UNIVERSIDADE FEDERAL DO RIO DE JANEIRO
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS
FACULDADE NACIONAL DE DIREITO

PROTEÇÃO DE DADOS PESSOAIS NAS REDES SOCIAIS

MATHEUS COUTO FERREIRA

Rio de Janeiro
2017 / 1° Semestre

MATHEUS COUTO FERREIRA

PROTEÇÃO DE DADOS PESSOAIS NAS REDES SOCIAIS

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Dr. Guilherme Magalhães Martins.

Rio de Janeiro
2017 / 1° Semestre

CIP - Catalogação na Publicação

Ferreira, Matheus Couto
F383p Proteção de dados pessoais nas redes sociais / Matheus Couto Ferreira. -- Rio de Janeiro, 2017.
68 f.

Orientador: Guilherme Magalhães Martins.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade de Direito, Bacharel em Direito, 2017.

1. Proteção de dados pessoais. 2. Redes sociais. 3. Relação de consumo. I. Martins, Guilherme Magalhães, orient. II. Título.

CDD 341.2738

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a).

MATHEUS COUTO FERREIRA

PROTEÇÃO DE DADOS PESSOAIS NAS REDES SOCIAIS

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Dr. Guilherme Magalhães Martins.

Data da Aprovação: __ / __ / ____.

Banca Examinadora:

_____
Prof. Dr. Guilherme Magalhães Martins

_____
Membro da Banca

_____
Membro da Banca

Rio de Janeiro
2017 / 1° Semestre

AGRADECIMENTOS

Agradeço aos meus pais por todo o apoio que me deram.

Agradeço à minha irmã e meu cunhado pelas conversas que muito contribuíram na minha formação.

Agradeço à toda minha família por estarem sempre me apoiando.

Agradeço à todos os meus amigos por alegrarem até mesmo os meus dias mais difíceis.

Agradeço à todos os professores da minha querida Faculdade Nacional de Direito pela sabedoria e valores que compartilharam.

Agradeço, em especial, ao meu orientador Guilherme Magalhães Martins por sua dedicação e apoio no desenvolvimento deste trabalho.

RESUMO

O objetivo principal deste trabalho é analisar a proteção de dados pessoais nas redes sociais através da definição dos principais conceitos envolvidos no tema, bem como da análise da relação de consumo que existe entre o usuário e a rede social. Serão expostos os momentos em que, durante a utilização das redes sociais, surgem riscos para os dados e os princípios que precisam ser respeitados para garantir a efetiva proteção, destacando a dificuldade que o usuário possui em verificar se os mesmos estão sendo cumpridos. Ao fim, serão listados métodos que podem ser utilizados para garantir a proteção, debatendo-se as controvérsias e a real eficácia dos mesmos.

Palavras-chaves: proteção de dados pessoais; redes sociais; relação de consumo.

ABSTRACT

The main objective of this study is to analyze the protection of personal data in social networks through the definition of the main concepts involved in the theme, as well as to analyze the consumer relationship that exists between the user and the social network. It will be exposed the moments in which, during the use of social networks, risks that compromise the security of the data arise and principles that needs to be respected to ensure the effective protection, highlighting the difficulty that the user has in verifying that the data protection is being respected. Finally, methods that can be applied to guarantee this protection will be listed, debating the controversies and their real effectiveness.

Keywords: personal data protection; social networks; consumer relationship.

SUMÁRIO

INTRODUÇÃO

A presente monografia tem o objetivo de analisar os principais conceitos relacionados a proteção de dados pessoais, comprovar a importância de preservar o direito à privacidade dos usuários das redes sociais, além de estudar os principais meios que podem ser utilizados para atingir esta proteção. Desta forma, é visado a exploração de um tema de suma validade para uma sociedade que vive em uma era informatizada onde a velocidade em que informações são obtidas e transmitidas não tem precedentes, demonstrando a importância do Direito se manter atualizado frente às novas tecnologias.

Neste ambiente de constantes novidades que é o mundo informatizado, o estudante de direito civil tem a essencial tarefa de se manter informado e disposto a enfrentar conflitos que talvez nunca foram imaginados pelo legislador ao tempo de criação das normas, mas que com o avanço tecnológico, demandam uma solução rápida, de modo a oferecer uma proteção àqueles que utilizam as ferramentas informatizadas e evitar que a ausência de uma resolução para o conflito seja utilizada como fundamento para o abuso de um direito.

Avançando esta discussão, podemos citar o posicionamento de Danilo Doneda frente às dificuldades que são enfrentadas ao se estudar os impactos da tecnologia:

> Entre a variedade de enfoques que costumam acompanhar esta empreitada, podemos destacar alguns elementos comuns, como a dificuldade em julgar os efeitos da utilização de novas tecnologias – o que já nos dá uma primeira mostra de dificuldades da aplicação do discurso jurídico neste campo. A tecnologia apresenta um caráter de imprevisibilidade que lhe é intrínseco; sua ação costuma dar-se em um universo amplo e complexo a ponto de tornar análises de impacto, projeções e testes, em última análise, de escassa serventia. Suas possibilidades e efeitos, por sua vez, vão além daquilo que o homem jamais teve possibilidade de administrar anteriormente.[1]

Mister se faz ressaltar a necessidade de que a relação do Direito com as novas tecnologias seja baseada na realidade da sociedade brasileira, entretanto, não pode ser descartada a eventualidade de se recorrer a ordenamentos externos a fim de procurar uma devida solução para problemas que vem surgindo com o uso maciço da tecnologia. Neste sentido, inicialmente, este trabalho se preocupará em detalhar os conceitos de privacidade e de dados pessoais, de modo que seja formada a base para as futuras discussões que serão apresentadas.

---

[1] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 37

No primeiro capítulo, será discutido o direito à privacidade e sua relação com os dados pessoais, sendo destacada a autonomia entre este direito e o direito à proteção de dados pessoais, de forma a caracterizar a importância do ordenamento brasileiro reconhecer a proteção de dados pessoais como um direito fundamental:

> O tratamento de dados pessoais, em particular por processos automatizados, é, no entanto, uma atividade de risco. Risco que se concretiza na possibilidade de exposição e utilização indevida ou abusiva de dados pessoais, na eventualidade desses dados não serem corretos e representarem erroneamente seu titular, em sua utilização por terceiros sem o conhecimento deste, somente para citar algumas hipóteses reais. Daí resulta ser necessária a instituição de mecanismos que possibilitem à pessoa deter conhecimento e controle sobre seus próprios dados – que, no fundo, são expressão direta de sua própria personalidade. Por este motivo, a proteção de dados pessoais é considerada em diversos ordenamentos jurídicos como um instrumento essencial para a proteção da pessoa humana e como um direito fundamental.[2]

No segundo capítulo, será apresentado o conceito de rede social e, em seguida, será detalhada a relação entre o usuário e a própria rede social, objetivando a comprovação que este relacionamento é o de consumo, mesmo não havendo uma aparente contraprestação por parte do usuário. Nesta linha de pensamento, serão expostos os princípios que devem formar a base de qualquer atividade entre o usuário e a rede social, destacando-se os elencados por Danilo Doneda como: princípio da publicidade, onde a existência de um banco de dados tem que ser informado para aqueles que tenham as suas informações armazenadas; princípio da exatidão, que impede a reprodução infiel dos dados pessoais; princípio da finalidade, pelo qual um dado pessoal só poderia ser armazenado se sua finalidade fosse compatível com o motivo de armazenamento; princípio do livre acesso, onde o usuário tem o direito de saber e acessar os seus dados que foram armazenados; e princípio da segurança física e lógica, um dos grandes questionamentos da atualidade, que define a proteção dos dados armazenados diante de extravios, acesso não autorizado, destruição e modificação[3].

Os mencionados princípios definem os limites e liberdades que as redes sociais possuem em relação ao dado pessoal, da mesma forma que fundamentam todas as formas de controle pelo usuário ou pelo próprio Estado brasileiro ante a violação da privacidade ou uso indevido.

---

[2] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011. p. 92

[3] Todos os princípios mencionados, bem como, seus conceitos estão presentes em: DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011. p. 100-101.

No terceiro e último capítulo, serão analisados os métodos de controle que podem ser realizados no ordenamento brasileiro, como a previsão de um consentimento expresso pelo usuário para o uso de seus dados, tratada numa das mais recentes normas a disciplinar sobre tecnologia, o Marco Civil da Internet, e a novidade jurídica do direito ao esquecimento por parte do usuário. Também será discutida outra forma de garantir a segurança dos dados, o *habeas data*.

Por fim, serão apresentadas as conclusões, na expectativa que o constante debate do tema reforce a sua importância.

1. PRIVACIDADE E DADOS PESSOAIS

1.1 Ponderações sobre o direito à privacidade na internet

O direito à privacidade não é um dos direitos que foram profundamente trabalhados e considerados como fundamentais desde os tempos remotos. Na verdade, a privacidade em si não era um assunto abordado extensamente pelas legislações até o início do século XX. Foram os avanços tecnológicos que forçaram o começo de uma discussão mais profunda acerca do tema. Tais avanços começaram a entrar em conflito com a esfera particular dos indivíduos na medida em que a tecnologia e os sistemas de informação expandiram o alcance, aumentaram a velocidade e assim facilitaram a obtenção de dados sobre a pessoa.

Laura Schertel Mendes, sobre o momento de origem de discussões sobre a privacidade, destaca:

> O início dos debates doutrinários sobre o direito à privacidade ocorreu como conseqüência da utilização de novas técnicas e instrumentos tecnológicos, que passaram a possibilitar o acesso e a divulgação de fatos relativos à esfera privada do indivíduo de uma forma anteriormente impensável. Isso pode ser percebido com o pioneiro artigo sobre privacidade de Warren e Brandeis, publicado na Harvard Law Review e intitulado "The Right to Privacy", no qual os autores denunciavam como a fotografia, os jornais e aparatos tecnológicos tinham invadido os sagrados domínios da vida privada e doméstica.[4]

Danilo Doneda afirma que a concepção originaria sobre a privacidade "(..) tem uma linha evolutiva. Em seus primórdios, marcada por um individualismo exacerbado e mesmo egoísta, portou a feição do direito de ser deixado só[5]". Ademais, esta característica individualista ainda está presente, de certa forma, na conceituação de privacidade atual, entretanto de maneira quase vestigial, por isto, Doneda ainda reforça que a privacidade hoje "compreende algo muito mais complexo do que o isolamento ou a tranquilidade"[6]. Atualmente, na área civil, o direito à privacidade é reconhecido por sua intima relação com os direitos da personalidade, se juntando a proteção do corpo, da imagem, do nome e da honra[7].

---

[4] MENDES, Laura Schertel**. Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008. p. 14.

[5] DONEDA, Danilo**. Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 8

[6] Idem. p. 10

[7] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação***: efetividade desse direito fundamental diante dos avanços da tecnologia da informação.* 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 37.

Após a Segunda Guerra Mundial podemos acompanhar um maior número de previsões sobre a privacidade nas declarações internacionais de direito:

> Diante desse cenário histórico, constata-se a rápida evolução do direito à privacidade. Uma vez reconhecido no plano internacional, aos poucos incorporou-se ao ordenamento jurídico interno de cada país – especialmente nas áreas civil e criminal – o que acarretou grande avanço doutrinário e jurisprudencial. Hoje, a maior parte dos países democráticos tutela a privacidade na própria Constituição, exceto alguns países da raiz do common law, como o Reino Unido, que reconhece o direito à privacidade mediante jurisprudência. Entretanto, ainda se observa a necessidade de maior avanço na tutela desse preceito, especialmente no que concerne à proteção dos dados pessoais diante das ameaças que pululam no meio da informática(...)[8]

No Brasil, o direito à privacidade é previsto no inciso X do artigo 5º da Constituição Federal de 1988. No texto constitucional ocorre uma variação na denominação deste direito uma vez que a redação do mencionado inciso refere-se à inviolabilidade da intimidade e da vida privada, e não da privacidade explicitamente[9].

Para um melhor esclarecimento, deve ser demonstrado o que seria a esfera da intimidade e suas diferenças em relação a vida privada. Tatiana Malta Vieira define:

> Intimidade reflete os pensamentos do indivíduo, suas ideias e emoções, relacionando-se a uma zona mais estrita da pessoa, àquilo que deve ser mantido em sigilo por revelar o íntimo do indivíduo; vida privada, de outro lado, é a vida pessoal e familiar do indivíduo, que pode ser de conhecimento daqueles que desfrutam de sua convivência.[10]

Logo, podemos perceber que a principal diferença entre os termos utilizados na Constituição Federal se encontra na escala de abrangência, sendo que o primeiro tem um alcance mais restrito marcado pela internalidade da pessoa, apesar de poder ser considerado um elemento do segundo.

---

[8] Idem. p.36

[9] 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 a indenização pelo dano material ou moral decorrente de sua violação;
(...)

[10] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 28.

A separação do direito à privacidade em conceitos distintos, entretanto, não oferece maiores problemas para o seu estudo, uma vez que não se encontra consolidada sua denominação na doutrina brasileira.

Sobre esta distinção podemos destacar a afirmação de Laura Schertel Mendes:

> Muito embora a norma suprema mencione ambos os termos, tal distinção não deve operar efeitos jurídicos na tutela da privacidade pelo direito brasileiro, porque, tanto o seu âmbito de proteção, como as suas limitações, assim como os efeitos de sua violação, independem da distinção entre "vida privada" e "intimidade", razão pela qual se entende que tal distinção não deve ser tratada juridicamente.[11]

Neste sentido, a utilização de dois termos para tratar do direito à privacidade pode ser consequência de uma preocupação do legislador em garantir a sua proteção e evitar que os conflitos doutrinários produzissem aberturas que limitassem seu alcance.

Conforme esclarecido por Danilo Doneda:

> A verdadeira questão que a terminologia constitucional nos apresenta é: se foram utilizados dois termos diversos, estaríamos diante de duas hipóteses diversas que devem ser valoradas de forma diferente? Responderemos que não, pelos seguintes motivos: (i) a ausência de uma clara determinação terminológica na doutrina e na jurisprudência, além do fato de ser a primeira vez que o tema ganha assento constitucional, podem ter sugerido ao legislador optar pelo excesso; (ii) a discussão dogmática sobre os limites entre ambos os conceitos, visto o alto grau de subjetividade que encerra, desviaria o foco do problema principal, que é a aplicação do direito fundamental da pessoa humana em questão, em sua emanação constitucional.[12]

Desta forma, aparenta ser mais eficaz para esta pesquisa fazer referência ao termo privacidade, em detrimento de intimidade e de vida privada apresentados no texto constitucional, uma vez que a violação de qualquer um dos dois termos configura um atentado ao direito à privacidade.

Contudo, nem mesmo o conceito de privacidade em si é livre de divergências doutrinárias, forçando-nos a focar naquele de maior abrangência, como assim nos fornece Laura Schertel Mendes:

---

[11] MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008. p. 20.

[12] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 110

> (...) entende-se que a definição mais adequada é a que faz prevalecer a ideia de controle do indivíduo sobre as suas informações, em detrimento da ideia de isolamento do indivíduo. Conceituada dessa forma, a privacidade reflete claramente a existência de uma autonomia do seu titular na conformação desse direito[13].

Hoje, podemos afirmar que esta autonomia do titular em exercer controle sobre suas informações não é mais uma busca exclusiva de uma parte da sociedade brasileira. Evidente que quanto maior for o índice de exposição de uma pessoa perante a mídia, maiores serão as chances da mesma ter sua privacidade invadida. Entretanto, vivemos uma era digital onde informações são transmitidas em segundos e a presença das redes sociais amplia ainda mais esta circulação de informações, logo qualquer usuário destas redes pode em algum momento ter uma de suas informações que deseja manter em segredo exposta. O risco de ter sua intimidade violada, no decorrer dos últimos anos, não é mais única das pessoas de destaque da mídia.

Cumpre observar que segundo pesquisa realizada pela TIC Domicílios[14], realizada em 23.465 domicílios em todo o território nacional, entre novembro de 2015 e junho de 2016, mostra que 58% da população brasileira usa a internet, o que representa cerca de 102 milhões de usuários. Comparando a pesquisa anterior, realizada em 2014, foi constatado um aumento de 5% na proporção de internautas. Tais dados demonstram a crescente proporção de indivíduos que utilizam a internet e que necessitam de garantias para a preservação de sua privacidade frente a disseminação do seu uso. Entretanto, este grande número comprova a difícil tarefa que o Estado brasileiro possui em suas mãos: garantir que cada um desses usuários tenham seus direitos respeitados.

Olhando para números como os apresentados anteriormente, não é de se espantar que cada vez mais são procurados meios do Estado exercer um maior controle sobre o tratamento dos dados na internet. Aqui cabe dizer que este "controle" não está relacionado à censura do

---

[13] MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008. p. 21.

[14] Resultados mencionados neste trabalho podem ser obtidos em: <http://www.brasil.gov.br/ciencia-e-tecnologia/2016/09/pesquisa-revela-que-mais-de-100-milhoes-de-brasileiros-acessam-a-internet>

conteúdo das informações nem sobre quem pode se utilizar da internet para se comunicar, pois este se caracteriza como uma violação da liberdade defendida por nossa Constituição Federal[15].

Controlar o tratamento de dados deve ser referente ao papel do Estado em garantir que o seu uso não seja abusivo, que o direito à privacidade seja respeitado, que o cidadão tenha acesso às suas informações e que possa a qualquer momento alterar ou remover os dados armazenados por uma entidade particular, que meios para punir violações da intimidade sejam criados, e principalmente, que haja transparência sobre os métodos empregados na manipulação de informações por administradores de serviços oferecidos na internet.

No Brasil, uma recente lei teve o objetivo de regulamentar as relações entre os cidadãos brasileiros e a internet. Trata-se da Lei 12.965 de 23 de abril de 2014, conhecida como o Marco Civil da Internet. Tal lei trouxe a difícil tarefa de definir princípios e parâmetros que devem funcionar de forma basilar na utilização da internet. Desta forma, o direito à privacidade não poderia deixar de ser analisado pelo legislador pois permeia todas as interações entre uma pessoa e o meio digital. A privacidade é tratada em dois momentos muito importantes no Marco Civil da Internet: ao serem definidos os princípios que a disciplina da internet no Brasil segue[16] e ao falar dos direitos que são assegurados à todos os brasileiros que utilizam esta rede mundial[17].

Com isto, podemos afirmar que o Brasil reconheceu a importância de avaliar e se atualizar sobre a sociedade digital que lhe compõe, tarefa que, frente aos avanços tecnológicos,

---

[15] 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:
(...)
IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença;
(...)

[16] Art. 3º. A disciplina do uso da internet no Brasil tem os seguintes princípios:
I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;

[17] Art. 7º. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
(...)

deverá ser repetida com uma frequência cada vez maior. Privacidade e tecnologia aparentam ser termos que sempre estarão em choque, com o avanço da segunda, um maior número de formas da violação da primeira irão aparecer.

1.2 O dado pessoal

Na internet de um modo geral, mas principalmente nas redes sociais, os conceitos de privacidade estão fortemente vinculados a duas ações tomadas pelos fornecedores desses serviços: o armazenamento de dados pessoais e o seu respectivo tratamento. Logo, para ser pesquisado o tema que aborda a proteção da intimidade do usuário das redes sociais, é essencial que anteriormente seja feita uma análise do que é um dado pessoal.

Primeiramente, é necessário o estudo das similaridades e das diferenças que encontramos ao definir dois termos comumente utilizados de maneira sinônima, o dado pessoal e a informação pessoal.

Doneda explica que a o dado pessoal tem uma conotação mais primitiva e mais fragmentada[18], assim, a principal diferença entre os dois termos seria que:

> (...) o dado estaria associado a uma espécie de "pré-informação", anterior à interpretação e ao processo de elaboração. A informação, por sua vez, alude a algo além da representação contida no dado, chegando ao limiar da cognição, e mesmo nos efeitos que esta pode apresentar para o seu receptor. Sem aludir ao significado ou conteúdo em si, na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega em sí também um sentido instrumental, no sentido de uma redução de um estado de incerteza. A doutrina não raro trata estes termos indistintamente[19].

Seguindo esta linha de raciocínio, Tatiana Malta Vieira exemplifica:

> Um exemplo de dado pessoal é o IP atribuído a um determinado computador quando este se conecta à rede. Apesar de essa informação não conduzir à identificação direta do internauta, tal identificação poderá ser conhecida a partir da interconexão do IP com outros dados armazenados pelo provedor de acesso à internet, cybercafé, lan-house, cyber office ou estabelecimento congênere[20].

---

[18] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 152.
[19] Idem. Ibidem
[20] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 224-225.

A indistinção no tratamento dos termos pela doutrina mencionada por Doneda se expande até mesmo para as normas que mencionam o assunto. Na lei 12.527, em seu artigo 4º, inciso I, são considerados como informação "dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato[21]". E mais precisamente, no mesmo artigo, inciso IV, que se define informação pessoal como: "aquela relacionada à pessoa natural identificada ou identificável[22]". Podemos perceber que o legislador não faz a distinção oferecida por Danilo Doneda, uma vez que considera como informação o dado mesmo que não processado, enquanto o autor mencionado afirma que a informação passa por um processo de depuração de seu conteúdo.

O Marco Civil da Internet é omisso em definir um conceito para dado pessoal que será utilizado pela lei, entretanto, podemos procurar uma definição mais precisa para o termo em um projeto de lei que visa regular o tratamento de dados pessoais. Trata-se do projeto de lei 5276-A do ano de 2016, que dispõe sobre o tratamento de dados pessoais com o objetivo de garantir o respeito aos direitos fundamentais da pessoa natural. No projeto inicial, em seu artigo 5º, inciso I, dado pessoal é definido como "dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa[23]".

Buscando uma fonte externa ao Brasil para definir o que seria um dado pessoal, se recorria à Directiva Europeia 95/46/CE, de 1995, que hoje se encontra revogada, que em seu artigo 2º proferia:

> «Dados pessoais», qualquer informação relativa a uma pessoa singular identificado ou identificável («pessoa em causa»); é considerado identificável todo aquele que possa ser identificado, directa ou indirectamente, nomeadamente por referência a um número de identificação ou a um ou mais elementos específicos da sua identidade física, fisiológica, psíquica, económica, cultural ou social[24];

---

[21] BRASIL. **Lei n° 12.527 de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso xxxiii do art. 5º, no inciso ii do § 3º do art. 37 e no § 2º do art. 216 da constituição federal; altera a lei nº 8.112, de 11 de dezembro de 1990; revoga a lei nº 11.111, de 5 de maio de 2005, e dispositivos da lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>, acesso em 12 jun. 17.

[22] Idem

[23] BRASIL, Câmara dos Deputados. **Projeto de Lei n. ° 5.276-A/2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=C2874759AD9F780699B58C8058EB45ED.proposicoesWeb2?codteor=1470645&filename=Avulso+-PL+5276/2016>, acesso em: 12 jun. 2017.

[24] UNIÃO EUROPEIA. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados

Atualmente, no âmbito da União europeia, deve ser feita referência ao Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa de 27 de abril de 2016, que em seu artigo 4º manifesta uma definição muito similar a diretiva revogada:

> «Dados pessoais», informação relativa a uma pessoa singular identificada ou identificável («titular dos dados»); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, económica, cultural ou social dessa pessoa singular[25];

A principal diferença que encontramos é que com a transição da norma de 1995 para a de 2016, houve uma maior preocupação em atualizar os termos, fazendo referência ao titular dos dados na mais recente, e exemplificando o que poderia ser considerado um identificador, termo fundamental para a construção da pessoa identificável.

Novamente, não é possível observar uma maior distinção entre dado pessoal e informação pessoal, mesmo na norma estrangeira. Desta maneira, não se demonstra eficiente prosseguir na discussão de dois termos tão conectados e similares. Devemos entender que o dado é mais primitivo que a informação e geralmente se encontra num estado em que ainda não foi transmitido e analisado frente a um conjunto de outros dados, mas quando se objetiva garantir o direito fundamental de privacidade devemos tratar do respeito tanto de dados quanto de informações pessoais.

Na contramão do afirmado, é de extrema importância diferenciar o dado pessoal do dado anônimo, uma vez que este último é uma das formas de preservar a intimidade das pessoas, desta forma, podemos definir o dado anônimo como um dado que não permite se identificar a pessoa ao qual se refere, em outras palavras, é aquele que não se consegue associar a uma pessoa identificada ou identificável[26].

---

pessoais e à livre circulação desses dados. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>, acesso em: 12 jun. 17.

[25] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 12 jun. 17.

[26] MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008. p. 71-72.

Ainda sobre este tipo de dados, Laura Schertel Mendes afirma:

> (...) após adquirirem a característica de anônimos, os dados não estão mais sujeitos à disciplina da proteção de dados pessoais, se tiverem sido tratados de modo a impossibilitar toda e qualquer identificação pessoal. Isso porque a tutela jurídica abrange apenas aqueles dados que se refiram à pessoa identificada ou identificável[27].

O anonimato dos dados é uma forma de proteção da pessoa que teve seus dados armazenados[28]. Ele é obtido com o emprego de técnicas, como a criptografia, que não permitam a identificação do usuário dono das informações, tornando-os indeterminados.

1.2.1 Classificação dos dados pessoais

Existem três tipos de dados pessoais: não sensíveis, sensíveis e de tratamento proibido. Para falar sobre cada um deles recorreremos aos conceitos apresentados por Tatiana Malta Vieira. Segundo a autora, os dados não sensíveis "correspondem à esfera privada de seu titular[29]", enquanto os dados sensíveis seriam aqueles que abrangem "valores atinentes ao âmbito da intimidade ou esfera confidencial, cujo acesso é mais restrito[30]". Os dados de tratamento proibido são da esfera do segredo de um indivíduo, "abrangendo as manifestações espirituais da pessoa características da vida íntima *strictu sensu*[31]" **.**

A denominação que ganhou força ao se falar de dados pessoais na internet, foi a de dados sensíveis. Estes são os dados pessoais que, ao lado dos de tratamento proibido, possuem a maior possibilidade de gerar danos quando são expostos, pois, com o uso deles, discriminações podem ser feitas. Para Doneda:

> (...) a prática do direito da informação deu origem a criação de uma categoria específica de dados, a dos dados sensíveis. Estes seriam tipos de informação que, caso sejam conhecidas e processadas, prestar-se-iam a uma potencial utilização discriminatória ou particularmente lesiva e que apresentaria maiores riscos potencias que a média, para a pessoa e não raro para uma coletividade. Alguns destes dados

---

[27] Idem. p. 72
[28] Idem. p. 71.
[29] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 228.
[30] Idem. Ibidem.
[31] Idem. Ibidem

> seriam as informações sobre raça, credo político ou religioso, opções sexuais, o histórico médico ou os dados genéticos de um indivíduo[32].

Um dado sensível, então, deve ser analisado em conformidade não mais apenas com o direito à privacidade mas também com o respeito ao princípio da igualdade, impedindo que sua obtenção e transmissão fundamente exclusão e tratamento diferenciado de quem se refere.

O grande problema proveniente da conceituação de dado sensível é relacionado a necessária avaliação de seu uso. Um dado somente é sensível quando utilizado de forma discriminatória, logo, a sua destinação influencia em sua caracterização. Se usado da maneira incorreta qualquer dado pode ser considerado sensível, da mesma forma que dados naturalmente considerados sensíveis, podem ser essenciais para a realização de uma atividade que não vise discriminação.

Nesta linha de raciocínio, e a título exemplificativo do uso necessário de dados sensíveis, Doneda profere:

> Tome-se, por exemplo, a pesquisa de caráter científico ou mesmo a atividade médica, para quais a importância de trabalhar com todos os dados possíveis, inclusive os sensíveis, é capital. Para situações deste tipo são frequentemente estabelecidos regimes de permissão do tratamento de dados sensíveis, quando a vedação é a regra não absoluta[33].

Ainda relacionado a possibilidade de qualquer dado ser sensível, Laura Schertel Mendes estabelece que seria fundamental falar em tratamento sensível de dados, afirmando que "é fundamental proteger também outros dados que, embora aparentemente insignificantes, podem vir a se tornar sensíveis, a depender do tipo de tratamento a que são submetidos[34]".

Nas palavras de Tatiana Malta Vieira:

> Ressalte-se que, mesmo os dados não sensíveis podem necessitar de proteção – garantindo-se sua integridade, autenticidade e confidencialidade – uma vez que, ao serem confrontados com outros dados, podem revelar aspectos que o titular gostaria de manter em sigilo, por afrontarem diretamente seu direito à privacidade. Ainda que certos dados pessoais não deixem transparecer mensagem significativa, quando

---

[32] DONEDA, Danilo. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 160-161
[33] Idem. p. 163
[34] MENDES, Laura Schertel. **Transparência e privacidade**: violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008. p. 64.

> analisados isoladamente, devem ser submetidos a procedimentos e medidas especiais de proteção, pois, uma vez agrupados, permitem a definição do perfil de seu titular[35].

Evidente a necessidade de uma análise sobre o objetivo pretendido ao usar dados sensíveis antes de decretar a proibição total do tratamento destes dados, como é destacado no regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa. Nas considerações deste regulamento, não é excluído o direito dos Estados-Membros em definir as circunstâncias de situações específicas de tratamento, inclusive determinando situações em que é lícito o tratamento de dados pessoais e até mesmo o tratamento das categorias especiais, como é o caso dos dados sensíveis[36].

Contudo, permitir até certo ponto o tratamento de dados sensíveis não é o mesmo que afirmar a possibilidade de seu uso indiscriminado. Mesmo no regulamento europeu existe a previsão de um tratamento especial aos dados sensíveis, como pode ser observado ao proferir que eles merecem proteção uma vez que "(...)o contexto do tratamento desses dados poderá implicar riscos significativos para os direitos e liberdades fundamentais"[37].

Com isto, ampliaríamos a visão de que o problema do tratamento indiscriminado não é exclusivamente referente a um tipo de dado em si, e assim destacaríamos a importância de um maior cuidado na utilização e proteção de qualquer dado, independentemente de sua classificação.

Por fim, é valido dizer que os dados de tratamento proibido, não possuem tamanhos questionamentos. Como o próprio nome se refere, não devem sofrer nenhum tipo de tratamento e devem ser protegidos legalmente contra o seu uso, de forma a garantir o direito à privacidade do indivíduo a que se refere.

1.2.2 Banco de dados

---

[35] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 229.

[36] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 12 jun. 17.

[37] Idem.

Também relacionado ao conceito de dado pessoal se encontra a figura do banco de dados. Trata-se de "um conjunto de informações estruturado de acordo com uma determinada lógica[38]". Ou seja, banco de dados é uma das formas de armazenagem do dado pessoal que objetiva sua organização para uma mais efetiva utilização.

O banco de dados pode ser considerado um dos principais símbolos da agressividade proveniente de um tratamento digital de dados pessoais. No momento em que a tecnologia permitiu uma sistematização e automação da análise dos dados, além de tornar rápido o cruzamento de diferentes informações sobre uma pessoa, muitas vezes proveniente de fontes diversas, o nível de detalhes sobre o perfil de uma pessoa atinge um nível espantoso. O banco de dados eletrônico permite o aumento de:

> "(...)sujeitos que podem ter acesso a um conjunto sempre mais detalhado e preciso de informações sobre terceiros, o que faz com que o estado jurídico desses dados se torne um dos pontos centrais que vão definir a própria autonomia, identidade e liberdade do cidadão contemporâneo[39]".

Hoje, já fazemos referência a algo maior que um banco de dados isolado. Como pode ser observado, a principal característica do mundo digital é a sua conectividade. O banco de dados ganha destaque no momento em que a internet permite a rápida comunicação de informações contidas em mais de um banco e o cruzamento de dados referentes a um indivíduo proveniente desses diferentes sistemas de armazenagem.

Esse multiplicidade de bancos de dados e as infinitas fontes de dados provenientes da internet é chamada de Big Data. Sobre o Big Data:

> O acentuado aumento no volume de informações pessoais colhidas e passíveis de serem submetidas a tratamento introduziu, nos últimos anos, um novo paradigma no tratamento de informação. A disponibilidade de diversos bancos de dados e de informação pessoal em volumes bastante consideráveis fez com que fossem desenvolvidos mecanismos capazes de prospectar informações não propriamente em um único banco de dados, porém em diversas fontes de informações disponíveis e, através de uma determinada sistemática que envolve o estabelecimento de correlações entre blocos de informações a princípio dispersos, gerar uma nova informação (Big Data)[40].

---

[38] DONEDA, Danilo. **O direito fundamental à proteção de dados pessoais**. In: MARTINS, Guilherme Magalhães (Coord.). Direito Privado e Internet. São Paulo: Atlas, 2014. p. 65

[39] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011. p. 93.

[40] DONEDA, Danilo. **O direito fundamental à proteção de dados pessoais**. In: MARTINS, Guilherme Magalhães (Coord.). *Direito Privado e Internet*. São Paulo: Atlas, 2014. p. 66

No caso de uma rede social, devido ao uso diário pela maioria de seus usuários e do volume de informações que são inseridas nelas, é possível entender porque devemos falar em uma proteção além do dado pessoal isolado, sendo necessária esta compreensão do que é um banco de dados e do que é Big Data. O fluxo continuo de informações que a rede social obtêm sobre um indivíduo não é exclusivamente proveniente das informações que o próprio compartilha, também envolve o que é compartilhado sobre um indivíduo por seus círculos de contatos. O banco de dados de uma rede social possui um volume espantosamente detalhado de informações sobre seus usuários, de forma que seu comprometimento ou uso indevido pode gerar danos muito graves ao indivíduo. Aqui falamos em uma proteção contra o uso abusivo por parte da empresa administradora da rede social, compartilhando dados sem o consentimento, mas também de uma proteção contra a invasão de terceiros não autorizados a estes bancos de dados, coletando informações que podem futuramente utilizar contra o usuário[41].

1.3 A importância da proteção de dados pessoais como um direito fundamental

O direito à privacidade é reconhecido como um direito fundamental, como já anteriormente trabalhado, na forma da inviolabilidade da intimidade e da vida privada, possuindo previsão expressa em nossa Constituição. Também já analisamos a importância de se manter os conceitos de privacidade e proteção de dados pessoais intimamente ligados. Em virtude dessas considerações podemos nos questionar se a própria proteção de dados não é um direito fundamental em si.

Segundo José Alfonso da Silva, os direitos fundamentais, referidos pelo mesmo como direitos fundamentais do homem são "situações jurídicas, objetivas e subjetivas, definidas no direito positivo, em prol da dignidade, igualdade e liberdade da pessoa humana[42]".

[41] A título de exemplo, podemos falar sobre o *doxing*, prática pela qual um terceiro não autorizado, geralmente um *cracker*, se utiliza de informações obtidas ilegalmente para atacar o dono de tais dados, seja com a divulgação de informações privadas como seu endereço ou opiniões, seja com a utilização de chantagens realizadas sob a promessa da não divulgação dos dados. A origem do termo *doxing* vem da palavra documento em inglês e de seu termo na linguagem computacional, comumente referido como docx.

[42] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 24a ed. São Paulo: Malheiros Editores, 2005. p. 179.

O problema surge quando consideramos essencial para a dignidade humana a privacidade e o sigilo, mas não reconhecemos que devemos tutelar sobre todos os outros atos realizados através de dados pessoais que não são referentes de maneira exclusiva a sua exposição. Para ficar mais claro o que está sendo argumentado é que o artigo 5º de nossa Constituição em seu inciso XII[43] menciona a inviolabilidade das cartas e comunicações telegráficas, não havendo dúvidas que o referido inciso trata da inviolabilidade da comunicação. Entretanto, pode ser gerada a dúvida se a proteção constitucional se estende a algo além da comunicação de dados, uma dúvida de consequências perigosas pois pode resultar na afirmação: se não fossem revelados publicamente dados de cidadãos, qualquer tratamento e utilização desses dados, não sofreria limitações.

Doneda visa acabar com estes questionamentos ao afirmar:

> Tal interpretação, além de dissonante com a visão segundo a qual privacidade e informações pessoais são temas sempre mais relacionados e, em muitas ocasiões, quase que indistinguíveis entre si – conforme atesta o mencionado desenvolvimento de leis que tratam da proteção de dados pessoais e também os documentos transnacionais que associam o caráter de direito fundamental à proteção de dados pessoais –, traz consigo o enorme risco de acabar por se tornar uma norma que sugere uma grande permissividade em relação à utilização de informações pessoais[44].

Ademais, toda e qualquer atividade realizada com o emprego de dados pessoais representa riscos não só a privacidade, quando ocorre a exposição não autorizada de informações. Também se encontram ameaçados a liberdade da pessoa, por exemplo, em governos ditatoriais o dado pessoal pode ser utilizado para traçar o perfil de opositores e iniciar uma perseguição política. No âmbito da igualdade e da dignidade, podemos relembrar a discussão de dados sensíveis, onde a utilização de certas informações pode culminar na exclusão e discriminação de um sujeito.

---

[43] 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:
(...)
XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;
(...)

[44] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011. p. 105.

Outra análise cabível para o reconhecimento da proteção de dados como um direito fundamental é compararmos as principais características desses direitos, e verificar se elas estão presentes quando falamos sobre proteção de dados. José Afonso da Silva lista como principais características em comum dos direitos fundamentais: a historicidade, a inalienabilidade, a imprescritibilidade e a irrenunciabilidade[45].

Historicidade é referente a todos os direitos, é a capacidade de surgirem e evoluírem de acordo com as provocações das demandas sociais. Não há dúvidas que o debate sobre proteção de dados é fruto de uma evolução histórica. Com o avanço tecnológico e principalmente com o surgimento da internet, a demanda por uma maior segurança de nossos dados é um efeito reflexo.

Ao serem considerados inalienáveis e irrenunciáveis, o que se está querendo dizer é que os direitos fundamentais não podem ser transferidos, negociados ou até mesmo renunciados. Pode ser levantado o contraponto que os dados pessoais podem sim ser renunciados ou negociados, uma vez que pode ser fornecido consentimento para a sua utilização, como é o caso da maioria dos contratos de redes sociais. Este se demonstra um pensamento incorreto por dois motivos. Primeiramente, não é renunciada a proteção, o que é liberado com o consentimento é o uso de dados que não viole a privacidade, dignidade e igualdade, logicamente esta liberação pode estar marcada por vícios, mas em nenhum momento é permitido a renúncia para utilização discriminatória dos dados. Segundo, existe a esfera dos dados de tratamento proibido, onde não existe a possibilidade do consentimento para a sua utilização.

A imprescritibilidade, para José Afonso da Silva, refere-se a inexistência de requisitos que importem a sua prescrição[46]. Complementa o autor que tais direitos jamais ficam inexigíveis pois "prescrição é um instituto jurídico que somente atinge, coarctando, a exigibilidade de direitos patrimoniais, não a exigibilidade de direitos personalíssimos (...)[47]". Uma vez que sempre existe a possibilidade de exercer estes direitos, podemos afirmar que não ocorre passagem temporal que fundamente a perda de sua exigibilidade.

---

[45] SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 24a ed. São Paulo: Malheiros Editores, 2005. p. 181.
[46] Idem. Ibidem.
[47] Idem. Ibidem.

Não podemos falar em perda do direito de exigir que dados pessoais sejam protegidos, o decorrer de tempo não é uma justificativa suficiente para que informações cruciais sobre um cidadão sejam utilizadas de maneira livre e sem o seu consentimento. Aceitar uma prescrição desta proteção é abrir espaço para que a falta de conhecimento sobre este direito por parte de uma pessoa seja abusada por aqueles que armazenam os dados.

Com isto, pudemos observar que as quatro características inerentes de um direito fundamental se encontram presentes no debate de proteção de dados pessoais, e são essenciais para alcançar o objetivo desta proteção que é a preservação da pessoa. Considerando a proteção de dados pessoais como um direito fundamental evitamos que discussões sobre a interpretação constitucional seja limitadamente referente a comunicação e interceptação de dados, ignorando discussões sobre tratamento e armazenagem. Como afirma Doneda, dentre os perigos de uma interpretação limitada da Constituição estaria a formação de "um hiato que segrega a tutela da privacidade[48]", e ainda sobre este tema:

> (...) este hiato possibilita a perigosa interpretação que pode eximir o aplicador de considerar os casos nos quais uma pessoa é ofendida em sua privacidade – ou tem outros direitos fundamentais desrespeitados – não de forma direta, porém por meio da utilização abusiva de suas informações pessoais em bancos de dados. Não é necessário ressaltar novamente o quanto hoje em dia as pessoas são reconhecidas em diversos relacionamentos não de forma direta, mas mediante a representação de sua personalidade, fornecida pelos seus dados pessoais, aprofundando ainda mais a íntima relação entre tais dados e a própria identidade e personalidade de cada um de nós[49].

Externamente ao Brasil, já podemos encontrar em alguns ordenamentos o reconhecimento expresso da proteção de dados como um direito fundamental. A Carta dos direitos fundamentais da União Europeia, em seu artigo 8º declara que todas as pessoas possuem direito à proteção de dados[50]:

> Artigo 8º
> Protecção de dados pessoais
> 1.Todas as pessoas têm direito à protecção dos dados de carácter pessoal que lhes digam respeito.
> 2.Esses dados devem ser objecto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo

[48] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011. p. 106.
[49] Idem. Ibidem.
[50] UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**, de 7 de dezembro de 2000. Disponível em: < http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>, acesso em: 12 jun. 17.

> previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva rectificação.
> 3.O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.

Assim, caracterizada e comprovada esta fundamentalidade da proteção de dados pessoais, não restam dúvidas que podemos falar em direito à proteção de dados, um direito completamente autônomo, que apesar de encontrar bases também na garantia de privacidade, estende sua tutela para todo e qualquer uso dos dados pessoais que venha a prejudicar o usuário. Podendo ser violado pela a exposição não autorizada do usuário ou pelo uso indiscriminado de informações obtidas através desses dados, mesmo que não os revele publicamente.

2. RELAÇÕES ENTRE AS REDES SOCIAIS E SEUS USUÁRIOS

2.1 Conceituando redes sociais

O próximo passo para este estudo é analisar as relações entre os usuários e as redes sociais, símbolos do grande avanço tecnológico na área do tratamento de dados. Mas antes de iniciarmos o tema destas relações é preciso conceituar o objeto do estudo, afirmando o que pode ser considerado uma rede social.

Podemos traçar a origem destas redes ao ano de 1995, quando Randy Conrads criou o site "classmates.com", cujo objetivo era a interação de seus usuários com antigos companheiros de escola para recuperar ou manter o contato[51].

Após esta data, ocorre um grande crescimento da popularidade dos sites de redes sociais, principalmente com o início dos anos 2000. Em 2003, surgem sites como o *MySpace e o Xing*[52], e o crescimento destas plataformas é exponencial, chamando a atenção de grandes empresas como o Google e o Yahoo! que criam seus próprios serviços[53].

Muitos destes sites possuíam alvos geográficos específicos demonstrados pela presença de uma única língua disponível para a sua utilização. Contudo, este fato não foi suficiente para criar uma barreira que impedisse os usuários de outras regiões, que não eram inicialmente o público esperado, conseguissem utilizar a rede social. Assim é afirmado:

> Muitos sites de redes sociais focam em pessoas de uma região geográfica específica ou grupo linguístico, apesar disto nem sempre determinar a constituição do site. O Orkut, por exemplo, foi lançado nos Estados Unidos com uma interface apenas em inglês, mas brasileiros, que falam português, rapidamente se tornaram o grupo de usuários dominantes[54].

---

[51] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales**. Madrid, 2009, p. 34.

[52] O *Xing* é uma rede social de origem alemã de contatos profissionais.

[53] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales**. Madrid, 2009, p. 35.

[54] BOYD, Danah M; ELLISON, Nicole B. **Social Network Sites: Definition, History, and Scholarship**. 2007. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full>, acesso em: 12 jun. 17.

Esta ampliação na população alvo pode ser observado em diversas redes sociais. Assim como no caso mencionado do *Orkut*[55], a rede social *Facebook* não possuía a língua portuguesa em seus primórdios, mas a popularidade no Brasil e o crescente número de usuários brasileiros forçou a adaptação do site até o ponto de existir uma empresa representante da rede em território nacional.

Hoje, as redes sociais estão presentes no dia a dia de um número cada vez maior de pessoas. Sabemos afirmar que o Facebook é uma rede social, assim como *Twitter*, *LinkedIn*, *My Space*, *Orkut*, dentre outras. Entretanto, formar um conceito que elenque todas as características essenciais para considerarmos uma rede como social, pode não ser uma tarefa tão fácil. Isto se deve pelo caráter mutável destas redes, que com a passagem dos anos, implementam novos recursos e também pelo surgimento de novas redes sociais que possuem diferentes finalidades.

O que podemos observar em todos os casos é que, independente da forma utilizada, o objetivo de uma rede social perante o seu usuário é o de conectá-lo a um grande número de pessoas possibilitando a interação virtual entre indivíduos. Em outros termos:

> Nós definimos sites de redes sociais como serviços baseados na web que permitem indivíduos (1) construir um perfil público ou semi-público dentro de um sistema, (2) articular uma lista de outros com os quais compartilham um relacionamento, e (3) ver e navegar suas listas de conexões e aquelas criados por outros dentro do sistema. A natureza e nomenclatura dessas conexões variam de site para site[56].

Outras características fundamentais contidas em todas elas podem ser: a finalidade principal de colocar pessoas em contato, permitir a interação entre todos os usuários da plataforma, permitir que os contatos entre os usuários sejam ilimitados e a forma de difusão viral da rede social, através dos próprios usuários, o que possibilita o seu grande crescimento[57].

---

[55] O *Orkut*, rede social filiada a empresa Google, de grande relevância no início da propagação das redes sociais no território brasileiro encontra-se desativado desde o dia 30 de setembro de 2014.

[56] BOYD, Danah M; ELLISON, Nicole B. **Social Network Sites: Definition, History, and Scholarship**. 2007. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full>, acesso em: 12 jun. 17.

[57] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales**. Madrid, 2009, p. 40.

É importante destacar que nas redes sociais as interações costumam ser entre pessoas que já se conhecem, mesmo assim não existe impedimento de interação com desconhecidos. Apesar disto, em muitas redes sociais, os usuários não estão procurando fazer novas amizades, e sim realizar comunicações com pessoas que já fazem parte de seu círculo social[58].

Uma rede social pode ser chamada de própria ou generalista quando seu principal foco for a formulação de perfis públicos e individuais que permitam a interação entre os usuários[59]. Outras características das redes sociais generalistas são a existência de uma gama de funcionalidades diferentes, o que fornece à seus usuários uma plataforma que integre diversas ferramentas em um mesmo lugar, e a fomentação de uma interação que ultrapasse o âmbito online e que possa se concretizar na vida cotidiana[60]. Temos como exemplo desta modalidade de rede, o Facebook e o Twitter.

Por outro lado, existem redes sociais impróprias, que seriam sites ou aplicativos que permitem a interação social, mas contenham um foco principal distinto disto, neste sentido:

> Há também redes sociais que poderíamos denominar como impróprias, que seriam aquelas que funcionam como um apêndice de outro serviço ou ferramenta, gravitando e existindo em função deste. Estas redes improprias podem oferecer um conjunto parcial de ferramentas típicas de interação encontradas nas redes sociais próprias, e podem ser mencionados como exemplos as redes sociais presentes em sites de comércio eletrônico (tais como o da *Amazon.com, eBay* ou o *Mercado Livre*) ou sites que tem como objetivo primordial o intercâmbio de conteúdo e não propriamente a interação social mas que também cultivam suas próprias comunidades de usuários (tais como *Slideshare* ou o próprio *YouTube*)[61].

As redes sociais impróprias podem ser subdivididas em duas categorias, sobre este tema:

> Dentre as redes sociais impróprias, pode-se ainda destacar que há ao menos duas categorias de grande importância. Uma delas é a das redes sociais estruturadas em torno do intercâmbio de conteúdo. Este conteúdo é geralmente alguma espécie de mídia eletrônica – como nos exemplos já mencionados, documentos e apresentações,

---

[58] Idem. Ibidem.

[59] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo***: para além da informação creditícia.* Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 77-78. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>, acesso em : 12 jun. 17

[60] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales**. Madrid, 2009, p. 41.

[61] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 78. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>, acesso em : 31 mai. 17

> no caso do *Slideshare* ou vídeos, no caso do *YouTube*, entre outros. A utilização de ferramentas típicas de redes sociais pode aumentar a eficácia deste intercâmbio de conteúdo, através da formação de comunidades de interesses específicos e do intercâmbio de opiniões e críticas, apenas para dar um exemplo[62].

A outra subcategoria corresponde as redes sociais que possuem o foco em relacionamentos profissionais[63]. Temos como exemplo deste tipo de rede o *Xing* e mais recentemente o *Linkedin*. Estas são chamadas de redes sociais de conteúdo profissional, e "se configuram como novas ferramentas de ajuda para estabelecer contatos profissionais com outros usuários[64]".

Superado o conceito de rede social, devemos analisar como funciona o modelo de negócios destas redes. Na maioria dos casos, o serviço é oferecido para os usuários de forma gratuita, o que pode levar aos usuários o questionamento de como os custos para manter funcionando sites de tamanho porte, são pagos.

A sustentabilidade de uma rede social pode ser estudada com uma divisão em duas fases. Na primeira fase o foco é atingir uma grande quantidade de usuários, de forma que sua base de usuário se expanda, mas que além dessa expansão, ocorra uma fidelização de seus usuários para que os mesmos utilizem a rede diariamente e mantenham seus perfis da forma mais atualizada possível. O segundo momento é o qual a rede social irá produzir capital, desta forma diferentes modelos de exploração podem ser utilizados, sendo o mais comum o de publicidade. A rede se utilizando dos dados que obteve do usuário é capaz de ofertar propagandas específicas para cada um de seus usuários, assim, seu lucro provém de outras empresas que pagam pela publicidade de suas marcas[65].

2.2 Caracterizando a relação de consumo

Uma vez finalizado o estudo sobre o conceito, passamos agora para a análise da relação que o usuário possui com a empresa administradora das redes sociais. É muito comum ouvirmos uma frase que afirma que se o serviço online é gratuito, nós somos o produto. Esta afirmação é

---

[62] Idem. Ibidem.
[63] Idem. Ibidem
[64] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales**. Madrid, 2009, p. 43.
[65] Idem. p. 47-59

baseada no modelo de negócios de muitos serviços da internet, que como falado anteriormente, utiliza os dados das pessoas como uma fonte para realizar um *marketing* específico, ofertando diretamente ao usuário aquilo que é considerado compatível com seu perfil, e desta forma a rede é sustentada pelos pagamentos de outras empresas que decidem anunciar seus produtos.

Entretanto, colocar o usuário no polo do produto pode descaracterizar a real relação que este possui com as administradoras das redes sociais. Chamando-o de produto, acabamos por distanciar diversas garantias que o mesmo possui e não reconhecemos a situação de vulnerabilidade que o mesmo se encontra, um produto é algo muito mais relacionado a coisa do que a pessoa e seus direitos fundamentais.

Logo, é necessária a superação desta afirmação que apesar de possuir um sentido compreensível, uma vez que o serviço é realmente "gratuito" para o usuário na maioria dos casos e o dinheiro que o sustenta é proveniente das informações coletadas, não é verdadeira porque o usuário é sim um consumidor do serviço oferecido pelas redes sociais. Isto pode ser ainda mais reforçado pela leitura de nosso Código de Defesa do Consumidor, que em seu artigo 2º define como consumidor toda "pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final[66]" e como fornecedor "toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços[67]". No momento em que o usuário realiza contratos para entrar nas redes sociais, este se torna um consumidor pois está utilizando um serviço ofertado por empresas. Neste sentido:

> Diante de tais formas de contratação, cuja gratuidade é infirmada pela existência de um correspectivo prestado pelo consumidor, pode-se falar em uma *nova moeda*, entendida como instrumento de pagamento e troca, que consiste, diretamente, nas informações pessoais e econômicas que nos pertencem (...)[68]

De maneira ainda mais específica:

---

[66] BRASIL. **Lei 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm >, acesso em 12 jun. 17.

[67] Idem.

[68] MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet**. 2ª ed. São Paulo: Revista dos Tribunais, 2014. p. 73-74.

> Tendo em vista, portanto, o valor econômico do capital das redes sociais e, assim, das informações que constituem as interações entre os perfis, já não há que mais que se falar em gratuidade das relações jurídicas entre os *sites* e seus membros, usuários e, portanto, consumidores do serviço oferecidos. Em que pesem precedentes em contrário, a manutenção de páginas pessoais nas redes sociais virtuais, ainda que não cobrada diretamente, é remunerada por meio dos contratos de publicidade e, portanto, constitui negócio jurídico oneroso, enquadrando se no conceito de serviço do art 3°, §2° da Lei 8.078/1990[69].

Uma dúvida que pode aparecer é referente a qual serviço a rede social oferece a seu usuário. A resposta para esse questionamento se encontra na jurisprudência, que afirma que as redes sociais atuam em uma relação de armazenamento de dados e disponibilização de acesso através de *links*, sendo assim, provedores de hospedagem, incorrendo assim no regime de responsabilidade civil dos mesmos[70].

Aqui, por fim, não falamos em uma equiparação ao status de consumidor, o usuário utiliza um serviço, e como falado anteriormente, o objetivo deste serviço é conectar pessoas, não sobrando dúvidas de que ele é o destinatário final, o consumidor em sua forma plena.

2.2.1 O contrato da rede social

Um dos principais elementos que caracteriza a relação de consumo entre o usuário e a rede social é a existência de um contrato que é celebrado entre as partes. Neste sentido, podemos nos revestir do conceito de contrato proferido por Orlando Gomes, que seria "(...)uma espécie de negócio jurídico que se distingue, na formação, por exigir a presença pelo menos de duas partes. Contrato é, portanto, negócio jurídico bilateral, ou plurilateral[71]"e ainda, tais contratos seriam "instrumentos jurídicos para a constituição, transmissão e extinção de direitos na área econômica[72]".

Existem diversas formas de contratos, mas o mais utilizado nos sites das redes sociais é o de adesão. Por esta razão faz se necessário apresentar o conceito de contrato de adesão:

> No contrato de adesão uma das partes tem de aceitar, em bloco, as cláusulas estabelecidas pela outra, aderindo a uma situação contratual que encontra definida em

---

[69] MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na Internet**. 2ª ed. São Paulo: Revista dos Tribunais, 2014. p. 101-102
[70] Idem. p. 103
[71] GOMES, Orlando. **Contratos**. 26. Ed. Atualização de Antonio Junqueira de Azevedo e Francisco Paulo de Crescenzo Marino. Rio de Janeiro: Forense, 2009. p. 4.
[72] Idem. p. 5

> todos os seus termos. O consentimento manifesta-se como simples adesão a conteúdo preestabelecido da relação jurídica.[73]

Esta predominância do contrato de adesão é justificada por suas próprias características. Trata-se de um contrato mais rápido, com uma forma de consentir mais simplificada e que coloca as partes em situação de desigualdade, predominando o interesse do fornecedor em detrimento ao do consumidor[74].

A forma contratual é marcada pela inexistência da discussão prévia entre as partes sobre o seu conteúdo, e com isto, as suas cláusulas devem ser aceitas ou não na integralidade dos blocos apresentados antecipadamente[75]. Nas palavras de Orlando Gomes:

> Aponta-se primeiramente que, nesse contrato, a fase das negociações preliminares não existe. Em princípio, assim sucede. O esquema contratual está pronto, devendo aceitá-lo integralmente quem se proponha a travar a relação concreta. Contudo, sempre há cláusulas que não podem ser preestabelecidas e, de modo geral, elementos imprevisíveis. De regra, por conseguinte, fica uma faixa, mais larga ou estreita, na qual cabem entendimentos prévios entre os contratantes, se bem que, as mais das vezes, o contrato prévio se destine somente à determinação de dados pessoais, dispensáveis, aliás, em vários contratos de adesão. Admite-se, outrossim, em prática chancelada por legislações, a possibilidade de modificar algumas cláusulas gerais, mediante acordo entre as partes. Quando ocorre, pode-se falar, a bem dizer, em negociações preliminares, dado que se travam entendimentos acerca do conteúdo do contrato a concluir, entendimentos que significam "tratativas"[76].

O problema de falar em modificações das cláusulas gerais do contrato de adesão das redes sociais se encontra no fato de que em muitos casos não existe qualquer mecanismo que permita o usuário propor esta modificação. Isto ocorre em função do modelo de adesão apresentado na internet de um modo geral, marcado pelas licenças *clipwrap* onde o usuário concorda com as cláusulas de contratação pelo simples ato de apertar o botão de aceitação[77].

Guilherme Magalhães Martins aponta uma solução para o problema falado anteriormente, dando oportunidades para o usuário oferecer suas propostas perante o contrato, em suas palavras:

---

[73] Idem. p. 128
[74] MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3a ed. São Paulo: Atlas, 2016. p. 129.
[75] Idem. Ibidem.
[76] GOMES, Orlando. **Contratos**. 26. Ed. Atualização de Antonio Junqueira de Azevedo e Francisco Paulo de Crescenzo Marino. Rio de Janeiro: Forense, 2009. p.133
[77] MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3a ed. São Paulo: Atlas, 2016. p. 131

> Será sempre possível, no caso da contratação eletrônica de consumo via Internet, evitar a incidência do contrato de adesão, dando ao cliente a oportunidade de propor um texto alternativo, ou a modificação de algumas cláusulas, o que poderia ocorrer até mesmo mediante a introdução de outro botão junto àquele relativo a aceitação pura e simples das cláusulas, remetendo a um formulário específico para a proposta de um texto alternativo[78].

Esta solução se demonstra de grande importância para as relações entre usuários e redes sociais pois o que podemos observar no cotidiano é que a maioria dos usuários realiza o cadastro e aceita o contrato, sem a devida leitura de suas cláusulas. Esta prática gera uma grande insegurança para a proteção de seus dados pessoais, uma vez que impede a verificação da existência de termos que autorizem o tratamento abusivo e caso eles existam, que o usuário possa propor novos termos que os corrijam.

2.2.2 Momento e local da celebração do contrato

Agora que já sabemos qual é o principal tipo de contrato utilizado, devemos fazer uma análise do momento e do local em que o mesmo é celebrado, uma vez que tais informações são essenciais para a definição de todos os procedimentos que serão seguidos caso ocorra alguma violação da proteção de dados do usuário.

O contrato da rede social se encontra sob a forma dos termos de serviço apresentados na maioria das redes sociais quando o usuário realiza seu cadastro. O momento em que o usuário aperta o botão aceitando tais termos e finalizando o seu cadastro é exatamente quando este contrato é firmado.

Sabemos então o momento em que o contrato é celebrado, mas ainda nos resta a dúvida sobre o local em que ele foi realizado. A importância de sabermos esta informação, como destaca Guilherme Martins, é a "(...) determinação do foro – nas hipóteses em que o foro de eleição for o do lugar de celebração do contrato-, e da lei aplicável[79]".

De acordo com nosso Código Civil, em seu artigo 435, "reputar-se-á celebrado o contrato no lugar em que foi proposto[80]". Este texto se demonstra ineficaz para a resolução do

---

[78] Idem. p. 130.
[79] Idem. p. 121.
[80] BRASIL. **Lei 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>, acesso em 12 jun. 17.

questionamento, uma vez que o contrato da rede social é proposto pela internet sem uma localização visivelmente explícita. Nas palavras de Guilherme Martins:

> Ocorre que, no caso das relações originadas via Internet, os instrumentos do Direito tradicional e codificado mostram-se mais uma vez insuficientes, haja vista que se mostra praticamente impossível determinar em qual território foram as mesmas levadas a efeito[81].

Diante desta situação, normalmente se recorre a Lei de Introdução às normas do Direito Brasileiro[82], anteriormente conhecido como Lei de Introdução ao Código Civil Brasileiro. Como aponta Guilherme Martins, não sendo possível reconhecer o local do contrato, "(...)aplica-se o critério do art. 9°, parágrafo segundo da Lei de Introdução ao Código Civil. Segundo o qual as obrigações contratuais se consideram constituídas no domicílio do proponente[83]". O CDC define em seu artigo 30 que o proponente nas relações de consumo será sempre o fornecedor, logo ocorreria uma prevalência da aplicação da lei do local do domicilio da administração da rede social em relação à aplicação da lei do local do domicilio do usuário, o colocando em situação de vulnerabilidade[84]. A predominância do fornecedor nessa relação "(...) levaria à conclusão de que se estaria dando prevalência a regras do mercado, em contraposição ao direito fundamental do consumidor de se ver tutelado e protegido[85]".

Uma possível solução para o problema apresentado pode ser obtida através da análise do artigo 101, inciso I do Código de Defesa do Consumidor. Nele, é definido a possibilidade de propor a ação de responsabilidade civil contra o fornecedor do serviço no local do domicilio do autor. Desta forma, é possível a aplicação da lei do domicilio do consumidor, e que o foro para a propositura da ação seja também o do mesmo[86], eliminando a prevalência dos interesses do prestador do serviço.

2.3 Os riscos da utilização dos dados pessoais pelas redes sociais

---

[81] MARTINS, Guilherme Magalhães**. Contratos eletrônicos de consumo**. 3a ed. São Paulo: Atlas, 2016. p. 122.
[82] BRASIL. **Decreto-Lei n° 4.657 de 4 de setembro de 1942**. Lei de Introdução as normas do Direito Brasileiro. Diário Oficial da União, Rio de Janeiro, RJ, 18 set. 1942. Disponível em: <http://www.planalto.gov.br/ccivil_03 /decreto-lei/Del4657compilado.htm>, acesso em 03 mai. 17.
[83] MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3a ed. São Paulo: Atlas, 2016. p. 122.
[84] Idem. Ibidem.
[85] Ibidem. Ibidem.
[86] MARQUES, Cláudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor**. São Paulo: Revista dos Tribunais, 2004. p. 444.

Como visto anteriormente, o modelo de contrato de adesão da rede social implica numa vulnerabilidade de seu usuário na medida que não coloca as partes em mesmo nível para a negociação das cláusulas contratuais. Assim, é necessário destacarmos os riscos que a utilização destes serviços oferece.

Impossível negar que, cada vez mais, as pessoas compartilham suas informações pessoais nas redes sociais, e de certa forma, as próprias redes incentivam esta ação. Nas palavras de Danilo Doneda:

> O incentivo ao compartilhamento de informações pessoais é também por vezes apregoado como uma nova tendência dominante ou, em uma variação, como um novo padrão de interação social, próprio das novas gerações. O fundador da rede social Facebook, Mark Zuckerberg, declarou certa vez que a abertura e o compartilhamento de informações pessoais corresponderia à uma evolução de uma "norma social", no sentido de que denotaria um mudança nos costumes socialmente percebidos como normais em relação ao fluxo de informações pessoais. Nesta declaração se pode perceber, ao mesmo tempo, uma tensão entre uma noção implícita de norma jurídica, utilizada para tutelar a privacidade e os dados pessoais em ocasiões nas quais estes encontrem-se em risco por conta das redes sociais, e a dita "norma social", que representaria, neste ponto de vista, uma evolução dos costumes, com vistas a uma nova percepção de normalidade representada pela abertura e compartilhamento de informações pessoais[87].

É importante frisar que existe um grande interesse por parte das próprias redes sociais para que haja um aumento do compartilhamento de dados pelo usuário, uma vez que seu modelo de negócios depende da maior quantidade de informações possíveis sobre uma pessoa. E afirmar que este alto nível de exposição de dados pessoais é atualmente uma norma social é o mesmo que se render "a uma forma de determinismo tecnológico fortemente influenciada por uma visão unilateral dos interesses em jogo no novo modelo de negócios proposto[88]".

Podemos então destrinchar o que é armazenado por algumas das principais redes, começando pelo Facebook. Em seus termos, a empresa destaca que coleta:

> (...)o conteúdo e outras informações fornecidas por você quando usa nossos Serviços, como quando se cadastra em uma conta, cria ou compartilha conteúdos, envia mensagens ou se comunica com os outros. Isso pode incluir informações presentes no conteúdo ou a respeito dele, como a localização de uma foto ou a data em que um arquivo foi criado. Também coletamos informações sobre como você usa nossos

[87]DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010.p. 82-83. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>, acesso em : 12 jun. 17

[88] Idem. p. 83.

> Serviços, por exemplo, os tipos de conteúdo que você vê ou com que se envolve e a frequência ou duração de suas atividades[89].

Os mesmos termos também falam sobre a coleta de conteúdos e informações fornecidas por outras pessoas que utilizam o serviço mas estão relacionadas ao usuário, informações sobre pagamentos incluindo o número do cartão de crédito, dados sobre o dispositivo utilizado para acessar a rede social, informações sobre o usuário proveniente de sites em que navega que utilizem os serviços do Facebook, informações sobre localização que incluem a localização do dispositivo baseado no GPS, dentre outras[90].

No caso do Twitter, outra rede social de grande popularidade, existe a coleta de informações básicas sobre a conta que o usuário criou, contendo dados pessoais como o nome, o nome de usuário, a senha de acesso, o endereço de e-mail utilizado no cadastro ou o número de telefone. Se o usuário aceitar, também serão fornecidos sua lista de contatos, e se o mesmo enviar um e-mail para entrar em contato com a empresa administradora, sua mensagem será armazenada. Ao utilizar o Twitter, o usuário está tornando pública informações como sua breve biografia de perfil, sua localização, seu website, sua data de nascimento e sua fotografia. A rede também armazena a localização geográfica de seus usuários e as mensagens privadas que o mesmo envia[91].

Por fim, como uma última fonte, o Instagram[92] afirma coletar o nome de usuário, a senha e o endereço de e-mail da conta registrada no serviço. Também armazena informações que são colocadas no perfil do usuário, como o nome, o sobrenome, foto e o número de telefone. Para utilizar a ferramenta que permite encontrar amigos, o usuário concorda com a utilização de sua lista de contatos pelo Instagram, se utilizar um site de mídia social de terceiros, todas as informações repassadas por este serão armazenadas. Em sua ferramenta de análise são coletados informações enviadas pelo dispositivo do usuário, tais como as páginas da internet que foram acessadas, sob a promessa que tais dados não seriam utilizados para identificar a pessoa individualmente[93]. Estes podem ser destacados como os principais dados coletados, mas a lista completa é ainda maior.

---

[89] Informações obtidas em: <https://www.facebook.com/about/privacy/>, acesso em: 12 jun. 17.
[90] Idem.
[91] Informações obtidas em: <https://twitter.com/privacy>, acesso em: 12 jun. 17.
[92] Em setembro de 2012 o Instagram, rede social com foco no compartilhamento de fotos, foi adquirido pelo Facebook.
[93] Informações obtidas em: <https://help.instagram.com/155833707900388/?ref=hc_fnav>, acesso em: 12 jun. 17.

Observadas as redes acima, podemos concluir que todas elas seguem um padrão, o de coletar a maior quantidade possível de dados em relação ao seu usuário, desde os mais simples como as informações necessárias para finalizar o cadastro até informações mais complexas como as atividades do dispositivo utilizado para acessar o serviço.

O estudo da agência espanhola de proteção de dados aponta três momentos de risco para os dados do usuário das redes sociais. O primeiro aconteceria quando é realizado o registro e a configuração do perfil. O segundo momento ocorreria com o uso habitual da plataforma. Por último, o momento em que o usuário deixasse de utilizar o serviço, solicitando a exclusão de seu perfil[94].

Durante o seu registro, o usuário precisa estar ciente sobre as formas de tratamento que seus dados serão submetidos, destacando Danilo Doneda que é necessária uma "política de privacidade clara e precisa e do recurso a outros meios que garantam que sua inscrição não se efetive sem o real conhecimento de suas consequências[95]". No Brasil, o Marco Civil da Internet determina que a utilização dos dados pessoais precisa de um consentimento expresso da pessoa à qual pertencem[96].

Ainda nesta fase, o usuário deve valorar quais são as informações que deseja publicar e compartilhar, também é nela que o mesmo deve configurar o grau de publicidade que esta informação conterá, o que é essencial para a futura proteção de sua intimidade[97]. Desta forma, "(...) um possível risco que pode surgir é que o usuário não estabeleça adequadamente seu perfil de privacidade no momento de registro, seja por desconhecimento ou porque a própria rede não dispõe destas opções de configuração[98]".

---

[94] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales**. Madrid, 2009, p. 73-75.

[95] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 84. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>, acesso em : 12 jun. 17

[96] Este tema será aprofundado no item 3.1 deste estudo.

[97] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales.** Madrid, 2009, p. 73.

[98] Idem. p. 74.

No segundo momento, que se inicia com o uso habitual da rede social, os riscos surgem com a publicação de conteúdo pelo usuário, o que poderia levar a uma invasão de seu direito à intimidade ou própria imagem[99]. Destaca-se que este risco pode se originar de conteúdo publicado pelo próprio usuário, ou até mesmo de um terceiro, sendo assim:

> (...) a princípio qualquer usuário controla os conteúdos que deseja publicar, mas nem sempre valora a priori as implicações que podem resultar a exposição de determinados conteúdos. Ademais, o controle da informação publicada em uma rede social é limitado, na medida em que qualquer pessoa ou contato pode publicar fotografias, vídeos e comentários em que aparecem imagens ou etiquetas com o nome de outro usuário. Este último fato, sem dúvida alguma, pode colocar em risco a integridade dos direitos mencionados[100](...)

Mesmo sendo o próprio usuário que voluntariamente fornece os dados, as imagens ou qualquer outro tipo de informação, muitas das redes sociais permitem que os serviços de busca encontrados na Internet indexem as informações contidas nestes perfis, o que pode levar a um número maior de pessoas do que o imaginado pelo usuário com a possibilidade de acessar seus dados[101].

Mais grave ainda, se uma informação sobre uma pessoa não foi publicada por ela mesma, e provém de um terceiro, este deveria possuir seu consentimento. Nas palavras de Danilo Doneda:

> Na utilização da rede social, há ainda a possibilidade de que terceiros que não sejam inscritos na rede tenham seus dados difundidos. Isto ocorre quando tais dados são introduzidos na rede social por usuários regularmente inscritos, que podem descrever a participação deste terceiro em algum evento, publicar fotografias nas quais este terceiro é retratado ou, de alguma outra forma, tratar os dados pessoais de terceiros sem que tenham autorização para tal. Nestes casos, apesar da divulgação não autorizada ter partido de um ato do usuário registrado da rede social, é relevante o fato de que a divulgação da informação de terceiro se dá através da estrutura da rede social elaborada exatamente para o fim de fomentar o intercâmbio de informações e obter proveito desta atividade, abrindo a possibilidade para que possa ser responsabilizada pelo eventual dano causado a este terceiro[102].

Esta mesma possibilidade de responsabilização também deve ser válida caso um usuário compartilhe alguma informação de outro sem a sua permissão, uma vez que mesmo este último

---

[99] Idem. Ibidem.
[100] Idem. Ibidem.
[101] Idem. p.74-75
[102] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo**: para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 84. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>, acesso em : 12 jun. 17

tendo um cadastro na rede, este fato por si só não autoriza que suas informações circulem indiscriminadamente.

Ao deixar a rede social, riscos também se apresentam, pois mesmo cancelando sua conta, não existem garantias que suas informações intimas não continuarão circulando ou sendo armazenadas[103]. O estudo da Agência Espanhola de Proteção de Dados aponta que em muitos casos a saída da rede social pelos usuários é realizada através de mecanismos complexos que contrastam com a facilidade oferecida ao criar o cadastro, e que muitas vezes não é realizada de forma efetiva, sendo mantidos os dados pessoais dos usuários a disposição dos responsáveis das redes[104].

Sobre este tema, Danilo Doneda profere:

> O cancelamento dos dados pessoais em uma rede é a face mais extrema de uma garantia genérica do controle dos usuários de uma rede sobre seus próprios dados. A necessidade de definir instrumentos para este controle genérico verifica-se, por exemplo, no imperativo de fazer com que o próprio design da interface das redes sociais não acabe por ofuscar ou dificultar o exercício desta opção. Outro exemplo implica em dar passo além do mero cancelamento, ao proporcionar mecanismos que permitam a um usuário obter cópias de todas as informações pessoais que ele próprio forneceu a uma rede social (das quais, muito provavelmente, não possui cópias sistematizadas). Estes mecanismos, que atualmente encontram-se em diversos graus de implementação em algumas redes sociais, permitem tanto uma gestão mais direta e simplificada dos próprios dados pessoais como também permite que o cancelamento das informações e a saída da rede não seja inibida pelo receio da perda definitiva destas pelo seu próprio titular[105].

Cumpre destacar que independente do momento, os dados pessoais armazenados pelas redes sociais sempre se encontram sob a ameaça de serem adquiridos por terceiros não autorizados. Os sites das redes sociais possuem o risco de serem invadidos por *crackers*, especialistas em informática que:

> (...) atuam de forma claramente maliciosa, com o objetivo de prejudicar alguém ou tirar proveito ou partido de uma informação obtida, não se confundindo com os hackers, em relação aos quais não se aplica qualquer conotação pejorativa, sendo

---

[103] AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. **Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales**. Madrid, 2009, p. 75.

[104] Idem. p. 101-102.

[105] DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. p. 112. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>, acesso em : 12 jun. 17

> igualmente capazes de invadir computadores alheios, mas também de impedir eventuais invasões[106].

Há também a possibilidade da obtenção não autorizada de dados por *crackers* mas que não envolva uma falha no sistema da rede social, e sim o próprio comportamento do usuário. Esta prática se utiliza de técnicas de análise do comportamento humano para a obtenção de senhas, e é chamada de *engenharia social*[107]. Trata-se de uma atividade que analisa o comportamento social para descobrir as senhas das pessoas, identificando que é comum, por exemplo, o uso de datas de nascimento, nomes e sobrenomes de pessoas próximas aos usuários como suas senhas[108].

2.4 Princípios para impedir o uso abusivo de dados pelas redes sociais

Exibidos os riscos presentes na relação do usuário com a rede social, serão analisados os princípios apresentados por Stefano Rodotá e Danilo Doneda, dentre outros autores, que devem ser respeitados pelas empresas administradoras das redes sociais para garantir uma utilização segura e não abusiva dos dados pessoais.

2.4.1 Princípio da publicidade

Este princípio, que muitas vezes é referido como princípio da transparência, define que todo banco de dados que armazene dados pessoais tem que ser de conhecimento público, sendo por meio de uma exigência de autorização prévia para funcionar, por meio de uma notificação a uma autoridade sobre o seu funcionamento ou através do envio periódico de relatórios[109].

Além disso, Tatiana Malta Vieira destaca:

> A obrigatoriedade de os responsáveis por bancos de dados informarem o público sobre sua existência encontra-se norteada pelo princípio da publicidade, impondo-se a divulgação da finalidade da operação e os procedimentos utilizados para tratamento

---

[106] MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet**. 2a ed. São Paulo: Revista dos Tribunais, 2014. p. 217-218.
[107] Idem. p. 221.
[108] Idem. p. 222.
[109] DONEDA, Danilo. ***A proteção dos dados pessoais como um direito fundamental***. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011. p. 100.

> de dados de caráter pessoal. Essas informações devem ser disponibilizadas em meio de ampla divulgação e de fácil acesso(...)[110]

Como fonte internacional, o regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa afirma que:

> O princípio da transparência exige que qualquer informação destinada ao público ou ao titular dos dados seja concisa, de fácil acesso e compreensão, bem como formulada numa linguagem clara e simples, e que se recorra, adicionalmente, à visualização sempre que for adequado. Essas informações poderão ser fornecidas por via eletrônica, por exemplo num sítio web, quando se destinarem ao público. Isto é especialmente relevante em situações em que a proliferação de operadores e a complexidade tecnológica das práticas tornam difícil que o titular dos dados saiba e compreenda se, por quem e para que fins os seus dados pessoais estão a ser recolhidos, como no caso da publicidade por via eletrônica. Uma vez que crianças merecem proteção específica, sempre que o tratamento lhes seja dirigido, qualquer informação e comunicação deverá ser redigida numa linguagem clara e simples que a criança compreenda facilmente[111].

Em seu artigo 5°, o regulamento também expressamente prevê que os dados pessoais devem ser tratados de forma lícita, leal e principalmente, de forma transparente.

Internamente no Brasil, podemos observar este princípio no art. 43 do Código de Defesa do Consumidor que estabelece que a abertura de cadastro, ficha, registro de dados pessoais e de consumo deve ser comunicada por escrito ao consumidor quando não for solicitada por ele[112].

No projeto de lei n° 5.276-A de 2016, temos a previsão expressa do princípio da transparência no inciso VI de seu artigo 6°, que define o que deve ser observado durante as atividades de tratamento de dados, garantindo aos seus titulares informações claras, adequadas e de fácil acesso sobre a realização do tratamento e os respectivos agentes de tratamento[113].

---

[110] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 253.

[111] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 12 jun. 17.

[112] BRASIL. **Lei n° 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm >, acesso em 12 jun. 17.

[113] BRASIL, Câmara dos Deputados. **Projeto de Lei n. ° 5.276-A/2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=C2874759AD9F780699B58C8058EB45ED.proposicoesWeb2?codteor=1470645&filename=Avulso+-PL+5276/2016>, acesso em: 12 jun. 2017.

2.4.2 Princípio da exatidão

Segundo este princípio, os dados coletados e armazenados pelas redes sociais devem ser fiéis a realidade, implicando em uma cuidadosa e correta coleta, bem como tratamento adequado, sendo necessário sua atualização constante para refletir a verdade sobre o usuário[114].

Alguns autores se referem a este princípio sob a denominação de princípio da veracidade, e segundo Catarina Sarmento e Castro, uma inexistência de correção ou de atualização destes dados geram grandes prejuízos para o usuário, logo, é uma obrigação dos responsáveis por manter os bancos de dados mantê-los atualizados[115].

No regulamento 2016/679 do Parlamento Europeu e do Conselho, temos a previsão deste princípio no artigo 5°, alínea "d", ao afirmar que os dados pessoais devem ser exatos e devem ser atualizados sempre que necessário, sendo adotadas todas as medidas adequadas para que no momento que exista uma inexatidão, a mesma seja apagada ou retificada sem demora[116].

Em território nacional, podemos observar o princípio da exatidão no parágrafo 3° do artigo 43 do Código de Defesa do Consumidor, afirmando que o consumidor ao encontrar inexatidão nos seus dados "(...)poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas[117]".

A preocupação do legislador com este princípio também é notada em uma análise do projeto de lei n° 5.276-A de 2016, que faz referência a qualidade dos dados em seu artigo 6°, inciso V, procurando garantir aos titulares dos dados "(...) a exatidão, a clareza, relevância e a

---

[114] DONEDA, Danilo. **O direito fundamental à proteção de dados pessoais**. In: MARTINS, Guilherme Magalhães (Coord.). Direito Privado e Internet. São Paulo: Atlas, 2014. p. 71.
[115] CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005. p. 237
[116] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 12 jun. 17.
[117] BRASIL. **Lei n° 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm >, acesso em 12 jun. 17.

atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento[118]".

2.4.3 Princípio da finalidade

A utilização de dados pela rede social deve obedecer a finalidade que a mesma comunicou à seu usuário no momento da celebração do contrato[119]. Danilo Doneda destaca a importância deste princípio:

> Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade)[120].

Este princípio também pode ser chamado de princípio da proporcionalidade, e é dele que surge o direito do usuário em negar a divulgação de sua informação, surgindo o direito de oposição, alcançando até mesmo os dados sobre sua pessoa que foram fornecidos por terceiros[121].

O artigo 5° do regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa estipula:

> 1. Os dados pessoais são:
> (...)
> b) Recolhidos para finalidades determinadas, explícitas e legítimas e não podendo ser tratados posteriormente de uma forma incompatível com essas finalidades; o tratamento posterior para fins de arquivo de interesse público, ou para fins de investigação científica ou histórica ou para fins estatísticos, não é considerado incompatível com as finalidades iniciais(...)

A necessidade da finalidade para a coleta e o armazenamento de dados é encontrada também no Marco Civil da Internet que declara em seu artigo 7°:

---

[118] BRASIL, Câmara dos Deputados. **Projeto de Lei n. ° 5.276-A/2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=C2874759AD9F780699B58C8058EB45ED.proposicoesWeb2?codteor=1470645&filename=Avulso+-PL+5276/2016>, acesso em: 12 jun. 2017.

[119] DONEDA, Danilo. **O direito fundamental à proteção de dados pessoais**. In: MARTINS, Guilherme Magalhães (Coord.). Direito Privado e Internet. São Paulo: Atlas, 2014. p. 72.

[120] Idem. Ibidem.

[121] CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005. p. 254

> Art. 7°. O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
> (...)
> VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

Ressalva-se que o direito de se opor a divulgação de dados encontra algumas limitações, onde é permitida a coleta e o repasse de dados se a mesma for imposta por um dispositivo legal, como são os casos da armazenagem de informações quando forem imprescindíveis para o combate e prevenção de epidemias, para a investigação criminal, para a segurança pública e para prevenir infrações penais[122].

2.4.4 Princípio do livre acesso

Através deste princípio, todo usuário de rede social tem direito a acessar o banco de dados no qual suas informações se encontram armazenadas, sendo possível que o mesmo obtenha cópias dos registros[123].

Posterior ao acesso é possível que o usuário exerça o controle de seus dados e promova a correção de informações incorretas, derivando tal ato tanto do livre acesso quanto do princípio da exatidão[124].

Stefano Rodotá, sobre este princípio, profere:

> Este é, antes de tudo, um instrumento diretamente acionável pelos interessados, que podem utilizá-lo não somente com a finalidade de simples conhecimento, mas também para promover propriamente a efetividade de outros princípios, Salienta-se, de fato, que entre os poderes atribuídos pelo direito de acesso existe também o de obter a correção, a integração ou eliminação dos dados coletados. Mas o exercício concreto desses poderes pressupõe a violação de um outro princípio, por exemplo, o da correção, da exatidão ou da finalidade: o princípio do acesso coloca-se, portanto,

---

[122] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 257.
[123] DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011. p. 100-101.
[124] Idem. Ibidem.

> em um plano diferente e surge como um instrumento para a atuação direta de um interesse individual e para garantir a efetividade de um (outro) princípio geral[125].

O titular dos dados pessoais pode exercer seu direito de acesso para conhecer, modificar ou atualizar suas informações independente da apresentação de justificativas[126], e o principal meio para realizar esta atividade, caso não consiga realizá-la ao entrar em contato direto com a rede social, é a ação de *habeas data*[127].

O artigo 13° do regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa expressamente reconhece esse direito de acesso aos dados ao determinar que:

> 2. Para além das informações referidas no n° 1, aquando da recolha de dados pessoais, o responsável pelo tratamento fornece ao titular as seguintes informações adicionais, necessárias para garantir um tratamento equitativo e transparente:
> (...)
> b) A existência do direito de solicitar ao responsável pelo tratamento acesso aos dados pessoais que lhe digam respeito, bem como a sua retificação ou seu apagamento, e a limitação do tratamento no que disser respeito ao titular dos dados, ou do direito de se opor ao tratamento, bem como o direito à portabilidade dos dados;
> (...)

No direito interno, podemos citar o caput e o parágrafo 3° do artigo 43 do Código de Defesa do Consumidor, que garante acesso às informações que são armazenadas sobre o usuário, bem como a possibilidade do mesmo exigir a correção de qualquer inexatidão[128].

2.4.5 Princípio da segurança física e lógica

Este princípio define que os dados pessoais dos usuários das redes sociais sejam protegidos contra riscos, que podem ser: o extravio, a destruição, a modificação não autorizada, a transmissão sem o consentimento do usuário e o acesso por terceiros não autorizados[129].

---

[125] RODOTÁ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 60.
[126] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 258.
[127] A ação de habeas data será aprofundada no item 3.2 do próximo capítulo.
[128] BRASIL. **Lei n° 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm >, acesso em 12 jun. 17.
[129] DONEDA, Danilo. **O direito fundamental à proteção de dados pessoais**. In: MARTINS, Guilherme Magalhães (Coord.). Direito Privado e Internet. São Paulo: Atlas, 2014. p. 72.

O princípio da segurança determina que os responsáveis por manter bancos de dados com dados pessoais de usuários utilize todos os meios técnicos e administrativos que garantam a sua segurança, reconhecendo que a atividade de armazenagem de dados é uma atividade de risco[130].

No regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa, o artigo 5° reconhece a importância de garantir a segurança dos dados:

> 1. Os dados pessoais são:
> (...)
> f) Tratados de uma forma que garanta a sua segurança, incluindo a proteção contra o seu tratamento não autorizado ou ilícito e contra a sua perda, destruição ou danificação acidental, adotando as medidas técnicas ou organizativas adequadas («integridade e confidencialidade»).

No Brasil, o zelo pela segurança dos dados pessoais pode ser observado no projeto de lei n° 5.276-A de 2016, que em seu artigo 6°, inciso VII, define que "devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão[131]".

---

[130] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 263.

[131] BRASIL, Câmara dos Deputados. **Projeto de Lei n. ° 5.276-A/2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_mostrarintegra;jsessionid=C2874759AD9F780699B58C8058EB45ED.proposicoesWeb2?codteor=1470645&filename=Avulso+-PL+5276/2016>, acesso em: 12 jun. 2017.

3. ANÁLISE DOS MÉTODOS DE PROTEÇÃO DE DADOS PESSOAIS

3.1 A necessidade do consentimento expresso pelos usuários das redes sociais para o uso de seus dados

Uma das formas de garantir a proteção de dados do usuário de uma rede social é a exigência de que qualquer atividade de tratamento seja consentida pelo usuário. É possível observar esta obrigação dentro do ordenamento jurídico brasileiro, assim como na jurisdição internacional.

O Marco Civil da Internet em seu artigo 7° estipula algumas garantias que protegem o usuário, dentre elas, o "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo consentimento livre, expresso e informado ou nas hipóteses previstas em lei[132]".

O regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa, ao tratar do consentimento do usuário, afirma:

> O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante declaração escrita, inclusive em formato eletrônico, ou uma declaração oral. O consentimento pode ser dado validando uma opção ao visitar um sitio web na Internet, selecionando os parâmetros técnicos para os serviços da sociedade da informação ou mediante outra declaração ou conduta que indique claramente nesse contexto que aceita o tratamento proposto dos seus dados pessoais. O silêncio, as opções pré-validadas ou a omissão não deverão, por conseguinte, constituir um consentimento. O consentimento deverá abranger todas as atividades de tratamento realizadas com a mesma finalidade. Nos casos em que o tratamento sirva fins múltiplos, deverá ser dado um consentimento para todos esses fins. Se o consentimento tiver de ser dado no seguimento de um pedido apresentado por via eletrônica, esse pedido tem de ser claro e conciso e não pode perturbar desnecessariamente a utilização do serviço para o qual é fornecido[133].

Adiante, em seu artigo 4°, o regulamento apresenta uma definição precisa do que seria o consentimento do usuário, que é "(...) uma manifestação de vontade, livre, específica,

---

[132] BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014. Disponível em: <http:// www.planalto.gov.br/ ccivil_03/_ato2011-2014/2014/lei/l12965.htm> , acesso em: 12 jun. 17.

[133] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 12 jun. 17.

informada e explícita, pela qual o titular dos dados aceita, mediante declaração ou ato positivo inequívoco, que os dados pessoais que lhe dizem respeito sejam objeto de tratamento[134]".

Nas palavras de Danilo Doneda, o consentimento do usuário:

> (...) é um dos pontos mais sensíveis de toda a disciplina de proteção de dados pessoais; através do consentimento, o direito civil tem a oportunidade de estruturar, a partir da consideração da autonomia da vontade, da circulação de dados e dos direitos fundamentais, uma disciplina que ajuste os efeitos desse consentimento à natureza dos interesses em questão[135].

É possível apresentar um questionamento sobre o porquê de não haver uma previsão legal dos limites do tratamento de dados, atribuindo essa limitação a autonomia da vontade do usuário que pode dispor da utilização dos seus dados livremente. Sobre este questionamento, Stefano Rodotá explica que esta preferência pelo consentimento do usuário em detrimento de uma norma que limitasse o tratamento de dados provém das dificuldades e desconfianças em se criar tal norma que estabeleceria um sistema de autorizações e proibições por via legislativa[136].

A crítica feita por Stefano Rodotá a esta postura que delega ao próprio usuário a tutela de seus dados, é que se estaria disciplinando a circulação de dados unicamente numa dimensão proprietária. Estaríamos tratando de dados como propriedade exclusiva do interessado, o que levaria à negociação de sua cessão de forma ilimitada e ignoraria uma outra dimensão, aquela ligada as consequências sociais da circulação de dados considerados sensíveis, pois estes geram práticas discriminatórias contra o usuário[137].

Outra crítica, apresentada por Danilo Doneda, é a real impossibilidade de se opor ao tratamento de dados, o que na verdade descaracterizaria propriamente o consentimento. O autor destaca que nas situações reais do cotidiano, o usuário não possui poder de autodeterminação, uma vez que não existe a real possibilidade de não concordar com o tratamento de dados[138].

No momento em que o usuário das redes sociais realiza seu cadastro, é obrigado a concordar com os termos que lhe são apresentados, e como discutido anteriormente, é ausente

---

[134] Idem.
[135] DANILO, Doneda. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 371.
[136] RODOTÁ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Rio de Janeiro: Renovar, 2008. p. 76
[137] Idem. p. 76-79
[138] DANILO, Doneda. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 373.

a possibilidade de ser feita uma contra proposta pelo usuário ao contrato que este deve aderir. Desta forma, é impossível para o usuário exercer o seu direito de oposição à forma que as administradoras de redes sociais irão lidar com seus dados pessoais. Nas palavras de Danilo Doneda: "A disparidade de meios entre a pessoa, de quem são exigidos os dados pessoais, e aquele que solicita faz a verdadeira "opção" seja tantas vezes a de "tudo ou nada", "pegar ou largar[139]".

Existe também uma pressão social que contribui para a dificuldade em se opor ao tratamento de dados da forma estabelecida nos contratos de uso das redes sociais. Estas redes se encontram tão fortemente ligadas a vida moderna das pessoas, que o simples fato de uma pessoa não possuir um perfil em uma delas pode gerar uma exclusão social. O temor dessa exclusão gera uma necessidade de participar destes serviços, ignorando os riscos que o tratamento inadequado dos dados pode causar a própria pessoa. Como falado anteriormente, o usuário não enxerga outra alternativa para participar da rede social que não implique na aceitação total dos termos apresentados.

Outro problema relacionado ao consentimento, está no fato de que o tratamento de dados realizados pelas redes sociais não é uma atividade visível para o usuário. Desta forma, é "nítida a extrema facilidade de mascarar os reais efeitos deste tratamento, tornando-os difíceis de serem identificados ou mesmo invisíveis[140]". Isto dificulta o usuário conseguir verificar se a utilização pela qual consentiu está realmente sendo respeitada por parte da administradora da rede.

Como consequências desta impossibilidade de verificação, temos que entender o consentimento como "um ato unilateral, cujo efeito é o de autorizar um determinado tratamento para os dados pessoais, sem estar diretamente vinculado a uma estrutura contratual[141]".

A importância de não encararmos o consentimento como algo relacionado ao contrato está na possibilidade de reconhecermos a sua revogação. Se o consentimento é uma forma de manifestação da autonomia da vontade, é inegável que a pessoa possui o direito de cancelar o seu consentimento a qualquer momento. Neste sentido:

---

[139] Idem. Ibidem
[140] Idem. p. 373-374.
[141] Idem. p. 378.

> Examinando a natureza do instituto e dos interesses em questão, deve-se reconhecer a possibilidade de revogação do ato pelo qual uma pessoa consente no tratamento de seus dados pessoais. Neste poder do sujeito, encontra-se o próprio sentido de autodeterminação em relação à construção de sua esfera privada, poder este que, ligado ao livre desenvolvimento da personalidade, merece a tutela do ordenamento[142].

A revogação do consentimento encontra, entretanto, uma enorme barreira ao falarmos das redes sociais. Como mencionado extensivamente durante este estudo, a inexistência da habilidade do usuário em contrapor os termos da rede social, faz com que a única forma do mesmo revogar a permissão do tratamento de seus dados ser a sua saída do serviço. Apesar disto, falar em revogação do consentimento é essencial para o estudo que está sendo realizado, principalmente, quando falarmos sobre o direito do usuário de solicitar a exclusão de todos os seus dados que foram armazenados[143].

3.2 Utilização do *habeas data* no âmbito civil como forma de verificar os dados que as redes sociais estão coletando

A ação de *habeas data*, é prevista na Constituição da República Federativa do Brasil de 1988, em seu artigo 5°, inciso LXXII[144], desta forma podemos perceber que o legislador originário teve a preocupação de reconhecer este meio de acesso à informações como um direito fundamental.

Danilo Doneda destaca a importância da existência desta ação:

> (...) o *habeas data* formalmente não representa uma mudança no perfil material do direito à privacidade, o fato é que ele serviu para atrair para si a responsabilidade pela sua efetividade. Assim, teve o mérito de chamar a atenção do operador e da sociedade para um direito que vinha sendo negligenciado[145] (...)

---

[142] Idem. p. 380-381

[143] Este direito será profundamente estudado no item 3.3, que irá focar no direito ao esquecimento.

[144] 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:
(...)
LXXII - conceder-se-á habeas data:
a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;
b) para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
(...)

[145] DANILO, Doneda. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 335.

O habeas data também possui lei específica que regulamenta o seu procedimento, trata-se da lei 9.507, de 12 de novembro de 1997, que em seu artigo 7° reconhece a possibilidade de propor ação[146]:

> I - para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registro ou banco de dados de entidades governamentais ou de caráter público;
> II - para a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo;
> III - para a anotação nos assentamentos do interessado, de contestação ou explicação sobre dado verdadeiro mas justificável e que esteja sob pendência judicial ou amigável.

Com isto, podemos observar que em sua previsão legal, o remédio constitucional do *habeas data* é indicado para uso frente entidades governamentais ou de caráter público, o que pode gerar dúvidas sobre a sua aplicabilidade em âmbito civil, por exemplo, sua possível utilização para obter informações sobre os dados que as redes sociais armazenam.

Sobre esta discussão, podemos nos remeter ao artigo 43 do Código de Defesa do Consumidor, que estabelece em seu caput e respectivos parágrafos, que todo consumidor, independentemente do que está disposto no artigo 86 do mesmo código, tem direito ao acesso as informações armazenadas em cadastros, fichas, registros arquivados sobre ele[147]. Aqui podemos observar a manifestação do princípio do livre acesso que já foi estudado anteriormente. O artigo supra mencionado entretanto não define as ferramentas que o usuário pode utilizar para ter seu direito garantido.

Acerca dessa ausência de previsão da ferramenta, Marcel Leonardi afirma:

> Nota-se que o caput do art. 43 faz referência ao art. 86 que, em sua redação proposta, previa expressamente a aplicação do *habeas data* à tutela dos direitos e interesses do consumidor. No entanto, o artigo foi vetado pelo Presidente da República, pois à época se entendia que o *habeas data* deveria ter aplicação restrita à defesa de direitos subjetivos públicos e, como tal, não poderia ser utilizado para tutelar direitos privados do consumidor, tendo sido ignorado que o art. 86 tinha mera função didática, servindo apenas para afastar dúvidas a respeito do cabimento do *habeas data* para a tutela dos direitos e interesses dos consumidores[148].

---

[146] BRASIL. **Lei n° 9.507 de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. Diário Oficial da União, Brasília, DF, 13 nov. 1997. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9507.htm>, acesso em 12 jun. 17.
[147] BRASIL. **Lei n° 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>, acesso em 12 jun. 17.
[148] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012. p. 199.

O mesmo autor ainda comprova a ineficácia deste veto uma vez que a redação original do parágrafo 4° do artigo 43 do Código de Defesa do Consumidor foi mantida[149], logo considerando os bancos de dados como entidades de caráter público não sobram discussões sobre a possibilidade de se utilizar a ação de *habeas data*, pois o inciso LXXII do artigo 5° da Constituição Federal prevê esta ação contra estas entidades[150].

Existem algumas barreiras que dificultam a aplicabilidade da ação. Danilo Doneda, por exemplo, destrincha o que pode ser a maior delas:

> Aquele que provavelmente é a maior limitação do *habeas data* não é perceptível pelo seu exame específico, porém deflui do contexto no qual se insere. O sistema de proteção de dados pessoas que tenha como instrumentos principais de atuação o recurso a uma ação judicial (e isso somente após um infestável périplo administrativo) não se nos apresenta como um sistema adequado às exigências da matéria. Os problemas relacionados ao tratamento de dados pessoais, conforme observamos, processam-se cada vez mais "em branco", sem que o interessado se aperceba. Este, nas situações em que sabe ou suspeita que seus dados armazenados em algum banco de dados seja errôneos, ou então, tem conhecimento do seu uso indevido – ou mesmo deseja simplesmente deseja fazer uma verificação – encontra-se diante da necessidade de recorrer a uma incerta via administrativa (cujo não atendimento, aliás, não acarreta penalidade objetiva ao responsável pelo armazenamento dos dados) e, no insucesso desta tentativa deve utilizar-se do *habeas data* que, ao contrário do *habeas corpus*, exige um advogado para sua interposição – um tratamento bastante inadequado para um interesse cuja atuação pede o recurso a instrumentos promocionais[151].

É importante que seja frisado que não é permitido que o usuário tente obter informações sobre seus dados diretamente pela via judicial. A súmula número 2 do Superior Tribunal de Justiça, impede que seja impetrada a ação de *habeas data* se não houver uma recusa do fornecimento por parte daquele que administra o banco de dados[152]. No caso das redes sociais, obter esta informação por meio do contato direto com a sua administradora pode ser uma tarefa de extrema dificuldade, mas tem caráter essencial pois o número de usuários deste serviço é de uma tamanha grandeza que se toda vez que um usuário quiser obter seus dados tiver que recorrer ao poder judiciário, ocorrerá uma aglutinação ainda maior de processos em um judiciário já superlotado.

---

[149] (...)
§ 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

[150] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012. p. 199.

[151] DANILO, Doneda**. Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 337.

[152] BRASIL. Superior Tribunal de Justiça. **Súmula n° 2**. Não cabe o habeas data (cf, art. 5., lxxii, letra "a") se não houve recusa de informações por parte da autoridade administrativa. Disponível em: <http://www.stj.jus.br/docs_internet/SumulasSTJ.pdf>, acesso em: 12 jun. 2017

Outro ponto importante a ser analisado sobre esta ação é que apesar de sua aparente gratuidade, pois não existe pagamento de despesas processuais, o usuário que deseje utilizá-la acaba tendo que arcar com os custos inerentes da ação judicial como, por exemplo, o pagamento de um advogado[153]. Esse custo, aliado a falta de conhecimento de seus direitos, diminui a eficácia deste meio de garantir a proteção dos dados pessoais.

Marcel Leonardi debate uma possibilidade de solucionar o problema do custo da ação, mas ao mesmo tempo indica a dificuldade de ser aplicada tal solução em razão da falta de consolidação da jurisprudência:

> Esse problema poderia ser minimizado se o profissional contratado pelo consumidor aceitasse trabalhar em troca do recebimento das verbas decorrentes do ônus da sucumbência, porém a controvérsia sobre o seu cabimento nas ações judiciais de *habeas data*. Há algumas decisões de tribunais estaduais entendendo que, por aplicação do princípio da sucumbência, previsto no art. 20 do Código de Processo Civil, é cabível a condenação. Por outro lado, o entendimento dos tribunais superiores é em sentido contrário, afastando a condenação nos ônus da sucumbência em tais hipóteses[154] (...)

A título explicativo, destaca-se que o conteúdo do artigo 20 citado pelo autor é referente ao antigo Código de Processo Civil de 11 de janeiro de 1973[155], hoje, o artigo equivalente a este é o artigo 85 do Código de Processo Civil de 2015[156].

Por todas as razões apresentadas, a ação de *habeas data* no âmbito civil como forma de verificação dos dados coletados pelas redes sociais, na prática é rara. Destaca a doutrina que é necessária a criação de um órgão que seja dedicado a proteção de dados, e que por meio dele, as atividades referentes a armazenagem de dados das redes sociais seja fiscalizada, além disso, tal órgão precisa possibilitar o fácil acesso do usuário à seus dados que foram armazenados sem que o mesmo precise recorrer ao judiciário[157]. Desta forma, seria possível reduzir a necessidade de impetrar a ação de *habeas data*.

---

[153] LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012. p. 204.
[154] Idem. p. 205.
[155] Art. 20. A sentença condenará o vencido a pagar ao vencedor as despesas que antecipou e os honorários advocatícios. Esta verba honorária será devida, também, nos casos em que o advogado funcionar em causa própria.
[156] Art. 85. A sentença condenará o vencido a pagar honorários ao advogado do vencedor.
[157] DANILO, Doneda. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 396-402

No ordenamento europeu, já é possível identificar uma preocupação com a existência de um órgão que exerça a fiscalização da utilização de dados pessoais, existindo sob a forma de autoridades de controle independente, que possuem um grande número de atribuições segundo o artigo 57° do regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa. Dentre elas podemos citar[158]:

> 1. Sem prejuízo de outras atribuições previstas nos termos do presente regulamento, cada autoridade de controlo, no território respectivo:
> a) Controla e executa a aplicação do presente regulamento;
> b) Promove a sensibilização e a compreensão do público relativamente aos riscos, às regras, às garantias e aos direitos associados ao tratamento. As atividades especificamente dirigidas às crianças devem ser alvo de uma atenção especial;
> (...)
> d) Promove a sensibilização dos responsáveis pelo tratamento e dos subcontratantes para as suas obrigações nos termos do presente regulamento;
> e) Se lhe for solicitado, presta informações a qualquer titular de dados sobre o exercício dos seus direitos nos termos do presente regulamento e, se necessário, coopera com as autoridades de controlo de outros Estados-Membros para esse efeito;
> f) Tarta as reclamações apresentadas por qualquer titular de dados, ou organismo, organização ou associação nos termos do artigo 80°, e investigar, na medida do necessário, o conteúdo da reclamação e informar ao autor da reclamação do andamento e do resultado da investigação num prazo razoável, em especial se forem necessárias operações de investigação ou de coordenação complementares com outra autoridade de controlo;
> (...)

Na opinião de Danilo Doneda, o órgão que deve ser criado para tutelar a proteção de dados pessoais no Brasil, precisa possuir o perfil de uma autoridade independente, como uma agência reguladora, pois o mesmo deve estar desvinculado de qualquer um dos poderes para que seja um órgão neutro[159]. Este órgão seria a peça fundamental para efetivar o direito de acesso aos dados sem que o usuário precisasse recorrer ao judiciário, por meio da ação de *habeas data*.

3.3 O direito ao esquecimento

[158] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 10 mai. 17.
[159] DANILO, Doneda. **Da privacidade à proteção de dados pessoais**. Rio de Janeiro: Renovar, 2006. p. 401-402

O direito ao esquecimento, é um direito que está crescendo em número de discussões na era digital. Ele estipula a possibilidade de uma pessoa solicitar que todos os seus dados pessoais sejam apagados de um sistema que os armazena[160].

Jeffren Rosen destaca que na teoria, o direito de ser esquecido busca endereçar um grande problema da era digital, sendo este a grande dificuldade de escapar do passado na Internet, uma vez que todas as fotos, publicações de *status* e *tweet* sobrevivem para sempre em uma nuvem virtual[161].

Segundo o mesmo autor, existe um dilema de posicionamentos referentes ao direito ao esquecimento, colocando os ideais europeus em choque com os pensamentos norte-americanos sobre o tema:

> Na Europa, as raízes intelectuais do direito a ser esquecido são encontradas nas leis francesas, que reconhecem *le droit à l'oubli* – ou o "direito ao oblívio" – um direito que permite que um criminoso condenado que cumpriu o tempo de sua pena e foi reabilitado possa protestar contra a publicação de fatos sobre sua condenação e encarceramento. Na America, em contraste, a publicação do histórico criminal de uma pessoa é protegido pela Primeira Emenda[162](...)

O autor ainda continua, afirmando que os legisladores europeus "acreditam que todos os cidadãos encaram a dificuldade de escapar do seu passado agora que a Internet grava tudo e não esquece nada – uma dificuldade que era limitada aos condenados criminalmente[163]".

No regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa, em seu artigo 17° é definido[164]:

> 1. O titular tem o direito de obter do responsável pelo tratamento o apagamento dos seus dados pessoais, sem demora injustificada, e este tem a obrigação de apagar os dados pessoais, sem demora injustificada, quando se aplique um dos seguintes motivos:

---

[160] MARTINS, Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet**. 2a ed. São Paulo: Revista dos Tribunais, 2014. p. 277-303

[161] ROSEN, Jeffrey. ***The Right to be Forgotten***. Disponível em: <https://www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>, acesso em: 12 jun. 2017.

[162] Idem.

[163] Idem.

[164] UNIÃO EUROPEIA. **Regulamento 2016/679 do Parlamento Europeu e do Conselho da Europa**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 12 mai. 17.

> a) Os dados pessoais deixaram de ser necessários para a finalidade que motivou a sua recolha ou tratamento;
> b) O titular retira o consentimento em que se baseia o tratamento dos dados nos termos do artigo 6°, n° 1, alínea a), ou do artigo 9°, n° 2, alínea a) e se não existir outro fundamento jurídico para o referido tratamento;
> c) O titular opõe-se ao tratamento nos termos do artigo 21, n° 1, e não existem interesses legítimos prevalecentes que justifiquem o tratamento, ou o titular opõe-se ao tratamento nos termos do artigo 21°, n° 2;
> d) Os dados pessoais foram tratados ilicitamente;
> e) Os dados pessoais têm de ser apagados para o cumprimento de uma obrigação jurídica decorrente do direito da União ou de um Estado-Membro a que o responsável pelo tratamento esteja sujeito;
> f) Os dados pessoais foram recolhidos no contexto da oferta de serviços da sociedade da informação referida no artigo 8°, n° 1.

No regulamento, observa-se a preocupação do legislador europeu em garantir aos cidadãos a possibilidade de ter seus dados apagados e, além disso, que esta ação seja realizada da forma mais rápida possível. Este posicionamento é claramente um resultado de princípios como o da finalidade e do livre acesso, e da possibilidade de revogar o consentimento fornecido no contrato.

É possível discutir a existência de três categorias do direito ao esquecimento, segundo Peter Fleischer[165]. A primeira é aquela referente a tutela dos dados disponibilizados pelo próprio usuário, em que o mesmo teria o direito inquestionável de poder apagar tais dados; a segunda trata da tutela de conteúdo que é postado pelo usuário, deletado pelo mesmo, mas que terceiros copiaram e repostaram; a terceira e última é a categoria que tutela sobre conteúdos postados por terceiros sobre uma pessoa[166].

Guilherme Magalhães Martins destrincha a polêmica referente a segunda categoria do direito ao esquecimento. O autor questiona se uma vez que um conteúdo removido pelo usuário de uma rede social seja repostado por outra pessoa, e esta pessoa seja contatada para apagar este conteúdo repostado mas não efetue tal ação, se a própria rede social deveria promover a remoção deste conteúdo mesmo sem a autorização de quem repostou[167].

O professor explica:

---

[165] Peter Fleischer é o conselheiro da empresa Google sobre privacidade global.

[166] FLEISCHER, Peter. ***Foggy thinking about the Right to Oblivion***. Disponível em: <http://peterfleischer.blogspot.com.br/2011/03/foggy-thinking-about-right-to-oblivion.html>, acesso em: 11 jun. 2017.

[167] MARTINS, Guilherme Magalhães. **O direito ao esquecimento na internet**. In: MARTINS, Guilherme Magalhães (Coord.). Direito Privado e Internet. São Paulo: Atlas, 2014. p.15.

> De acordo com a proposta europeia do direito ao esquecimento, a resposta certamente seria que sim. De acordo com o regulamento, quando alguém deseja deletar os seus dados pessoais, o serviço provedor da Internet deve atender à solicitação sem demora, a não ser que a retenção do dado seja necessária ao exercício do à livre expressão, definido pelos estados membros nas suas próprias leis locais[168].

Identifica-se que um dos maiores questionamentos ao direito ao esquecimento é em relação ao balanço entre direito a proteção de dados, que culmina na possibilidade do mesmo exigir a remoção de determinado conteúdo, e a liberdade de expressão. Este questionamento é a base das discussões acerca da terceira categoria do direito ao esquecimento, em que devem ser pensados os limites do direito de exigir que um terceiro apague uma informação que tenha publicado sobre uma pessoa[169].

Viviane Reding[170], em discurso perante a *Innovation Conference Digital, Life, Design* afirma:

> O direito de ser esquecido claramente não é um direito absoluto. Há casos onde existe legitimidade e interesse legalmente justificado em manter dados nos bancos de dado. Os arquivos de jornais são um bom exemplo. Está claro que o direito de ser esquecido não pode se tornar um direito ao apagamento total da história. Também não pode o direito a ser esquecido tomar precedente sobre a liberdade de expressão ou a liberdade da mídia[171].

Uma última análise que podemos realizar é a importância do direito ao esquecimento como uma garantia da real exclusão dos dados armazenados pelas redes sociais, quando o usuário decide encerrar seu cadastro. É comum observarmos uma prática de manter os dados disponíveis por um tempo, no qual o usuário poderia reativar seu cadastro recuperando suas informações. É interessante esta postura pois permite que o usuário se arrependa da exclusão de seu perfil sem que o mesmo perca suas informações, mas também deveria existir a possibilidade da exclusão, à pedido do próprio usuário, se realizar de forma imediata. Neste ponto, o direito ao esquecimento nos moldes da União Europeia pode ser uma ferramenta essencial para alcançar este objetivo.

---

[168] Idem, p. 15-16.
[169] Idem. p. 17.
[170] Viviane Reding é atualmente membro do Parlamento Europeu, ao tempo de seu discurso ocupava o cargo de vice presidente da Comissão Européia.
[171] REDING, Viviane. ***The EU data protection reform 2012: Making Europe the standard setter for modern data protection rules in the digital age***. Discurso na Innovation Conference Digital, Life, Design, realizada em Monique em 22 de janeiro de 2012. Disponível em: <http://europa.eu/rapid/pressReleasesAction.do ?reference=SPEECH/ 12/26&format=PDF>, acesso em: 11 jun. 2017.

3.4 A responsabilização civil das redes sociais

Caso todos os princípios e métodos de proteção de dados falhem, e o usuário da rede social veja seus dados pessoais expostos sem sua autorização, tratados de maneira abusiva, ou obtidos ilegalmente por terceiros, é necessário discutir a responsabilidade da administradora do serviço.

Na relação entre o usuário e a rede social, que inicia com a realização do seu cadastro e com a concordância aos termos apresentados pelo serviço, impera o princípio da responsabilidade objetiva, ou seja, as empresas responsáveis pelo serviço devem ser responsabilizadas pelos danos originados pelo descumprimento de algum princípio da proteção de dados ou de uma cláusula contratual, independentemente da existência de dolo ou culpa, que caracteriza um defeito na prestação do serviço.[172].

Tatiana Malta Vieira se manifesta sobre a justificativa de ocorrer a responsabilidade objetiva afirmando:

> O tratamento de dados pessoais impõe-se como uma atividade de risco, implicando a responsabilização objetiva e o dever de indenizar por qualquer acidente ou quebra de segurança que cause danos morais ou materiais ao titular, como a violação do sigilo ou da integridade das informações[173].

Considera-se defeituoso, segundo o parágrafo 1° do artigo 14 do Código de Defesa do Consumidor[174]:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> § 1° O serviço é defeituoso quando não fornece a segurança que o consumidor dele pode esperar, levando-se em consideração as circunstâncias relevantes, entre as quais:
> I - o modo de seu fornecimento;
> II - o resultado e os riscos que razoavelmente dele se esperam;
> III - a época em que foi fornecido.
> (...)

---

[172] VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação**: efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007. p. 267.
[173] Idem. Ibidem.
[174] BRASIL. **Lei n° 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>, acesso em 12 jun. 17.

Desta forma, pode ser afirmado que qualquer falha na segurança da rede social que leve a obtenção não autorizada dos dados pessoais de um usuário por um terceiro gera responsabilidade para a sua administradora, obrigando-a a indenizar o usuário afetado. No mesmo sentido, se a rede social faz um tratamento dos dados fora do previsto contratualmente, ou mesmo que previsto, de maneira abusiva e que viole os princípios de proteção, está caracterizada a necessidade de reparo perante o titular dos dados.

O que gera dúvidas é a responsabilidade civil da rede social perante conteúdo sobre uma pessoa mas que foi publicado por um terceiro. Isto pode se manifestar pela postagem não autorizada de uma informação ou até mesmo pela criação de um perfil falso com o objetivo de causar danos à imagem de uma pessoa, violando também o princípio da exatidão dos dados pessoais.

Para responder o questionamento, recorremos ao parágrafo 3° do artigo 14 do Código de Defesa do Consumidor[175]:

> Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.
> (...)
> § 3° O fornecedor de serviços só não será responsabilizado quando provar:
> I - que, tendo prestado o serviço, o defeito inexiste;
> II - a culpa exclusiva do consumidor ou de terceiro.
> (..)

Como salienta Guilherme Magalhães Martins, existe uma divergência na doutrina sobre a responsabilidade do fornecedor dos serviços de rede social perante o conteúdo gerado por terceiro. Uma parte da doutrina defende que este fato estaria contido nos riscos da atividade da rede social, logo existiria o dever imediato de reparação por parte da administradora quando houvesse uma lesão a pessoa por conteúdo publicado sem sua autorização. Outra parte, defende que o posicionamento anterior causaria o chamado dever geral de vigilância, onde a rede social se veria forçada a vigiar constantemente todo o conteúdo produzido e postado, o que não faria parte da sua atividade intrínseca. Para esta segunda corrente a rede social somente seria responsabilizada caso fosse notificada do conteúdo danoso e demorasse excessivamente para a

[175] Idem.

remoção do mesmo, o que culminaria com a responsabilização da rede social solidariamente com a pessoa que produziu o conteúdo. Uma última corrente jurisprudencial existe dentro do Superior Tribunal de Justiça, aponta o professor Guilherme Martins, nela a rede social se eximiria da responsabilidade no momento que armazenasse o número do protocolo IP, que seria suficiente para a identificação do usuário que criou o conteúdo danoso, uma vez que não é dever desta rede executar a fiscalização das informações postadas por cada usuário.

Cabe por fim ressaltar, que a reparação do dano causado numa rede social, vai além do dever de indenização, como destaca Guilherme Magalhães Martins: "A retirada de uma informação ofensiva, assim como a sua retificação ou, conforme o caso, a retratação por parte do responsável, dentre outras prestações de fazer ou não fazer, possuem grande importância nessa técnica de eliminação do dano[176]".

[176] MARTINS. Guilherme Magalhães. **Responsabilidade civil por acidente de consumo na internet**. 2a ed. São Paulo: Revista dos Tribunais, 2014. p. 364.

CONCLUSÃO

O estudo sobre a proteção de dados pessoais nas redes sociais é marcado por uma constante evolução. Por tratar de tema relacionado a uma tecnologia que se transforma constantemente, é necessário que o seu debate se mantenha sempre atualizado e disposto a rediscutir tudo aquilo que já foi anteriormente definido.

Apesar de atualmente algumas redes sociais estarem intimamente interligadas ao dia a dia das pessoas, ainda é relativamente nova toda a discussão sobre normas que garantam a efetiva proteção de dados. Em razão disto, ainda é muito aberta a conceituação de diversos termos envolvidos no estudo, como a diferença entre dado pessoal e informação pessoal.

O direito à privacidade já foi a única base da discussão sobre proteção de dados, mas hoje já é reconhecido que, apesar deste direito fundamental estar fortemente ligado a esta proteção, não é mais o único direito relacionado ao tema. Já se fala em proteção de dados pessoais como um direito fundamental em si, pois este envolve além da privacidade, outros direitos como o da igualdade e o da dignidade humana.

Quando uma rede social realiza um tratamento abusivo de dados, ou expõe sem o consentimento do seu usuário alguma informação sobre o mesmo, este sofre não só danos em sua intimidade mas também na sua honra. Quando ocorre o tratamento de um dado sensível, aquele relacionado a esfera mais íntima de um indivíduo, este pode sofrer discriminações ou até mesmo perseguições.

Com o estudo dos princípios que precisam fundamentar qualquer tratamento de dados, pudemos perceber que as redes sociais precisam respeitar: a exatidão dos dados, providenciando atualizações constantes de seus bancos de dados sobre as informações que armazenam; o direito à publicidade, indicando sempre a existência de um banco de dados e informando quais são os dados armazenados por estes; a finalidade da coleta de dados, não sendo possível que arbitrariamente a rede social utilize os dados para um objetivo que não informou ao usuário, ou que não foi concordado pelo mesmo; o direito ao livre acesso, permitindo ao usuário ter acesso aos dados que foram armazenados e se houver a detecção de alguma inexatidão, que ocorra a correção; e o princípio da segurança física e lógica, pelo qual as redes sociais precisam garantir a máxima segurança dos dados que armazenam.

Todos os métodos para a proteção de dados analisados nesta pesquisa apresentaram algum tipo de controvérsia. Ao falarmos da exigência do consentimento do usuário para o tratamento de dados, foi possível perceber como este requisito isoladamente não satisfaz a tutela que é visada, pois o usuário não possui condições de estabelecer uma contra proposta ao contrato onde expresse o seu consentimento, sendo obrigado a aceitá-lo sem a possibilidade de discutir uma modificação que melhor zele pela segurança de suas informações. Aliado a isto, o contrato no estilo *clipwrap*, em que basta um clique para que o mesmo seja aceito, contribui para a expansão do hábito dos usuários das redes em concordar com termos sem a sua devida leitura, o que leva ao desconhecimento da escala de permissão de tratamento de dados pela qual consentiu.

O estudo sobre o *habeas data* como um método para o usuário verificar os dados que foram coletados demonstrou que, mesmo depois de superada a discussão sobre o seu cabimento no âmbito civil, este ainda não é a forma mais eficaz para atingir o objetivo da proteção de dados pessoais, pois requer um procedimento no judiciário que sofre de uma superlotação, e gera custos ao titular dos dados.

Como observado no decorrer das exposições, um dos principais problemas da proteção de dados se baseia na dificuldade que o usuário das redes sociais encontra para utilizar os meios que possam garantir o cumprimento de seu direito. Por isso, é essencial que seja criado um órgão que exerça não só a fiscalização do cumprimento das normas brasileiras pelas redes sociais, mas que também realize atividades de conscientização da população sobre os seus direitos na Internet, incluindo assim as redes sociais.

Por se tratar de uma relação de consumo entre a pessoa e a prestadora do serviço, é fundamental que a responsabilidade desta última seja objetiva nos casos de falha da prestação do serviço, o que inclui o tratamento inadequado dos dados pessoais e falhas na sua segurança que possibilitem a obtenção desses dados por pessoas não autorizadas. Se um terceiro conseguiu acesso aos dados de maneira ilícita, está evidente que a administradora da rede social falhou no cumprimento de seu serviço, uma vez que não zelou pela segurança de seu sistema.

Ainda sobre este tema, o questionamento sobre a responsabilidade da rede social por dano causado por um perfil falso não possui uma resposta consagrada. A divergência doutrinaria

contudo não impede afirmarmos que independentemente da posição adotada, a rede social deve ser responsabilizada caso uma pessoa entre em contato e exija a exclusão de um conteúdo publicado indevidamente, e que lhe gere dano, e, diante deste fato, a rede social se mantenha inerte.

Em suma, para garantir a eficaz proteção dos dados pessoais nas redes sociais, é necessário um conjunto de medidas simultâneas. É indispensável que existam normas que tutelem por esse direito, que exista um órgão que fiscalize o tratamento de dados e trabalhe para conscientizar os usuários sobre os riscos que estão envolvidos nas redes sociais, e também, que o próprio usuário crie interesse sobre o assunto e assim cobre das prestadoras de serviço o cumprimento de seu direito fundamental.

REFERÊNCIAS BIBLIOGRÁFICAS

AGENCIA ESPAÑOLA DE PROTECCIÓN DE DATOS; INSTITUTO NACIONAL DE TECNOLOGÍAS DE LA COMUNICACIÓN. ***Estudio sobre la privacidad de los datos personales y la seguridad de la información en las redes sociales***. Madrid, 2009.

BRASIL. **Constituição da República Federativa do Brasil de 1988.** Brasília: Senado, 05.10. 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>, acesso em: 12 jun. 17.

_____. **Decreto-Lei n° 4.657 de 4 de setembro de 1942**. Lei de Introdução as normas do Direito Brasileiro. Diário Oficial da União, Rio de Janeiro, RJ, 18 set. 1942. Disponível em: <http://www.planalto.gov.br/ccivil_03 /decreto-lei/Del4657compilado.htm>, acesso em 12 jun. 17.

_____. **Lei n° 5.869 de 11 de janeiro de 1973**. Institui o Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 jan. 1973. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/L5869.htm>, acesso em 12 jun. 17.

_____. **Lei n° 8.078 de 11 de setembro de 1990**. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da União, Brasília, DF, 12 set. 1990. Disponível em: <https://www.planalto.gov.br/ccivil_03/Leis/L8078.htm>, acesso em 12 jun. 17.

_____. **Lei n° 9.507 de 12 de novembro de 1997**. Regula o direito de acesso a informações e disciplina o rito processual do *habeas data*. Diário Oficial da União, Brasília, DF, 13 nov. 1997. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9507.htm>, acesso em 12 jun. 17.

_____. **Lei n° 10.406 de 10 de janeiro de 2002**. Institui o Código Civil. Diário Oficial da União, Brasília, DF, 11 jan. 2002. Disponível em: <http://www.planalto.gov.br/ccivil_03/ leis/2002/L10406.htm>, acesso em 12 jun. 17.

_____. **Lei n° 12.527 de 18 de novembro de 2011**. Regula o acesso a informações previsto no inciso xxxiii do art. 5º, no inciso ii do § 3º do art. 37 e no § 2º do art. 216 da constituição federal; altera a lei nº 8.112, de 11 de dezembro de 1990; revoga a lei nº 11.111, de 5 de maio de 2005, e dispositivos da lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da União, Brasília, DF, 18 nov. 2011. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm>, acesso em 12 jun. 17.

_____. **Lei nº 12.965, de 23 de abril de 2014**. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da União, Brasília, DF, 24 abr. 2014.

Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> , acesso em: 12 jun. 17.

_____. **Lei nº 13.105, de 16 de março de 2015**. Código de Processo Civil. Diário Oficial da União, Brasília, DF, 17 mar. 2015. Disponível em: <http://www.planalto.gov.br/ ccivil_03/_ato2015-2018/2015/lei/l13105.htm> , acesso em: 12 jun. 17.

_____. Câmara dos Deputados. **Projeto de Lei n. ° 5.276-A/2016**. Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Disponível em: <http://www.camara.gov.br/proposicoesWeb/prop_ mostrarintegra;jsessionid=C2874759AD9F780699B58C8058EB45ED.proposicoesWeb2?codteor=1470645&filename=Avulso+-PL+5276/2016>, acesso em: 12 jun. 2017.

_____. Superior Tribunal de Justiça. **Súmula n° 2**. Não cabe o habeas data (cf, art. 5., lxxii, letra "a") se não houve recusa de informações por parte da autoridade administrativa. Disponível em: <http://www.stj.jus.br/docs_internet/SumulasSTJ.pdf>, acesso em: 12 jun. 2017.

BOYD, Danah M; ELLISON, Nicole B. **Social Network Sites:** Definition, History, and Scholarship. 2007. Disponível em: <http://onlinelibrary.wiley.com/doi/10.1111/j.1083-6101.2007.00393.x/full>, acesso em: 12 jun. 17.

CASTRO, Catarina Sarmento e. **Direito da informática, privacidade e dados pessoais**. Coimbra: Almedina, 2005.

DONEDA, Danilo. **A proteção dos dados pessoais como um direito fundamental**. In: Revista Espaço jurídico – v. 12, n.º 11. p. 91-108. Joaçaba: UNOESC, 2011.

_____. **A proteção de dados pessoais nas relações de consumo:** para além da informação creditícia. Escola Nacional de Defesa do Consumidor. Brasília: SDE/DPDC, 2010. Disponível em: <http://www.justica.gov.br/seus-direitos/consumidor/Anexos/manual-de-protecao-de-dados-pessoais.pdf>, acesso em : 12 jun. 17

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

_____. **O direito fundamental à proteção de dados pessoais**. In: MARTINS, Guilherme Magalhães (Coord.). **Direito Privado e Internet**. São Paulo: Atlas, 2014

FLEISCHER, Peter. ***Foggy thinking about the Right to Oblivion***. Disponível em: <http://peterfleischer.blogspot.com.br/2011/03/foggy-thinking-about-right-to-oblivion.html>, acesso em: 12 jun. 2017.

GOMES, Orlando. **Contratos**. 26. Ed. Atualização de Antonio Junqueira de Azevedo e Francisco Paulo de Crescenzo Marino. Rio de Janeiro: Forense, 2009.

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2012.

MARQUES, Cláudia Lima. **Confiança no comércio eletrônico e a proteção do consumidor**. São Paulo: Revista dos Tribunais, 2004.

MARTINS, Guilherme Magalhães. **Contratos eletrônicos de consumo**. 3ª ed. São Paulo: Atlas, 2016.

_____. **O direito ao esquecimento na internet**. In: MARTINS, Guilherme Magalhães (Coord.). Direito Privado e Internet. São Paulo: Atlas, 2014. p.15.

_____. **Responsabilidade civil por acidente de consumo na internet**. 2ª ed. São Paulo: Revista dos Tribunais, 2014.

MENDES, Laura Schertel. **Transparência e privacidade:** violação e proteção da informação pessoal na sociedade de consumo. 2008. 156 f. Dissertação (Mestrado em Direito) – Universidade de Brasília, Brasília, 2008.

REDING, Viviane. ***The EU data protection reform 2012****: Making Europe the standard setter for modern data protection rules in the digital age*. Discurso na Innovation Conference Digital, Life, Design, realizada em Monique em 22 de janeiro de 2012. Disponível em: <http://europa.eu/rapid/pressReleasesAction.do?reference=SPEECH/12/26&format=PDF>, acesso em: 12 jun. 2017.

RODOTÁ, Stefano. **A vida na sociedade da vigilância** – a privacidade hoje. Rio de Janeiro: Renovar, 2008.

ROSEN, Jeffrey. ***The Right to be Forgotten***. Disponível em: <https:// www.stanfordlawreview.org/online/privacy-paradox-the-right-to-be-forgotten/>, acesso em: 12 jun. 2017.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 24ª ed. São Paulo: Malheiros Editores, 2005

UNIÃO EUROPEIA. **Carta dos Direitos Fundamentais da União Europeia**, de 7 de dezembro de 2000. Disponível em: < http://www.europarl.europa.eu/charter/pdf/text_pt.pdf>, acesso em: 12 jun. 17.

_____. **Directiva 95/46/CE do Parlamento Europeu e do Conselho da Europa**, de 24 de outubro de 1995, relativa à protecção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>, acesso em: 12 jun. 17.

_____. **Regulamento 2016/679 do Parlamento Europeu e do Conselho**, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE. Disponível em: <http://eur-lex.europa.eu/legal-content/pt/TXT/PDF/?uri=CELEX:32016R0679&from=EN>, acesso em: 12 jun. 17.

VIEIRA, Tatiana Malta. **O direito à privacidade na sociedade da informação:** efetividade desse direito fundamental diante dos avanços da tecnologia da informação. 2007. 297 f. Dissertação (Mestrado em Direito, Estado e Sociedade) – Universidade de Brasília, Brasília, 2007.