A REGULAMENTAÇÃO DA COLETA DE DADOS: OS ATUAIS MODELOS DE PROTEÇÃO DE DADOS NO MUNDO E A LGPD

Luisa Ferreira Gonzalez Penna
Advogada associada ao escritório Montaury Pimenta Machado & Vieira de Mello.
E-mail: luisa.penna@montaury.com.br

Sumário: 1. Introdução - 2. Novas tecnologias - 3. A importância das novas tecnologias e dos dados para o mundo contemporâneo - 4. A coleta de dados e o direito à privacidade - 5. A regulamentação da coleta de dados - 6. O sistema europeu de proteção de dados - 7. O sistema americano de proteção de dados - 8. O sistema brasileiro de proteção de dados - a LGPD - 9. Conclusão - Referência bibliográficas

1. Introdução

Ante o crescimento exponencial da produção de dados na rede, haja vista a transposição da maioria das relações e interações humanas para o mundo digital, há de se notar que os dados vieram a representar nas últimas décadas um valioso bem, muito cobiçado por agentes privados, assim como por governos.

Isso porque, a coleta de dados possibilita não apenas a identificação e interpretação de certas informações, mas também a recombinação de informações que, por meio de algoritmos derivados das novas tecnologias, permitem o conhecimento a respeito da dinâmica do inconsciente individual.

Dessa forma, o conhecimento sobre gostos, interesses, costumes e hábitos dos indivíduos se tornou muito relevante, principalmente ao mercado que pode, a partir dos dados coletados e das informações – e recombinações de informações – por eles extraídas, estimular, ou até mesmo direcionar comportamentos de modo a maximizar o consumo.

Ocorre que, a coleta de dados, além de um importante ativo para as sociedades empresárias, passou a representar também uma verdadeira ameaça ao direito fundamental à privacidade, no sentido em que a existência da disponibilidade de informação pessoal pode gerar a sua exposição e utilização indevida ou mesmo abusiva por terceiros,[1] o que gera uma série de questionamentos para o campo do direito.

Assim, diante da problemática que a coleta intensificada de dados pessoais passou a representar ao direito da privacidade, é que se verificou a necessidade, em escala mundial, de regulamentar a matéria, de modo a permitir o uso das novas tecnologias, porém com a preservação de direitos fundamentais.

Nesse sentido, o presente artigo busca analisar os principais modelos de proteção de dados em vigência no mundo, abordando-se o sistema europeu de proteção de dados e o sistema americano de proteção de dados. Ainda, se irá analisar o sistema brasileiro de proteção de dados, com a recente incorporação no ordenamento jurídico brasileiro da Lei nº 13.709/2018, denominada Lei Geral de Proteção de Dados - LGPD.

1. DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais. em. In MARTINS, Guilherme Magalhães (Org.). *Direito Privado e Internet*. São Paulo: Editora Atlas, p. 61, 2014.

2. Novas tecnologias

Antes de adentrar especificamente na análise sobre os atuais e principais modelos de proteção de dados no mundo, é necessário fazer uma breve contextualização a respeito do que são as denominadas "novas tecnologias", a importância da coleta de dados pessoais na denominada economia informacional, bem como quais os principais problemas que podem advir do seu uso.

A definição tradicional do termo "tecnologia" engloba o conhecimento técnico e científico e a aplicação deste conhecimento através de sua transformação no uso de ferramentas, processos e materiais criados e utilizados a partir de tal conhecimento.

No que tange especificamente as ditas "novas tecnologias", presentes desde o final do século 20, deve-se ter em mente que estas são produtos do surgimento da internet ou da rede,[2] que, em definição técnica, consiste em uma "rede aberta decorrente da conexão de várias redes entre si, perfazendo-se a comunicação por meio de um conjunto de protocolos denominados Transmission Control Protocol/Internet Protocol - TCP/IP".[3 e 4]

A internet foi primeiramente concebida após a Segunda Guerra Mundial, de início denominada "ARPANET", para posteriormente se transformar em "World Wide Web", presente até os dias de hoje.

Devido ao momento vivido quando foi concebida, a internet devia ter como característica principal uma arquitetura descentralizada. Usada primeiramente para fins militares, era essencial que não houvesse um centro de controle ou computador central para a troca de informações, visto que a descentralização possibilita a preservação dos demais e, assim, possibilita a manutenção da troca de informações.[5]

Além disso, a internet também incentiva a troca contínua de informações entre os usuários da rede, permitindo que o usuário seja tanto receptor de informações como criador delas.[6]

3. A importância das novas tecnologias e dos dados para o mundo contemporâneo

Como já mencionado, a rede, em seus primórdios, tinha como finalidade principal o auxílio em operações militares. Em seguida, passou a ser usada para fins educacionais e depois para auxiliar no aumento da produtividade na era da economia industrial.

Ocorre que, a partir da década de 1990, se percebeu uma nova finalidade para a rede. Percebeu-se que a contínua troca de informações, por meio da internet passou a produzir um conglomerado de dados, os quais constituem hoje um dos maiores ativos no mercado, deixando de ser apenas um fator auxiliar na produtividade da era da economia industrial, para se tornar, a partir da década de 1990, um produto por si só.[7]

Tais dados passaram a ser de extrema valia, principalmente para agentes privados, que viram nos dados uma forma de maximização de sua produção e de consumo e, mais adiante, uma forma de manipulação de hábitos e costumes. Com a crescente produção de dados e o igualmente crescente interesse de agentes privados – e de governos – nos dados gerados, é que se deu início à denominada era da economia informacional, já propriamente consolidada nos dias de hoje.

A denominada economia informacional ou economia da informação é um termo que passou a ser usado a partir da década de 1970 para denominar a crescente e exponencial importância que as informações – de todos os tipos – passaram a desempenhar junto ao mercado, auxiliando nos meios de controle de produção e melhorando a produtividade.[8]

Com o passar dos anos, mais precisamente entre as décadas de 1970-1990, a informação deixou de ser um mero fator de auxílio na produtividade para assumir um papel mais central na economia, estando a informação mais acessível e em maior número.

Com a facilidade de acesso e o denominado "dilúvio de informações",[9] a informação passou a invocar uma verdadeira transformação das sociedades empresárias e suas hierarquias, visto que agora estas possuíam novos meios de comunicação e recursos para a obtenção de informações a respeito do público consumidor.

Recursos como os de obtenção de informações a respeito da correlação entre mulheres de determinada idade e localização e as suas preferências a determinado estilo literário, os quais podem ser facilmente obtidos por meio dos dados inseridos e coletados pela rede, permitem a visualização pelo mercado a respeito de uma determinada demanda, a qual será direcionada o seu produto ou serviço.

2. Manuel CASTELLS, ao tratar do surgimento da internet, afirma que esta se trata de uma rede que não é passível de controle a partir de nenhum centro, sendo composta por milhares de redes autônomas e com inúmeras maneiras de conexão. CASTELLS, Manuel. A sociedade em rede. Tradução de Roneide Venancio Majer, 18ª ed. São Paulo: Paz e Terra, p. 65, 2017.
3. MARTINS, Guilherme Magalhães. Responsabilidade civil por acidente de consumo na internet. São Paulo: Ed. RT, p. 30, 2008.
4. O Marco Civil da Internet, Lei nº 12.965/2014 apresentou em seu art. 5º, inciso I, uma definição semelhante, afirmando-se internet como "um sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes".
5. FILHO, Eduardo Tomasevicius. O Marco Civil da Internet e a Liberdade de Mercado. In LUCCA, Newton; FILHO, Adalberto Simao; LIMA, Cintia Rosa Pereira (Org.). *Direito & Internet III, Tomo II: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, p. 49.
6. FORGIONI, Paula A; MIURA, Maira Yuriko Rocha. O Princípio da Neutralidade e o Marco Civil da Internet no Brasil. In LUCCA, Newton; FILHO, Adalberto Simao; LIMA, Cintia Rosa Pereira (Org.). *Direito & Internet III, Tomo II: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, p. 111.
7. CASTELLS, Manuel. A sociedade em rede. 18ª ed. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, p. 135, 2017.
8. BENKLER, Yochai. The Wealth of Networks: How Social Production Transforms Markets and Freedom. Yale University Press, p. 31, 2006.
9. O filósofo Pierre LÉVY identifica o aumento exponencial de dados no chamado "dilúvio de informações", na qual se tem a proliferação do trânsito de informações e uma consequente "inundação" de dados de forma exponencial e anárquica. LÉVY, Pierre. Cibercultura. 3ª ed. Tradução de Carlos Irineu da Costa, São Paulo: Editora 34, p. 13-15, 2011.

Assim é que na sociedade informacional – derivada da economia da informação – a produção de mercadorias e o oferecimento de serviços advêm quase que majoritariamente da coleta e análise de dados obtidos pela rede.

Dessa forma, a rede com sua capacidade de coletar dados de forma exponencial deu início à uma nova revolução industrial, com o surgimento de um quarto setor informacional em um ambiente que era anteriormente marcado pelos setores da agropecuária, indústria e serviços.

Um exemplo da capacidade de monetização dos dados são os reiterados escândalos que cada vez mais vem à tona a respeito do vazamento[10] ou, em alguns casos, a própria venda de dados sem consentimento dos consumidores/usuários,[11] que diversas gigantes do mercado vêm sofrendo ou praticando.

4. A coleta de dados e o direito à privacidade

Ante o interesse e a valorização dos dados pessoais, bem como dos diversos casos de vazamento e/ou venda de dados pessoais, é que passou a se perceber que a incessante coleta, tratamento e o armazenamento de dados pode representar uma ameaça ao direito fundamental da privacidade previsto no ordenamento jurídico brasileiro como um direito fundamental.[12]

A violação ao direito à privacidade se verifica não só na venda ou vazamento de dados, mas também na retenção indevida de dados pessoais para finalidades e utilidades injustificáveis.

Basta analisar, por exemplo, algumas políticas e termos de uso de provedores de aplicação. Muitos deles requerem acesso e permissão para a coleta de dados e informações para muito além do que seria razoável dado a finalidade e utilidade daquele dispositivo. Assim, questiona-se a real intenção dessa coleta maciça de dados.

Situações como o do Facebook, que veio à tona em 2018,[13] demonstram os riscos decorrentes do uso indevido de dados pessoais. No caso, a empresa foi acusada de comercializar dados pessoais coletados pelo aplicativo à empresa Cambridge Analytica – sociedade especializada em pesquisas eleitorais – com o intuito de manipular e influenciar as últimas eleições americanas.

Diante deste acontecimento, constatou-se as consequências que a coleta, tratamento e armazenamento de dados pessoais podem causar aos indivíduos, bem como às empresas, tendo em vista a grande perda tanto financeira como de prestígio das partes envolvidas.

Dessa forma, verifica-se que a coleta, tratamento e armazenamento de dados pessoais pode ocasionar uma violação coletiva de direitos fundamentais, como o direito à privacidade, além de notáveis prejuízos para os agentes privados.[14]

Foi à vista de tais problemas decorrentes da coleta de dados pessoais que se verificou a necessidade de regulamentar a matéria, com diversos ordenamentos jurídicos do mundo normatizando o assunto, sendo inclusive o respeito à privacidade um dos fundamentos da LGPD, recente lei brasileira que dispõe sobre a proteção de dados no Brasil.[15]

5. A regulamentação da coleta de dados

Como visto, o conflito entre a coleta de dados pessoais e a proteção do direito à privacidade se tornou uma tendência na atual sociedade.

10. A famosa empresa americana Yahoo já foi vítima de um dos maiores casos de vazamento de dados da história http://g1.globo.com/tecnologia/noticia/2016/09/yahoo-anuncia-vazamento-de-dados-que-atinge-500-milhoes-de-usuarios.html.
11. Recentemente a C&A passou por um escândalo a respeito da venda de dados de seus clientes: https://www.tecmundo.com.br/seguranca/122281-exclusivo-lojas-c-vendem-dados-clientes-r-50-internet.htm
12. Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
(...) X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.
13. *How Trump Consultants Exploited the Facebook Data of Millions*. Matthew Rosenberg, Nicholas Confessore and Carole Cadwalladr. Publicado em 17 de março de 2018 pelo jornal *The New York Times*. Disponível em https://www.nytimes.com/2018/03/17/us/politics/cambridge-analytica-trump-campaign.html. Acesso em 23 de janeiro de 2019.
14. No caso Cambridge Analytica, as multas aplicadas ao Facebook já chegam na ordem dos 10 milhões de euros. Itália multa Facebook em €10 milhões por vender dados de usuários https://g1.globo.com/economia/tecnologia/noticia/2018/12/10/italia-multa-facebook-em-euro-10-milhoes-por-vender-dados-de-usuarios.ghtml. Acesso em 23 de janeiro de 2019.
15. Art. 2º, inciso I da Lei nº 13.709/2018.

Dito isso, é que começaram a surgir propostas de regulamentação do uso das novas tecnologias no sentido de promover a proteção de dados e, por conseguinte, de proteger o direito fundamental à privacidade.

Contudo, antes mesmo de adentrar as diversas propostas e sistemas de regulamentação de coleta de dados pessoais, deve-se deixar claro que a regulamentação é necessária, sendo ela o único caminho para que a sociedade possa fazer o uso das novas tecnologias e dos meios de produção, em geral, sem que se instaure uma ordem de insegurança jurídica e violação de direitos fundamentais e liberdade.

Dessa forma, passa-se agora a análise das respostas legislativas escolhidas por diversos países no sentido de regulamentar tal situação, respostas essas que serviram para influenciar e inspirar a regulamentação brasileira sobre proteção de dados, com a recente edição da Lei nº 13.709/2018, a LGPD.

6. O sistema europeu de proteção de dados

As primeiras iniciativas legislativas versando sobre os limites a serem impostos à utilização das novas tecnologias surgiram a partir da década de 1970. Desde então, as leis sobre proteção de dados passaram por uma grande evolução, tendo o professor Viktor Mayer-Schönberger identificado quatro gerações de leis.[16]

Pois bem. Apesar de desde a década de 1970 já existirem leis tratando a respeito da proteção de dados, foi a partir da década de 1980 que se iniciou de fato uma tradição de leis e normas mais vigorosas quanto à proteção de dados e privacidade.

A Convenção nº 108 do Conselho Europeu de 1981, a chamada Convenção de Estrasburgo, foi muito positiva visto que foi a pioneira a introduzir normas a respeito da proteção de dados, tendo se proposto a definir conceitos, estabelecer regras e prever direitos dos titulares dos dados gerados. Tal Convenção estimulou a proliferação de iniciativas normativas para um modelo robusto de tutela, tendo se tornado referência no mundo todo.[17]

Dado a peculiaridade do velho continente e do seu sistema normativo, o modelo europeu de proteção de dados era composto por diretivas, regulamentos, decisões vinculantes e orientações de diversos níveis hierárquicos, com uma multiplicidade de meios regulamentadores, que partiam sempre de orientações gerais e estabeleciam normas cada vez mais específicas sobre os limites de coleta, tratamento e armazenamento de dados.

Até maio de 2018, a Diretiva 95/46/CE era o principal texto regulamentador dentro do sistema europeu de proteção de dados. A referida Diretiva traduziu os principais conceitos no campo da proteção dos dados na União Europeia – como o conceito de dados pessoais – assim como estabeleceu uma série de princípios a serem observados sobre a matéria.

A Diretiva ainda previu certos direitos básicos dos titulares dos dados tratados, assim como estabeleceu regras para as operações de transferência internacional de dados.

Ainda, de modo a garantir que as suas medidas fossem observadas, a Diretiva previu que os Estados-membros deveriam estabelecer "autoridades públicas responsáveis pela fiscalização da aplicação no seu território das disposições adotadas pelos Estados-membros nos termos da presente diretiva".[18] Quanto às autoridades públicas fiscalizadoras, se entendeu que estas deveriam exercer com total independência as funções que lhes forem atribuídas.

Além da Diretiva 95/46/CE, outras diretivas, que visavam a sua complementação, foram também criadas de modo a expandir o alcance e a aplicação das normas e princípios previstos na Diretiva 95/46/CE para outras áreas de controle antes não abrangidas pelo sistema.

Cita-se a Diretiva 2002/58/CE12, do Parlamento Europeu e do Conselho Europeu, a respeito do tratamento de dados pessoais e a proteção da privacidade no setor das comunicações eletrônicas. Por se tratar de uma norma destinada a tratar um segmento específico, ela trouxe consigo medidas mais específicas, como a guarda de dados de conexão para fins de faturamento dos serviços de conexão prestados, a utilização de dados pessoais em listagens públicas (como listas telefônicas) e a utilização dos denominados *cookies*.[19]

16. A respeito das gerações identificadas por Mayer-Scönberger, cumpre mencionar que a primeira geração de diplomas legais tratando sobre proteção de dados se iniciou em 1970 e se caracterizou pelo fato de que as referidas leis refletiam o estado da tecnologia e a visão dos juristas no início da evolução dos computadores. Danilo DONEDA exemplifica essa primeira geração de leis com a Lei de Hesse alemã e o *Privacy Act* norte-americano, de 1974. Diante da falta de previsibilidade e da ausência de experiência no tratamento dessas tecnologias, essas primeiras leis possuíam um caráter de proteção mais abstrato e geral, algo que inviabilizou uma proteção de dados mais efetiva. A segunda geração se iniciou no final da década de 1970, sendo essa geração caracterizada pela estruturação a partir do entendimento da privacidade como uma liberdade negativa, sem o enfoque no fenômeno computacional em si. A terceira geração se deu na década de 1980 e foi marcada pela preocupação com a efetividade da proteção da privacidade e com uma participação mais ativa do indivíduo, prevendo-se, portanto, uma proteção um pouco mais robusta quanto ao direito à privacidade. Já a quarta geração é a geração de leis mais atuais, nas quais se entende a proteção à privacidade não mais com um enfoque individualista, mas sim de forma coletiva, com a previsão de instrumentos que permitam uma proteção coletiva da privacidade e dos dados. Outra importante inovação vista na quarta geração de leis é a previsão de autoridades independentes que tenham como finalidade a fiscalização e a garantia da proteção de dados, levando em consideração o não equilíbrio entre o sujeito em relação às sociedades empresárias e o Estado, principais interessados na coleta de dados. DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais. In MARTINS, Guilherme Magalhães. (Org.). *Direito Privado e Internet.* São Paulo: Editora Atlas, p. 66-69, 2014.
17. GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. p. 4. Disponível em https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em 17 de maio de 2018.
18. Art. 28º, 1. Da Diretiva 95/46/CE.
19. *Cookies* são arquivos de texto muito simples, cuja composição depende diretamente do conteúdo do endereço *web* visitado. Por exemplo, a maioria dos *sites* armazenam informações básica, como endereços IP e preferências de idioma cores e senhas. "O que são *cookies*?" Por Gabriel Gugik. Disponível em https://m.tecmundo.com.br/web/1069-o-que-sao-cookies-.htm. Acesso em 18 de maio de 2018.

Apesar das Diretivas acima citadas, as mesmas deixaram de ser o principal texto normativo europeu sobre proteção de dados, visto que em 25 de maio de 2018, passou a vigorar o General Data Protection Regulation, o GDPR (Regulamento 2016/679 do Parlamento Europeu e do Conselho).

O GDPR, idealizado desde 2010 e aprovado em 2016, é a mais completa regulamentação sobre proteção de dados pessoais em vigor na Europa. Com eficácia para todos os dados de cidadãos europeus, manuseados dentro ou fora da União Europeia, sua importância se dá tendo em vista ter esse texto apresentado expressivas alterações em relação à Diretiva 45/96/CE.

O novo regulamento geral sobre proteção de dados se destaca pelo fato de que trouxe previsões que buscam reforçar os direitos dos usuários, as competências das autoridades de proteção de dados, assim como busca incentivar – e também desestimular, por meio de pesadas sanções, principalmente econômicas[20] – certos comportamentos por parte dos responsáveis pela coleta e tratamento de dados.

Além disso, com o GDPR, as sociedades empresárias agora têm uma série de novas atribuições e passam a atuar de forma preventiva no assunto. Pode-se citar medidas como a obrigatoriedade de nomeação de um encarregado de proteção de dados (Data Protection Officer - DPO); a realização de auditorias internas; a elaboração de uma política de tratamento de dados pessoais; a criação de procedimentos que garantam a proteção dos dados pessoais; a elaboração de comunicados sobre privacidade; a preparação de procedimentos de resposta a solicitações dos titulares dos dados e a manutenção da documentação apropriada como evidência de todo o processo.[21]

Em vigor desde maio de 2018, o GDPR já vem sendo aplicado, produzindo seus plenos efeitos, o que resultou em uma maior atenção sobre a proteção de dados pessoais. Várias empresas já sofreram com a aplicação das sanções previstas pelo GDPR, podendo-se citar aqui a multa de 50 milhões de euros aplicada à Google por um Tribunal francês,[22] ou mesmo a multa aplicada ao aplicativo de namoro alemão Knuddels,[23] tendo lhe sido aplicada uma multa menor, de 20 mil euros.

Sobre a diferença entre as multas aplicadas para a Google e para a Knuddels, é importante destacar que multa muito menor fora aplicada à empresa alemã tendo em vista que esta cumpriu com as obrigações exigidas pelo GDPR para conter os danos advindos do vazamento de dados.

O fato de a Knuddels ter cumprido com a obrigação de notificar a autoridade fiscalizadora e os usuários afetados dentro do prazo de 72 horas[24] de quando tomou conhecimento do vazamento, bem como a sua transparência em lidar com o assunto, tendo adotado medidas de reforço de segurança dos dados, foram fatores considerados no momento de aplicação da multa.

Assim, verifica-se que a Europa, pioneira na regulamentação da coleta e uso de dados pessoais, passou, com a aprovação e vigência do GDPR, a contar com um sistema muito mais aprimorado e completo, o qual já está provocando mudanças quanto à coleta e o uso de dados pessoais por agentes privados.

7. O sistema americano de proteção de dados

Já com relação ao sistema norte-americano de proteção de dados, cumpre mencionar, desde logo, que este muito se distingue do sistema europeu.

20. O GDPR, visando dar maior eficácia à adoção das medidas que estabelece, determinou sanções econômicas às sociedades empresárias que descumprirem com as suas normas, impondo multas que podem alcançar o patamar de 4% sobre a faturamento anual global das sociedades empresárias ou o valor de fixo de € 20.000.000,00, dependendo do qual for maior.
21. LEMOALLE, Edouard; CARBONI, Guilherme. Lei Europeia de Proteção de Dados Pessoais - GDPR e seus efeitos no Brasil. Disponível em https://www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais. Acesso em 19 de maio de 2018.
22. OLIVEIRA, Jaqueline Simas de. *Google é multado em 50 milhões de euros na França por violação ao GDPR*. Disponível em https://www.jota.info/opiniao-e-analise/artigos/google-e-multado-em-50-milhoes-de-euros-na-franca-por-violacao-ao-gdpr-24012019. Acesso em 8 de julho de 2019.
23. MANANCOURT. Vincent. *German watchdog issues first GDPR fine*. Disponível em: https://globaldatareview.com/article/1177149/german-watchdog-issues-first-gdpr-fine. Acesso em 8 de julho de 2019.
24. Artigo 33º, 1 do Regulamento 2016/679 do Parlamento Europeu e do Conselho - GDPR.

O modelo norte-americano de regulação é extremamente diferente do modelo europeu tendo em vista ser os Estado Unidos um país caracterizado pela adoção de um modelo federalista muito forte, com alto nível de descentralização. Devido à essa característica de descentralização é que não há nos Estados Unidos – ainda – uma legislação federal específica que regulamente a proteção de dados de forma geral e abrangente.[25]

No entanto, não se pode afirmar que os americanos não possuem qualquer legislação sobre proteção de dados. Isso porque, no ordenamento jurídico norte-americano existem inúmeras leis federais setoriais que tangenciam o tema da proteção de dados, contudo dentro de um setor específico, como o de telecomunicações, financeiro, saúde, entre outros.

Como exemplos de leis setoriais sobre proteção de dados pode-se citar o Privacy Act[26] de 1974, Children`s Online Privacy Protection Act[267] de 1998, Health Insurance Portability and Accountability Act[28] de 1996 e o The Financial Services Modernization Act [29] de 1914, que atendem à necessidade de proteção de dados dentro dos seus respectivos setores.

Importante mencionar também que alguns estados americanos já estão adotando leis próprias para a proteção de dados pessoais, como a recente aprovação da The California Consumer Privacy Act of 2018,[30] lei estadual que estabelece direitos dos usuários sobre os seus dados, bem como obrigações das empresas que coletam dados.

Para citar algumas das importantes disposições desta lei, tem-se a previsão do direito dos usuários à exclusão de seus dados e a recusa a venda de seus dados a terceiros. A lei, no entanto, entrará em vigor em 2020.

Dessa forma, o modelo americano de proteção de dados é caracterizado pela existência de leis específicas e setoriais, e assim se diferencia do modelo europeu segundo o qual vigora um modelo de adoção de uma lei geral para o assunto, a ser observado por todos os setores, como ocorreu com a Diretiva 95/46/CE e, agora, com o GDPR.

No entanto, diante da crescente importância que a proteção de dados pessoais passou a representar no mundo contemporâneo, é que cada vez mais os americanos estão vislumbrando a necessidade de uma lei geral sobre o assunto, válida em todos os Estados americanos, de forma a assegurar uma regulamentação mais abrangente e a qual possa garantir maior segurança jurídica para todas as atividades que envolvem a coleta e uso de dados pessoais, em todos os Estados.

O governo americano de Trump já anunciou que está trabalhando em uma potencial lei geral para regulamentar a proteção de dados pessoais no país, tendo, supostamente já consultado empresas como o Facebook, Google, AT&T e outras.[31]

Esse movimento é endossado por representantes de gigantes no mercado de tecnologia, que vêm se posicionando no sentido ser necessária a edição de uma lei federal para regulamentar a matéria,[32] com a previsão expressa de hipóteses nas quais a coleta de dados é autorizada, e medidas de segurança a serem adotadas para o exercício dessa atividade, de modo a evitar violações à privacidade.

Algumas iniciativas legislativas já estão em trâmite, como a proposta preliminar do Consumer Data Protection, apresentado pelo senador Ron Wyden,[33] que busca estabelecer regras e responsabilidades para empresas – inclusive criminais para os seus executivos – com faturamento superior a 50 milhões de dólares e com mais de 1 milhão de usuários.

Não se trata propriamente de um projeto de lei geral de proteção de dados, vez que não estabelece princípios gerais e regras a serem observadas sobre coleta e uso de dados pessoais.

De todo modo, para citar algumas das questões que esse projeto preliminar de *bill* visa regular, se encontram previsões a respeito da obrigatoriedade de empresas oferecerem um relatório anual ao Federal Trade Comission - FTC[34] – sobre as práticas adotadas para a proteção de dados pessoais, bem como a consolidação do FTC como entidade responsável pela fiscalização e punição de infrações à privacidade dos usuários, ampliando os seus poderes.

Outra proposta legislativa é Data Care Act of 2018,[35] apresentada pelo senador Brian Schatz em coautoria de outros 14 senadores. Esse projeto de lei tem como objetivo introduzir métodos padronizados a serem observados na coleta e uso de dados, exigindo que todos os profissionais de tecnologia protejam as informações do usuário. Também não se trata de uma lei geral sobre proteção de

25. GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. p. 10. Disponível em https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em 17 de maio de 2018.
26. É a lei federal vigente que estabelece os princípios e regras para a coleta, armazenamento, uso e comunicação de dados pessoais em atividades estatais conduzidas pelas agências federais.
27. Cria salvaguardas para a interação de crianças com menos de 13 (treze) anos com a internet em geral e no que diz respeito a sua privacidade.
28. Lei federal que trata da privacidade e proteção de dados médicos. A referida lei traz disposições padrões de segurança, física e técnica, para dados relacionados à saúde em formato eletrônico; a obrigação de notificar os titulares dos dados, e muitas vezes à Secretaria de Saúde e à mídia local no caso de vazamento ou violações de dados pessoais.
29. Esta lei federal visa regular a coleta, uso e divulgação de informações financeiras. É aplicável a instituições como bancos, corretoras e seguradoras. Essa lei também limita a divulgação de informações pessoais não públicas e, em alguns casos, exige que as instituições financeiras notifiquem suas práticas de privacidade e concedam aos titulares dos dados a optar por não compartilhar suas informações pessoais.
30. Texto disponível em https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375. Acesso em 23 de janeiro de 2019.
31. *White House reportedly working on federal data privacy policy*. Disponível em https://www.engadget.com/2018/07/27/white-house-federal-data-privacy-policy/
32. O CEO da Apple, Tim Cook, defendeu esse posicionamento no discurso proferido no evento 40th International Conference of Data Protection and Privacy Commissioners - ICDPPC, em 24 de outubro de 2018.
33. Texto disponível em https://assets.documentcloud.org/documents/5026543/Wyden-Privacy-Bill.pdf. Acesso em 24 de janeiro de 2019.
34. O FTC, criado em 1914, é o órgão independente do governo responsável pela proteção do consumidor e a eliminação e prevenção de práticas comerciais desleais e enganosas.
35. Texto disponível em https://www.schatz.senate.gov/imo/media/doc/Data%20Care%20Act%20of%202018.pdf. Acesso em 24 de janeiro de 2018.

dados nos termos do GDPR, mas visa prever certas medidas mais protetivas à privacidade dos usuários.

A respeito do estabelecimento de autoridades fiscalizadoras para garantir a proteção de dados, se verifica que o sistema norte-americano ainda não estabeleceu uma autoridade fiscalizadora específica para a proteção de dados. O que se tem hoje são órgãos já existentes e não exclusivos do governo que atuam como agências reguladoras, sendo responsáveis pelo cumprimento das leis vigentes, igualmente separados por setores econômicos, de modo que sua atuação não é necessariamente homogênea.[36]

Nesse ponto, cumpre destacar ainda que a FTC vem sendo, até o momento, a principal agência responsável pela punição de vazamento de dados/venda de dados pessoais.

Visto estes dois modelos de proteção de dados muito distintos, passa-se agora à análise do modelo adotado pelo Brasil, o qual muito se assemelha com o modelo europeu.

8. O sistema brasileiro de proteção de dados - a LGPD

Tratando especificamente do Brasil, é importante notar que até muito pouco tempo atrás, o País carecia de uma lei geral sobre proteção de dados, apesar de já há muito tempo este tema estar em discussão.

Antes da promulgação da LGPD – lei promulgada em 14 de agosto de 2018 – o País já contava com uma série de dispositivos legais que tangeciavam a proteção do direito à privacidade relacionada à coleta de dados pessoais, como a própria Constituição Federativa da República de 1988, o Marco Civil da Internet, o Código de Defesa do Consumidor, a Lei de Acesso à Informação, Lei do Cadastro Positivo,[37] entre outros diplomas normativos.

Apesar dos diplomas legais acima citados, a matéria ainda necessitava de uma regulamentação mais ampla e detalhada, a qual pudesse disciplinar, expressamente, as hipóteses em que é permitida a coleta de dados, o regramento para tratamento de dados pessoais, as medidas de segurança a serem adotadas, bem como o estabelecimento de sanções para coibir violações ao novo regulamento.

Assim, após o trâmite de diversos projetos de lei sobre o assunto no Congresso Nacional[38] nos últimos anos, o Projeto de Lei nº 4.060/2012, originado na Câmara dos Deputados, foi aprovado no início de 2018, tendo o presidente à época, Michel Temer, sancionado a nova lei, Lei nº13.709/2018.

Da leitura do texto da Lei nº 13.709/2018, é possível perceber que esta sofreu muita influência do GDPR. Assim como o GDPR, a LGPD define o que são dados pessoais;[39] positiva princípios a serem observadas no tratamento de dados pessoais;[40] prevê as diversas situações em que a coleta de dados é autorizada;[41] estabelece direitos dos titulares de dados;[42] estabelece a figura do "encarregado pelo tratamento de dados pessoais",[43] assim como prevê sanções pesadas para o descumprimento de suas disposições.[44] Ainda, é importante mencionar que a lei é aplicável tanto a agentes privados como públicos, bem como dispõe sobre a coleta e armazenamento de dados realizada tanto na rede como fora dela.

Além disso, a LGPD regulamenta também situações mais específicas de coleta de dados, como a coleta de dados de crianças e adolescentes,[45] assim como dá um tratamento diferenciado para a coleta de dados sensíveis.[46]

Dessa forma, verifica-se que a LGPD, assim como o GDPR, buscou ser a principal fonte regulamentadora sobre proteção de dados pessoais no País, abrangendo todas as atividades de coleta de dados – *online* e *offline*, tanto pelo poder público como por agentes privados – se distinguindo do sistema americano, no qual ainda não há uma lei geral sobre o assunto, apenas leis setoriais.

A respeito da instituição de uma autoridade garantidora da observância das normas sobre proteção de dados, há de se destacar que esta fora inicialmente vetada pelo presidente Michel Temer, por vício de iniciativa na propositura da matéria. No entanto, no final de 2018, foi publicada a Medida Provisória nº 869, a qual instituiu a Autoridade Nacional de Proteção de Dados - ANPD.

Sobre a ANPD cumpre mecionar que esta trata-se de órgão vinculado à Presidência, mas com autonomia técnica, tendo lhe sido conferida uma série de atribuições para a fiscalização e efetivação das obrigações e direitos estabelecidos pela LGPD.

Quanto à escolha da ANPD ser um órgão da administração pública federal, integrante da Presidência da República, mas dotado de "independência técnica", acredita-se que é necessário um certo grau de independência desse órgão para com a Administração, principalmente para garantir a aplicação e adoção das medidas pelo poder público.

36. GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. p. 13. Disponível em https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em 17 de maio de 2018.
37. Lei nº 12.965/2014, Lei nº 8.078/1990, Lei nº 12.527/2011 e Lei nº 12.414/2011, respectivamente.
38. Como os Projetos de Lei nº 330/2013, de iniciativa do Senado Federal, e nº 5.276/2016, de iniciativa do Poder Executivo.
39. "informação relacionada a pessoa natural identificada ou identificável." Art, 5º, inciso I da Lei nº 13.709/2018.
40. Artigo 6º.
41. Artigo 7º.
42. Artigo 17 e seguintes.
43. Artigo 41.
44. Artigo 52.
45. Artigo 14.
46. Artigos 11, 12 e 13. A respeito dos dados sensíveis, cumpre mencionar que estes são definidos pela lei como "dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural".

Contudo, também não deveria ser o órgão desvinculado totalmente da Administração vez que a ausência do Estado pode acarretar na preponderância de interesses de agentes meramente privados, frustrando o objetivo principal da possível lei de proteção de dados, que é a proteção da privacidade sob uma concepção coletiva.

Assim, tem-se que a criação da ANPD foi medida extremamente importante para a instituição de um sistema forte e eficaz de proteção de dados. Isso porque, sem a implementação de uma autoridade fiscalizadora, seria muito provável que as disposiões da LGPD se esvaziassem, frustrando o objetivo da Lei.

9. Conclusão

O presente artigo buscou analisar o surgimento das novas tecnologias e ascendência da sociedade da informação e das suas implicações para o direito fundamental à privacidade.

Isso porque os dados, e, consequentemente, as informações coletadas na rede se tornaram um ativo muito valioso para o mercado atual, assim como para os governos, motivo pelo qual se verificou a sua coleta, tratamento e armazenando de formas abusivas e sem o conhecimento do titular dos dados produzidos, gerando uma prática de violação reiterada de dados e do direito à privacidade dos usuários da rede.

Nesse sentido, é que se observou um movimento da sociedade – e do direito – em buscar soluções para as novas questões que se colocaram. Assim, é que se tornou necessário que os ordenamentos jurídicos, em escala mundial, adotassem medidas regulatórias de proteção de dados, com o intuito de impedir a violação à privacidade de seus indivíduos, motivo pelo qual surgiram diversos diplomas legais estrangeiros os quais buscaram estabelecer meios de proteção contra a coleta abusiva de dados, estabelecendo certas diretrizes a serem observadas, medidas práticas a serem adotadas, assim como a instituição de órgãos fiscalizadores.

Sobre os modelos regulatórios adotados, destacou-se o modelo europeu e o modelo americano. O primeiro, com a introdução da mais nova e relevante norma sobre o tema, o *General Data Protection Regulation* - GDPR o qual já está provocando sérias mudanças no comportamento da maioria das grandes empresas no que tange à coleta e tratamento de dados. A mencionada regulação se mostra ser, em seu texto, um diploma legal bem rígido e sério quanto à proteção de dados de cidadãos europeus, inclusive para além da Europa, resultando numa preocupação e adequação mundial das empresas a esse novo regulamento.

Já o modelo americano se diferencia do modelo europeu por não contar com uma lei geral sobre proteção de dados, apenas com leis setoriais as quais, com a crescente tendência mundial de maior preocupação com a proteção de dados, vêm se mostrando insuficiente.

No que se refere ao modelo adotado pelo do Brasil, como é possível perceber, até 2018 o Brasil contava com um sistema de proteção de dados muito mais semelhante ao sistema americano, contando com uma série de diplomas normativos que abordavam a proteção e dados dentro de um determinado setor.

Com a aprovação da LGPD, no entanto, o Brasil se inclui agora dentro do rol dos países que dispõem de uma lei geral e abrangente, fortalecendo a sua posição no que se refere à proteção de dados pessoais.

Referência bibliográficas

BENKLER, Yochai. *The Wealth of Networks: How Social Production Transforms Markets and Freedom*. Yale University Press, 2006.

CASTELLS, Manuel. A sociedade em rede. 18ª ed. Tradução de Roneide Venancio Majer. São Paulo: Paz e Terra, 2017.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006, 448 p.

DONEDA, Danilo. O Direito Fundamental à Proteção de Dados Pessoais. In MARTINS, Guilherme Magalhães. (Org.). *Direito Privado e Internet.* São Paulo: Editora Atlas, p. 66-69, 2014.

FILHO, Eduardo Tomasevicius. O Marco Civil da Internet e a Liberdade de Mercado. In LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cintia Rosa Pereira (Org.). *Direito & Internet III, Tomo II: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, p. 49-64, 2015.

FORGIONI, Paula A.; MIURA, Maira Yuriko Rocha. O Princípio da Neutralidade e o Marco Civil da Internet no Brasil. In LUCCA, Newton; FILHO, Adalberto Simão; LIMA, Cintia Rosa Pereira (Org.). *Direito & Internet III, Tomo II: Marco Civil da Internet* (Lei nº 12.965/2014). São Paulo: Quartier Latin, p. 109-135, 2015.

GUIDI, Guilherme Berti de Campos. Modelos regulatórios para proteção de dados pessoais. Disponível em https://itsrio.org/wp-content/uploads/2017/03/Guilherme-Guidi-V-revisado.pdf. Acesso em 17 de maio de 2018.

LEMOALLE, Edouard; CARBONI, Guilherme. Lei Europeia de Proteção de Dados Pessoais - GDPR e seus efeitos no Brasil. Publicado em 12 de fevereiro de 2018. Disponível em https://www.jota.info/opiniao-e-analise/artigos/lei-europeia-de-protecao-de-dados-pessoais. Acesso em 19 de maio de 2018.

LEONARDI, Marcel. Tutela e privacidade na Internet. São Paulo: Saraiva, 2011.

LESSIG, Lawrence. C*ode Version 2.0*. New York: Basic Books, 2006, 410 p.???

LÉVY, Pierre. Cibercultura. 3ª ed. Tradução de Carlos Irineu da Costa, São Paulo: Editora 34, 2011.

MARTINS, Guilherme Magalhães. *Responsabilidade civil por acidente de consumo na internet.* São Paulo: *Editora Revista dos Tribunais*, 2014, 448 p.????

RODOTÀ, Stefano. A vida na sociedade de vigilância: a privacidade hoje. Rio de Janeiro: Renovar, 2008, p.???

TENE, Omar; POLONETSKY, Jules. *Privacy in the Age of Big Data: A Time for Big Decisions*. Stanford Law Review, 64 Stan. L. *Rev. Online 63* de fevereiro de 2012.