiTrust*. Disponível em: <http://www.hathitrust.org/>. Acesso em 03 de janeiro de 2016.

⁸ *Battery* é a violação do direito de ter o próprio corpo deixado em paz, por atos danosos ao corpo, como um corte, ferida de bala etc. *Assault* é a ameaça de infligir danos ao corpo da pessoa. Ambos são tanto um tipo de *tort* quanto um tipo de *crime* no *common law*.

⁹ *Personal Immunity: The right to one's person may be said to be a right of complete immunity: to be let alone. The corresponding duty is, not to inflict an injury, and not, within such proximity as might render it successful, to attempt the infliction of an injury. In this particular the duty goes beyond what is required in most cases; for usually an unexecuted purpose or an unsuccessful attempt is not noticed. But the attempt to commit a battery involves many elements of injury not always present in breaches of duty; it involves usually an insult, a putting in fear, a sudden call upon the energies for prompt and effectual resistance. There is very likely a shock to the nerves, and the peace and quiet of the individual is disturbed for a period of greater or less duration. There is consequently abundant reason in support of the rule of law which makes the assault a legal wrong, even though no battery takes place. Indeed, in this case the law goes still further and makes the attempted blow a criminal offense also.* COOLEY, Thomas McIntyre. A treatise on the law of torts, or the wrongs which arise independent of contract. Chicago: Callaghan and company, 1879, p. 29. In: *HathiTrust*. Disponível em: <http://www.hathitrust.org/>. Acesso em 03 de janeiro de 2016.

Originalmente, Warren e Brandeis descreveram o direito à privacidade como um direito já existente na *Common Law*, o qual incorporava proteções para a personalidade violada de cada indivíduo. A *Common Law*, diz os autores, assegura a cada indivíduo o direito de determinar, ordinariamente, até que ponto seus pensamentos, sentimentos e emoções devem ser comunicados aos outros¹⁰. O direito à privacidade, para esses autores americanos, significa que cada indivíduo tem o direito de escolher compartilhar ou não compartilhar com outros as informações sobre sua vida privada, hábitos, atos e relações¹¹.

Warren e Brandeis defendiam ser necessário para o sistema legal reconhecer o direito da privacidade porque quando uma informação sobre a vida privada de um indivíduo é tornada disponível para os outros, ela tende a influenciar e até mesmo causar dano no núcleo mais central da personalidade do indivíduo.

A concepção original do direito à privacidade de Warren e Brandeis incorporava, assim, um *insight* psicológico, o que era pouco explorado naquela época, em que a personalidade de um indivíduo, especialmente a imagem que tem de si mesmo, pode ser afetada e às vezes distorcida ou danificada quando informações sobre aquela vida privada são disponibilizadas a terceiros, ou seja, o direito à privacidade era o direito de cada indivíduo de proteger sua integridade psicológica, exercendo controle sobre informações que refletiam e aferravam a sua personalidade¹².

¹⁰ BRANDEIS, Louis D. WARREN, Samuel D. The right to privacy. *In: Harvard Law Review*, vol. 4, n. 5, dec. 15, 1890, p. 198.

¹¹ BRANDEIS, Louis D. WARREN, Samuel D. The right to privacy, cit., p. 216.

¹² Estes autores alocaram cuidadosamente o direito à privacidade dentro do contexto da altamente esquemática jurisprudência do direito americano do final do século XIX. Warren e Brandeis colocaram o direito à privacidade dentro da categoria mais geral do direito de o indivíduo ser deixado em paz. O próprio direito de ser deixado em paz foi parte de um direito ainda mais geral, o direito de gozar a vida, o qual era, por sua vez, parte do direito fundamental do indivíduo à própria vida. O direito à vida foi parte de uma tríade familiar de direitos fundamentais próprios do indivíduo, refletido na quinta emenda da Constituição Americana. GLANCY, Dorothy J. The invention of the right to privacy. *In: Arizona Law Review*. Vol. 21, n. 1, 1979, pp. 2-3.

Contrariando as decisões da Suprema Corte na época, Warren e Brandeis dissociaram o direito à privacidade tanto do direito à liberdade quanto do direito à propriedade. O direito à liberdade, segundo eles, assegura amplos privilégios civis, mas não a privacidade. O direito à propriedade, compreendendo interesses materiais individuais, contrastava com a preocupação com assuntos espirituais do direito à privacidade¹³.

2.2. O DESENVOLVIMENTO DA PRIVACIDADE NA EUROPA

No âmbito europeu, a primeira legislação a tratar da proteção de dados foi a *Hessisches Datenschutzgesetz*¹⁴, a Lei de Proteção de Dados do Estado de Hesse, na Alemanha Ocidental, de 7 de outubro de 1970.

Em 1973, a Suécia passou a ser o primeiro país europeu a ter uma lei nacional sobre proteção de dados. Esta lei sueca foi responsável por introduzir conceitos, como o registro central de informação de processamento de dados pessoais e o procedimento de licenciamento, do qual o registro público foi aberto ao escrutínio dos cidadãos e consumidores, usado como uma

¹³ GLANCY, Dorothy J. The invention of the right to privacy. In: *Arizona Law Review*. Vol. 21, n. 1, 1979, p. 4. Nas décadas seguintes, seguiu-se intenso debate sobre a delimitação do significado de privacidade. Dentre os diversos autores que trataram do tema, merece destaque o entendimento de Willian L. Prosser, que defende que o direito à privacidade compreende quatro distintos tipos de violação a diferentes interesses do indivíduo, os quais são reunidos por um mesmo nome, mas que não têm quase nada em comum, excerto que cada um representa uma interferência contra o direito do demandante de ser deixado em paz. Estes quatro *torts* foram assim descritos: (1) intrusão na reclusão ou solidão, ou na sua vida privada (*intrusion*); (2) divulgação pública de fatos privados embaraçosos sobre o demandante (*public disclosure of private facts*); (3) publicidade na qual o demandante é apresentado de modo equivocado para o público (*false light in the public eye*); e (4) apropriação, para obtenção de vantagem, do nome ou da imagem do demandante (*appropriation*). PROSSER, William L. Privacy. In: *California Law Review*, n. 3, vol 48, agosto de 1960, p. 389.

¹⁴ BUNDESREPUBLIK DEUTSCHLAND. HESSEN. *Datenschutzgesetz von 7. Oktober 1970*. In: *Datenschutz*. Disponível em: https://www.datenschutz.rlp.de/downloads/hist/ldsg_hessen_1970.pdf. Acesso em julho de 2016.

ferramenta de cumprimento da lei pelas agências de proteção de dados. Estes conceitos foram o pilar das primeiras legislações europeias de proteção de dados¹⁵.

A primeira diferença em relação à privacidade entre o novo e o velho mundo a se levar em conta é o aspecto temporal. Enquanto nos Estados Unidos a discussão ganhava corpo ainda no século XIX, na Europa só se passa a uma preocupação mais concreta no pós-guerra, justamente depois da invenção do computador. A privacidade americana, no seu sentido inicial, dizia respeito ao direito de não ser incomodado, era uma derivação do direito à vida, de não ter nenhum mal infligido ao corpo, o que posteriormente foi levado para o aspecto moral. Não ser incomodado, ser deixado em paz, ou simplesmente “ser deixado só” são os sentidos possíveis do *right to privacy*.

O movimento pela privacidade que surge na segunda metade do século XX na Europa se desvincula do sentido físico do *right to privacy* americano. A preocupação aqui é com o novo paradigma tecnológico que potencializou o processamento de dados através do uso do computador. Preocupa-se, então, com os dados pessoais e com o controle sobre eles.

A preocupação dos europeus com a privacidade também difere da preocupação dos americanos no sentido de que a proteção dos dados pessoais é uma medida necessária, inicialmente, contra o Estado, numa relação vertical, ao passo que nos Estados Unidos, o direito à privacidade surge como uma garantia contra os abusos cometidos por particulares, ou seja, horizontalmente.

As raízes da privacidade nos Estados Unidos estão em um direito do indivíduo, de caráter negativo, enquanto que as raízes europeias, estão também na sociedade, apresentando características de direito positivo, no qual se exige do Estado que

¹⁵ A legislação sueca foi logo seguida pelos outros países escandinavos. Na Dinamarca e Noruega, com uma lei tanto para o setor privado quanto o público em 1978; Finlândia em 1988. Cf. BURKERT, Herbert. Privacy - Data Protection: a German/European Perspective. In: ENGEL, Christoph; KELLER, Kenneth (ed.). *Governance of Global Networks in the Light of Differing Local Values*. Baden-Baden: Nomos, 2000, p. 48.

se tomem medidas para garantir a proteção de dados pessoais, como a instalação de órgãos de controle, além de a proteção visar grupos minoritários que podem sofrer discriminações com a exposição de seus dados pessoais. Na Europa se desenvolve o aspecto social da privacidade.

Stefano Rodotà, autor italiano, tratava o direito à privacidade como “*o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir a sua própria esfera particular*”. Tais definições não se excluem, mas, muito pelo contrário, incluem progressivamente novos aspectos de liberdade em um conceito mais abrangente de privacidade¹⁶.

3. AS TRÊS DIMENSÕES DA PRIVACIDADE

Privacidade é, como chama Solove, uma *umbrella word*¹⁷, ou seja, uma palavra guarda-chuva, que abriga distintos direitos da mesma família. Dentro do rol dos direitos da privacidade, destacam-se o direito ao sigilo, o direito à intimidade, o direito à imagem, o direito à honra, o direito à proteção dos dados pessoais.

Dworkin¹⁸ ensina que a privacidade pode ser a) territorial, quando é legítimo que se faça o que se deseja num espaço demarcado; b) pode ser uma questão de confidencialidade, quando por exemplo, as pessoas podem manter suas convicções políticas na esfera privada; por último, c) a privacidade também significa soberania quanto a decisões pessoais. A privacidade, assim, manifesta-se de várias maneiras, a depender do contexto, fazendo-se representar em uma ou mais dimensões, simultaneamente, inclusive.

¹⁶ RODOTÀ, Stefano. *A vida na sociedade de vigilância – a privacidade hoje*. Rio de Janeiro: Renovar, 2008, p. 15.

¹⁷ SOLOVE, Daniel J. *Understanding privacy*. Kindle edition. Cambridge, London: Harvard University Press, 2008.

¹⁸ DWORKIN, Ronald. *Domínio da vida: aborto, eutanásia e liberdades individuais*. São Paulo: Martins Fontes, 2003, p. 74.

Nos debates sobre privacidade, nota-se a *privacy* americana, que apesar de na sua origem derivar do direito à vida, desenvolve-se num contexto de tutela da liberdade, enquanto o modelo de privacidade que surge na Europa coloca a privacidade na perspectiva da dignidade.

Uma invasão da privacidade pode se constituir como uma ofensa intrínseca contra a dignidade individual. Intrínseca porque causa dano independentemente das consequências circunstanciais advindas da conduta danosa.

As ofensas contra a dignidade individual diferem das ofensas contra a liberdade individual. A autonomia (liberdade) se refere à capacidade de as pessoas criarem suas próprias identidades e deste modo moldarem suas próprias vidas. Já a dignidade, no sentido aqui empregado, se refere ao nosso senso de respeito que se impõe a nós mesmos.

Ao contrário do que ocorre na perspectiva da autonomia, deve-se anotar que a compreensão da privacidade na concepção de dignidade sofre maior influência de normas intersubjetivas que definam as formas de conduta, comumente associadas ao respeito entre as pessoas. Não é raro buscar fundamento para a privacidade nas formas sociais de respeito que cada um deve ao próximo, numa comunidade. Assim entendida, a privacidade pressupõe pessoas que são incorporadas socialmente, cuja identidade e autoestima dependam do desempenho das normas sociais, das quais a violação constitui um dano “intrínseco”¹⁹.

Seja numa forma mais próxima de sua concepção enquanto liberdade, seja enquanto dignidade, buscar identificar qual o direito lesado parece ser uma atividade possível quando identificado o bem jurídico violado.

3.1. A ESTRUTURA TRIDIMENSIONAL DA

¹⁹ POST, Robert C. Three concepts of privacy. In: *Yale Law School Legal Scholarship Repository*. Disponível em: http://digitalcommons.law.yale.edu/fss_papers. Acesso em junho de 2016, p. 2092

PRIVACIDADE

Ao se atribuir a característica de “privado” a uma certa coisa, a um determinado assunto, quer se dizer que há uma restrição onde alguém tem um nível de acesso mais profundo que outra pessoa. Há uma relação desigual aqui: uma pessoa tem mais acesso que outra, tendo o poder de restringir, de controlar esse acesso. Essa é a chave para o entendimento da privacidade, já que carrega o significado de proteção contra o acesso indesejado à coisa por terceiros.

O termo “acesso” pode ter uma conotação física, direta, concreta, bem como uma conotação metafórica. Esta última se refere tanto ao controle que a pessoa exerce sobre quem tem acesso às informações ela, quanto ao controle que ela tem sobre quais pessoas tem ou terão capacidade de interferir ou intervir nas decisões que são relevantes para ela²⁰.

Quando o controle de acesso se refere a algo físico, como um quarto de uma residência em que a pessoa que o habita pode determinar quem pode lá entrar, está a se falar em uma dimensão espacial da privacidade.

O controle de acesso, quando faz referência a coisas intangíveis, pode ser dividido em dois tipos: i) um é relativo à proteção contra a interferência indesejada ou à heteronomia nas nossas decisões e ações, a dimensão decisional da privacidade; ii) o outro é relativo à proteção da informação, a dimensão informacional da privacidade.

Seja em qual for a dimensão da privacidade em que se manifesta o controle de acesso, é necessário ter em mente que tais dimensões não existem de forma isolada. Pelo contrário, as dimensões coexistem, de forma que haverá situações onde será difícil dizer a que dimensão da privacidade determinado assunto diz respeito.

²⁰ RÖSSLER, Beate. *The value of privacy*. Cambridge: Polity, 2015, posição 304.

Assim, haverá situações em que determinado assunto da privacidade estará inserido em uma dimensão da privacidade, bem como aquelas em que tal assunto se encontra na intersecção de duas dimensões ou mesmo imerso nas três. São situações complexas em que se identifique mais de uma dimensão da privacidade, ou nas quais haja dúvida em qual dimensão determinado assunto se encaixa.

3.2. DIMENSÃO DECISIONAL DA PRIVACIDADE

A privacidade em sua dimensão decisional é o tipo de proteção que se dá ao modo de vida do indivíduo, incluindo aí as suas escolhas, seus gostos, seus projetos, suas características. Tal proteção recobre certos tipos de comportamento em público, o estilo de vida e as decisões e ações mais fundamentais, como ir em determinada igreja ou o que estudar²¹.

A estrutura desta dimensão da privacidade remonta a uma tradição da jurisprudência americana que fundamenta as liberdades reprodutivas, tais como o direito de usar métodos anti-concepcionais e o direito ao aborto, uma tradição que chega a confundir as chamadas liberdades civis com os direitos de privacidade.

A privacidade decisional estabelece um espaço de manobra no tráfico social que é necessário para a autonomia individual sem que haja interferência alheia. O indivíduo deve agir dentro da sua esfera de liberdade sem que se sinta intimidado pelos olhares indesejados. A pessoa (observando-se, é claro, a licitude dos seus atos) não deve a ninguém explicação sobre suas decisões, sobre seu comportamento ou sobre o seu jeito de vida, muito pelo contrário, deve-se esperar moderação, reserva e indiferença dos outros em relação a tudo aquilo que não lhes disser respeito²².

²¹ RÖSSLER, Beate. *The value of privacy*. Cambridge: Polity, 2015, posição 2064.

²² RÖSSLER, Beate. *The value of privacy*. Cambridge: Polity, 2015, posição 2151.

A autodeterminação pessoal e a autonomia, neste ponto, significam o direito de ser o autor da própria história, ou seja, que a vida da pessoa não seja objeto de comentários, interpretações distintas da realidade por pessoas não autorizadas a permear camadas restritas da personalidade.

A privacidade em sua dimensão decisional protege as pessoas de serem mal interpretadas ou julgadas fora de contexto em um mundo em que as se costuma prestar atenção de modo superficial, um mundo no qual informação é confundida facilmente com conhecimento. O verdadeiro conhecimento sobre uma pessoa é produto de um processo lento de mútua relação²³.

As relações sociais do indivíduo variam de grau, desde as mais próximas (família, amigos) às mais distantes (desconhecidos). Cada grau tem acesso a determinados aspectos da pessoa. A família conhece detalhes mais íntimos; colegas de faculdade conhecem um lado daquela pessoa, assim como os professores conhecerão outro. Um estranho olhar superficialmente, tendo na maioria das vezes a aparência da pessoa como única informação sobre ela. Cada relação destas é constituída através de diferentes aspectos da vida da pessoa e em cada uma dessas relações a privacidade protege aqueles aspectos que podem ser entendidos como não essenciais para a relação, e assim, irrelevantes.

A privacidade pode ser violada não somente por comentários negativos, objeções e olhares indesejados, mas também pela interferência positiva, inclusive pela aprovação. Se alguém faz comentários sobre a roupa de outrem, ou um elogio inoportuno, por mais que seja um ato positivo, será uma interferência no modo de agir daquela pessoa.

O núcleo da privacidade decisional é garantir que a pessoa em sua integralidade seja capaz de viver uma vida tranquila. Assim, a privacidade decisional acaba abrangendo uma privacidade corporal também, já que a privacidade de uma pessoa pode

²³ ROSEN, Jeffrey. *The unwanted gaze: the destruction of privacy in America*. New York: Vintage Books, 2001, p. 8.

ser violada não só quando são levantados questionamentos sobre seu jeito de viver, mas também quando comentários indesejados são feitos sobre o seu corpo²⁴.

As atitudes que se esperam para que seja respeitada a privacidade decisional são a moderação, a reserva e até a indiferença. A essas atitudes soma-se outra, a tolerância. Geralmente, usa-se a palavra tolerância para um contexto em que os costumes e as ações dos outros encontram na pessoa desaprovação e antipatia; uma ideia contrária à dela, seja um posicionamento político, religioso ou a opinião sobre uma estrela da música *pop*. Mas a tolerância, no contexto da privacidade decisional, está relacionada a saber se uma dada pessoa permite que outra tenha influência em suas decisões pessoais. E essa influência não se dá apenas em aspectos negativos, mas também positivos, como um encorajamento, um elogio. Se pessoas se sentam na mesa ao lado em um restaurante, cabe, a quem está do lado, simplesmente não prestar atenção²⁵.

A proteção da privacidade em sua dimensão decisional tem um ponto de encontro com a dimensão informacional. Muitos dos assuntos que dizem respeito ao modo de viver da pessoa acabam virando dados, os chamados dados sensíveis, cuja proteção é uma das principais preocupações na chamada sociedade da informação.

3.3. DIMENSÃO ESPACIAL DA PRIVACIDADE

Quando se fala da dimensão espacial da privacidade, volta-se àquela que é a mais tradicional dimensão da privacidade de todas, aquela dimensão original, de onde todo assunto relativo à privacidade se originou. É a privacidade do lar, a privacidade de um cômodo da casa, de um determinado lugar físico.

A vida privada dentro de espaços protegidos segue uma

²⁴ RÖSSLER, Beate. *The value of privacy*. Cambridge: Polity, 2015, posição 2261.

²⁵ RÖSSLER, Beate. *The value of privacy*, cit., posição 2294.

dinâmica diferente da vida que se leva exposta a olhares de qualquer um que se cruza o caminho. A proteção do lar dá a liberdade necessária para se viver uma vida digna, permitindo que cada um desenvolva sua personalidade como bem lhe aprouver.

Numa lamentável passagem de nossa História, saber que o indivíduo presta culto doméstico para determinada religião foi muito útil aos nazistas para o seu plano de extermínio dos judeus. A todos deve ser assegurado um espaço físico que seja um ambiente de proteção à personalidade, onde o homem exercitará sua liberdade como forma de autorrealização. O termo “privacidade espacial” acaba não revelando toda a riqueza desta dimensão da privacidade. A vida doméstica vai além de um mero espaço. Aqui há o encontro das dimensões espacial e decisional. O espaço doméstico é onde pode-se, por excelência, praticar livremente nosso modo de viver.

A Constituição Federal, em seu artigo 5º, XI, diz que “a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial”. A proteção aqui prevista não é a mesma dada pelo direito de propriedade. São duas coisas completamente diferentes. A inviolabilidade da casa é direito de privacidade, protege o ambiente privado do lar, as relações que ali se desenvolvem livres do julgamento social. Não se trata do direito ao bem que é o imóvel, mas do reino de liberdade que representa para aqueles que ali vivem, que ali se realizam dignamente.

O caso *Masacres de Ituango Vs. Colombia* da Corte Interamericana de Direitos Humanos é bastante relevante para o reconhecimento de uma dimensão espacial da privacidade. A Corte assentou naquele caso que não se pode afastar da ideia de domicílio a ideia de vida privada, já que estão intrinsecamente ligadas. A casa é o ambiente vital para o desenvolvimento da vida privada

Algumas normas do direito interno visam a proteção da privacidade em sua dimensão espacial, como nos limites impostos ao direito de construir, pelo art. 1.301 do Código Civil, que estabelece uma distância mínima para a construção de janelas, varandas etc. em relação ao terreno vizinho. Assim, busca-se uma convivência harmoniosa entre os moradores de cada casa, evitando o intrometimento na vida alheia através da diminuição do contato físico entre cada lar, bem como os olhares indiscretos. De modo semelhante, o artigo 1.303 trata do tema em relação à zona rural: “Na zona rural, não será permitido levantar edificações a menos de três metros do terreno vizinho.”

3.4. DIMENSÃO INFORMACIONAL DA PRIVACIDADE

Um ponto de partida interessante para se tratar a privacidade informacional foi elaborado por Solove, que defende que a privacidade deve ser concebida de baixo para cima, ao invés de cima para baixo. Isso quer dizer que a privacidade deve ser olhada a partir dos contextos particulares, e não apenas como algo abstrato²⁶.

Solove elaborou o que ele chama de taxonomia²⁷ da privacidade (*taxonomy of privacy*), para, segundo ele, dar um entendimento mais pluralístico da privacidade, focando nas atividades que podem criar e que criam problemas de privacidade. Para o autor americano, uma violação de privacidade ocorre quando determinada atividade causa problemas que afetam uma matéria ou atividade privada²⁸.

Nesta taxonomia, existem quatro grupos básicos que representam atividades danosas: coleta de informação;

²⁶ SOLOVE, Daniel J. *Understanding privacy*. Kindle edition. Cambridge, London: Harvard University Press, 2008, posição 131.

²⁷ Taxonomia, segundo o Dicionário Priberam da Língua Portuguesa, significa a teoria ou nomenclatura das descrições e classificações científicas.

²⁸ SOLOVE, Daniel J. *Understanding privacy*, cit., posição 1280.

processamento de informação; disseminação de informação; e invasão.

O primeiro grupo de atividades que afetam a privacidade é a coleta de informação, subdividida em *surveillance* (vigilância, consistindo em observar, escutar, registrar a atividade de alguém) e *interrogation* (interrogação, que consiste em várias formas de questionamento ou investigação em busca de informação).

O segundo grupo de atividades envolve o modo como a informação é armazenada, manipulada e utilizada, ou seja, o processamento de informação, que subdivide-se em *aggregation* (combinação de várias partes de dados sobre uma pessoa); *identification* (ligar a informação a um particular); *insecurity* (envolve a falta de cuidado em proteger a informação de vazamentos e acesso indevido); *secondary use* (uso de uma informação para um propósito diferente daquele para qual ela foi coletada); *exclusion* (não permissão do titular dos dados de saber sobre os dados que os outros têm sobre ele e participar no manejo e uso dos mesmos).

O terceiro grupo de atividades envolve a disseminação de informação: *breach of confidentiality* (quebra de promessa de manter uma informação pessoal em segredo); *disclosure* (revelação de uma informação verdadeira sobre uma pessoa que afeta o jeito com que os outros julgam sua reputação); *exposure* (envolve a revelação da nudez, do sofrimento ou de funções corporais de outrem); *increased accessibility* (forma de ampliar a acessibilidade à informação); *blackmail* (chantagem, ameaça em revelar informações pessoais); *appropriation* (envolve o uso da identidade do titular dos dados para servir a outros objetivos e interesses); *distortion* (consiste em disseminar informações falsas ou enganosas sobre indivíduos. Todas as formas de disseminação de informação envolvem a propagação, transferência de dados pessoais ou a ameaça de fazê-los.

No quarto e último grupo estão as atividades que

envolvem as invasões nos assuntos particulares das pessoas: *intrusion* (envolve os atos invasivos que perturbam a tranquilidade ou solidão de alguém; *decisional interference* (é a incursão nas decisões do titular de dados em relação a seus assuntos particulares).

Solove²⁹ organizou estes grupos em volta de um modelo que começa na pessoa a que se referem os dados, o indivíduo cuja vida é mais afetada diretamente pelas atividades classificadas na taxonomia. Desse indivíduo, várias entidades coletam informação, sejam elas outras pessoas, empresas ou o governo. A coleta de informação, por si só, pode configurar uma atividade danosa, apesar que nem toda atividade de coleta é perigosa ou cause danos à pessoa.

Os chamados “*data holders*”, tipo de agente de tratamento, estão entre aqueles que coletam os dados e fazem o tratamento, ou seja, armazenamento, combinação, manipulação, busca e uso dos dados coletados, fase esta que Solove chama de processamento de informação.

A Lei nº. 13.709, de 14 de agosto de 2018, que dispõe sobre a proteção de dados pessoais no Brasil (LGPD), refere-se ao tratamento como sendo toda operação realizada com dados pessoais, como as que se referem a coleta, produção, percepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5º, X).

Após o processamento, os *data holders* transferem para outros a informação ou a liberam, resultando na fase conhecida por disseminação de informação. Todo o caminho percorrido desde a coleta de informações até a disseminação da informação reflete o afastamento dos dados pessoais do controle do indivíduo. A cada fase, fica mais difícil exercer o controle sobre eles.

²⁹ SOLOVE, Daniel J. *Understanding privacy*. Kindle edition. Cambridge, London: Harvard University Press, 2008.

O último grupo, referente às “invasões”, afasta-se dos grupos anteriores pelo fato que a informação aqui não é um elemento preponderante. A *intrusion* fica mais bem inserida no contexto da privacidade espacial, enquanto que a *decisional interference* é a própria dimensão decisional da privacidade.

O autor coloca num mesmo plano diferentes dimensões da privacidade para tentar, de uma forma organizada, explicar a privacidade através dos problemas concernentes a ela. Discorda-se, aqui, desse tipo de organização apenas por colocar num mesmo lugar coisas diferentes. A teoria tridimensional da privacidade situa cada dimensão em seu devido lugar, por isso a opção por sua utilização neste trabalho.

Na maioria das vezes, quando se diz que um indivíduo sofreu uma violação da privacidade, na verdade, o que se está querendo dizer é que ocorreram várias violações em vários direitos da privacidade, e até em dimensões diferentes desta. Uma pequena postagem em uma rede social pode facilmente ferir o direito à honra, à imagem, à proteção de dados pessoais, à intimidade etc. Por conseguinte, determinada violação à privacidade, alcançado mais de uma dimensão, exige uma resposta mais complexa, compreensiva de todos os matizes da violação.

Os problemas da privacidade se situariam nos pontos, nas interseções das dimensões da privacidade, o que dá liberdade para se trabalhar determinado assunto de modo muito mais organizado e eficiente que o proposto por Solove. É muito mais apropriado examinar um caso de violação de privacidade, primeiro, a partir do próprio caso (por exemplo, se houve vazamento de dados, se uma foto foi publicada sem autorização, se alguém foi acusado injustamente de um crime numa postagem de rede social etc.), segundo, localizando o problema dentro das dimensões da privacidade que lhe são pertinentes (se vazamento de dados, na dimensão informacional; se calúnia, dimensão decisional), de forma a encontrar se houve de fato violação e qual o direito violado (honra, imagem, intimidade etc.), para então

admir a consequência jurídica adequada.

Ocorre que os contornos da privacidade em sua dimensão informacional ainda apresentam outros desafios, sobretudo quando considerado o intenso e cada vez mais complexo uso de ferramentas tecnológicas para mineração de dados.

3.4.1. PESSOAS IDENTIFICADAS, IDENTIFICÁVEIS E NÃO-IDENTIFICÁVEIS

Quando se fala em privacidade informacional, um conceito central é o *Personally Identifiable Information (PII)*, termo originalmente da área de segurança da informação, trata-se de qualquer informação relativa a uma pessoa identificada ou passível de identificação. Informações como o nome, o número de um documento de identidade, carteira de motorista, título eleitoral ou do cadastro de pessoas físicas, placa do veículo, cartão de crédito, impressão digital, rosto, dados genéticos entram dentro dessa categoria pelo potencial que têm de identificar (aquele que estava no anonimato) o indivíduo.

O conceito de *Personally Identifiable Information* emerge no contexto do desenvolvimento do computador desde a segunda metade do século XX, quando os sistemas de armazenamento de dados computadorizados permitiram novas técnicas capazes de ligar estes dados às pessoas³⁰, em que pese não haver uma definição uniforme.

Informação pessoal e dados pessoais são termos talvez mais vistos, mas partem de uma concepção mais restrita. Enquanto estes termos se referem a uma pessoa identificada, que se destaca como indivíduo, a PII abrange também aquele que pode ser identificado.

Paul Schwartz e Daniel Solove³¹ apresentam o modelo

³⁰ SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *In: New York University Law Review*, [s. l.], v. 86, n. December, p. 1814–1894, 2011, p. 1817.

³¹ *Ibidem*, p. 1878.

que eles chamam de PII 2.0, abrangendo essas duas categorias (informação sobre uma pessoa identificada e informação sobre uma pessoa identificável), mas também indicam uma terceira categoria, a da informação sobre uma pessoa não-identificável, que leva apenas um risco remoto de identificação. Em relação a esta última categoria, levando em consideração os meios que possam razoavelmente ser utilizados para (re)identificação, tais dados não são relacionáveis a uma pessoa.

Os conceitos acima apresentados ganham importância quando se verifica que a Lei Geral de Proteção de Dados Pessoais (Lei nº. 13.709, de 14 de agosto de 2018) aborda a questão da anonimização, tendo esta por utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo (art. 5º, XI).

É preciso compreender a utilidade e as diversas possibilidades de anonimização dentro do contexto de um modelo econômico em que a mineração de dados pessoais tornou-se uma das principais formas de financiamento da chamada nova economia. Diante do desafio de se implementar as garantias relativas à autodeterminação informacional prevista da LGPD, não é raro que o recurso à anonimização seja apontado como um dos modos de se buscar equilibrar os interesses de todos os envolvidos. Contudo, como ocorre com boa parte dos temas que envolvem aplicação de tecnologia às relações jurídicas, ainda vivenciamos os primeiros estágios dos debates sobre seus impactos e consequências.

3.4.2. PROBLEMAS COM A ANONIMIZAÇÃO E O RISCO DE REIDENTIFICAÇÃO

Ohm³² critica o modelo de anonimização (*release-and-*

³² OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *In: UCLA Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1712.

forget model), apresentando advertência que não pode ser negligenciada quanto o foco é a proteção da privacidade: quando o administrador anonimiza os dados, ele os lança, tanto publicamente quanto de forma privada, para um terceiro ou mesmo internamente para outros funcionários, e depois não faz qualquer tentativa de descobrir o que aconteceu com esses dados depois de lançados.

Por se tratar de técnicas já difundidas, os métodos utilizados para anonimização acabaram gerando uma confiança em demasia naquele que seria o papel da arquitetura, nos moldes em que Lessig³³ a coloca como reguladora do comportamento no ciberespaço.

Abre-se espaço para se indagar se todos os usuários da rede possuiriam o mesmo nível de proteção, ou se o indivíduo comum, com conhecimentos básicos acerca da tecnologia, que apenas a utiliza como ferramenta para realizar tarefas corriqueiras, ficaria exposto à ação de sujeitos com maior nível de conhecimento ou acesso a equipamentos: um “superusuário”.

O mito do superusuário³⁴, ou seja, aquele poderoso

³³ LESSIG, Lawrence. *Code: version 2.0*. New York: Basic Books, 2006. P. 123.

³⁴ OHM, Paul. The myth of the superuser: fear, risk, and harm online. *UC Davis Law Review*, [s. l.], v. 41, n. 4, p. 1327, 2008. O superusuário, no entendimento do citado autor, é aquele que possui poder, a habilidade de controlar ou alterar computadores e redes, que um usuário comum não possui (p. 1333). Podemos aqui tentar rotular os *hackers*, que se fazem presentes no imaginário popular de maneira caricata e que aparecem constantemente no noticiário. Geralmente utilizam ferramentas para conquistar mais poder, como programas de computador altamente sofisticados. Não percebemos de vista, contudo, que depois de certo tempo, aquela ferramenta símbolo de seu poder acaba sendo difundida, passando a ser acessível ao usuário comum. Ohm argumenta que existe uma tendência de que a designação de superusuário desapareça na medida em que a técnica que dominava se torne ultrapassada, corriqueira, e cita como exemplo o CD, que tempos atrás somente algumas pessoas tinham o conhecimento capaz de fazer cópias daquela mídia utilizando o *drive* do computador. No ano em que o seu artigo foi escrito, 2008, já existiam aplicativos que facilitavam a qualquer usuário o processo de cópia de CD ou DVD e, comparando com hoje, mais de dez anos depois, com o advento do *streaming* e suas facilidades, o interesse naquelas mídias físicas fica restrito a uma parcela pequena de pessoas. O superusuário que antes tinha habilidades de copiar as músicas de um CD é só mais um usuário comum hoje.

usuário de computador, difícil de ser localizado, imune às restrições tecnológicas e ciente das lacunas legais, é uma das críticas feitas por Ohm a uma visão mais otimista da anonimização, como aquela de Schwartz e Solove, para os quais o fato de a reidentificação de uma pessoa ser possível não necessariamente implica que isto aconteça.

A crítica de Ohm é severa: no final das contas, é necessário que se abandone a ideia de que se pode proteger a privacidade apenas removendo as informações sobre uma pessoa identificável (PII)³⁵. O cenário caótico sobre esse tipo de dado é comparado pelo professor americano com o jogo Whack-A-Mole³⁶, em que, quando uma toupeira sai do buraco e o jogador a acerta com a marreta, outras saem pelos outros buracos. Assim estariam dispostos os dados sobre uma pessoa identificável: quando se resolvesse o problema de um, apareceriam mais outros.

Schwartz e Solove³⁷ discordam neste ponto, afirmando que seu modelo PII 2.0 pode ser operacional e previsível. Ohm inclusive critica o termo “*anonymize*”, entendendo ser errado e que há a necessidade de se corrigir a retórica utilizada nos debates sobre privacidade.

Sobre este tópico, Latanya Sweeney³⁸ afirma que o termo “anônimo” (*anonymous*) implica que os dados não podem ser manipulados ou relacionados para identificar qualquer indivíduo e que mesmo quando uma informação anonimizada é compartilhada com terceiros, ela está longe de ser “anônima”.

Basta que algum dado seja vinculado a identidade real de alguma pessoa para que qualquer associação entre este dado e

³⁵ OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. *In: UCLA Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1742.

³⁶ *Ibidem*, 1742.

³⁷ SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. *In: New York University Law Review*, [s. l.], v. 86, n. December, p. 1814–1894, 2011, p. 1884.

³⁸ SWEENEY, Latanya. Maintaining Patient Confidentiality When Sharing Medical Data Requires a Symbiotic Relationship Between Technology and Policy. *Retrieved March*, [s. l.], n. May, p. 1–21, 1997.

uma identidade virtual (como o perfil ou avatar de uma pessoa ou aquela identidade que se cria anonimizada em uma base de dados) vai quebrar o anonimato. Por isso a reidentificação causa preocupação, não só em relação à exposição de dados identificáveis, mas de todos os dados que podem contribuir para a capacidade de se estabelecer ligações (*linkability*³⁹) entre os dados, abrindo a possibilidade para futuros danos.

A novel legislação brasileira (art. 12 da Lei Geral de Proteção de Dados Pessoais) não considera como dados pessoais aqueles que foram anonimizados, salvo quando o processo de anonimização ao qual foram submetidos (a) for revertido utilizando meios próprios; ou (b) quando, com esforços razoáveis, puder ser revertido. A razoabilidade dos esforços para reidentificação de dados anonimizados deve levar em consideração fatores objetivos, como o custo e o tempo necessários para reverter o processo, de acordo com as tecnologias disponíveis, e a utilização de meios próprios.

Não se perca de vista que aqueles dados utilizados para formação de perfil comportamental de determinada pessoa natural poderão ser considerados como dado pessoal se a pessoa for identificada, recebendo a tutela da LGPD, na forma do § 2º do artigo 12.

Em um estudo que é um marco na privacidade informacional, Latanya Sweeney⁴⁰ conduziu experimentos utilizando dados do censo dos Estados Unidos de 1990, apontando que 87% da população norte-americana à época (216 milhões de 248 milhões de pessoas) era identificável de forma única apenas pela combinação de três informações: do ZIP *code*, da data de nascimento completa e do sexo. Metade da população dos Estados Unidos (132 milhões, 53%) era identificável apenas utilizando-

³⁹ OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. In: *UCLA Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1746.

⁴⁰ SWEENEY, Latanya. Simple demographics often identify people uniquely. *Carnegie Mellon University*, Data Privacy Working Paper 3. Pittsburgh 2000, [s. l.], p. 1–34, 2000.

se a informação do lugar (“*city, town, or municipality*”), do sexo e data de nascimento. Indicando o *county*, o sexo e a data de nascimento, 18% da população poderia ser identificada.

Dados simples permitiram que a professora Sweeney realizasse tal façanha, expondo a fragilidade do modelo de anonimização da época. Ohm afirma que o modelo de anonimização e reidentificação dos cientistas da computação é um jogo de adversários (*adversarial game*) em que a figura do adversário é a pessoa que tenta reidentificar os dados, não importando se as razões que a levam a isto sejam boas ou más. Stalkers⁴¹, investigadores, colegas intrometidos, empregadores, vizinhos, a polícia, analistas de segurança do Estado, anunciantes ou qualquer um interessado em associar um indivíduo com dado são adversários em potencial⁴².

Diante do contexto acima apresentado, deve-se refletir se aos dados anonimizados também merecem receber algum tipo de tutela, já que pode existir um risco de serem reidentificados, quebrando todo anonimato anteriormente conquistado. Apesar das pesquisas apontarem para os inconvenientes e os riscos da adoção do modelo *release-and-forget*, a adoção de um modelo no qual os dados desvinculados de uma pessoa física tenham alguma espécie de proteção ainda parece algo distante.

4. CONCLUSÃO

A privacidade é uma das palavras mais multifacetadas que se pode trazer ao debate, com seus vários sentidos atribuídos em vários tempos e por várias culturas. Sua compreensão remete a um conceito fluido, melhor compreendido quando dividido em três dimensões distintas, porém complementares (decisional, informacional e espacial). Em cada uma dessas dimensões se pode

⁴¹ NARAYANAN, Arvind; SHMATIKOV, Vitaly. *De-anonymizing Social Networks*. Disponível em: <https://arxiv.org/abs/0903.3276>. Acesso em 22 de abril de 2018.

⁴² OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. In: *UCLA Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1724.

identificar os problemas a elas relativos e, a partir daí, localizar o direito violado.

Esse modelo tridimensional da privacidade tem outra utilidade, que é permitir um melhor detalhamento de cada problema relativo à privacidade e assim chegar, de forma mais precisa, à extensão do dano. Assim, feito este caminho, descobrir como reparar o dano à privacidade passa a ser uma atividade mais próxima do caso concreto, atenta às várias peculiaridades deste. Evita-se, desse modo, que a busca da reparação seja lastreada em ilações generalistas e que ocorra um tabelamento informal do *quantum* indenizatório.

A privacidade enfrenta um desafio atual, que é se reinventar numa sociedade da informação, numa nova revolução tecnológica construída nas bases da anterior. Toda estrutura de fluxo de informação construída nas décadas anteriores serve de suporte para esta nova fase do desenvolvimento tecnológico. *Big data*, internet das coisas e vigilância são termos cada dia mais comuns e levam às grandes preocupações com a privacidade.

O processo de anonimização é de fundamental importância dentro da temática da privacidade informacional, onde a informação em uma base de dados pode ser manipulada para dificultar a identificação dos titulares dos dados. Numa sociedade onde a informação circula a todo tempo, é importante que se proteja os indivíduos contra os riscos da identificação. Por isso se tutela os dados que identifiquem a pessoa e, também, aqueles que possam identificá-la. Isto porque algumas informações são capazes de estabelecer um vínculo direto com uma pessoa, enquanto outras, por mais que não o façam diretamente, quando associadas a mais dados, acabam resultando na identificação.

O aspecto tecnológico sempre fez parte do desenvolvimento histórico da privacidade, e agora, mais que nunca, parece dar um tom de primazia à dimensão informacional dela. Mas é importante não olvidar de que deve haver um diálogo entre as dimensões da privacidade na perspectiva dos problemas

decorrentes das novas tecnologias, como forma de tentar enfrentar a complexidade e velocidade com que novas questões surgem neste campo de estudo.



5. REFERÊNCIAS

- BRANDEIS, Louis D. WARREN, Samuel D. The right to privacy. *In: Harvard Law Review*, vol. 4, n. 5, dec. 15, 1890.
- BUNDESREPUBLIK DEUTSCHLAND. HESSEN. Datenschutzgesetz von 7. Oktober 1970. *In: Datenschutz*. Disponível em: https://www.datenschutz.rlp.de/downloads/hist/ldsg_hessen_1970.pdf. Acesso em julho de 2016.
- BURKERT, Herbert. Privacy - Data Protection: a German/European Perspective. *In: ENGEL, Christoph; KELLER, Kenneth (ed.). Governance of Global Networks in the Light of Differing Local Values*. Baden-Baden: Nomos, 2000.
- COOLEY, Thomas McIntyre. A treatise on the law of torts, or the wrongs which arise independent of contract. Chicago: Callaghan and company, 1879. *In: HathiTrust*. Disponível em: <http://www.hathitrust.org/>. Acesso em 03 de janeiro de 2016.
- DWORKIN, Ronald. *Domínio da vida: aborto, eutanásia e liberdades individuais*. São Paulo: Martins Fontes, 2003.
- GLANCY, Dorothy J. The invention of the right to privacy. *In: Arizona Law Review*. Vol. 21, n. 1, 1979.
- LESSIG, Lawrence. *Code: version 2.0*. New York: Basic Books, 2006. P. 123.
- NARAYANAN, Arvind; SHMATIKOV, Vitaly. *De-anonymizing social networks*. Disponível em:

- <https://arxiv.org/abs/0903.3276>. Acesso em 22 de abril de 2018.
- OHM, Paul. Broken promises of privacy: responding to the surprising failure of anonymization. In: *UCLA Law Review*, [s. l.], v. 57, n. 6, p. 1701–1777, 2010, p. 1746.
- _____. The myth of the superuser: fear, risk, and harm online. *UC Davis Law Review*, [s. l.], v. 41, n. 4, p. 1327, 2008, 1335.
- POST, Robert C. Three concepts of privacy. In: *Yale Law School Legal Scholarship Repository*. Disponível em: http://digitalcommons.law.yale.edu/fss_papers. Acesso em junho de 2016.
- PROSSER, William L. Privacy. In: *California Law Review*, n. 3, vol 48, agosto de 1960.
- RODOTÀ, Stefano. *A vida na sociedade de vigilância – a privacidade hoje*. Rio de Janeiro: Renovar, 2008.
- _____. *Il mondo nella rete: quali i diritti, quali i vincoli*. Roma-Bari: GLF Laterza, 2014
- _____. *Intervista su privacy e libertà*. Roma-Bari: GLF Laterza, 2005.
- ROSEN, Jeffrey. *The unwanted gaze: the destruction of privacy in America*. New York: Vintage Books, 2001.
- RÖSSLER, Beate. *The value of privacy*. Cambridge: Polity, 2015.
- SCHWARTZ, Paul M.; SOLOVE, Daniel J. The PII Problem: Privacy and a New Concept of Personally Identifiable Information. In: *New York University Law Review*, [s. l.], v. 86, n. December, p. 1814–1894, 2011, p. 1884.
- SOLOVE, Daniel J. *Understanding privacy*. Kindle edition. Cambridge, London: Harvard University Press, 2008.
- SWEENEY, Latanya. Maintaining Patient Confidentiality When Sharing Medical Data Requires a Symbiotic Relationship Between Technology and Policy. *Retrieved March*, [s. l.], n. May, p. 1–21, 1997.

- _____. Simple demographics often identify people uniquely. *Carnegie Mellon University, Data Privacy Working Paper 3*. Pittsburgh 2000, [s. l.], p. 1–34, 2000.
- WESTIN, Alan. *Privacy and freedom*. New York: Atheneum, 1967.