A PROTEÇÃO LEGAL DOS DADOS PESSOAIS COMO EFETIVAÇÃO DO DIREITO À PRIVACIDADE

MARCELO CRESPO[1]

SUMÁRIO: Introdução. 1 Novos modelos de negócios baseados em dados. 1.1 Privacidade e dados pessoais em um mundo Orwelliano e Kafkiano. 1.2 Quando os serviços são grátis, nós somos o produto. 2 Um panorama sobre a proteção aos dados pessoais na lei brasileira. 3 Breves comentários sobre os projetos de leis de proteção aos dados pessoais. Considerações finais a título de conclusão. Referencias bibliográficas.

Introdução

A evolução tecnológica está sendo capaz de nos proporcionar incríveis experiências que muitos ainda encontram dificuldade para compreender, tais como fenômenos disruptivos econômico-sociais, como o surgimento de empresas como a Uber ou a circulação de criptomoedas como o Bitcoin.[2] A ampla disseminação da internet[3] e da *world wide web*[4], aliado ao fato de que seu acesso tem-se dado primordialmente por equipamentos móveis tem sido fundamental neste cenário,

---

[1] Advogado, bacharel em Direito pela Faculdade de Direito de Sorocaba (2002), atuante nas áreas do direito digital, criminal e compliance. Doutor (2012) e Mestre (2008) em Direito Penal pela Faculdade de Direito de São Paulo. Especialista em Segurança da Informação e também em Direito Penal pela Universidade de Salamanca. Certified Compliance and Ethics Professional International (CCEP-I) pela Society of Corporate Compliance and Ethics (SCCE). Professor concursado na Faculdade de Direito de Sorocaba (FADI). Coordenador do curso de pós-graduação em Direito Digital e Compliance no Damásio Educacional. E-mail: marcelo.crespo@prof.fadi.br.

Resumo: O presente texto discorre sobre como a tecnologia transforma o cotidiano social, em especial pela oferta de produtos e serviços que dependem de fornecimento e análise de dados pessoais, o que decorre dos novos modelos de negócios derivados do uso da tecnologia. Esta situação é comentada sob a perspectiva da necessidade de proteção aos dados pessoais com a finalidade de conferir aos indivíduos a concretização do direito fundamental àprivacidade.

Palavras-chave: Dados pessoais. Privacidade. Direitos fundamentais. Internet. Segurança da informação.

Abstract: “This paper discusses how technology transforms social everyday life, especially by offering products and services that depends on the supply and analysis of personal data, which stems from the new business derived from the use of technology. This situation is commented from the perspective of the need of personal data protection in order to give individuals the realization of the fundamental right to privacy. Keywords: Personal data – privacy – fundamental rights – internet – security information.”

[2] Para maiores detalhes sobre o Bitcoin, vide: CRESPO, Marcelo Xavier de Freitas. Bitcoin: breves considerações sobre a criptomoeda. Disponível em: <https://canalcienciascriminais.com.br/bitcoin-breves-consideracoes-sobre-a-criptomoeda/>. Acesso em: 05. ago. 2015; e CRESPO, Marcelo Xavier de Freitas. Ainda sobre as criptomoedas: considerações em face do Sistema Financeiro Nacional. Disponível em: <https://canalcienciascriminais.com.br/ainda-sobre-as-criptomoedas-consideracoes-em-face-do-sistema-financeiro-nacional/>. Aceso em: 12.ago.2015.

[3] Muito resumidamente poder-se dizer que a internet é uma rede que conecta milhões de computadores pelo mundo.

[4] A web, também em resumo, é uma ferramenta de acesso à internet, usando o protocolo HTTP para transferir informações, dependendo de browsers (navegadores) como o Internet Explorer, Chrome, Safari, que permitem aos usuários, mediante cliques em links, acesso a arquivos hospedados em outras máquinas.

que é formado por massivas coletas e tratamento de dados pessoais. Trata-se do mundo em uma perspectiva de *big data*.[5]

Nos últimos anos também se pode notar, empiricamente, um aumento nas produções de textos e mídias explicativas dos fenômenos relacionados à tecnologia e suas repercussões no nosso cotidiano. Esse aumento, embora representado por algumas publicações de indiscutível qualidade, lamentavelmente também abarca uma série de aventureiros e "estelionatários" que insistem em discorrer sobre temas que mal compreendem e, mesmo assim, intitulam-se especialistas em direito digital, muitas vezes fornecendo explicações equivocadas ou meramente opinativas, sem o devido fundamento jurídico. Também há, infelizmente, profissionais da área jurídica que, em busca de algum momento de fama, optam por perseguir qualquer mínima aparição nas mídias, sempre comentando os últimos acontecimentos relacionados ao direito e tecnologia, igualmente sem se preocupar com detalhes técnicos ou éticos.

Assim, é importante que a academia siga exercendo seu importante papel, delineando teorias, apresentando questionamentos, soluções, críticas e sugestões aos desafios da tecnologia em nossas vidas. Afinal, com a seriedade acadêmica fundada em pesquisas é que se poderá buscar respostas e explicações às repercussões jurídicas da tecnologia em nossas vidas.

Registre-se que, com tais assertivas, não se quer dizer que opiniões não acadêmicas não tenham importância, mas, sinalizar que a atenção deve ser redobrada quanto a estas, já que atualmente vivemos em tempos de protagonismo das pós-verdades[6] e tendo a internet dado voz a "legiões de imbecis."[7]

Mas, para além de preocupações com textos e informações de qualidade, merece protagonismo a preocupação com a proteção a dados pessoais num

[5] *Big Data* relaciona-se com conjuntos de dados tão grandes (estruturados e não estruturados) que sua análise depende de aplicações não tradicionais, isto é, com técnicas minuciosas de coleta, armazenamento, análise, compartilhamento, consulta e segurança da informação (proteção a eles). Os dados componentes de *big data* servem como base para análises dos negócios, impactando-os significativamente em razão da possibilidade de decisões estratégicas, porque tem caráter preditivo e de conhecimentos específicos sobre as características dos usuários/clientes/consumidores. Embora se desconheça o surgimento da expressão, ela ganhou maior exposição a partir dos anos 2000, quando Douglas Laney articulou o conceito de big data fundado em (i) volume (já que as coletas derivam de enorme quantidade de fontes), (ii) velocidade (já que os dados fluem em velocidades sem precedentes); e, (iii) variedade (já que são gerados em diversos formatos).

[6] Trata-se de substantivo que representa o momento social em que fatos objetivos têm menos influência para moldar a opinião pública do que emoções e crenças pessoais.
O Oxford Dictionaries afirma que o termo "pós-verdade" foi usado pela primeira vez em 1992 por Steve Tesich, mas que houve um pico de utilização mais recentemente, tendo crescido o uso em 2000% no ano de 2016. Sobre isso, vide "O que é 'pós-verdade', a palavra do ano segundo a UniversidadedeOxford",disponível em:
<https://www.nexojornal.com.br/expresso/2016/11/16/O-que-%C3%A9-%E2%80%98p%C3%B3s-verdade%E2%80%99-a-palavra-do-ano-segundo-a-Universidade-de-Oxford>. Acesso em: 25 set. 2017, às 14h43min.

[7] Umberto Eco disse, em 10.06.2015, por ocasião do recebimento de título de Doutor Honoris Causa na Universidade de Turim, que "As mídias sociais deram o direito à fala a legiões de imbecis que, anteriormente, falavam só no bar, depois de uma taça de vinho, sem causar dano à coletividade. Diziam imediatamente a eles para calar a boca, enquanto agora eles têm o mesmo direito à fala que um ganhador do Prêmio Nobel. O drama da internet é que ela promoveu o idiota da aldeia a portador da verdade."

contexto de privacidade, se é que se pode considerá-la existente em tempos atuais.

Aliás, privacidade e intimidade são conceitos de difícil conceituação e que, no Direito, não se definiu se são autônomas ou interdependentes. Fato é que os aspectos da integridade moral dos direitos da personalidade sofrem, constantemente, intromissões alheias. Por isso mesmo Rodotà já disse que juntamente da percepção dos riscos do progresso tecnológico está a consciência da impossibilidade de detê-lo, mesmo que a evolução apresente aspectos negativos.[8]

No plano internacional, o art. 12 da Declaração Universal dos Direitos do Homem de 1948 dispõe que "Ninguém será sujeito à interferência em sua vida privada, em sua família, em seu lar ou em sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques."[9] A Constituição Federal de 1988, por sua vez, garantiu o direito à vida privada e à intimidade como direito fundamental, em seu artigo 5º, X, mas, como dito, não os define.

A falta de definição e consenso reflete uma diversidade de tratamentos da questão.

Sobre os conceitos de privacidade e intimidade podemos afirmar, assim, que há duas teorias: a) uma que se apoia na diferenciação da teoria das esferas, onde privacidade e intimidade são termos distintos; e b) outra que, devido à profusão do conceito norte-americano de *privacy*, entende que os conceitos devem ser entendidos como sinônimos e tutelados de forma única. Na doutrina brasileira não há sistematização, o que se evidencia pela verificação de que autores tratam do tema de maneiras bastante distintas. Por outro lado, nossa Constituição aparentemente aproxima-se da teoria das esferas, apesar de que, no que tange à jurisprudência, os termos são tratados como sinônimos. Eis, assim, um perfeito cenário para uma verdadeira confusão conceitual entre privacidade e intimidade.

Cabe à doutrina a responsabilidade de realizar uma profunda reflexão com vistas a superar essa confusão conceitual. De qualquer forma, é a definição de dados pessoais que estabelecerá o nível de proteção a eles conferidos. Atualmente, no Brasil algumas leis mencionam apenas características de dados pessoais, sem, contudo, trazer uma definição. Tal discussão está no centro do debate de uma nova lei de Proteção de Dados Pessoais, representada por alguns projetos de leis, em especial o nº 5.276, de 2016, enviado ao Congresso pelo Poder Executivo após elaboração, pelo Ministério da Justiça, de um anteprojeto que passou por consulta pública.

1 Novos modelos de negócios baseados em dados

1.1 Privacidade e dados pessoais em um mundo Orwelliano e Kafkiano

Orwelliano poderia ser um adjetivo a definir o atual estágio mundial em face da tecnologia: amplamente conectado e vigiado, especialmente porque há uma

[8] RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. p. 41-42.
[9] Documento disponível em: <http://www.onu-brasil.org.br/documentos_direitoshumanos.php>. Acesso em: 25 set.2017, às 21h35min.

constante e crescente fiscalização das nossas vidas pelos governos e empresas privadas.[10] Kafkiano, por sua vez, pode ser outro adjetivo a definir o atual estágio social na medida em que remete a algo surreal, de absoluta submissão ao imaginário.[11] Afinal, vivemos tempos onde nossos dados são o novo petróleo, e tempos onde se fala não na possibilidade, mas na certeza de que, em algum momento, nossos dados serão indevidamente expostos indevidamente.

Para ilustrar a perspectiva Kafkiana, vale mencionar a narrativa curiosa e preciosa de Janet Vertesi.[12]

Janet Vertesi é professora de Sociologia na renomada Universidade de Princeton e tomou uma decisão arrojada, de difícil concretização: quando engravidou, decidiu que ia evitar que seus dados dispostos na *web* pudessem inferir seu estado gravídico. [13] Em outras palavras, ela tentou passar sua gravidez despercebida perante empresas cujas atuações dependem fortemente de análise de dados. É que em um mundo altamente conectado, a simples aquisição de pacotes de fraldas pela *web* já seria suficiente para que, em geral, empresas tomassem conhecimento de que estava grávida. E ela não queria ser importunada por propagandas.

Parece uma decisão estranha? Sua opção foi pertinente na medida em que as grávidas têm os dados pessoais com maior valor de mercado, havendo pesquisas que apontam que eles podem valer até quinze vezes mais do que os de uma mulher não grávida. [14] Em geral, as grávidas se encontram em situações de constantes tomadas de decisões importantes e que se estendem pela vida de seu filho.

Assim, Vertesi faz um relato sobre *big data*, mas, ao contrário, isto é, sobre como é difícil evitar que nossos dados sejam coletados, que sejamos localizados, monitorados e inseridos em bancos de dados sem nosso consentimento.[15]

[10] O termo "Orwelliano" surgiu para se referir ao regime ficcional (mas que mostra grande realidade na atualidade) do livro "1984" de Eric Arthur Blair, conhecido pelo pseudônimo de "George Orwell" e que retrata a ampla fiscalização e controle de determinado governo na vida das pessoas. A obra foi escrita a partir da narrativa de Winston Smith, um homem com uma vida aparentemente insignificante e que recebe a missão de perpetuar a propaganda do regime por meio da falsificação de documentos públicos e da literatura, no intuito de registrar que tudo o que o governo faz está correto. Smith fica desiludido com sua existência miserável e, assim, inicia uma rebelião contra o sistema.

[11] O termo "Kafkiano" ganhou maior destaque na língua inglesa e significa algo complicado, labiríntico, surreal, como as situações verificadas nas obras de Franz Kafka, um dos escritores mais influentes do século XX, nascido em Praga, e que publicou obras como "Metamorfose" (publicado em 1915 e narra o caso de Gregor Samsa, que após acordar de um pesadelo, vê seu corpo transformado em um inseto daninho) e "O Processo" (publicado em 1925 e que conta o caso de Josef K., envolto em um obscuro processo sobre um crime que desconhece).

[12] Pudemos discorrer sobre tal relato também no artigo "Intimidade e Privacidade em face do Marco Civil (lei nº 12.965/14). In: ALMEIDA FILHO, José Carlos de Araújo; MEIRELLES, Delton R. S.; PIMENTEL, Fernanda (org.) Processo e Conexões Humanas. Petrópolis: 2014, pp. 159/186.

[13] O programa do evento no qual houve a participação de Vertesi pode ser encontrado em <http://www.theorizingtheweb.org/2014/ttw14-print-program.pdf.>. Acesso em: 25 set. 2017, às 12h14min.

[14] How One Woman Hid Her Pregnancy From Big Data. Disponível em: <http://mashable.com/2014/04/26/big-data-pregnancy/#5wwUCU3si8q7. Acesso em: 25 set. 2017, às 22h25min.

[15] O evento no qual Janet Vertesi compartilhou sua experiência foi o "Theorizing the web", cuja página da programação pode ser encontrada em: <http://theorizingtheweb.tumblr.com/>. Acesso em: 25 set.2017, às 22h27min.

A saga de Janet Vertesi teve início quando ela pediu que ninguém do seu relacionamento fizesse menções à sua gravidez nas redes sociais. Para isso, telefonou e escreveu individualmente para amigos e familiares. Assim que lhes dava a boa notícia da gravidez, aproveitava para solicitar que não falassem sobre o assunto.[16] O segundo passo foi utilizar o The Onion Router[17] – TOR – para acessar as páginas que desejava e impedir que fosse rastreada por *cookies*.[18] Também preferiu fazer compras *offline*, com pagamento em dinheiro em vez de cartões e precisou até alugar um armário para que suas compras lá fossem entregues com vistas a que as aquisições não fossem vinculadas a ela.

Por agir assim, na tentativa de evitar que seus dados fossem analisados contra sua vontade, deparou-se com uma situação bastante peculiar. Ao tentar comprar um carrinho de bebê, seu marido utilizou cerca de quinhentos dólares em cartões presente (*gift cards*) de uma famosa loja, mas não obteve êxito, porque isso desencadeou um alerta para o lojista, que teve que informar este tipo de operação para as autoridades como forma de se evitar a "lavagem" de dinheiro.

Outro aspecto que tornou a conduta de Vertesi alvo de desconfiança das autoridades foi o fato de ter utilizado o TOR como *software* de acesso à internet. É que a sua utilização, embora possa ter sido para fins legítimos, é visto pelas agências de segurança dos Estados Unidos como um indicativo de que alguém pretende fazer algo ilícito.[19]

Vê-se, assim, a problemática situação onde o aparente desejo de se manter anônimo tornou a professora um alvo de investigação, porque suas condutas amoldaram-se em práticas indiciárias de ilícitos. Algo bastante preditivo e violador das liberdades públicas, especialmente se pensado sob a óptica da Constituição Federal do Brasil. Vertesi provou que se forem tomadas medidas para evitar o rastreamento de dados, pode-se até mesmo conseguir o resultado oposto, incrementando as atenções sobre nós, o que se mostra realmente kafkiano.

1.2 Quando os serviços são grátis, nós somos o produto

[16] Mesmo assim, um tio residente na Austrália enviou mensagem felicitando-a e, em resposta, ela o bloqueou e apagou os registros de conversas com ele nas redes sociais.

[17] Tor é um software livre e de código aberto que permite anonimato ao navegar na Internet. É uma espécie de browser, mas cuja funcionalidade principal é a ocultação do I.P. da máquina conectada à internet. Vide www.torproject.org.

[18] *Cookies* são arquivos que armazenam, de forma temporária, o que o internauta está fazendo enquanto navega na web, como endereços de e-mails, a cidade de onde se está acessando a web, preferências de buscas etc. As informações geralmente possuem formato de texto e ocupam ínfimo espaço no disco rígido do computador.

[19] Vide: Suprema Corte dos EUA autoriza FBI a hackear qualquer computador anônimo. Disponível em: <http://meiobit.com/342817/suprema-corte-eua-autoriza-fbi-investigar-qualquer-computador-conectado-com-ip-desconhecido-tor-vpns-principais-alvos-usuarios-em-todo-mundo-podem-ser-afetados/>. Acesso em: 25 set.2017, às 15h26min. Vide, ainda, O FBI hackeou mais de 8 mil computadores em 120 países com um único mandado. Disponível em: <https://motherboard.vice.com/pt_br/article/pgzeab/fbi-hackeou-mais-de-8-mil-computadores- em- 120-pases-com-um-unico-mandado>. Acesso em: 25 set.2017, às 15h27min.

"Quando os serviços são grátis, você é o produto", é o que costumamos ouvir desde o surgimento da internet e dos serviços que aceitamos utilizar diariamente quase sempre sem ler os termos e condições de uso ou a política de privacidade de dados.

Em muitos casos na atualidade o modelo de negócios funda-se na exibição de publicidade, o que faz com que os dados dos usuários ganhem importância ímpar, já que, com eles, as propagandas são direcionadas de forma muito mais específica, resultando em atingimento de consumidores com muito maior precisão. Também há casos em que pode não haver a publicidade, mas dados do usuário são captados a partir do preenchimento de cadastro por ele mesmo, de forma espontânea e com seu consentimento. Também há coleta de dados baseadas em interações e comunicações com outros usuários. Em todos os casos anteriores, a coleta de dados é uma verdadeira fonte de poder e dinheiro.

Há serviços que oferecem versões gratuitas e, conforme crescem, passam a vender espaço publicitário para empresas ou ofertar o acesso a estes dados para as que estejam dispostas a pagar por eles. Mas que não se enganem: serviços pagos também podem agir assim. Apesar disso, tais modelos podem ser praticados de forma ética e em conformidade com a legislação e respeitando os direitos do consumidor.

Um caso bastante curioso é o do Instagram e as fotos de seus usuários que foram parar no jornal "The New York Times".[20] Houve uma parceria do jornal com o mencionado provedor de aplicações, o que constava dos termos e políticas de uso da rede social, mas que, mesmo assim, pegou muitos de surpresa, porque jamais imaginaram que poderiam ter suas fotos estampadas no jornal de grande circulação. Ninguém leu os termos aplicáveis ao Instagram, mas, neste caso, as pessoas não se ofenderam na medida em que os donos das fotos haviam fotografado a neve dos Estados Unidos, tendo sido uma honra para os escolhidos.

Ainda sobre o Instagram, em 2013 houve mudança na sua política, mas seus termos não foram esclarecidos de forma adequada aos usuários, como, por exemplo, a venda de fotos dos usuários. [21] Por tal razão, a National Geografic cogitou deixar a plataforma do aplicativo, ocasião em que essa mensagem recebeu nada menos que trinta e oito mil curtidas, deixando clara a insatisfação das pessoas com a mudança. Por seu turno, o Instagram se manifestou informando que seus termos haviam sido mal interpretados e que os trechos polêmicos seriam retirados, o que fez com que voltassem atrás e anulassem as alterações.[22]

Mas é importante ressaltar que nem sempre a coleta e tratamento de nossos dados significará algo ruim. É com eles que conseguimos personalizações de conteúdos baseadas em intreresses dos usuários, podemos melhorar nossa

[20] Instagrammers discover front-page NYT placement by chance. Disponível em: <https://www.poynter.org/news/instagrammers-discover-front-page-nyt-placement-chance>. Acesso em: 25 set.2017, às 22h33min.

[21] Instagram muda termos de serviço e quer usar suas fotos para ganhar dinheiro. Disponível em: <https://www.poynter.org/news/instagrammers-discover-front-page-nyt-placement-chance>. Acesso em: 25 set.2017, às 22h34min.

[22] Instagram desiste de reformular seus termos de serviço. Disponível em: <https://www.tecmundo.com.br/instagram/34456-instagram-desiste-de-reformular-seus-termos-de-servico.htm>. Acesso em 25 set.2017, às 22h36min.

navegação, tornando-a mais eficiente, podemos ter facilidades ao não precisar digitar senhas todas as vezes em que formos acessar um determinado *website* etc.

Também é preciso dizer que, mesmo quando o serviço é cobrado, isso não impede que os dados pessoais sejam usados. Veja-se, por exemplo, o caso da Netflix, que pode analisar — e de fato analisa — nossos dados para ofertar séries e filmes mais alinhados com os gostos do assinante. O mesmo pode-se dizer de análises das transações bancárias e com cartões de crédito, que podem permitir aos bancos ofertar produtos mais específicos para seus clientes.

Programas de fidelidade também se prestam a conhecer mais dos clientes, não sendo apenas um meio de recompensar os mais fiéis. Assim, as interações com a empresa — ou grupo de empresas — é monitorado para que sejam ofertadas promoções e produtos específicos. Então, mesmo com pagamento, nossos dados são analisados e não deixamos de ser produtos por conta disso.

Também é preciso considerar que o fato de pagar por um produto não faz dele melhor que outros, que terá atendimento melhor ou que nossos dados não serão coletados.

Mas o que há de mal em coletar a tratar nossos dados? Por si só, nada. O problema é que quando não temos ciência do que ocorre com eles, este vício no consentimento frustra nossa expectativa de privacidade e, ainda, mostra os valores das empresas e o respeito que elas têm pelos seus clientes.

O melhor cenário seria termos pleno conhecimento e compreensão de quais dados são coletados e como são utilizados pelas empresas e governo.

Exemplos de uso de nossos dados são as experiências que temos com as plataformas Facebook, Instagram e WhatsApp. Nenhum deles tem versão paga, mas todos exploram nossos dados de forma massiva. Aliás, todos agora são pertencentes ao mesmo grupo econômico (são todos pertencentes ao Facebook). Todos os nossos textos, curtidas, interações e compartilhamentos são analisados e usados para segmentar publicidade. E é estranho como muitas pessoas acham receoso preeencher o CPF em alguns estabelecimentos, mas ignoram que nossas interações nas redes sociais mostram muito mais de nós que o mencionado documento. Apesar de tais plataformas terem políticas de privacidade, as possibilidades de uso de nossos dados é tão grande que mal podemos compreender o que de fato é ou pode ser feito com eles.

Quem nunca pesquisou um produto numa loja digital e, dias depois, passou a ver anúncios dele em outros websites? Isso nada mais é que análise de dados, fazendo remarketing. O mesmo vale para os informes “pessoas que compraram isso também compraram...”

A Google, por exemplo, monitora a nossa localização para melhorar os serviços prestados, sendo possível verificarmos onde estávamos em determinado dia e horário. E, sendo usuário dos produtos Google, não é possível fazer cessar essa grande devassa em nossas vidas, havendo alguma possibilidade de reduzir o rastreamento, mas não impedi-lo.

A atualidade é baseada em dados e não há motivos para pressupor que o futuro será diferente, com novos modelos de negócios baseados em coleta e análise de

dados, propiciando lucros enormes para as empresas e um constante monitoramento dos cidadãos. Pode-se dizer, assim, que a vigilância é o atual modelo de negócios da internet e nada indica que isso mudará.

2 Um panorama sobre a proteção aos dados pessoais na lei brasileira

O Brasil não dispõe, atualmente, de uma lei específica de proteção de dados pessoais. De fato, há leis setoriais que, em seus respectivos âmbitos, tratam parcialmente do tema.

Nesta perspectiva, podemos mencionar, inicialmente, a lei nº 8.078/90 — Código de Defesa do Consumidor — sobre os dados dos consumidores.

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> §1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> §2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> §3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
>
> §4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> §5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.

As normas acima apontam que o consumidor deve ter acesso às informações arquivadas sobre si nos bancos de dados (art. 43, "caput"), sendo que elas devem ser objetivas, claras e verdadeiras, proibindo-se informações negativas por prazo superior a cinco anos (§1º).[23]

O Código de Defesa do Consumidor exige que a inserção de um consumidor em bancos de dados seja-lhe comunicada quando não tiver, por ele, sido solicitada (§2º). A ele, dá-se, ainda, o direito de retificar dados inexatos, com o prazo de cinco dias para que o responsável informe a realização da alteração solicitada (§3º).

Considerando que os parágrafos 4º e 5º declaram que os bancos de dados e cadastros dos consumidores e os serviços de proteção ao crédito e congêneres são de caráter público, estipulam que, operada a prescrição relativa à cobrança de débitos do consumidor, é vedado que os sistemas de proteção ao crédito forneçam informações que impeçam ou dificultem novo acesso ao crédito pelo consumidor. Há, aqui, indubitável preocupação em não discriminar o consumidor em face da desproporcionalidade da utilização de seus dados pessoais fora de um contexto da atual dívida.

[23] Prazo aplicado para os cadastros relativos à negativação por dívidas.

Verifica-se, assim, que o sistema de proteção aos dados pessoais previsto no Código de Defesa do Consumidor é, por um lado, destinado a não permitir abusos contra o consumidor, mas, por outro, insuficiente para proteger cidadãos em geral, já que se refere apenas aos dados dos consumidores. E nem todas as relações havidas no âmbito da web são de caráter consumerista, restando grande parte dos cidadãos desprotegidos quanto à coleta e tratamento de seus dados.

Para além do microssistema de proteção aos dados dos consumidores, pode- se mencionar a lei nº 12.414/12 — "Lei do Cadastro Positivo" — que traz as seguintes disposições:

> Art. 3º Os bancos de dados poderão conter informações de adimplemento do cadastrado, para a formação do histórico de crédito, nas condições estabelecidas nesta Lei.
>
> §1º Para a formação do banco de dados, somente poderão ser armazenadas informações objetivas, claras, verdadeiras e de fácil compreensão, que sejam necessárias para avaliar a situação econômica do cadastrado.

Vê-se, assim, que a mencionada lei é uma espécie de complemento ao Código de Defesa do Consumidor, mas aqui com maior detalhamento quanto ao histórico de crédito. Assim, é possível a constituição de bancos de dados com informações pessoais sobre o histórico de crédito (art. 3º), mas precisam conter registros claros, objetivos e, acima de tudo, adequados à necessária avaliação econômica do cadastrado (§1º). Não são admitidos, portanto, bancos de dados com informações que não se prestem a análise creditícia.

O sistema brasileiro conta, ainda, com a lei nº Lei 12.527/11, popularmente conhecida como "Lei de Acesso à Informação", que regulamentou o acesso a informações, previsto nos artigos 5º, inciso XXXIII, e 37, parágrafo 3º, inciso II, e 216, parágrafo 2º da Constituição Federal.

Subordinam-se à mencionada lei os órgãos públicos que fazem parte da administração direta dos Poderes Executivo, Legislativo, Judiciário, incluindo-se os Tribunais de Contas e o Ministério Público, bem como autarquias, fundações públicas, empresas públicas, sociedades de economia mista e demais instituições sob o controle direto ou indireto da União, dos Estados, do Distrito Federal e dos Municípios, com aplicação estendida às instituições privadas sem fins lucrativos que desenvolvam ações de interesse público e recebam recursos públicos. Verifica-se, assim, que o acesso pretendido pela lei é de informações contidas em bancos de dados de entes públicos. A lei destina-se a garantir, antes da proteção dos dados pessoais, o acesso à informação. É um contexto oposto ao da proteção cujo aspecto normalmente se traz sob a perspectiva de não divulgação ou uso que possam violar a privacidade dos indivíduos.

Para além das normas sobre a proteção mais específica dos dados, há que se considerar, ainda, aspectos civis e criminais que merecem ser mencionados.

Nesta perspectiva, insta mencionar o artigo 20 da Lei nº 10.406/2003 (Código Civil), que se refere à divulgação de dados de interesse público que possam interferir na reputação de um indivíduo, nos seguintes termos:

> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber,

> se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.

Logo, se, pela natureza dos dados divulgados, temos que podem ser de utilidade pública, a exemplo de nome, telefone, endereço, e-mail, situação de cadastro fiscal na Receita Federal do Brasil ou de Órgãos de Proteção ao Crédito, o que recebem status de Dados Pessoais de acesso público, mas, isto não significa que os dados cadastrais são públicos e de uso irrestrito, vez que eles pertencem ao seu Titular e há limitações para formação de registros descritas na lei.

Como dito, a norma acima se relaciona com a divulgação de dados cadastrais que possam interferir na reputação de um indivíduo. Evidentemente, não sendo este o caso (não se tratando de dados de um indivíduo) o dispositivo não se aplica. Isso não significa que o responsável pela coleta e tratamento de dados não possa vir a arcar com responsabilidades em face do mau uso.

Afinal, há uma cláusula geral de responsabilidade civil que impõe a obrigação de indenizar quem causar dano a outrem.

Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo.
Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem. (grifo nosso)

Por ato ilícito entende-se o seguinte:

> Art. 186. Aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito.
> Art. 187. Também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes.

A falha na prestação dos serviços que possam expor outros a dano poderá, então, ser alvo de responsabilização tanto pelo Código de Defesa do Consumidor (quando o cliente for destinatário final do produto/serviço) bem como pelo Código Civil (nos casos em que não houver relação de consumo protegidas pelo Código de Defesa do Consumidor).

Há, portanto, inegável possibilidade de responsabilização civil ou consumerista, a depender do tipo de violação e agentes envolvidos. Isso pode se aplicar a uma série de situações, tais como vazamento indevido de dados, divulgação de dados falsos, enfim, qualquer situação que possa expor terceiros a danos patrimoniais ou morais.

Nota-se, assim, que apesar de haver algumas normas que tratem de cadastros com dados pessoais, nenhuma delas é específica ao ponto de delinear os princípios que devem nortear a coleta e tratamento dos dados, não havendo previsão de órgão específico de fiscalização, e sem que se prevejam consequências da falha na proteção dos dados pessoais. É mais que desejável, portanto, uma lei de proteção aos dados pessoais.

3 Breves comentários sobre os projetos de leis de proteção aos dados pessoais

Até o presente momento há três projetos que tratam da proteção de dados pessoais em tramitação no Congresso Nacional: o PL 5276/2016, o PLS 330/2013 e o PL 4060/2012. Cada qual prevê distintas garantias e também situações de riscos à privacidade e a outras liberdades fundamentais. Em geral, os projetos pretendem regular o consentimento entre os titulares dos dados e os responsáveis pelos seus respectivos tratamentos.

Os projetos mencionados oferecem diferentes garantias ao direito à privacidade, embora ainda seja necessário harmonizar a proteção de dados pessoais com os direitos fundamentais da liberdade de expressão e o direito à informação.

Apesar do PL 5.276/16 ser o que nos parece mais bem estruturado, até porque se baseia em modelo europeu já bastante discutido e em *vacatio legis*, nenhum dos projetos cria o órgão público específico e independente para fiscalizar a proteção aos dados pessoais. O que mais se aproxima disso é justamente o 5.276/16, que atribui responsabilidades específicas para a regulação e a fiscalização da implementação da lei por um órgão competente a ser designado na regulamentação da lei. Sem um órgão regulador há sérias chances de que o projeto, tornando-se lei, não seja concretizado. É que, sem um órgão independente, os titulares dos direitos terão o ônus de enfrentar a distribuição desigual de interesses das grandes corporações face à privacidade.

Por outro lado, o importante conceito de autodeterminação informativa (presente nos projetos 5276/2016 e 4060/2012) deve ser tratado com cautela, porque pode legitimar o "direito ao esquecimento", que tem sido entendido como o direito das pessoas demandarem em juízo, que buscadores cancelem listas de informações sobre estas pessoas após pesquisas em seus nomes. O assunto é polêmico e merece ser tratado com independência e maturidade.

Todos os projetos possuem, de alguma forma, exceções para as atividades de investigação das forças públicas de segurança. Justifica-se que a exceção seria necessária para as atividades de investigação de casos que precisam de agilidade na resolução. Todavia, é possível constatar que os governos têm construído aparatos de vigilância, com as pessoas sendo seus alvos constantes. O vigilantismo desenfreado é uma realidade que deve ser limitada por critérios razoáveis relativos ao tratamento dos dados pessoais também pelos órgãos públicos e de segurança.

Uma questão importante é a menção à Lei de Acesso à Informação. Explica- se: tal menção é necessária quando o tratamento de dados pessoais for feito por órgãos da administração pública, ainda que a aplicação da mencionada lei já esteja subentendida, vez que deve-se reforçar a obrigação de transparência. A Lei de Acesso à Informação no art. 31, §3º, inciso V, determina que as informações pessoais podem ser publicadas sem consentimento se forem necessárias para a proteção do interesse público, o que tem gerado alguns bons resultados, como as remunerações de funcionários públicos que recebem supersalários de forma ilegal.

Os projetos também permitem o tratamento de dados para a realização de pesquisas estatísticas, embora não tragam delimitações precisas sobre o alcance e limites destas atividades, podendo gerar brechas e abusos no tratamento dos dados

pessoais sem o consentimento dos seus respectivos titulares. Deve, assim, haver uma clara definição do que se entende por pesquisa estatística, quem são os possíveis atores que executam este tipo de atividade e quais as finalidades de tais pesquisas.

No mais, o PL 5276/2016 é resultado de uma ampla e frutífera discussão com toda a sociedade brasileira e foi construído de forma colaborativa com engajamento social por meio de duas consultas públicas realizadas no fim do ano de 2010 e começo do ano de 2015, a partir da iniciativa do Ministério de Justiça em colocar o texto do então Anteprojeto de Lei de Proteção de Dados Pessoais sob escrutínio público nas plataformas online culturadigital.br/dadospessoais e pensando.mj.br/dadospessoais.

A forma pela qual o texto foi consolidado mostra que houve consenso entre diversos setores da sociedade, com a busca de uma redação equilibrada.

Tecnicamente considerado, o PL 5.276/16 sistematiza de forma orgânica os conceitos e princípios de dados pessoais, delimitando seu escopo de aplicação e critérios interpretativos necessários para sua aplicação. Há importantes temas tratados, tais como: i) os direitos dos cidadãos de acesso, retificação, correção e oposição ao tratamento de seus dados pessoais; ii) regras que tratam do início ao término do tratamento de dados pessoais e também sobre a responsabilidade civil de toda a cadeia de agentes nela inserida; iii) um capítulo específico para a proteção dos dados pessoais do cidadão frente ao Poder Público; iv) a regulação da transferência internacional dos dados pessoais; v) mecanismos de incentivo para o setor regulado, dedicando um capítulo específico para boas práticas.

Além disso, prevê a criação de um órgão de fiscalização (embora dependa de regulamento) e, dentre os projetos existentes, é o que se mostra capaz de suprir a lacuna no ordenamento jurídico da falta de uma lei específica para o tema, trazendo segurança jurídica para o cidadão, empresários e Administração Pública.

Verifica-se, assim, ainda que em termos breves, a importância e complexidade dos projetos em face do tema — proteção dos dados pessoais — que visa garantir o direito à privacidade, mas vai além, numa verdadeira regulação de direitos constitucionais amplamente considerados. É indiscutível, assim, a importância da existência de uma boa lei sobre proteção aos dados pessoais no Brasil.

Considerações finais a título de conclusão

É inegável que a tecnologia tem sido protagonista de diversas alterações significativas em nossos cotidianos, para o Bem e para o Mal.

Aparatos tecnológicos têm ajudado a salvar vidas, têm tornado nossas vidas mais dinâmicas, encurtado distâncias e criado interações por linguagens que jamais havíamos imaginado, como os “emojis” ou os “memes”. Por outro lado, além de permitir uma vigilância quase desenfreada, ainda propicia diversos tipos de ilícitos.

Mas não se pode matar o mensageiro e culpar a tecnologia pelas situações de risco à nossa privacidade. Melhor que isso é compreender os modelos de negócios

baseados em dados para, assim, poder propor medidas que sejam aptas a proteger os cidadãos.

Quanto a isso, nosso sistema jurídico traz normas inequívocas sobre a existência de um direito à privacidade e à intimidade, embora não haja conceitos legais de ambos. Isto, todavia, não pode significar que não podem e não devem ser imediatamente protegidos dos abusos empresariais e estatais de monitoramento e vigilância derivados do *big data*.

Por todo o exposto, mostra-se mais que necessária uma agenda de conscientização das pessoas quanto à necessidade de resguardarem sua privacidade, além da necessária inovação legislativa para que advenha lei de proteção aos dados pessoais. Afinal, apesar do reconhecimento da existência do direito à privacidade, ele somente poderá ser concretizado no atual estágio social mediante a existência de lei e órgãos de proteção aos dados pessoais.

Referências bibliográficas

a) Artigos e livros:

ALEXY, Robert. **Teoría de los derechos fundamentales**. Tradução Ernesto Garzón Valdés. Madrid: Centro de Estudos Constitucionais, 1993.

CRESPO, Marcelo Xavier de Freitas. **Intimidade e Privacidade em face do Marco Civil (lei nº 12.965/14).** In: ALMEIDA FILHO, José Carlos de Araújo; MEIRELLES, Delton R. S.; PIMENTEL, Fernanda (org.) *Processo e Conexões Humanas*. Petrópolis: 2014.

_____. **Sobre os sites que divulgam dados pessoais: uma análise sob a perspectiva criminal**. Disponível em:<https://canalcienciascriminais.com.br/sobre- os-sites-que-divulgam-dados-pessoais-uma-analise-sob-a-perspectiva-criminal/>. Acesso em: 29 jul. 2015.

_____. **Bitcoin:** breves considerações sobre a criptomoeda. Disponível em: <https://canalcienciascriminais.com.br/bitcoin-breves-consideracoes-sobre-a-criptomoeda/>. Acesso em: 05 ago. 2015.

_____. **Ainda sobre as criptomoedas**: considerações em face do Sistema Financeiro Nacional. Disponível em: <https://canalcienciascriminais.com.br/ainda-sobre-as-criptomoedas-consideracoes-em-face-do-sistema-financeiro-nacional/>. Acesso em: 12 ago. 2015.

_____. **Relações extraconjugais na mira dos crimes digitais:** o caso Ashley Madison. Disponível em: <https://canalcienciascriminais.com.br/relacoes-extraconjugais-na-mira-dos-crimes-digitais-o-caso-ashley-madison/>. Publicado em 19 ago. 2015.

DONEDA, Danilo. **Os direitos da personalidade no Código Civil.** A parte geral do

novo código civil: estudos na perspectiva civil-constitucional. Coord. Gustavo Tepedino. 2.ed. Rio de Janeiro: Renovar, 2003.

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

_____. **Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais**. In: *Âmbito Jurídico*, Rio Grande, 51, 31/03/2008. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_ leitura&artigo_id=2460>. Acesso em: 10 mar. 2009.

DOTTI, René Ariel. A liberdade e o direito à intimidade. Senado Federal. **Revista de informação legislativa.** Brasília, Ano 17, n. 66, 1980.

FERRAZ JÚNIOR, Tércio Sampaio. Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado. **Revista dos Tribunais**, Cadernos de Direito Constitucional e Ciência Política. São Paulo, ano 1, pp. 77-90, 1992.

RODOTÀ, Stefano**. A vida na sociedade da vigilância: a privacidade hoje**. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

SARMENTO E CASTRO, Catarina. **Direito da informática, privacidade e dados pessoais:** A propósito da legalização de tratamentos de dados pessoais (incluindo vídeo vigilância, telecomunicações e Internet) por entidades públicas e por entidades privadas, e da sua comunicação e acesso. Coimbra: Almedina, 2005.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela**. 2. ed. São Paulo: Editora Revista dos Tribunais, 2005.

b) Reportagens:

Instagrammers discover front-page NYT placement by chance. Disponível em: <https://www.poynter.org/news/instagrammers-discover-front-page-nyt- placement-chance>.

Instagram muda termos de serviço e quer usar suas fotos para ganhar dinheiro. Disponível em: <https://www.poynter.org/news/instagrammers-discover-front-page-nyt-placement-chance>.

Instagram desiste de reformular seus termos de serviço. Disponível em: <https://www.tecmundo.com.br/instagram/34456-instagram-desiste-de- reformular-seus-termos-de-servico.htm>.

How One Woman Hid Her Pregnancy From Big Data. Disponível em <http://mashable.com/2014/04/26/big-data-pregnancy/#5wwUCU3si8q7>.
O FBI hackeou mais de 8 mil computadores em 120 países com um único mandado. Disponível em: <https://motherboard.vice.com/pt_br/article/pgzeab/fbi-hackeou-

mais-de-8-mil-computadores-em-120-pases-com-um-unico-mandado>.
O que é 'pós-verdade', a palavra do ano segundo a Universidade de Oxford". Disponível em: <https://www.nexojornal.com.br/expresso/2016/11/16/O-que-%C3%A9-%E2%80%98p%C3%B3s-verdade%E2%80%99-a-palavra-do-ano-segundo-a-Universidade-de-Oxford>.

Suprema Corte dos EUA autoriza FBI a hackear qualquer computador anônimo. Disponível em: <http://meiobit.com/342817/suprema-corte-eua-autoriza-fbi-investigar-qualquer-computador-conectado-com-ip-desconhecido-tor-vpns- principais-alvos-usuarios-em-todo-mundo-podem-ser-afetados/>.