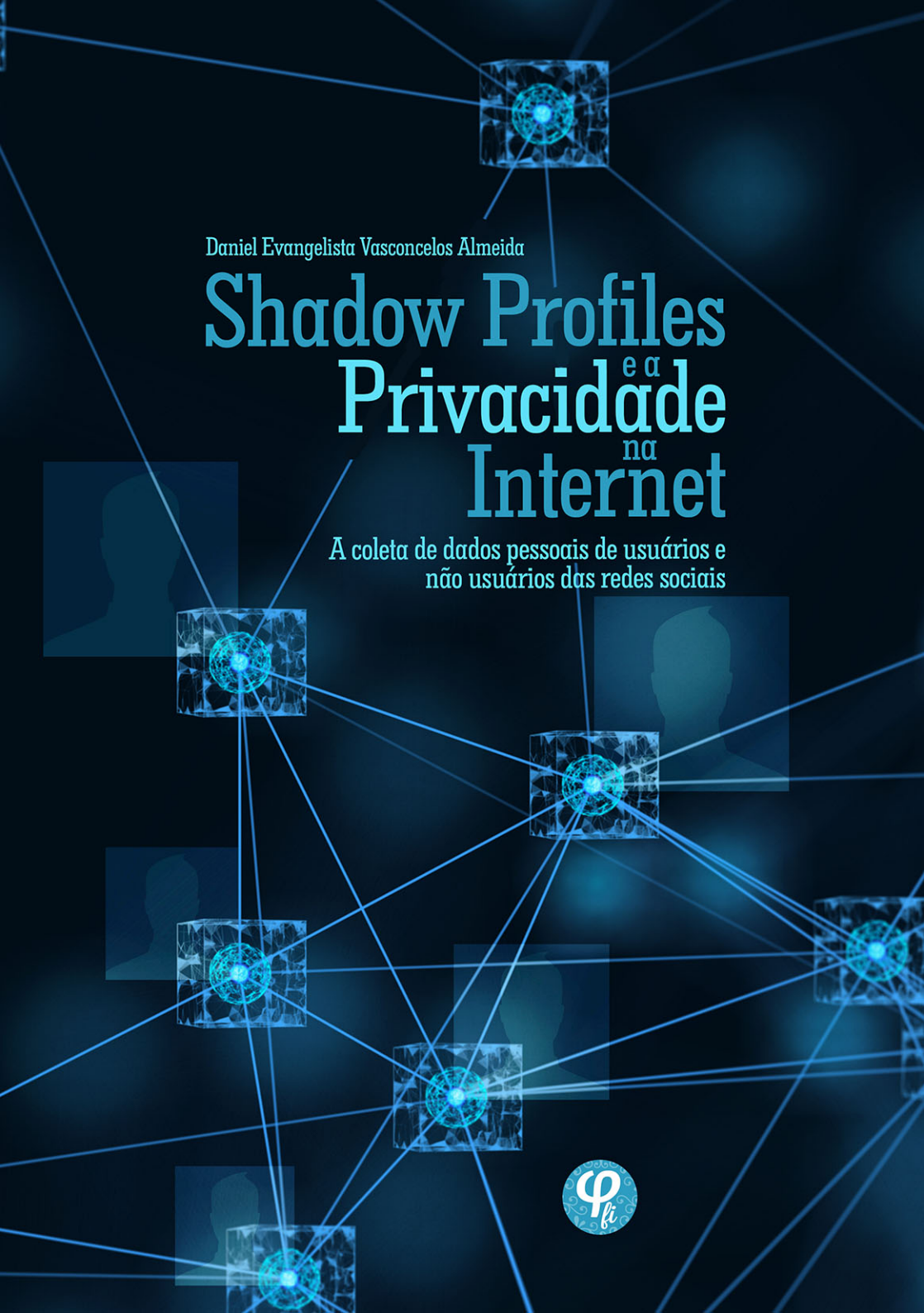
Daniel Evangelista Vasconcelos Almeida

Shadow Profiles e a Privacidade na Internet

A coleta de dados pessoais de usuários e não usuários das redes sociais



Um fenômeno recente – as redes sociais, que surgiram em 2003 – mostra-se de um lado como um meio de interação social, mas de outro como uma preocupação, tendo em vista o grande número de informações pessoais sobre os usuários que são compartilhadas, muitas das vezes sem o consentimento ou até mesmo sem o conhecimento efetivo destes. Com o avanço da Internet e o aumento do número de usuários das redes sociais, é preciso que se discuta a coleta e o uso indiscriminado de dados pessoais em vista do direito à privacidade. A privacidade na Internet deve ser lida como controle das informações pessoais, em contrapartida à visão clássica de exclusão do outro ou, ainda, o direito de ser deixado só. Os usuários não leem os termos de uso e política de privacidade e mesmo que o fizessem não poderiam modificar as cláusulas, dada à natureza de termo de adesão digital. Os provedores coletam mais dados dos usuários do que eles disponibilizam ativamente e, além disso, coletam dados inclusive de não usuários. Toda essa informação coletada sem o consentimento e, às vezes até sem conhecimento, é considerada Shadow Profile. Com a interpretação dos conteúdos do direito à privacidade é possível se chegar a uma tutela efetiva na Internet, não sendo necessária a criação de novos direitos. O livro irá abordar os direitos da personalidade, focando no direito à privacidade e seus desdobramentos em decorrência da Internet.

9 788556 965417

editora fi.org

CC BY SA

Shadow Profiles e a Privacidade na Internet

Direção Editorial

Lucas Fontella Margoni

Comitê Científico

Prof. Dr. Leonardo Macedo Poli
Pontifícia Universidade Católica de Minas Gerais (PUC Minas)

Prof. Dr. Taisa Maria Macena de Lima
Pontifícia Universidade Católica de Minas Gerais (PUC Minas)

Prof. Dr. Rodrigo Almeida Magalhães
Pontifícia Universidade Católica de Minas Gerais (PUC Minas)

Prof. Dr. Rodolfo Mário Veiga Pamplona Filho
Universidade Salvador (UNIFACS)

Shadow Profiles e a Privacidade na Internet

A coleta de dados pessoais de usuários e não usuários das redes sociais

Daniel Evangelista Vasconcelos Almeida

Diagramação: Marcelo A. S. Alves
Capa: Carole Kümmecke - https://www.behance.net/CaroleKummecke

O padrão ortográfico e o sistema de citações e referências bibliográficas são prerrogativas de cada autor. Da mesma forma, o conteúdo de cada capítulo é de inteira e exclusiva responsabilidade de seu respectivo autor.

Todos os livros publicados pela Editora Fi
estão sob os direitos da Creative Commons 4.0
https://creativecommons.org/licenses/by/4.0/deed.pt_BR

http://www.abecbrasil.org.br

Dados Internacionais de Catalogação na Publicação (CIP)

ALMEIDA, Daniel Evangelista Vasconcelos

Shadow profiles e a Privacidade na Internet: a coleta de dados pessoais de usuários e não usuários das redes sociais [recurso eletrônico] / Daniel Evangelista Vasconcelos Almeida -- Porto Alegre, RS: Editora Fi, 2019.

189 p.

ISBN - 978-85-5696-541-7

Disponível em: http://www.editorafi.org

1. Shadow Profile; 2. Direitos da Personalidade; 3. Privacidade; 4. Direito de não ser conhecido; 5. Internet; Direito Digital.; I. Título.

CDD: 199

Índices para catálogo sistemático:
1. Direito 340

“Os adolescentes equipados com confessionários eletrônicos portáteis são apenas aprendizes treinando e treinados na arte de viver numa sociedade confessional – uma sociedade notória por eliminar a fronteira que antes separava o privado e o público, por transformar o ato de expor publicamente o privado numa virtude e num dever públicos, e por afastar da comunicação pública qualquer coisa que resista a ser reduzida a confidências privadas, assim como aqueles que se recusam a confidenciá-las.”

Zygmunt Bauman

Dedico este trabalho aos meus pais, João e Célia
fonte de inspiração para querer sempre mais.
À minha irmã Juliana Evangelista,
companheira de vida e parceira acadêmica.

Lista de abreviaturas e siglas

ANPD	Autoridade Nacional de Proteção de Dados
ARPANET	Advanced Research Projects Agency Network
BGB	Bürgerliches Gesetzbuch
CDC	Código de Defesa do Consumidor
CPC	Código de Processo Civil
DARPA	Defense Advanced Research Projects Agency
GPS	Global Position System
HTML	Hyper Text Markup Language
LGPD	Lei Geral de Proteção de Dados Pessoais
MCI	Marco Civil da Internet
OCDE	Organização para a Cooperação e Desenvolvimento Econômico
SEO	Search Engine Optimization
SERASA	Centralização de Serviços dos Bancos
SPC	Serviço de Proteção ao Crédito
STJ	Superior Tribunal de Justiça
TICs	Tecnologias de Informação e Comunicação
URL	Uniform Resource Locator
WWW	World Wide Web

Sumário

Prefácio **15**
Rodolfo Pamplona Filho

1 ..... **19**
Introdução

2 ..... **27**
Introdução à era digital: a importância da informação

2.1 A quebra de paradigma na Internet com a WEB 2.0 31

2.2 O avanço das redes sociais e o futuro da Internet com a WEB 3.0 35

2.3 O avanço das redes sociais e a coleta indiscriminada de dados pessoais: Shadow Profile 37

3 ..... **43**
Uma abordagem dos direitos da personalidade

3.1 A Privacidade e a Intimidade como um desdobramento dos direitos da personalidade em sua concepção clássica 53

3.2 A proteção dos dados pessoais como sendo uma tutela da privacidade 62

4 ..... **69**
Evolução dos conteúdos do direito à privacidade para se alcançar uma proteção eficaz dos direitos da personalidade na internet

4.1 Direito de autodeterminação 75

4.2 Direito de exclusão 78

4.3 Direito ao esquecimento 80

4.4 Direito de acesso e modificação 84

4.5 Direito de não ser conhecido 90

5 95
Análise dos termos de uso e política de privacidade: regras gerais

5.1 Contratos Eletrônicos 96

5.2 A massificação dos contratos: crise contratual 99

5.3 A abusividade e invalidade de cláusulas restritivas de direitos no termo de adesão digital 104

5.4 Venire Contra factum proprium 110

6 115
Análise específica dos termos de uso e política de privacidade das redes sociais

6.1 Facebook 116

6.2 Instagram 130

6.3 Google 136

7 151
Os shadow profiles e a violação dos direitos de personalidade dos usuários e dos não usuários das redes sociais

7.1 A tutela da privacidade na era da ausência da privacidade 154

7.2 O *Shadow Profile* do usuário 157

7.3 O *Shadow Profile* do não usuário 158

7.4 A informação como meio de exploração e a sua valorização na sociedade 161

8 169
Conclusão

Referências 177

Prefácio

Rodolfo Pamplona Filho[1]

No mesmo dia em que a jovem Professora **Juliana Evangelista** alcançou o patamar máximo nos estudos avançados de pós-graduação, com a obtenção do título de Doutorado que atesta a sua "maioridade acadêmica", foi designada a banca de mestrado de seu jovem (e também talentoso) irmão, o Professor **Daniel Evangelista Vasconcelos Almeida**.

Fui eu convidado para, em um único turno, avaliar publicamente em bancas na Pontifícia Universidade Católica de Minas Gerais os dois irmãos, o que, dada a peculiaridade, foi prontamente aceito, mesmo sem conhecer pessoalmente a dupla.

E qual não foi a surpresa, para mim, ao ler o conteúdo dos dois textos!

Duas verdadeiras pérolas, com uma profundidade e abrangência admiráveis, que encantou os avaliadores e, em especial, o subscritor destas linhas.

E é justamente o fruto daquela dissertação de **Daniel Evangelista** que tenha a honra de ora prefaciar.

---

[1] Professor Associado de Direito Civil da Universidade Federal da Bahia. Professor Titular de Direito Civil e Direito Processual do Trabalho do Curso de graduação em Direito e do Mestrado em Direito, Governança e Políticas Públicas da UNIFACS — Universidade Salvador. Juiz Titular da 32ª Vara do Trabalho de Salvador/BA. Mestre e Doutor em Direito das Relações Sociais pela Pontifícia Universidade Católica de São Paulo — PUC-SP. Máster em Estudios en Derechos Sociales para Magistrados de Trabajo de Brasil pela UCLM — Universidad de Castilla-La Mancha/Espanha. Especialista em Direito Civil pela Fundação Faculdade de Direito da Bahia. Membro e Presidente Honorário da Academia Brasileira de Direito do Trabalho. Membro e Presidente da Academia de Letras Jurídicas da Bahia e do Instituto Baiano de Direito do Trabalho. Membro Efetivo da Academia Brasileira de Direito Civil — ABDC, Instituto Brasileiro de Direito Civil — IBDCivil e Instituto Brasileiro de Direito de Família — IBDFAM.

"SHADOW PROFILES: A tutela dos direitos da personalidade do usuário e do não usuário das redes sociais" é a mais inovadora dissertação de Mestrado que li nos últimos tempos.

Tratando de tema pouco estudado no Brasil, mas de enorme repercussão prática, o jovem autor estreia no meio editorial com perfil de veterano, com alentado texto defendido no dia 01 de dezembro de 2017, em banca composta pelos Professores Doutores **Leonardo Macedo Poli** (orientador) e **Taisa Macena de Lima**, além deste professor como avaliador externo, que, unanimemente, lhe outorgou o título com a nota 100 e distinção *cum laude*, além de ter sido recomendada a publicação.

O tema é fascinante e arrepia quem não está acostumado com o mundo digital.

De fato, imaginar a existência de **Shadow Profiles** já atiça a curiosidade de qualquer um, pois saber que, mesmo que não se tenha um perfil em uma rede social, há possibilidade da plataforma possuir dados que podem constituir um perfil completo, é algo quase apavorante.

E imaginar, na singeleza deste novo mundo, de que basta que o usuário aceite os termos de uso para que este perfil oculto fique visível para todos faz com que se pense quais são os limites da privacidade na contemporaneidade, uma vez que tal coleta de dados pessoais é feita, inclusive, com base em termos de uso e políticas de privacidade.

Refletir sobre isso com base na teoria dos Direitos da Personalidade faz com que se descortinem novos horizontes e – talvez! – seja possível vislumbrar outros caminhos e diretrizes.

Se o tema é fascinante, seu autor (seguindo a mesma maravilhosa herança genética) é também encantador!

Tão jovem, já é Doutorando em Direito Empresarial pela UFMG, depois de obter o mencionado título de Mestre em Direito Privado pela PUC Minas (e, antes, Especialista em Direito Civil e Processo Civil pela FEAD, além de ter cursado a disciplina de Internet Law da University of Geneva). Profissionalmente, já atua

no magistério superior como Professor de Direito Civil da FAMIG e da pós-graduação *Stricto Sensu* da PUC Minas, além de exercer a advocacia.

Como não ficar impressionado com tanto talento?

Na condição de leitor privilegiado da dissertação que gerou o livro e confessadamente fã da dupla talentosa de irmãos, notadamente do autor desta obra, faço questão de publicamente recomendá-la, na certeza de que mais brilhantes textos ainda surgirão para o deleite dos leitores e esclarecimento da comunidade jurídica brasileira e internacional.

Salvador, 01 de julho de 2018.

1

Introdução

Um fenômeno recente – as redes sociais, que surgiram em 2003 – mostra-se de um lado como um meio de interação social, mas de outro como uma preocupação, tendo em vista o grande número de informações pessoais sobre os usuários que são compartilhadas, muitas das vezes sem o consentimento ou até mesmo sem o conhecimento efetivo destes. Cada plataforma digital possui o seu termo de uso e respectiva política de privacidade. Fato é que o usuário, ao utilizar um serviço digital não tem o poder de modificar a forma como serão coletados, utilizados e tratados os dados pessoais.

Nesse viés, é preciso que no Direito Digital a privacidade seja tratada como controle e este deve ser dado ao usuário sobre suas informações pessoais. Entretanto, é raro um usuário que lê os termos de uso e política de privacidade de uma plataforma, até mesmo porque em nada ele poderia modificar estas, sendo que em caso de discordância, poderia apenas deixar de utilizar o serviço.

Uma rede social coleta diversos dados pessoais do usuário, os quais muitas das vezes são fornecidos sem o consentimento expresso e informado. Conforme se verá nesta dissertação, o *Facebook*, por exemplo, coleta informações do usuário que este não fornece ativamente, tais como informações de seus contatos, de sua localização, *cookies* entre outras. É evidente que nem todas as informações se mostram como dados sensíveis, podendo ser utilizadas pela plataforma para se traçar um perfil do usuário, sem que sejam efetivamente exibidas.

Estes dados que a plataforma possui sobre o usuário que não são visíveis e são coletadas sem que este forneça ativamente formam a primeira vertente do *Shadow Profile*, em tradução literal, perfil sombrio. Trata-se, nesta vertente, de toda a informação que a plataforma possui sobre o usuário que não é visível a ninguém além da própria plataforma. É como se o perfil tivesse quatro camadas, uma visível apenas ao usuário (informações como número de telefone e cartão de crédito, por exemplo), a segunda visível ao usuário e suas conexões, a terceira visível a todos os usuários da rede, mesmo que não esteja na conexão de amigos (fotos, *posts* e comentários por exemplo) e a quarta, que se refere aquelas informações que nem o usuário nem suas conexões possuem acesso, mas que foram coletadas pela plataforma.

A preocupação com os *Shadow Profiles* começou em 2011, com uma reclamação de um cidadão Austríaco chamado Max Shcrems contra o *Facebook,* pedindo a exclusão definitiva de toda e qualquer informação que fora coletada sem que o usuário tivesse efetivamente disponibilizado (COMPLAINT, 2016). O referido usuário pediu à rede social um arquivo com todas as suas informações, uma espécie de perfil *off-line*, que pela legislação europeia é um direito de todos. De posse dessas informações, o usuário constatou que o *Facebook* tinha o seu E-mail secundário, telefone, informações sobre fotos e publicações já deletadas, informações sobre amizades desfeitas, dentre outras, que ou não foram disponibilizadas pelo usuário ou não eram visíveis ou até mesmo tinham sido deletadas. Assim, foi solicitada a exclusão definitiva destes dados.

Na mesma reclamação foi constatado que o *Facebook* possui dados de não usuários. Como a rede social sincroniza os dados da agenda de um usuário, acaba coletando informações sobre pessoas que não possuem um perfil digital. Assim, antes mesmo de se tornar um usuário, a rede já sabe quem é aquele indivíduo, quais são suas conexões na vida real, possivelmente a profissão, idade, hábitos entre outras informações. É comum, por exemplo, um usuário

enviar um convite para um não usuário se juntar a rede e neste momento já existir um "pré-perfil" estabelecido, com a exibição inclusive de algumas fotos que aquele indivíduo tem na rede, bem como os amigos que ali estão presentes. Essas informações coletadas sobre um não usuário também se denominam *Shadow Profile*, sendo a segunda vertente possível.

Nesse caso, a plataforma, por meio de seus usuários coleta dados sobre não usuários. Questiona-se, pois, a possibilidade dessa coleta, bem como se existe violação à direitos de personalidade.

Claro que já se tem uma base para o direito ao esquecimento. Por mais que qualquer informação na rede seja eterna, é dado aos usuários o direito de serem literalmente esquecidos pela Rede, através da exclusão de seus dados. Porém, é possível questionar se há um direito de não ser sequer conhecido. Há que se indagar se é legal a coleta de informações dos usuários quer seja fornecida pelo próprio quer seja por terceiro.

Nesse sentido, existem duas vertentes de *Shadow Profiles*, ambas discutíveis sobre o prisma dos direitos de personalidade. A primeira consiste nos dados sobre um usuário que são coletados sem o consentimento expresso ou até mesmo conhecimento do usuário e a segunda se refere às informações de quem sequer faz parte da plataforma. Assim, em ambos os casos é preciso se discutir eventual violação de direitos da personalidade, bem como se é possível responsabilizar a rede por tal violação. Assim sendo, a presente pesquisa discute se há violação aos direitos de personalidade do usuário e do não usuário das redes sociais com a ocorrência do que se denomina de *Shadow Profile*.

Como os dados pessoais podem refletir a personalidade do usuário na Internet, a pesquisa teve como hipótese a possível violação de direitos da personalidade com a criação de *Shadow Profile*, quer seja a partir de um usuário, quer seja a partir de um não usuário. Isso porque é possível a manifestação da personalidade e a construção da pessoalidade também no mundo digital, mormente através das redes sociais.

Caso uma pessoa decida pelo não uso de mídias sociais na Internet ela tem o direito de ter o controle de seus dados pessoais, o que importa no não conhecimento destes por parte dos provedores de conteúdo. Assim, partiu-se da premissa de que em alguns casos, com a formação de um *Shadow Profile* há violação de direitos da personalidade. O objetivo desta dissertação é compreender como é o tratamento dos dados pessoais na Internet, questionando a sua proteção, tratamento e coleta principalmente nas redes sociais, investigando os *Shadow Profiles* para que se evidencie uma possível violação de direitos da personalidade.

A Internet é hoje uma realidade, a qual revolucionou e revoluciona a forma como a sociedade vive (PINHEIRO, 2016). Observe que atualmente é comum as empresas venderem produtos através da rede mundial de computadores, o que aumenta o alcance destas no mercado, tamanha é a importância da Internet que já foi, inclusive, considerada bem indispensável à vida (CORTE ALEMÃ..., 2013).

É certo que a própria Internet também cresceu bastante. Com o avanço do tempo aumenta-se a acessibilidade a este dispositivo. Para mostrar esse avanço, o site Blue Blus[1] fez um gráfico no ano de 2012 mostrando as mudanças na Internet no desde 2002. Naquele ano, eram 569 milhões de usuários (9,1% da população mundial), em 10 anos esse número praticamente quadruplicou, subindo para 2,27 bilhões (33% da população mundial). Antes se usavam aproximadamente 46 minutos de Internet por dia, atualmente são 4 horas. O número de sites aumentou cerca de 18.500%, de 3 milhões para 555 milhões de sites.

Em se tratando de redes sociais também houve um aumento nos dados, antes a primeira e maior rede social, a Friendster, tinha 3 milhões de usuários. Em 2012, o Facebook, maior rede social do momento, contava com mais de 900 milhões de usuários. Já no ano

---

[1] Informação disponível em: http://www.bluebus.com.br/esse-infografico-mostra-o-quanto-a-Internet-mudou-nos-ultimos-10-anos-veja/. Acesso em: 05 jul. 2016.

de 2015, o Facebook contava com 1,5 bilhões de usuários[2], sendo que atualmente existem mais de 1,9 bilhões de usuários[3]. Ainda, a referida rede possui um projeto intitulado de Internet.Org, que tem o objetivo de levar o acesso à plataforma aos cantos mais remotos do planeta, aumentando ainda mais o número de usuários[4].

Diante das mudanças que o avanço das TICs – Tecnologias de Informação e Comunicação – trouxe, no capítulo 2 foi feita uma abordagem introdutória à era digital. Foi evidenciado como a comunicação é importante para a sociedade, e a Internet, uma importante ferramenta para a disseminação de informação pelo mundo. Mostrou-se o surgimento das redes sociais e a mudança de paradigma da Web 1.0 para a Web 2.0 e posteriormente Web 3.0.

Vale dizer que o crescimento das redes sociais reflete a Web 2.0 (O'REALLY 2005), fenômeno que caracteriza a Internet como uma rede a ser alimentada tanto pelos provedores quanto pelos usuários. É evidente a importância que as redes sociais têm na vida das pessoas, tendo em vista o aumento constante no uso destas. Mais ainda, por ser um fenômeno recente, ainda não se tem uma cultura sólida formada a respeito do uso da Internet, o que leva a um mau uso da ferramenta.

Um dos objetivos desta dissertação é investigar a tutela dos direitos da personalidade do usuário e do não usuário das redes sociais. Assim, no capítulo 3 foi feita uma abordagem histórica deste instituto, mostrando como se formou uma teoria afirmativista dos Direitos da Personalidade, bem como a existência de cláusula geral de proteção.

Ao utilizar a Internet, a privacidade deveria ser uma preocupação constante dos usuários. Este direito é um desdobramento do exercício dos direitos da personalidade, devendo, pois, ser tutelado. Assim, ainda no capítulo 3 trabalhou-se com a

---

[2] Informação disponível em <https://www.Internet.org/about>. Acesso em 05 jul. 2016.

[3] Informação disponível em <http://g1.globo.com/tecnologia/noticia/facebook-chega-a-194-bilhao-de-usuarios-em-todo-o-mundo-no-1-trimestre-de-2017.ghtml> acesso em: 04 de maio de 2017

[4] Informação disponível em < http://newsroom.fb.com/company-info/>. Acesso em 05 jul. 2016.

tutela da privacidade, que no direito digital pode ser entendida como a proteção dos dados pessoais.

Evidente que a privacidade, em sua concepção clássica, remonta a ideia do "Right to be let alone", ou seja, o Direito de ser deixado só. Mas é difícil se afirmar o que é íntimo e o que é privado na rede, tratando-se de uma diferenciação teórica (LEORNADI, 2011). Assim, não se diz que a informação deva ser mantida em segredo para que garanta ao usuário a sua privacidade. No capítulo 4 estudou-se a evolução dos conteúdos do direito à privacidade a partir das teorias da interpretação para que se faça a compatibilização dos conceitos com a nova realidade fática.

Não é necessária a criação de novos institutos para se tutelar a privacidade na Internet, basta que se faça uma interpretação dos contornos existentes para se chegar a uma tutela efetiva dos direitos. Trabalhou-se com a ideia de que no Direito Digital, conforme Stefano Rodotà (2014), a privacidade remonta ao direito de seguir a própria informação onde quer que ela esteja e de se opor a qualquer interferência. Fala-se, pois, no governo de si, ou seja, a possibilidade de se afirmar na rede. Foram propostas cinco novas interpretações do direito à privacidade na Internet, quais sejam, Direito de Autodeterminação, Direito de Exclusão, Direito ao Esquecimento, Direito de Acesso e Modificação e Direito de Não Ser Conhecido.

A privacidade dos usuários é definida por um termo de adesão digital, tendo em vista que não existe a possibilidade de se modificarem as cláusulas contidas no contrato. O usuário, ao discordar de alguma condição de uso, pode apenas abster-se de utilizar a plataforma. Evidente que os usuários não têm o hábito de ler os termos de uso, não que isso tenha algum efeito na proteção de sua privacidade, pois nada poderá ser modificado. Mas existe a possibilidade de, conhecendo a política de privacidade, o usuário decida a forma como irá utilizar a rede.

No capítulo 5 foi feita uma análise geral do que se denominou de termo de adesão digital. Trabalhou-se O marco teórico esboçado por Enzo Roppo (2009) que defende a crise da teoria clássica

contratual, afirmando que o elemento vontade deixa de ser o preponderante de um contrato. Tutela-se o contrato pelo seu aspecto objetivo, razão pela qual é válido o contrato feito por adesão, o que não implica a validade absoluta de cláusulas restritivas de direitos. Assim, pode-se invalidar uma ou outra cláusula sem que deixe de existir contrato.

Buscando uma análise concreta dos Shadow Profiles, no capítulo 6 foi feita uma análise específica das principais redes sociais em funcionamento no Brasil, quais sejam, Facebook, Instagram e Google, analisando-se tanto o termo de uso como a política de privacidade. Com a análise específica, é possível concluir quais cláusulas são inválidas, quais são os dados coletados sem o devido consentimento dos usuários e quais são os usos feitos dessas informações.

Em verdade, quando um provedor de conteúdo utiliza um dado pessoal geralmente é para venda ou marketing. Fala-se hoje em ditadura do algoritmo, já que todos têm uma reputação digital, ou seja, são avaliados de acordo com os seus próprios hábitos, o que pode influenciar em diversas esferas da vida do usuário. Assim no capítulo 7 foi feita a retomada dos conceitos de privacidade juntamente com a análise dos termos de uso, investigando a violação dos direitos de personalidade com a existência dos Shadow Profiles.

2

Introdução à era digital: a importância da informação

A sociedade muda com o avanço da tecnologia. Diversas transformações podem ser notadas, as quais antes inimagináveis. Com a Internet, os indivíduos são expostos a uma vasta gama de informações, é o que Alvin Toffler (1980) denomina de terceira onda. Alvin Toffler foi um escritor norte-americano, que nasceu em 1928 e faleceu em 2016, conhecido pelos seus escritos sobre o futuro, especificamente sobre a revolução que a tecnologia opera.

Nos anos 70, ainda no início da Internet, ele destacou a sociedade da informação. Argumentava que a sociedade teria dois relógios, um analógico e um digital; um para o mundo real e outro para o mundo virtual/digital (TOFFLER, 1980). Neste último, não há limite de tempo ou espaço, diversas ações podem ser realizadas simultaneamente em diferentes lugares do mundo: é o que se observa hoje em dia. É possível se comunicar com qualquer pessoa, simultaneamente, com áudio e vídeo (videoconferência), em um procedimento bem simples.

Isso é uma quebra de paradigma com o passado. Podem-se destacar três grandes marcos para a informação, quais sejam, a invenção da prensa mecânica por Gutenberg em 1439, o que posteriormente deu início à imprensa; o telégrafo, potencializado pelo código Morse em 1835; e, por fim, a invenção da Internet na década de 60 (BRIGGS, 2006).

Antes da prensa mecânica, qualquer notícia ou informação circulava através de manuscritos e eram restritas a poucas pessoas. Com a invenção do referido equipamento, automatizou-se o processo de escrita, massificando a produção, possibilitando uma maior disponibilização de conteúdo. Entretanto, ainda se esbarrava em barreiras físicas, tendo em vista que a circulação de um jornal, por exemplo, era feita em determinado território.

Quando foi inventada a prensa mecânica, não havia um meio de transporte eficaz que possibilitava a circulação rápida, que só surgiu no século XIX com as ferrovias. Nos Estados Unidos da América, no ano de 1865, havia 90 mil quilômetros de trilhos, número este que saltou para 320 mil já no ano de 1870 (BRIGGS, 2006). Esse tipo de transporte, pensado primariamente para passageiros, era um importante meio de difusão de notícias. Existia o entrave territorial, tendo em vista que somente poderia ser utilizado dentro de um continente. Mais ainda, havia barreiras geográficas, por não se poder instalar trilhos em relevos acentuados.

A forma utilizada para a comunicação entre os continentes europeu e americano era o navio. Entre 1776 e 1940, mais de 30 milhões de imigrantes europeus chegaram aos Estados Unidos da América (BRIGGS, 2006). Assim como a ferrovia, os navios eram um importante meio para se transmitir informação. Entretanto, era necessário aumentar o alcance desta com uma certa velocidade, pois uma viagem em um transatlântico levava em média 18 dias e dez horas (BRIGGS, 2006).

Iniciou-se então o implemento de um meio de comunicação entre dois pontos. Foi criado no século XVIII o telégrafo, que objetivava suprir a necessidade de se transmitir informações (BRIGGS, 2006). Esbarrava-se, ainda, em dois entraves, quais sejam, a ligação entre continentes e a ausência de um código padrão. Em 1858, foi instalado o primeiro cabo transatlântico por Charles Bright, que foi capaz de solucionar, embora precariamente, o primeiro entrave. O segundo foi resolvido por Samuel Morse, com o código Morse, em 1835 (BRIGGS, 2006).

O código Morse é um sistema de padronização representativo de letras, números e sinais de pontuação, através de um sinal codificado. Era possível transmitir informações a um espaço cada vez maior, com uma velocidade de 40 palavras por minuto. Somente nos Estados Unidos, no ano de 1846, havia mais de 1600 quilômetros de linhas para telégrafo (GANDELMAN, 2001).

Contudo, ainda não havia simultaneidade, nem a possibilidade de transmissão sem fio, desta feita foram iniciadas pesquisas sobre a radiotelegrafia. Em 1897, Guglielmo Marconi fundou a *Wireless Telegraph and Signal Company,* voltada exclusivamente para planejar e vender equipamentos sem fio a grandes clientes comerciais e ao governo. Existia o problema do sigilo, tendo em vista que as mensagens transmitidas pelo radiotelegrafo eram captadas por qualquer aparelho receptor e não só pelo destinatário (BRIGGS, 2006).

Com o avanço da tecnologia, foi possível a invenção do rádio. Com ele, uma notícia poderia circular livremente pelo espaço, devido a seu suporte abstrato. Assim, uma família que vivia afastada de um centro urbano poderia ter acesso à informação através do rádio. No ano de 1912, estima-se que existiam 122 clubes de transmissão sem fio nos Estados Unidos. Já no fim do ano de 1922 existiam mais de 572 licenças para o funcionamento de estações de transmissão de rádio (BRIGGS, 2006).

Com a estabilização do rádio, surgiu uma nova forma de comunicação: a televisão. O primeiro serviço de transmissão de televisão foi inaugurado em 11 de maio de 1928 (BRIGGS, 2006). Todavia, esbarrava também em limites físicos de propagação das ondas de rádio ou televisão, além de só se transmitir sons ou imagens entre a empresa e o consumidor. Ainda havia a necessidade de se aumentar a possibilidade de circulação de informações e o conteúdo destas.

No cenário pós-guerra, especificamente, durante a Guerra Fria, no fim da década de 60, surgiu o protótipo da Internet, denominado de ARPANET – Advanced Research Projects Agency

Network. Trata-se de uma rede de computadores financiada pelo Departamento de Defesa norte-americano encomendado à DARPA – Defense Advanced Research Projects Agency. O objetivo era a ligação entre bases militares dos Estados Unidos, para que, no caso de um ataque soviético, pudesse ser feita a imediata comunicação, ou até mesmo prevenir danos (BRANT, 2014).

No início da década de 70, universidades começaram a se conectar à rede, ampliando-a ainda mais. Ainda em um contexto acadêmico e militar, Tim Berners-Lee, um físico britânico, conhecido como o pai da Internet, inicia uma série de pesquisas sobre a possibilidade de disponibilização da rede para todos usuários. Ele inventou a linguagem HTML – Hyper Text Markup Language, assim nasceu em 1989, em Genebra na Suíça, a World Wide Web, o WWW, que todos os usuários digitam ao navegar na Internet. Em 1993, Marc Andreessen cria o Browser Mosaic, facilitando a navegação na rede (BRANT, 2016). No ano de 1996, Larry Page e Sergey Brin criam o Google, um motor de buscas que facilita ainda mais o uso da rede.

No final da década de 90, o que se viu foi uma verdadeira expansão da Internet, passando de uma rede militar e acadêmica para uma rede doméstica. Surgiram os sites pessoais, *Ecommerce,* redes sociais, Internet Banking e diversas outras facilidades.

Percebe-se que a evolução da sociedade em termos de tecnologia é gradual, mas exponencial. É o que Gordon Moore, criador da Lei de Moore[1], sustentava. Segundo ele, a cada 18 meses, a capacidade de processamento de informações dobraria pelo mesmo custo. Atualmente, a capacidade de processamento de informações é alta, e continua crescendo com o avanço da tecnologia, confirmando a sua teoria.

Em sua obra "The Third Wave", Alvin Toffler (1980) afirma que a evolução da humanidade poderia ser dividida em três ondas. A base para esta afirmação seria o que a humanidade considera

[1] Informação disponível em: <https://pt.wikipedia.org/wiki/Lei_de_Moore>. Acesso em: 10 jul. 2016.

como riqueza. Assim, a primeira onda é marcada pelo início da agricultura, momento em que o homem deixa de ser nômade, cultivando a terra e atribuindo valor ao produto obtido, seja por meio do escambo ou por meio de uma moeda de troca. A segunda onda é marcada pela revolução industrial, momento em que se tem uma massificação da produção e do consumo. Nesta época, a riqueza é marcada pela propriedade privada, pelo trabalho e pelo capital. Por fim, tem-se a terceira onda, que é denominada por ele como Era da Informação. Assim leciona Patrícia Peck Pinheiro (2016):

> Na Era Digital, o instrumento de poder é a informação, não só recebida, mas refletida. A liberdade individual e a soberania do Estado são hoje medidas pela capacidade de acesso à informação. Em vez de empresas, temos organizações moleculares, baseadas no indivíduo. A mudança é constante e os avanços tecnológicos afetam diretamente as relações sociais. Sendo assim, o Direito Digital é, necessariamente, pragmático e costumeiro, baseado em estratégia jurídica e dinamismo. (PINHEIRO, 2016, p. 74)

Com o aumento dos meios de comunicação, a capacidade de processamento de dados, bem como o surgimento da Internet, tem-se uma sociedade com uma vasta velocidade e quantidade de transmissão de informações. Assim, é preciso que se repense a proteção do indivíduo nessa era, tendo em vista a vulnerabilidade que pode existir em razão da circulação e exposição de seus dados pessoais.

2.1 A quebra de paradigma na Internet com a WEB 2.0

Conforme o dicionário Aurélio, a palavra Internet designa um substantivo feminino e tem por definição

> Qualquer conjunto de redes de computadores ligadas entre si por roteadores e gateways, como, p. ex., aquela de âmbito mundial, descentralizada e de acesso público, cujos principais serviços oferecidos são o correio eletrônico (q. v.), o chat (q. v.) e a Web (q.

> v.), e que é constituída por um conjunto de redes de computadores interconectadas por roteadores que utilizam o protocolo de transmissão TCP/IP. (FERREIRA, 1999)

Entretanto, o conceito está ultrapassado, pois o acesso à informação não mais se limita aos computadores. É possível que o acesso seja feito por telefones, tablets, relógios e até mesmo por eletrodomésticos e carros, o que se denomina de Internet das Coisas. Por sua vez, o Marco Civil da Internet – MCI, em seu artigo 5º, inciso I, considera Internet como "o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;" (BRASIL, 2014).

Perceba que no conceito do Marco Civil não se atribui a necessidade de computadores. Considera-se a Internet autônoma, como sendo o protocolo de códigos capazes de interligar usuários através de um terminal, que é um dispositivo informático que se conecta à rede mundial de computadores. Portanto, é possível que se tenha uma rede de computadores sem Internet, desde que a ligação seja uma rede local e restrita. Um exemplo seriam as redes privadas em empresas para partilhar documentos. Entretanto, caso haja a ligação com a rede mundial através de um provedor, se terá Internet.

A Internet, originalmente, foi concebida para ser um provedor de conteúdo e informação, ou seja, uma forma de acessá-los pelos provedores. Nesse cenário, o usuário era mero expectador, apenas recebia informação, mas isso mudou com a Web 2.0. Pode-se dizer que existem provedores de Backbone, acesso, hospedagem, conteúdo e informação (ALMEIDA, 2015).

O provedor de Backbone é aquele que oferece a estrutura da Internet. Como visto, a Internet nada mais é que uma rede de computadores e dispositivos conectados. Essa conexão é feita, ao final, pelo provedor de Backbone. A palavra inglesa, que em tradução literal significa "Espinha Dorsal", funciona como tal órgão

do corpo humano, ou seja, sustenta toda a estrutura e mantém a troca de informações. Esse provedor não possui ligação direta com o consumidor final, apenas viabiliza a conexão que é feita através do provedor de acesso.

O provedor de acesso é o que liga o consumidor/usuário à Internet, ou seja, é o intermediário entre o dispositivo e o provedor de Backbone. Hoje se discute a possibilidade dessa conexão ser em parte gratuita, o que se denomina de *Zero Rating*. Entretanto, entende-se que desde a regulamentação do Marco Civil pelo decreto nº 8.771/2016 (BRASIL, 2016), não é mais possível a distribuição gratuita de parte de serviço de comunicação, ou seja, o provedor de acesso pode ser pago ou gratuito, mas nunca parcialmente gratuito, isso ao menos no Brasil. Evidente que esse posicionamento é recente, tanto que a doutrina defendia a possibilidade de se oferecerem serviços parcialmente gratuitos na rede, conforme expõe Almeida (2015).

Assim, o provedor de acesso liga o usuário ao provedor de Backbone, que por sua vez irá ligar ao provedor de hospedagem. O provedor de hospedagem é aquele que guarda em si a informação a ser acessada. Ou seja, ele é como se fosse o armário, que possui o conteúdo, o qual não foi por ele gerado. Esse conteúdo é alimentado pelo provedor de conteúdo.

Provedor de conteúdo é o serviço que apresenta a informação a ser acessada pelo usuário na rede, a qual é alimentada pelo provedor de informação. Assim, no caso do Facebook, a plataforma seria o provedor de conteúdo, enquanto que os usuários seriam os provedores de informação.

Em síntese, conforme Almeida (2015), são exemplos de provedores de Backbone, a Brasil Telecom e a Embratel; a OI Velox é um exemplo de provedor de acesso; a LocaWeb é um exemplo de provedor de hospedagem; enquanto que as mídias e as redes sociais, como por exemplo, o Facebook, Twitter, Instagram e outros, são provedores de conteúdo, sendo que os usuários seriam os provedores de informação. Isso na denominada Web 2.0

(O'REALLY, 2005), na qual os usuários assumem um papel fundamental na Internet, gerando conteúdo em provedores, através de blogs e redes sociais por exemplo. Referido fenômeno caracteriza a Internet como uma rede a ser alimentada tanto pelos provedores quanto pelos usuários.

A conotação de Web 2.0 é para se estabelecer uma quebra de paradigma. Antes das redes sociais, o provedor era quem fornecia todo o conteúdo (Web 1.0). Hoje há uma multiplicidade de agentes na rede, o que remete a importância da manutenção da privacidade dos usuários, principalmente ante ao crescimento das redes sociais (LACERDA, 2017).

Inicialmente, a Internet era a forma de acessar informação gerada pelo próprio Website. Entretanto, no início do século XXI mudou-se essa forma através do Geosites, uma plataforma do Yahoo que permitia aos usuários a criação de seus próprios websites. Ainda, no ano de 2003 surgiu a primeira rede social que se tem conhecimento, a *friendster*. Com ela, os usuários interagiam uns com os outros, criando a informação.

Percebe-se que hoje os usuários ganham papel de destaque, tendo em vista que eles irão criar o conteúdo nas redes sociais, por exemplo. Isso se deve ao fato da população está cada vez mais conectada. Atualmente são mais de 3 bilhões de usuários na Internet. Além disso, são mais de 1 bilhão de sites disponíveis[2].

Até mesmo o número de usuários em redes sociais é assustador. Só o Facebook, maior rede social em atividade, possui 1,9 bilhões de usuários. Através dos e-mails, é possível perceber como o mundo está cada vez mais conectado, uma vez que, por segundo, são enviados aproximadamente 2,5 milhões de e-mails, 67% são Spam. No Instagram, são publicadas 781 fotos por segundo[3].

---

[2] Informação disponível em: < http://www.Internetlivestats.com/>. Acesso em: 10 jul. 2017.
[3] Informação disponível em <http://www.Internetlivestats.com/>. Acesso em 10 jul 2017

2.2 O avanço das redes sociais e o futuro da Internet com a WEB 3.0

Indo além da WEB 2.0, Andrew Murray (*apud* TEFFÉ, MORAES, 2017) identifica a WEB 3.0. O referido autor distingue a Web 2.0 (a Web participativa) da Web 3.0 (a Web semântica ou a Web inteligente).

> No cenário marcado pela chamada Web 3.0, a tecnologia atua no sentido de organizar o conteúdo, visando à interação inteligente e personalizada do usuário com o material disponibilizado na rede. Os provedores vêm trabalhando no sentido de desenvolver mecanismos para expandir as suas capacidades de intuição, tendo como objetivo deduzir o que o internauta deseja, a partir de seu comportamento na Internet. Busca-se entregar informações personalizadas e, até mesmo, coisas que estariam relacionadas ao que o usuário solicitou, mas se "esqueceu" de escrever. Na Web semântica, é dado significado à informação, o que permite que computadores e pessoas trabalhem melhor em cooperação. A Web 3.0 tem como um de seus principais objetivos tornar a rede mais acessível em nível de informações; surge para facilitar a vida dos usuários, modificando expressivamente a forma como o conteúdo é organizado e apresentado (MURRAY, Andrew *apud* TEFFÉ, MORAES, 2017).

Essa Internet cada vez mais inteligente expõe ainda mais os usuários, principalmente no contexto em que as redes sociais são utilizadas. Na sociedade da informação, o destaque é bem visto. Utiliza-se a Internet sem o devido cuidado. A rede social se torna um verdadeiro centro de disputa de atenções, já que a forma como as pessoas são vistas é importante, pois refletem a sua vida. Há um desejo "de ser visto", notado, percebido para além daquela comunidade real em que se encontram (MARICHAL, 2013). Por excelência, a rede social necessita do outro, da alteridade.

> Rede social é gente, é interação, é troca social. É um grupo de pessoas, compreendido através de uma metáfora de estrutura, a

> estrutura de rede. Os nós da rede representam cada indivíduo e suas conexões, os laços sociais que compõem os grupos. Esses laços são ampliados, complexificados e modificados a cada nova pessoa que conhecemos e interagimos (RECUERO, 2015, p. 83).

Fala-se em sociedade do espetáculo, na qual a riqueza passa a ser a representação da vida por imagens. "O espetáculo não é um conjunto de imagens, mas uma relação social entre pessoas, mediatizada por imagens." (DEBORD, 2003, p. 14). Neste sentido, Gui Debord (2003) afirma que os indivíduos prezam por serem notados, gostam da exposição. Nesta sociedade, não é um espanto existirem empresas especializadas em curtir e impulsionar publicações, prática muito comum no mercado asiático (JÁ, 2017).

Isso pode ser agravado ante a diferença de uso entre os nativos e imigrantes digitais, definição proposta por Aranzazu Bartolomé Tutor (2015). O autor afirma que os adultos são imigrantes digitais e as crianças e adolescentes são os nativos, pois já nasceram junto com a Internet e, por isso, têm facilidade no uso da tecnologia. Como consequência de serem nativos digitais, os menores compartilham informações diversas e não se preocupam com certos aspectos. Minimizam a importância que é devida e não dão atenção para os seus dados pessoais, intimidade e privacidade. O autor cita no texto a necessidade de se proporcionar adequado conhecimento e controle dos dados pessoais.

Aranzazu Bartolomé Tutor (2015) estuda as mudanças que as novas tecnologias trouxeram no mundo. Afirma que mais que sujeitos passivos, na Internet, os usuários são sujeitos ativos, ao passo que podem fazer parte de diversas redes sociais e fazer contato com milhares de pessoas. Fala ainda em sociedade tecnológica, que seria aquela na qual se compartilha informações pessoais na rede, o que leva a uma certa renúncia à própria privacidade. Afirma que há uma mudança de paradigma, isso porque os usuários assumem uma certa perda de privacidade em troca da liberdade de uso dessas ferramentas tecnológicas.

Sobre o assunto, Pierre Levy (1999), que utiliza a nomenclatura de "Cibercultura", mostra as peculiaridades dessa sociedade e confronta os desafios que irão ser enfrentados. Interessante apontar que, já na introdução, ele afirma ser confiante nas mudanças positivas que a Internet trouxe, mostrando-se otimista. Indo além, Henry Jenkins (2008) fala em cultura da convergência, que seria a convergência dos meios de comunicação, cultura participativa e inteligência coletiva. Segundo o autor, o atual cenário é marcado pela integração entre produção e agentes.

A realidade atual é a concentração dos dados pessoais em serviços informáticos, o que pode ser um risco. Veja que no dia 19 de junho de 2017, o canal de notícias BBC apresentou reportagem na qual afirmou que dados de aproximadamente 200 milhões de cidadãos norte-americanos foram expostos, já que poderiam ser acessados por qualquer usuário do *Amazon*, serviço de e-commerce (PERSONAL, 2017). A maioria dos cidadãos sequer sabia da existência dessas informações, ou seja, não houve consentimento para uso.

É preciso que se discuta a forma de proteção da personalidade dos usuários, em virtude da vasta gama de informação que as plataformas digitais possuem sobre estes e que é denominada de dados pessoais. Parte dos dados que as redes sociais possuem se traduzem como dados sensíveis, dizendo respeito às informações como raça, etnia, religião, opção sexual e outras do gênero, daí a importância da proteção.

2.3 O avanço das redes sociais e a coleta indiscriminada de dados pessoais: Shadow Profile

Quando um provedor de conteúdo utiliza um dado pessoal, geralmente é para venda ou marketing. Fala-se hoje em ditadura do algoritmo. Todos têm uma reputação digital, ou seja, são avaliados de acordo com os seus próprios hábitos. Isso pode influenciar em diversas esferas da vida do usuário. Veja que já há o registro de uma

patente pelo Facebook, que objetiva a concessão de empréstimo com base nos amigos que se têm na rede social (JUNQUEIRA, 2015).

Embora os usuários forneçam ativamente informações às plataformas, algumas vezes estas coletam dados sem que o usuário saiba. Por isso, afirma-se que as redes sociais sabem mais dos usuários do que eles gostariam. Essas informações que não foram fornecidas, mas coletadas através de um consentimento viciado do usuário, denominam-se *Shadow Profiles*.

Tal prática foi conhecida através do caso Max Schrems vs. Facebook. Em 2011, o estudante de direito austríaco Max Schrems apresentou uma reclamação contra o Facebook após ter solicitado uma cópia *off-line* de todos os seus dados (COMPLAINT, 2016). Foi constatado que a rede social possuía muito mais informação do que ele havia fornecido. Era mantido um perfil sombrio, que não aparecia para ele, mas que a rede sabia da existência para classificar o usuário de acordo com seus hábitos e gostos.

Em resposta à acusação, Andrew Noyes, gerente de relações públicas do Facebook, negou veemente que mantinha perfis sombras, ao argumento de que:

> Nós podemos enviar e-mails para seus amigos, convidando-os a entrar no Facebook. Mantemos endereço de e-mail e nome para que você saiba quando eles se juntam o serviço dos convidados. Esta prática é comum entre quase todos os serviços que envolvem convites de compartilhamento de documentos para o planejamento do evento. A afirmação de que o Facebook está fazendo algum tipo de perfil sombrio é simplesmente errada, além disso, o Facebook oferece mais controle do que outros serviços, permitindo às pessoas eliminarem o seu endereço de e-mail do Facebook ou recusarem convites que recebem. Ainda, como parte da oferta às pessoas dos serviços de mensagens, nós permitimos que as pessoas possam eliminar mensagens que recebem na sua caixa de entrada e mensagens que enviam. No entanto, as pessoas não podem excluir uma mensagem que enviar a partir de caixa de entrada do destinatário ou uma mensagem que você recebe de pasta enviadas do remetente. Esta é a maneira como qualquer serviço de mensagens existente trabalha. Achamos que é também

> consistente com as expectativas das pessoas. Estamos ansiosos para fazer esses e outros esclarecimentos à DPA irlandês. (LOCKE, 2016, tradução nossa)[4]

Andrew Noyes justificou a coleta de informações dizendo que estas eram necessárias ao funcionamento da rede e que todas as outras fazem isso. Ademais, afirma-se que "o Facebook está mapeando a população em uma conexão social com ou sem a ajuda do usuário" (RUTHRUFF, 2016, tradução nossa)[5]. Nesse contexto, observa-se o que se denomina *big data*, ou sociedade da informação.

Um simples dado pode levar a diversos outros. Em uma pesquisa feita pelo *El País*, foi constatado que com apenas 800 números de telefones dos Estados Unidos é possível se chegar a dados de todos os Americanos (CRIADO, 2016), isso simplesmente utilizando metadados.

Constata-se que as redes sociais em geral coletam mais informações do que necessitam, as quais dizem respeito a um usuário e até mesmo um não usuário. Por isso, têm-se duas vertentes de *Shadow Profiles*. A primeira diz respeito àquelas informações sobre um usuário que não foram fornecidas por ele de maneira ativa, tais como localização atual, e-mail, telefone secundário, hábitos na Internet, gostos, preferências capturadas através da navegação, entre outros. A segunda se refere a informações de não usuários que a rede possui, por exemplo,

---

[4] Tradução de: "We enable you to send e-mails to your friends, inviting them to join Facebook. We keep the invitees' e-mail address and name to let you know when they join the service. This practice is common among almost all services that involve invitations--from document sharing to event planning--and the assertion that Facebook is doing some sort of nefarious profiling is simply wrong. In addition, Facebook offers more control than other services by enabling people to delete their e-mail address from Facebook or to opt-out of receiving invites. Also, as part of offering people messaging services, we enable people to delete messages they receive from their inbox and messages they send from their sent folder. However, people can't delete a message they send from the recipient's inbox or a message you receive from the sender's sent folder. This is the way every message service ever invented works. We think it's also consistent with people's expectations. We look forward to making these and other clarifications to the Irish DPA."

[5] Tradução de: "Facebook is mapping the human population one social connection at a time with or without your help."

endereço de e-mail, telefone e nome que estejam na agenda de contatos de um usuário.

Conforme se verá nos tópicos 5 e 6, os termos de uso e política de privacidade, em geral, permitem que se faça a coleta dessas informações. A plataforma, através de um usuário, captura dados de um não usuário. Assim, por meio do mapeamento de informações, é possível se chegar a diversas conclusões sobre o perfil de um não usuário.

Desse modo, quando alguém convida um não usuário a integrar uma determinada rede social, esta já possui informação suficiente para dizer quais amigos daquela pessoa estão na rede. É como se a pessoa já estivesse na rede social, faltando apenas que ele aceite o termo de uso para aparecer.

Afirma-se que as redes sociais funcionam em camadas. A primeira camada é visível a todos os usuários, são informações básicas, como nome e foto de perfil. A segunda, são aquelas informações que os usuários restringem a sua rede de contatos, tais como fotos e posts. A terceira, que é uma camada sombra, não aparece para os usuários. São as informações que a plataforma possui a respeito deste para mapear seus gostos e gerar conteúdo direcionado, captando a sua atenção e preferência. A quarta e última camada também é sombra, não aparece na rede. Refere-se àquelas informações que a plataforma possui sobre um não usuário, categorizando-o para que quando este venha a integrar à rede, esta sugira amizades e conexões, fornecendo inclusive conteúdo através dos gostos da pessoa.

Nesta classificação de camadas, tem-se que as duas primeiras são visíveis aos usuários e passíveis de controle. Por outro lado, as duas últimas, além de não visíveis, não é dado o poder de controle às pessoas. Não é possível a autodeterminação, ou seja, se a rede social, através de seu perfil de uso, identificar uma certa informação para gerar um determinado conteúdo, o usuário não poderá mudá-lo, a não ser que mude seu perfil de uso.

Na denúncia feita por Max Schrems, foi constatado que o Facebook possuía diversas informações que não haviam sido fornecidas pelo usuário. Com base na legislação europeia, o austríaco solicitou seus dados e descobriu essas camadas ocultas. Pensando na proteção do usuário na era da informação, ele criou o Europe vs. Facebook[6], uma organização com sede na Europa, que tem como objetivo proteger a privacidade e intimidade dos usuários na Internet. Assim, é necessário que se faça uma digressão sobre os direitos da personalidade, especificamente sobre o direito à privacidade e intimidade para que se analise a eventual violação destes com os *Shadow Profiles*.

[6] Informação disponível em: <http://europe-v-facebook.org/>. Acesso em: 10 jun. 2016.

3

Uma abordagem dos direitos da personalidade

Todo ser humano é pessoa e toda pessoa possui personalidade jurídica. Entende-se a personalidade como um instituto *sui generis*, de um lado como sendo a aptidão genérica para contrair direitos e obrigações na ordem civil e, de outro, vista como os direitos da personalidade. Neste capítulo discute-se a segunda vertente.

Conforme Schereiber (2011), o marco inicial para se investigar os direitos da personalidade é a segunda metade do século XIX. A expressão "foi concebida por jusnaturalistas franceses e alemães para designar certos direitos inerentes ao homem, tidos como preexistentes ao seu reconhecimento por parte do Estado." (SHCREIBER, 2011, p.5). Observa-se que existem direitos que o homem possui que são considerados essenciais à condição humana, sem os quais o indivíduo pode, inclusive, não ser considerado pessoa.

Essa doutrina veio em resposta ao Estado Liberal do século XVIII e XIX. Com a revolução liberal na França, cunhou-se a ideologia da liberdade como maior direito do homem. Assim, era possível a renúncia a qualquer direito, mesmo que fosse visto como essencial, pois esta renúncia "era vista como legítima porque fundada na 'livre manifestação de vontade' do renunciante" (SCHEREIBER, 2011, p. 4).

Viu-se uma necessidade de proteger o homem dele mesmo. Estas renúncias aos direitos tidos como essenciais poderiam trazer prejuízos ao indivíduo. Assim, havia a necessidade de se tutelar o homem no campo privado. Neste cenário afirmava-se que os

direitos da personalidade eram absolutos, imprescritíveis, inalienáveis e indisponíveis. Entretanto, existia a barreira do liberalismo, que fez com que surgisse a corrente dos negativistas comandada por Savigny, Von Thur e Ennerccerus, os quais negavam a existência dos direitos da personalidade (SCHEREIBER, 2011). Mais do que isso, entre os afirmativistas, não foi um consenso a natureza e rol de proteção.

> Não havia, por exemplo, consenso sobre quais eram os direitos da personalidade. Falava-se com frequência no direito ao próprio corpo, no direito à honra e no direito à vida, mas alguns autores acrescentavam, ainda, o direito ao nome e outros direitos. Havia mesmo quem incluísse no rol o direito à propriedade, cuja natureza patrimonial representava, para outros, a própria antítese dos direitos da personalidade. Para parte da doutrina, não havia ainda "direitos da personalidade" no plural, mas um único "direito geral da personalidade". Os desacordos, enfim, eram muitos. (SCHREIBER, 2011, p. 5)

Aos poucos foi se estabelecendo um conceito sobre a personalidade, vigorando, desde então, a dualidade, sendo está entendida no aspecto subjetivo e objetivo. O aspecto subjetivo se revela como a capacidade jurídica, ou seja, a aptidão para atos da vida civil. Esta vertente pode sofrer limitação, já que existem pessoas incapazes e capazes. Por sua vez, no âmbito objetivo, a personalidade é o conjunto de atributos intrínsecos do ser humano, sendo considerada objeto de proteção do ordenamento jurídico.

A concepção dos direitos da personalidade é paralela à evolução dos direitos humanos. Segundo Fernandes (2014), muitos autores consideram que as expressões direitos fundamentais e direitos humanos são sinônimas. Mas, segundo esse mesmo autor, os direitos dos homens remontam à ideia de um direito natural, ainda não positivado. Já os direitos humanos são aqueles que teriam salvaguarda no âmbito do direito internacional, enquanto que os direitos fundamentais são os tutelados pelas legislações internas de cada Estado.

Os direitos fundamentais surgiram da necessidade de se proteger o homem tanto contra o abuso do poder estatal, quanto nas relações que estabelecer, sejam com o Estado ou não. Assim é que se afirma que os direitos fundamentais possuem eficácia vertical (nas relações dos cidadãos com o Estado) e horizontal (nas relações entre iguais). É comum a diferenciação dos direitos fundamentais em gerações, conforme a tutela histórica que lhes foram sendo dadas.

A primeira geração de direitos fundamentais tem sido definida como aquela que salvaguardou os direitos relacionados à liberdade. Remonta ao surgimento do liberalismo e ao rompimento com o modelo de Estado anterior, qual seja, absolutismo. Conforme Fiuza (2011), foi necessário impor limites à atuação do poder Estatal, assegurando, desse modo, que as pessoas fossem livres e iguais, não se admitindo, portanto, a intervenção estatal na esfera privada. Nesse contexto histórico, as constituições, de um modo geral, tutelaram as liberdades individuais face ao Estado, bem como protegeram os direitos civis e políticos.

Já no século XX, conforme Fernandes (2014), surge a segunda geração de direitos fundamentais, pois nesse contexto histórico fez-se necessária a tutela dos direitos sociais, culturais e econômicos. Observe que o capitalismo e a revolução industrial que impulsionaram o rompimento com o modelo de Estado absolutista e fortaleceu os vínculos com modelo liberal de Estado, também impulsionaram uma maior desigualdade social. Assim é que, conforme Fiuza (2011), o Estado passou a ter que garantir outros direitos às pessoas – os sociais – de forma que a própria lógica capitalista não fosse frustrada. Explica-se, o liberalismo levado a extremo se tornou um meio de opressão das camadas da população economicamente inferiores que dão sustentáculo ao próprio sistema; fez-se, portanto, necessária a intervenção estatal para que fosse garantida não só a igualdade formal entre as pessoas, mas a igualdade material, ou seja, a efetivação de direitos sociais.

No contexto pós-guerra, conforme Fernandes (2014), surgem os direitos de terceira geração, garantindo a necessidade de tutela

de bens ligados à fraternidade, tais como o direito à paz, direito ao meio ambiente sustentável e equilibrado, direito de comunicação, direito ao livre desenvolvimento, entre outros.

Ainda, em 1948, com a Declaração Universal dos Direitos Humanos, consagrou-se a dignidade da pessoa humana como fundamento da liberdade e "valor central da ordem jurídica internacional" (SCHEREIBER, 2011, p. 7). Portanto, o homem foi tutelado em vista da sua dignidade, sendo este o cerne de proteção, ou seja, protege-se a condição humana. Assim, considera-se a pessoa como a finalidade de proteção.

Paulo Bonavides (2016) acrescenta outras gerações de direitos fundamentais. Informa que no mundo moderno houve a diminuição das barreiras geográficas, daí a necessidade de surgimento de uma sociedade mais aberta. O autor fala em uma quarta geração de direitos, tais como a democracia, informação e ao pluralismo. Segundo Fernandes (2014), autores como José Alcebíades Oliveira Júnior e Dirley da Cunha Junior incorporam à quarta geração de direitos fundamentais, os direitos relacionados à biotecnologia, tais como manipulação genética, mudança de sexo, entre outros.

Ainda, conforme Fernandes (2014), é possível argumentar sobre uma quinta geração de direitos fundamentais, todos eles correlacionados ao direito à vida e à paz. Desta feita, afirma o autor que as novas tecnologias trazem novos desafios e passa a ser necessária a salvaguarda de direitos como a identidade individual, direito ao patrimônio genético e à proteção contra o abuso de técnicas de clonagem.

Cabe ressaltar que a divisão em gerações de direitos fundamentais tem cunho histórico e o surgimento de uma nova geração não faz com que sejam excluídos os direitos reconhecidos na anterior. A sociedade se transforma e faz surgir a necessidade de proteção de novos direitos que, em razão de um contexto histórico, não poderiam ser reconhecidos em um momento anterior.

Como dito, a evolução dos direitos da personalidade é paralela aos direitos fundamentais. Não se afirma que um instituto exclui ou contempla o outro. Nesse sentido, André Couto e Gama afirma que:

> Adianta-se a conclusão de que a coexistência que ocorreria entre os *direitos fundamentais* e os *Direitos da Personalidade* – aqueles, no Direito Público, e estes, no Privado – deve-se pela marcante tendência da compartimentalização do Direito, já que se tratam de *institutos* cuja semelhança é marcante e, no entendimento de muitos estudiosos, uma mesma coisa. Conclui-se, aqui, o longo período de desenvolvimento embrionário de institutos e ideias indissociáveis dos *Direitos da Personalidade*, os quais tornaram possíveis estes últimos na próxima era da humanidade. (COUTO E GAMA, 2014, p. 59)

O referido autor chegou a essa conclusão após apresentar a teoria positivista dos direitos da personalidade, ou seja, após afirmar pela existência destes. André Couto e Gama (2014) afirma que os direitos humanos são inerentes à pessoa, não necessitam de constar de textos legislativos. Em paralelo surgem os direitos da personalidade para a proteção do homem entre seus pares, no campo do direito privado.

Importante dizer que os ordenamentos jurídicos, desde Napoleão com o Código Civil francês de 1808, passaram por um momento histórico da codificação. Naquele momento, pensava-se em concentrar as leis em um único livro. Surgiram importantes códigos, como o BGB - Bürgerliches Gesetzbuch, o Código Civil Alemão. Entretanto, com o passar do tempo, surgiu a tutela de novos direitos, os chamados microssistemas, institutos jurídicos que possuem regras especiais.

Um exemplo é a Propriedade Intelectual, microssistema do direito privado que visa à proteção daquele acervo imaterial, seja da pessoa natural ou não natural, haja vista que a pessoa jurídica pode ser titular de direitos sobre obras, ainda que de forma derivada (POLI, 2008). Diversos são os marcos legais deste instituto; em âmbito internacional tem-se a Convenção de Berna e a Convenção

de Paris, a primeira normatizando os direitos autorais e a segunda a Propriedade Industrial.

A Convenção de Berna, de 9 de setembro de 1886, foi ratificada no Brasil pelo Decreto Legislativo nº 94, de 4 de dezembro de 1974, e promulgada pelo Decreto nº 75.699, de 6 de março de 1975, conforme expresso em Gandelman (2001). Por sua vez, a Convenção de Paris é datada de 1880 e criou o sistema internacional de proteção à Propriedade Industrial. Entretanto, a referida Convenção foi revista em "Bruxelas (1900), Washington (1911), Haia (1925), Londres (1934), Lisboa (1958) e Estocolmo (1967)" (COELHO, 2011, p. 150-151).

A proteção do autor e inventor não está exclusivamente dentro do Código Civil, fala-se, portanto, no movimento de descodificação. Como não é possível abarcar todo ordenamento jurídico privado dentro de um único código, estabelece-se uma norma base, sendo essa o centro daquele ramo jurídico e as outras normas, complementares. Assim, no caso do direito privado, o código civil é o centro e os microssistemas o complementam.

Fala-se ainda em constitucionalização do Direito Privado (FIUZA, 2011). Esse movimento é caracterizado pela leitura das normas de direito privado à luz dos princípios e valores constitucionais. Isso não significa retirar autonomia do direito civil.

> Falar em constitucionalização do Direito Civil não significa retirar do Código Civil a importância que merece como centro do sistema, papel este que continua a exercer. É no Código Civil que iremos buscar as diretrizes mais gerais do Direito Comum. É em torno dele que gravitam os chamados microssistemas, como o imobiliário, o da criança e do adolescente, o do consumidor e outros. Afinal, é no Código Civil, principalmente na posse e na propriedade, na teoria geral das obrigações e dos contratos, que o intérprete buscará as normas fundamentais do microssistema imobiliário. É a partir das normas gerais do Direito de Família e da própria Parte Geral do Código Civil que se engendra o microssistema da criança e do adolescente. [...] Não se pode furtar ao Código Civil o trono central do sistema de Direito Privado. Seria

> incorreto e equivocado ver neste papel a Constituição (FIUZA, 2011, p. 118-119)

Daí que se decorre a afirmação de que o princípio da dignidade da pessoa humana orienta e legitima todo o sistema jurídico de proteção à personalidade no Brasil (AMARAL, 2008). Como as normas de Direito Privado devem ser lidas à luz da constituição, a dignidade da pessoa humana, princípio fundamental da Constituição da República de 1988, orienta inclusive a proteção dos direitos da personalidade.

Isso não retira a centralidade do Código Civil de 2002, que dedicou o capítulo II (arts. 11 a 21) aos Direitos da Personalidade (BRASIL, 2002). A análise deste instituto deve ser feita a partir do Código Civil, mas sem excluir a interpretação conjunta com as normas de Direito Público. Por isso é importante a evolução dos direitos fundamentais para a proteção dos direitos da personalidade.

Assim, a dignidade se manifesta em três pilares, os direitos humanos, "como categoria a que prevalentemente recorrem a Filosofia do Direito e o Direito Internacional" (ASCENÇÃO, 2013, p. 6), os direitos fundamentais, "a que se dedicam em especial o Direito Constitucional e a Ciência Política" (ASCENÇÃO, 2013, p. 6) e os direitos da personalidade, "que são objeto mais próprio das leis civis" (ASCENÇÃO, 2013, p. 6).

Há que se ressaltar que houve a repersonificação do Direito Privado. Conforme Cesar Fiuza (2011), nos séculos XIX e XX, período da codificação, a base para o Direito era a autonomia da vontade, a propriedade privada e a família, o que mudou com o liberalismo. Com a máxima liberdade da vontade, houve a massificação dos contratos, assim, o contrato é visto como uma necessidade.

Nasce a teoria preceptiva, segundo a qual o contrato vale não apenas porque as partes assim o desejaram, mas porque o seu cumprimento interessa a toda sociedade. Assim, a autonomia da vontade é substituída pela autonomia privada. Não mais se fala em proteger a autonomia da vontade, mas sim o homem, pois "as coisas

têm preço, mas a pessoa tem dignidade." (ASCENÇÃO, 2013, p. 6). Muda-se o centro gravitacional do Direito das Obrigações e do Direito das Coisas, passando a ser ocupado pelo ser humano.

O homem passa a ser a base do direito privado, sendo tutelados os seus direitos enquanto tal, os quais se traduzem como direitos da personalidade. Assim conclui Cesar Fiuza (2011):

> Diz-se que os pilares de sustentação do Direito Civil, família, propriedade e autonomia da vontade, deixaram de sê-lo. O único pilar que sustenta toda a estrutura é o ser humano, a dignidade da pessoa, sua promoção espiritual, social e econômica. Esse pilar está, por sua vez, enraizado na Constituição. (FIUZA, 2011, p. 96)

A importância de a pessoa ser o centro de proteção do Direito Civil é que a sua tutela não é restrita às previsões legais, ou seja, não há um rol taxativo dos direitos da personalidade. Por mais que o Código Civil de 2002, nos artigos 11 a 21 tutelem especificamente certos direitos, tal como o direito ao nome, não se exclui a tutela daquilo que for personalíssimo a uma pessoa e não estiver expresso na legislação. Tal conclusão decorre da leitura do artigo 12 do Código Civil, que normatiza que "pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei." (BRASIL, 2002). Da leitura do citado artigo, conclui-se que não há uma definição fechada do que são direitos da personalidade. É o que defende Anderson Schreiber (2011):

> Como se vê, a ausência de previsão no Código Civil não encerra, antes, estimula o debate em torno do reconhecimento de "novas" esferas essenciais de realização da pessoa humana. No Brasil, empreende-se atualmente necessário esforço para a construção de critérios aptos a distinguir, em meio à criatividade própria das ações judiciais, aqueles interesses que são realmente merecedores de tutela à luz do ordenamento jurídico pátrio. A iniciativa é imprescindível para evitar a banalização do instituto que se tornou, na nossa prática judicial, o principal *front* de proteção da pessoa humana: a indenização por dano moral. (SCHREIBER, 2011, p. 16)

Anderson Schreiber (2011) defende que se tem um rol aberto de direitos da personalidade, tratando-se de uma cláusula que não exclui certos direitos, já que "a pessoa, na sua substância, é a âncora da fundamentação da ordem jurídica." (ASCENÇÃO, 2013, p. 13). Em se tratando de novos fenômenos, tais como a Internet e as redes sociais, surgiram novas ramificações que ensejarão tutela em vista dos direitos da personalidade.

A própria nomenclatura adotada leva a essa conclusão. Perceba que se diz direitos da personalidade, ou seja, existem vários direitos que são inerentes à condição humana. Conforme defende Diogo Luna Moureira (2011), toda pessoa possui sua pessoalidade, entendida como a condição de ser pessoa, bem como possui personalidade. Não há restrição no ordenamento jurídico do conceito de pessoa, há, tão somente, restrição ao conceito de capacidade. Entretanto, a capacidade e a personalidade são conceitos distintos. Logo, a falta da primeira não implica a ausência de proteção da pessoa enquanto tal. Assim, adota-se a tipicidade aberta dos Direitos da Personalidade, posto que o fim maior é a proteção do homem, não sendo possível se limitar a sua tutela em um rol taxativo.

> Adotar a tipicidade fechada de direitos da personalidade em lei ordinária seria mesmo inconstitucional, posto que a hermenêutica jurídica contemporânea parte da premissa de que a ordem jurídica é um sistema aberto de normas, podendo abarcar novas construções jurídicas de proteção à pessoa. (NAVES, SÁ, 2017, p. 37)

Sobre o tema, Carlos Alberto Bittar (1999) afirma que os direitos da personalidade possuem duas vertentes, uma originária e uma expansiva, a qual se adapta conforme o avanço da sociedade. Tem-se assim:

> a) os próprios da pessoa em si (ou originários), existentes por sua natureza, como ente humano, com o nascimento; b) e os referentes às suas projeções para o mundo exterior (a pessoa como ente

> moral e social, ou seja, em seu relacionamento com a sociedade) (BITTAR, 1999, p. 10).

A "extensão" dos Direitos da Personalidade é a sua própria classificação (BITTAR, 1999). A finalidade de se enumerar quais são os direitos atinentes à personalidade é de reconhecer as inúmeras dimensões desses direitos, enfim, sua extensão. Não quer dizer que enumerar direitos de personalidade é limitar a tutela àqueles ali descritos, pois, conforme Carlos Alberto Bittar (1999), estes estão em constante expansão. Na doutrina existem diversas classificações, sendo que uma das mais aceitas é a de Adriano de Cupis (1961), decompondo os Direitos da Personalidade em seis espécies:

> I – Direito à vida e à integridade física.
> II – Direito sobre as partes destacadas do corpo e do direito sobre o cadáver.
> III – Direito à liberdade.
> IV – Direito ao resguardo (direito à honra, ao resguardo e ao segredo).
> V – Direito à identidade pessoal (direito ao nome, ao título e ao sinal pessoal).
> VI – Direito moral de autor (CUPIS, 1961, p. 53).

Carlos Alberto Bittar (1999) distribui os direitos da personalidade em:

> a) direitos físicos; b) direitos psíquicos; c) direitos morais; os primeiros referentes a componentes materiais da estrutura humana (a integridade corporal, compreendendo: o corpo, como um todo; os órgãos; os membros; a imagem, ou efígie); os segundos, relativos a elementos intrínsecos à personalidade (integridade psíquica, compreendendo: a liberdade; a intimidade; o sigilo) e os últimos, respeitantes a atributos valorativos (ou virtudes) da pessoa na sociedade (o patrimônio moral, compreendendo: a identidade; a honra; as manifestações do intelecto) (BITTAR, 1999, p. 17).

Pode-se, ainda, destacar a classificação de Orlando Gomes (1999) que disciplina:

> Consideram-se atualmente direitos à integridade física:
> a) o direito à vida;
> b) o direito sobre o próprio corpo. O direito sobre o próprio corpo subdivide-se em direito sobre o corpo inteiro e direito sobre partes separadas, compreendendo os direitos de decisão individual sobre tratamento médico e cirúrgico, exame médico e perícia médica.
> Admitem-se como direitos à integridade moral:
> a) o direito à honra;
> b) o direito à liberdade;
> c) o direito ao recato;
> d) o direito à imagem;
> e) o direito ao nome;
> f) o direito moral do autor (GOMES, 1999, p. 153).

A classificação dos direitos da personalidade pela doutrina não reflete um modelo fechado de proteção, mas tão somente reflete uma didática meramente exemplificativa. Malgrado a doutrina distinguir as espécies existentes dos direitos da personalidade, esses direitos estão em perene expansão, com surgimento de novas situações fáticas que clamam tutela jurídica.

3.1 A Privacidade e a Intimidade como um desdobramento dos direitos da personalidade em sua concepção clássica

Protege-se o ser humano enquanto pessoa, sem distinção. No âmbito dos direitos da personalidade, como dito, há uma cláusula geral de proteção, mas existem desdobramentos. Dentre eles está o Direito à Privacidade, o qual é visto como a possibilidade de a pessoa não ter certos aspectos de sua vida expostos.

Röeder (1846, apud DONEDA, 2006), doutrinador alemão, é considerado percursor de tal direito. Ele afirmou existir um direito natural à vida privada. Sobre isso, Danilo Doneda (2006) afirma que o que Röeder fez foi interpretar o tratamento dado à privacidade,

atribuindo-lhe conteúdo jurídico. O autor ensina que a sociedade sempre cunhou uma noção geral de privacidade, remontando aos ensinamentos da Grécia e China antigas. No entanto, o conteúdo não possuía juridicidade. Ocorre que a valoração da privacidade era feita de forma diversa da que é feita hoje, o que não pode ser ignorado.

> Levar em conta a natureza e o valor conferido à esfera privada em determinadas sociedades, de todo modo, é indispensável para realizar a valoração de sua configuração atual. A ela corresponderam funções diversas em gênero e amplitude, funções que hoje devem ser conhecidas para adequá-las ou não ao nosso momento. (DONEDA, 2006, p. 121)

O autor afirma ser importante observar a sistemática passada, por mais que esta não seja a forma atual de proteção. O contexto atual teve surgimento cunhado na ideia de exclusão do outro. O marco inicial é o artigo "The Right to Privacy", publicado em 1890 na faculdade de Havard por Samuel Warren e Louis Brandeis (apud SCHREIBER, 2011). O foco central do artigo[1] foi o *right to be let alone*, ou seja, o direito de ser deixado só. A privacidade foi vista como a proteção da vida íntima de cada ser humano. Nesse período, não se via como um direito positivo, no sentido de se fazer algo, mas uma conotação negativa, calcada na abstenção. Os indivíduos deviam não violar a privacidade, entendida como vida íntima do outro.

Todavia, é preciso ampliar esta ideia, tendo em vista a sua correlação com bens materiais, como a propriedade. Nessa fase, a proteção da privacidade assemelhava-se com a proteção da propriedade privada, tendo em vista que os indivíduos deveriam respeitar a privacidade dentro da esfera privada, por exemplo, o lar. É o que defende Danilo Doneda (2006):

---

[1] O artigo foi escrito em virtude de uma notícia feita com base na esposa de um dos autores, razão pela qual eles defenderem o deixado de ser deixado só, sendo respeitada a privacidade.

> A cumplicidade entre a proteção da privacidade e da propriedade, não obstante, tem então início, e assume diversas conotações dependendo do momento e do ponto de vista assumido: se é o da exclusão, o da dicotomia entre situações subjetivas patrimoniais e não patrimoniais, do direito subjetivo, da exploração econômica ou da eficiência. Nos países do *common law*, por exemplo, é fato que a vase da elaboração jurisprudencial das regras de proteção da *privacy* baseiam-se na proteção da propriedade privada, em especial nos institutos de *trespass, nisance e conspiracy*. No Brasil, notamos que a inviolabilidade do domicílio e da correspondência – nas quais se inclui o direito à privacidade – estão presentes em todas as Constituições brasileiras, desde a Constituição do Império, de 1824. Assim é possível uma chave de leitura da evolução da privacidade em termos proprietários, que é inclusive coerente com várias das teorias que hoje procuram justificar desta forma o assunto. (DONEDA, 2006, p. 116/117)

Nessa passagem, o autor argumenta que a evolução da privacidade é paralela com a propriedade privada, entretanto, a primeira não pode ser limitada ao cômputo da segunda. Assim continua Danilo Doneda (2006):

> Esta importância histórica como ponto de análise comparativa não pode, no entanto, servir como fundamentação para novas modalidades de leitura da privacidade como propriedade – tal como acontece, por exemplo, ao se considerar a informação pessoal como um bem. (DONEDA, 2006, p. 117)

O autor concluiu que essa evolução conjunta não é negativa, desde que não se limite o direito da personalidade em análise. Em verdade, existem esferas da vida privada que são despidas de conteúdo patrimonial e merecem proteção, além de que o conteúdo dos direitos da personalidade é despido de valoração econômica.

O Livro 1984, do autor George Orwell (2009), narra uma situação que enseja a proteção da privacidade e demonstra que esta pode ser despida de qualquer conteúdo patrimonial. O livro conta a

história do Grande Irmão[2], um ditador que observa todos os aspectos da vida de seus governados, impondo inclusive a forma de pensar. Isso mostra que existem aspectos da vida de um indivíduo que ele não quer compartilhar com ninguém, pois todos têm direito à privacidade. Entretanto, existem autores que ainda defendem a privacidade à luz da propriedade. É o caso da Patrícia Peck Pinheiro (2016) que leciona:

> Todo indivíduo deve ter direito a proteção de suas propriedades e de sua privacidade. Isso é indiscutível. No tocante à propriedade, há tanto bens tangíveis como intangíveis. Nesse sentido, suas informações, em última análise, são um ativo de sua propriedade e, portanto, merecem proteção. Mas será que a Sociedade Digital caminha nesse sentido, ou estamos indo para o lado oposto?
> O grande paradigma não está no conceito ético ou mesmo filosófico se a privacidade deve ou não ser protegida (claro que deve ser), mas sim no modelo de negócios estabelecido, visto que a informação virou não apenas a riqueza do século XXI como também a moeda de pagamento. (PINHEIRO, 2016, p. 95)

O que a autora conclui é que o conteúdo da privacidade pode ter valor econômico. Como visto, na atual sociedade a informação tem valor. Vive-se na terceira onda, conforme defendido por Alvin Toffler (1980). As informações pessoais inseridas na Internet possuem valor econômico e podem ser utilizadas como moeda de troca.

Contudo, o caminho para a proteção não pode ser em vista do seu aspecto material, mas sim do seu aspecto imaterial. A privacidade do indivíduo deve ser respeitada não porque ele tem o direito material sobre sua informação pessoal, mas porque pode ser prejudicial o compartilhamento de certas informações de sua vida privada.

---

[2] O livro é fonte de inspiração para o *reality show* Big Brother, presente em diversos países, no qual os participantes são confinados em uma casa e vigiados 24 horas por dia. O programa é feito no formato de um jogo, no qual o vencedor ganha uma quantia em dinheiro.

O ordenamento jurídico brasileiro estabelece a positivação de tal direito no artigo 21 do Código Civil de 2002, como um desdobramento dos direitos da personalidade. Nele há a menção de que "a vida privada da pessoa natural é inviolável" (BRASIL, 2002). Mais do que isso, tal ordenamento atribuiu status de direito fundamental, ao positivá-lo no artigo 5º, inciso X, normatizando que "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" (BRASIL, 1988). Ambas as normas garantem o direito da privacidade e atribuem um valor econômico acaso tenha violação. Não se tutela em razão do seu valor material, mas existindo violação, essa é uma das formas de se compensar a vítima. A privacidade é ainda tutelada no artigo 12[3] da Declaração Universal dos Direitos do Homem adotado pela Organização das Nações Unidas em 1948 – e no artigo 17[4] do Pacto Internacional dos Direitos Civis e Políticos – adotada pela mesma organização no ano de 1966.

A forma como a privacidade foi pensada, lida como o direito de ser deixado só, não coaduna com a proteção do indivíduo na sociedade da informação. Pois bem, existe um direito do indivíduo de ser deixado só, de excluir o outro. Mas, e no caso das redes sociais, nas quais há sempre uma interação com outros indivíduos, existe privacidade? Anderson Schereiber (2011) leciona que não é porque o indivíduo saiu da esfera privada (entendida aqui como sua residência) que ele abdicou de sua privacidade. Esse direito deve ser respeitado sempre.

---

[3] Artigo 12 – "Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências ou ataques." (Disponível em <https://www.unicef.org/brazil/pt/resources_10133.htm>. Acesso em 10 abr. 2017)

[4] Artigo 17 – "Ninguém será objeto de ingerências arbitrárias ou ilegais em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques ilegais a sua honra e reputação. 2. Toda pessoa tem direito à proteção da lei contra essas ingerências ou esses ataques." (Disponível em <http://www.planalto.gov.br/ccivil_03/decreto/1990-1994/d0592.htm>. Acesso em 10 abr. 2017)

Sobre a intimidade[5] na Internet, Aranzazu Bartolomé Tutor (2015), citando Jareno Leal, afirma que não se fala mais em intimidade na rede, mas sim "extimidad". Para o autor, na rede sempre se terá uma interação entre pessoas, a qual além de premissa da rede social é almejada pelo usuário, ou seja, ele compartilha uma informação privada, que em certos casos pode ser inclusive íntima. Assim, o conceito de "extimidad" seria o íntimo se manifestando na rede, com a interação do outro, mas sem perder a tutela jurídica.

Na era da informação, a privacidade deve ser lida como o direito de controle. O indivíduo deve ter o controle de seus dados pessoais e poder se abster que estes sejam utilizados indevidamente.

> Em uma sociedade caracterizada pelo constante intercâmbio de informações, o direito à privacidade deve se propor a algo mais que àquela finalidade inicial, restrita à proteção da vida íntima. Deve abranger também o direito da pessoa humana de manter o controle sobre os seus dados pessoais. Mais sutil, mas não menos perigosa que a intromissão na intimidade doméstica de uma pessoa, é a sua exposição ao olhar alheio por meio de dados fornecidos ou coletados de forma aparentemente inofensiva, no preenchimento de um cadastro de hotel ou no acesso a um site qualquer da Internet. O uso inadequado desses dados pessoais pode gerar diversos prejuízos ao seu titular. (SCHREIBER, 2011, p. 129/130)

---

[5] É difícil a diferenciação do que é intimidade e o que é privacidade. Os autores que argumentam pela diferenciação apontam que a vida privada é mais ampla do que a intimidade da pessoa. Argumenta-se que a vida privada é composta de informações que a pessoa escolhe se deseja divulgar, enquanto que a intimidade se refere à identidade da pessoa, como se fosse mais restrita que a primeira. Porém, a diferenciação conceitual não implica na falta de tutela, tendo em vista que ao se falar em privacidade se está tutelando a parte da vida da pessoa que não se deseja dar conhecimento a terceiros. "Os termos "vida privada" e "intimidade" fazem menção específica a determinadas amplitudes do desenvolvimento da proteção da privacidade, como a teoria dos círculos concêntricos de Hubmann, que apresentaram maior importância em um determinado contexto e momento histórico. Aplicá-las à atual problemática dos dados pessoais, por exemplo, somente poderia ser feito com um raciocínio extensivo – o que, por si só, mitigaria os pressupostos de sua existência. Utilizar o termo privacidade parece a opção mais razoável e eficaz." (DONEDA, 2008)

O que Anderson Schreiber (2011) defende vai ao encontro com a doutrina de Stefano Rodatà (2008), no sentido de que a privacidade é vista como o direito de perseguir a própria informação e se opor ao uso de dados pessoais. Nesse sentido, leciona Rodotà:

> De sua tradicional definição como "direito a ser deixado só" passa-se, justamente pela influência da tecnologia dos computadores, àquela que constituirá um constante ponto de referência na discussão: "direito a controlar o uso que os outros façam das informações que me digam respeito". Em fase mais recente surge outro tipo de definição, segundo a qual a privacidade se consubstancia no "direito do indivíduo de escolher aquilo que está disposto a revelar aos outros". (RODOTÀ, 2008, p. 74-75).

Assim, a noção de privacidade deixa o pilar negativo, de abstenção do outro, de uma esfera de não liberdade, passando para a esfera do controle, na qual o indivíduo possui o direito de controlar a própria informação. Tamanha a importância da privacidade no mundo atual, que ela foi um dos três pilares do Marco Civil da Internet, lei brasileira que regulamenta a Internet, sendo considerada um modelo a ser seguido (BRANT, 2014).

O Marco Civil da Internet, lei 12.965/2014, foi promulgado pela então presidente Dilma Rousseff, no dia 23 de abril de 2014, durante o evento denominado de NETmundial na cidade de São Paulo. A referida lei tem como objetivo estabelecer "princípios, garantias, direitos e deveres para o uso da Internet no Brasil" (BRASIL, 2014).

Seu contexto de criação remonta às investigações feitas pelo serviço de inteligência dos Estados Unidos, denunciado por Edward Snowden no ano de 2013 (BRANT, 2014), o que foi tratado como um escândalo mundial. Ficou provado que o serviço de inteligência americana monitorava os e-mails dos governantes de diversos países, entre eles o Brasil. Assim, a então presidente, ao realizar o discurso de abertura da 68ª Assembleia-Geral das Nações Unidas, no dia 24 de setembro de 2013, afirmou que:

> Recentes revelações sobre as atividades de uma rede global de espionagem eletrônica provocaram indignação e repúdio em amplos setores da opinião pública mundial.
> No Brasil, a situação foi ainda mais grave, pois aparecemos como alvo dessa intrusão. Dados pessoais de cidadãos foram indiscriminadamente objeto de interceptação. Informações empresariais – muitas vezes, de alto valor econômico e mesmo estratégico - estiveram na mira da espionagem.
> [...]
> Sem ele – direito à privacidade - não há verdadeira liberdade de expressão e opinião e, portanto, não há efetiva democracia
> [...]
> Por essa razão, o Brasil apresentará propostas para o estabelecimento de um marco civil multilateral para a governança e uso da Internet e de medidas que garantam uma efetiva proteção dos dados que por ela trafegam. (ROUSSEFF, 2016).

A partir desse momento acelerou-se a elaboração do projeto de lei para que fosse lançado no NET mundial, evento internacional de tecnologia que aconteceria em São Paulo no ano seguinte. Evidente que o processo de elaboração do Marco Civil é mais antigo do que o escândalo denunciado por Edward Snowden.

Conforme Cássio Brant (2014), a primeira tentativa de se criar um marco regulatório da Internet teve como objetivo a penalização. Foi um projeto de lei proposto pelo senador Eduardo Azeredo, no ano de 1999. A preocupação era eminentemente penal e não tratava dos direitos e garantias dos usuários, apenas a penalização destes. Iniciou-se então uma série de críticas sobre o projeto, sendo denominado de "AI-5 da Internet" (BRANT, 2014, p. 31).

O referido projeto não foi aprovado. Iniciou-se no ano de 2007 um movimento conjunto pela Secretaria de Assuntos Legislativos do Ministério da Justiça e a Escola de Direito da Fundação Getúlio Vargas do Rio de Janeiro, com o objetivo de se aprovar um marco regulatório de natureza cível para a Internet. Assim nasceu o projeto de lei conhecido como Marco Civil.

Importante salientar que a lei foi a primeira no Brasil a passar por uma discussão online com toda a população, sobre os pontos a

serem legislados, o que se denomina de processo dialético de votação. Em verdade, após a elaboração de um esboço, foi criado um site no qual se disponibilizou tal documento, permitindo que todos os usuários da Internet pudessem ali comentar os dispositivos e inclusive responder aos comentários de outros usuários. Diversas foram as contribuições da sociedade. O pensamento do legislador nesse momento foi coerente. Ora, nada mais justo do que realizar uma consulta pública na Internet para que ela seja regulada, tendo em vista que os usuários poderiam contribuir com a regulamentação para o melhor uso da ferramenta.

O Marco Civil é sustentado por três pilares básicos, a privacidade dos usuários, a liberdade de expressão e a neutralidade da rede. Conforme afirmou Tim Berners-Lee, criador do World Wide Web é "um fantástico exemplo de como os governos podem desempenhar um papel positivo na promoção dos direitos da *web* e mantê-la aberta" (BRANT, 2014, p. 41). Mais ainda, conforme Stefano Rodotà (2016), é necessário que se conceba uma Carta de Direitos da Internet, para que se garanta a proteção que os usuários merecem, tendo em vista as novas situações jurídicas que surgem com a Internet. Nesse sentido, Miguel Reale (2009) leciona que cabe ao Direito respaldar as situações novas que surgem, quer seja com leis, quer seja com costumes, jurisprudência e princípios gerais. Deve haver regulamentação para os atos praticados na rede mundial de computadores. Não se diz que é sempre necessária a criação de uma norma escrita, tendo em vista que com a interpretação das normas existentes consegue-se tutelar os direitos e garantias individuais, conforme se verá no tópico 4. No entanto, algumas situações específicas necessitarão de uma norma posta, como no caso do Direito Penal, que possui o princípio da reserva legal, segundo o qual só há crime se houver previsão em lei.

A aludida lei vem positivar o direito à privacidade, ao qual há referência expressa nos artigos 3º, inciso II, 8º e 11[6]. Ainda, em

[6] Art. 3º A disciplina do uso da Internet no Brasil tem os seguintes princípios:

outras passagens, o Marco Civil normatizou a proteção aos dados pessoais, a inviolabilidade da intimidade e da vida privada e a inviolabilidade e sigilo do fluxo das comunicações pela Internet.

O Direito à Privacidade, na forma como exposta na legislação, remete a um conceito aberto. Assim, na era digital, pode-se afirmar que a proteção dos dados pessoais reflete a proteção da privacidade (PINHEIRO, 2016). Ora, qualquer violação da privacidade do indivíduo na rede será feita através do uso dos seus dados pessoais. Garantir a proteção destes dados é o mesmo que garantir a proteção da privacidade.

3.2 A proteção dos dados pessoais como sendo uma tutela da privacidade

Toda a informação sobre a pessoa é considerada dado pessoal, tais como nome, idade, sexo, renda, entre outras. Tudo o que serve para identificar e distinguir um indivíduo é considerado dado pessoal. Conforme norma do Decreto 8.771, de 11 de maio de 2016, que regulamenta o Marco Civil, dado pessoal é aquele "relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos, quando estes estiverem relacionados a uma pessoa" (BRASIL, 2016).

Dentre essas informações, podem-se distinguir os dados sensíveis, que seriam aquelas informações que revelem origem étnica, preferência religiosa e sexual, ou seja, dados que podem servir de base para uma discriminação. Por sua vez, têm-se os dados não sensíveis, os quais não têm essa propensão.

II - proteção da privacidade;

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. (BRASIL, 2014)

Tamanha a importância da proteção dos dados pessoais, que além de constar expressamente em disposições do Marco Civil, foi publicada a lei geral para a proteção de dados pessoais, Lei nº 13.709, de 14 de agosto de 2018, que ainda não é vigente (BRASIL, 2018).

A lei geral de proteção de dados pessoais – LGPD - tem sua origem em um debate público ocorrido entre 2010 e 2011, e que, através da plataforma "Pensando o Direito"[7], passou por uma elaboração dialética tal qual o Marco Civil, ou seja, a população pôde opinar sobre as disposições legais através da Internet, sugerindo mudanças, criticando ou elogiando as normas (BRASIL, 2017). O projeto contava com 52 artigos, assim divididos:

- Escopo e aplicação – arts. 1º ao 4º
- Dados pessoais, dados anônimos e dados sensíveis – arts. 5º, 12 e 13
- Princípios – art. 6º
- Consentimento – arts. 7º ao 11
- Término do tratamento – arts. 14 e 15
- Direitos do titular – arts. 16 ao 21
- Comunicação, interconexão e uso compartilhado de dados – arts. 22 ao 27
- Transferência Internacional de dados – arts. 28 ao 33
- Responsabilidade dos agentes – arts. 34 ao 41
- Segurança e sigilo de dados pessoais – arts. 42 ao 47
- Boas práticas – arts. 48 e 49
- Como assegurar estes direitos, garantias e deveres? – art. 50
- Disposições Transitórias – arts. 51 e 52 (BRASIL, 2017)

A Lei foi publicada com algumas alterações, sendo que a principal foi o veto presidencial à Autoridade Nacional de Proteção de Dados (ANPD), que constava no artigo 55 da Lei. Segundo o então presidente Michel Temer, "Os dispositivos incorrem em

---

[7] Informação disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/ >. Acesso em: 10 ago. 2016.

inconstitucionalidade do processo legislativo, por afronta ao artigo 61, § 1º, II, 'e', cumulado com o artigo 37, XIX da Constituição."[8]

Contudo, a supressão foi muito criticada. Com a pressão feita pela sociedade, o presidente editou a Medida Provisória 869, de 27 de dezembro de 2018, que alterou a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados. Assim, espera-se que a autoridade regulamente a atividade de provedores que utilizam dados pessoais.

A LGPD repete a definição do decreto regulamentador do Marco Civil, apenas acrescenta a definição de dado sensível, sendo este entendido como aqueles que revelem a origem racial ou étnica, as convicções religiosas, filosóficas ou morais, as opiniões políticas, a filiação a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual, bem como dados genéticos.

Ainda, a lei define uma nova espécie de dado, qual seja, o anônimo, sendo entendido como aqueles relativos a um titular que não possa ser identificado, nem pelo responsável pelo tratamento nem por qualquer outra pessoa, tendo em conta o conjunto de meios suscetíveis de serem razoavelmente utilizados para identificar o referido titular.

A necessidade de proteger os dados pessoais é maior com o avanço da tecnologia. A capacidade de processamento destes dados é maior quando feita por computadores do que quando feito pelo homem. Isso se denomina Big Data.

> O Big Data consiste em um conjunto de soluções tecnológicas capaz de analisar um grande volume de dados a velocidades surpreendentes, de formas que um ser humano não seria capaz. Um exemplo de aplicação prática foi realizado pela Polícia de Chicago, que desenvolveu um programa estilo "Minority Report" para criar uma lista com nomes de pessoas propensas a se envolver

[8] Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Msg/VEP/VEP-451.htm>

> em crimes violentos totalmente baseada em informações coletadas sobre elas na Internet. No entanto, o projeto foi severamente criticado e considerado de certo modo racista. (PINHEIRO, 2016, p. 96)

A partir da década de 70, com o aumento da capacidade de processamento de dados por computadores, surgiram as primeiras iniciativas legislativas de tutela de dados pessoais (DONEDA, 2006). Nessa época, conforme Mayer-Schöenberger (2001, p.228), a preocupação fundamental era a necessidade de uma tutela coletiva, no sentido de impor limites técnicos ao tratamento de dados pessoais.

Um exemplo disso foi a Lei Federal Alemã de Proteção de Dados (Bundesdatenschutzgesetz) e a decisão sobre o Censo Populacional (Volkszählungsurteil) (CHAVES, 2010). A referida lei garantia a proteção dos dados pessoais, e foi promulgada em 1977. Dessa forma, sua aplicação deve-se muito à referida decisão.

O Parlamento Federal Alemão aprovou, em 1982, uma lei convocando um plebiscito populacional a ser realizado no ano seguinte. Haveria um recenciamento da população, no qual os dados recolhidos poderiam ser rastreados até os cidadãos recenseados e serem empregados para outras finalidades que não o recenseamento. Isso gerou uma série de discussões, até que o Tribunal Constitucional Federal decidiu em 25/12/1983 pela inconstitucionalidade parcial do recenseamento (CHAVES, 2010). Em suma, ele poderia ser feito, entretanto, deveria ser respeitada a finalidade da coleta dos dados pessoais.

> A sentença do Tribunal Constitucional Federal anulou parcialmente a lei de censo populacional e forjou a noção de um direito constitucional de autodeterminação informativa, estruturando os fundamentos da proteção de dados alemã (DESIMONE apud CHAVES, 2010).

Conforme Laura Mendes (2014), a preocupação fundamental não é simplesmente com a criação de um banco de dados nacional,

mas com a possibilidade de cruzamento de informações entre os diversos bancos de dados. Em 1980, a Organização para a Cooperação e Desenvolvimento Econômico (OCDE) criou o primeiro instrumento internacional contendo princípios acerca da tutela de dados pessoais. Foram 5 grandes princípios consagrados, quais sejam, da publicidade, exatidão, finalidade, livre acesso e segurança física e lógica (DONEDA, 2006).

Por publicidade se entende que a existência de banco de dados deve ser pública, sem que isso implique a sua divulgação. A exatidão se refere à representação da realidade. A finalidade é a determinação para que o uso do dado coletado seja feito com base no fim informado ao interessado antes da coleta. O livre acesso é a possibilidade de acessar os dados pessoais a qualquer tempo. Por fim, o princípio da segurança física e lógica é o princípio que garante a integridade dos bancos de dados.

> Estes princípios, mesmo que fracionados, condensados ou então adaptados, podem ser identificados em diversas leis, tratados, convenções ou acordos entre privados. Eles são o núcleo das questões com as quais todo ordenamento deve se deparar ao procurar fornecer sua própria solução ao problema da proteção dos dados pessoais. (DONEDA, 2006, p. 217)

O princípio que merece maior atenção é o da finalidade. Anderson Schreiber (2001) o define como princípio da especificação dos propósitos, afirmando que "o propósito da coleta de dados pessoais seja sempre informado ao titular dos dados, vedando-se qualquer utilização para finalidade diversa da declarada" (SCHREIBER, 2011, p. 151).

Nestes termos, não se pode realizar a coleta indiscriminada de dados, garantindo-se, dessa forma, a proteção da privacidade do usuário. O Marco Civil normatiza tal princípio em seu artigo 7º, inciso VIII. A norma afirma que os dados só podem ser coletados para fins que justifiquem a sua coleta, não sejam proibidos pela lei,

e que estejam especificados nos termos de uso e políticas de privacidade.

A mesma proteção é garantida na lei de proteção de dados pessoais. O lei amplia ainda mais a tutela destes dados, ao exigir que o tratamento de dados pessoais seja feito apenas com o consentimento livre, expresso, específico e informado do titular. Todavia, conforme se verá no capítulo 5, esse consentimento dado ao aceitar os termos de uso de algum serviço não é considerado expresso.

Assim sendo, existe a necessidade de se tutelar a privacidade a partir dos dados pessoais, o que, em tese, ensejaria a criação de novos Direitos. Entretanto, no capítulo seguinte será abordado como é possível proteger a privacidade com o sistema de proteção que já existe.

4

Evolução dos conteúdos do direito à privacidade para se alcançar uma proteção eficaz dos direitos da personalidade na internet

O fenômeno jurídico está em constante evolução, tendo em vista que a sociedade muda os valores que clamam tutela. Assim, se diz que o Direito está em constante mutação. Valores que antes não tinham importância, hoje são tutelados e vice-versa, surgindo novos fenômenos que, dada a relevância, mudam o ordenamento jurídico.

A Internet é um destes fenômenos, o qual deu origem ao denominado Direito Digital, ou, como alguns denominam, Direito das Novas Tecnologias, ou, até mesmo, Direito Informático e Cibernético. Fato é que as novas tecnologias mudam a forma de se viver e têm atuação no campo jurídico. Questiona-se a necessidade de se criarem novas leis para a tutela das situações que acontecem dentro da Internet. Mais ainda, há quem discuta a necessidade de criação de um ramo autônomo do Direito, com regras específicas.

No entanto, conforme fundamenta Patrícia Peck Pinheiro (2016), não há necessidade de criação de um ramo autônomo, pois o "Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e instituídos que estão vigentes e são aplicados até hoje [...]" (PINHEIRO, 2016, p. 77). A autora defende a desnecessidade de tutela específica das situações que acontecem na Internet.

Realmente, há um sentimento de ausência de normas quando surgem situações fáticas novas. Entretanto, basta a aplicação do

ordenamento jurídico existente que se consegue a proteção destas situações. Ressalta-se aqui, as situações penais, que, no ordenamento jurídico brasileiro, precedem de norma específica, já que vigora o princípio *"Nullum crimen, nulla poena sine praevia lege",* ou seja, não há crime, nem pena sem lei anterior que os defina. Ressalvadas situações penais[1], é plenamente possível a interpretação das normas existentes para que seja feita a proteção do indivíduo. Assim conclui Patrícia Peck Pinheiro:

> Com a Internet não há diferença: não existe um Direito da Internet, assim como não há um direito televisivo ou um direito radiofônico. Há peculiaridades do veículo que devem ser contempladas pelas várias áreas do Direito, mas não existe a necessidade da criação de um Direito Específico. (PINHEIRO, 2016, p. 78)

Não é necessário criar novos direitos para a proteção do usuário da Internet, basta que se aplique a ordem jurídica existente,

---

[1] Um exemplo de lei penal criada em razão da tecnologia é a Lei 12.737, de 30 de novembro de 2012, conhecida popularmente como lei Carolina Dieckmann, atriz brasileira. A referida atriz, ao levar o seu computador para uma assistência técnica, teve fotos íntimas vazadas na Internet. Assim, foi alterado o Código Penal, tipificando o delito de invasão de dispositivo informático, previsto no artigo 154-A, que assim tipifica: "Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.
§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.
§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
§ 4º Na hipótese do § 3o, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
I - Presidente da República, governadores e prefeitos;
II - Presidente do Supremo Tribunal Federal;
III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

ampliando alguns conceitos através das teorias da interpretação. Evidente que houve uma mudança nos paradigmas hermenêuticos. Observando as teorias da interpretação, vê-se que houve uma crise, entendida como reestruturação dos conceitos, desde a era da codificação.

Na França, com o Código Civil de Napoleão, surgiu a escola da Exegese (FIUZA, 2011). Acompanhando o movimento da codificação, pensava-se que na aplicação da lei, o Juiz recebia o Direito pronto do legislador. Assim, não havia a possibilidade de se ampliarem os conceitos fechados do sistema jurídico. Trabalhava-se com a ideia da dispensa da interpretação, pois *interpretatio cessat in claris* (A interpretação cessa nas coisas claras). Para a Escola da Exegese, a Lei é fonte suficiente de todo o Direito, estando pronta e acabada. Admitiam-se, apenas, as interpretações pelos métodos gramatical e sistemático, por meio dos quais se buscava a vontade do legislador (FIUZA, 2011).

Enquanto na França existia esse movimento, na Alemanha, com o BGB, surgiu a Escola Histórica, tendo como expoente Savigny (FIUZA, 2011). O Direito era visto como uma criação histórica, derivada da vontade do povo, materializado na legislação. "O dever legislativo é o de oferecer suporte aos costumes, a esse Direito vivo, histórico, temporal, a fim de lhe diminuir as incertezas." (FIUZA, 2011, p. 102). Construía-se o Direito com base na vontade da sociedade, razão pela qual, ao interpretar a norma, o intérprete deve pesquisar a vontade histórica do legislador, adequando apenas a sua aplicação.

Ainda no século XIX, surge o pensamento de Auguste Comte, que deu origem ao positivismo. Para ele, o legislador deve buscar regulamentar os fatos sociais de modo que o Estado aplique o Direito sem qualquer conteúdo moral (FIUZA, 2011).

Para Hans Kelsen (2006), o Direito deve ser analisado em si e per si, ou seja, sem qualquer valoração moral, daí decorrendo a sua obra "Teoria Pura do Direito". Para ele, o sistema jurídico deveria ser posto e não admitia interpretação extensiva ou integração, ou

seja, só havia fato jurídico se houvesse norma escrita. Trabalhava-se com a ideia de um sistema fechado, no qual o Direito teria todas as respostas escritas nas leis.

Hans Kelsen (2006) defendia a nulidade de duas normas caso houvesse antinomia entre elas, pois em um sistema que se diz lógico, não pode existir conflito. Contrapondo à Kelsen, Ronald Dworkin defendia que dentro do sistema jurídico, que também era fechado, havia tão somente uma lógica formal de validade, ou seja, havendo duas normas conflitantes, uma delas deixaria de existir ante ao vício de forma (FIUZA, 2011).

Surge então no século XX, a denominada Jurisprudência de valores, na qual se via o Direito como ciência voltada para a conduta ética, ou seja, aplicar valor moral à norma posta. Em um fenômeno pós-positivismo, acredita-se que o Direito só existe de forma concreta "na medida em que compõe interesses" (FIUZA, 2011, p. 107).

A partir de meados do século XX, diversas obras foram publicadas dentro da corrente denominada de Teoria da Argumentação Jurídica. Theodor Viehweg (1979), doutrinador alemão, publicou o livro "Tópica e Jurisprudência", no qual ele retomou o pensamento aristotélico de dialética. Ao aplicar o Direito, o juiz pode se deparar com mais de uma solução possível, devendo optar por uma para se aplicar ao caso. Trabalha-se com a dialética, ou seja, opiniões opostas, há que se ponderar argumentos para ao final se decidir. Assim, Viehweg (1979) define o Direito como jurisprudência, pois acredita que aquele seja a arte de pensar problemas através da tópica, do caso concreto, já que o Direito só assume significado a partir deste. Para Viehweg (1979), cria-se um sistema de normas jurídicas que se renova a partir de cada interpretação. O ordenamento jurídico pode partir de um sistema fechado, mas este é modificado através das interpretações dadas em casos concretos. A interpretação deve ter como ponto de partida a realidade fática, buscando a melhor solução dentro do ordenamento posto e não o contrário.

Esse modelo interpretativo/argumentativo não necessita que se abandone o sistema jurídico. O ordenamento deve ser composto por normas e ser visto como completo em si. "O que deve abandonar, definitivamente, é a ideia de sistema fechado" (FIUZA, 2011, p. 100).

Assim, não há a necessidade de se criarem novos institutos para se tutelar a privacidade hoje. O que é necessário é a ampliação dos conceitos, fazendo com que novas situações sejam protegidas. Portanto, a ideia da autodeterminação do indivíduo, sendo entendida como o controle das informações pessoais e, consequentemente, como proteção da privacidade, não necessita de criação de nova lei.

A autodeterminação é objeto de ampliação do direito da privacidade. Trabalha-se com a doutrina do *Self-determination*, que é a possibilidade do usuário controlar suas informações.

> A partir da reflexão sobre a tutela das informações pessoais no ambiente virtual, recentemente, uma nova expressão vem aparecendo nos estudos de pesquisadores desta temática: a "autodeterminação informativa", que ora é colocado como um direito, ora como um princípio, mas sem perder a sua definição maior, que se constitui no poder do indivíduo determinar e controlar a utilização de seus dados pessoais. (MENDONÇA, 2017)

A autodeterminação não necessita de um novo direito de privacidade, quer seja no âmbito privado, quer seja no público. Isso decorre do fato de existir uma cláusula geral dos direitos da personalidade, bem como rol aberto de proteção dos direitos fundamentais.

> De maneira um pouco diferente se posiciona Ana Maria Navarro (2012): a autora afirma, com propriedade, que o direito à autodeterminação informativa poderia já ser considerado como fundamental no ordenamento jurídico brasileiro e, portanto, poderia ser declarada pelos juízes e tribunais do país ou pelas instituições públicas brasileiras, em suas atividades deliberativas, por força de uma interpretação constitucional construtiva com

> base no art. 5º, parágrafo 2º da Constituição de 1988. Isto porque, segundo ela, a não declaração expressa de um direito fundamental não implica na sua não existência, e a própria Constituição Federal Brasileira consagra o seu art. 5º como uma cláusula aberta, podendo ser considerados como fundamentais todos aqueles direitos que se extraem das "penumbras" de outras garantias constitucionais expressas, interpretadas em conjunto. Assim, ainda que não defenda claramente a colocação expressa da autodeterminação informativa no rol de direitos fundamentais, a autora corrobora o entendimento dos autores já citados no que tange à importância indiscutível de considera-la como fundamental, para, a partir de então, construir uma legislação infraconstitucional eficiente na tutela dos dados pessoas dos cidadãos. (MENDONÇA, 2017)

O que a autora defende é o conceito aberto dos direitos da personalidade e dos direitos fundamentais. Parte-se do pressuposto que o bem jurídico tutelado é o indivíduo e que os seus valores mudam ao longo do tempo. Assim, situações antes que não eram imagináveis, como a exposição que se tem nas redes sociais, são tuteladas por estes conceitos abertos. Portanto, é necessário tão somente novas interpretações do direito de privacidade.

Quando afirma-se pela existência da necessidade de se tutelar a privacidade na Internet, dando o poder de controle aos usuários sobre os seus dados pessoais, não se defende a criação de novos direitos. Em verdade, trabalha-se apenas com a extensão dos conceitos já existentes, já que os mecanismos atuais são capazes de proteger a privacidade na Internet.

Não significa que existem mecanismos suficientes para garantir de maneira fática essa proteção. A privacidade pode ser tutelada com as leis existentes, mas, na prática, essa proteção pode não ser possível por ausência de ferramentas não jurídicas a fim de viabilizá-la.

O ordenamento jurídico garante a tutela do usuário, mas faltam mecanismos para se operacionalizar. A promulgação do Marco Civil da Internet e até mesmo a lei de proteção de dados

pessoais, tão somente ampliam a interpretação da cláusula geral dos direitos da personalidade que garante a proteção da privacidade.

Existe base para a proteção da privacidade da Internet, mesmo não existindo, ainda, uma norma específica para a tutela dos dados pessoais. A lei de proteção de dados pessoais, quando promulgada, não inovará a ordem jurídica, mas criará meios de se ampliar a tutela já existente no ordenamento jurídico.

Dentre as inovações que a Internet traz à privacidade, pode-se afirmar que existem os seguintes direitos: Direito de autodeterminação; Direito de exclusão; Direito ao esquecimento; Direito de acesso e modificação; e Direito de não ser conhecido.

Novamente, não se trata de uma criação jurídica que enseja a tutela por normas específicas, filia-se ao entendimento de que a interpretação pode suprir a falta de normas. Nesse sentido, a nomenclatura é uma criação a partir de um esforço teórico, que não importa em criação de novos Direitos.

Até mesmo porque a proteção da privacidade como originalmente pensada, ou seja, o direito de ser deixado só, não acabou. Ainda existe esse direito na Internet. Ora, um usuário pode exigir que não falem sobre ele ou que respeitem o âmbito de seu perfil em uma rede social. Assim, novas situações não excluem as antigas, mas apenas harmonizam a interpretação jurídica.

4.1 Direito de autodeterminação

Como visto, a privacidade atualmente remonta ao conceito de autodeterminação. Tutelar este direito é dar ao usuário o poder de controle sobre os seus dados pessoais, garantindo que ele possa se abster do uso de suas informações em determinadas maneiras.

> As teorias atuais de "privacidade como controle" enfatizam o papel da escolha e a autodeterminação individual em relação a outros valores. A este respeito, estas teorias podem ser descritas como gerenciamento de informações onde o controle é conseguido através do gerenciamento subjetivo e expressão de preferências

> pessoais. Assim, os indivíduos são considerados capazes de determinar o que é bom para si mesmos e, consequentemente, decidir reter ou divulgar mais ou menos informações pessoais. O controle é então conceituado como um processo individual, dinâmico e flexível, pelo qual as pessoas podem tornar-se acessíveis aos outros ou se fechar. Como Birnhack diz, a privacidade como controle é "...a visão de que um direito à privacidade é o controle que um ser humano autônomo deve ter sobre sua informação pessoal, em relação à sua coleta, processamento e outros usos, incluindo transferências subsequentes". Nesta visão, o controle toma a forma do direito dos indivíduos de saber quais informações sobre si mesmas são coletadas; Para determinar quais informações são disponibilizadas a terceiros; e para acessar e potencialmente corrigir seus dados pessoais. (LAZARO, LE MÉTAYER, 2015, tradução nossa)[2]

Christophe Lazaro e Daniel Le Métayer (2015) definem, então, que o direito de autodeterminação possui três aspectos, quais sejam, o da coleta, uso e correção. O usuário deve saber quais informações sobre si são coletadas. Ainda, é necessário que ele tenha conhecimento pleno sobre o uso destas, sendo informado a ele, inclusive, quais são disponibilizadas a terceiros. Por fim, é preciso que se garanta a possibilidade de correção de seus dados pessoais. Dessa maneira se terá a autodeterminação informativa, pois há, correlato, um dever de informar. Ora, sendo o usuário titular dos dados, ele deve ser informado sobre o uso deste.

---

[2] Tradução de: "Current "privacy as control" theories emphasize the role of choice and individual self-determination over other values. In this regard, they can be described as information management theories where control is achieved through the subjective management and expression of personal preferences.18 Accordingly, individuals are deemed to be able to determine what is good for themselves and consequently to decide to withhold or disclose more or less personal information.19 Control is then conceptualized as an individual, dynamic and flexible process whereby people can either make themselves accessible to others or close themselves. As M. Birnhack puts it, privacy as control is "...the view that a right to privacy is the control an autonomous human being should have over his or her personal information, regarding its collection, processing and further uses, including onward transfers."20 In this view, control takes the shape of the right of individuals to know what information about themselves is collected; to determine what information is made available to third parties; and to access and potentially correct their personal data." (**Control over personal data**: True remedy or fairy tale? Christophe Lazaro e Daniel Le Métayer)

Na Europa, a General Data Protection Regulation[3], conhecida como a reforma da diretiva de proteção de dados pessoais, evidencia ainda mais a necessidade de um direito de autodeterminação informativa. Nela, dentre outros direitos, ficou definido que o *Take-or-leave-it consent*, segundo o qual o consentimento obrigatório para o uso de algum serviço não é necessariamente válido para fins de processamento de dados pessoais, sendo necessário um consentimento informado do usuário.

Em verdade, na maioria das vezes, para se utilizar um serviço é necessário o consentimento para que sejam processados os dados pessoais. Então, na Europa se definiu que o processamento de dados pessoais é distinto da coleta e um não implica o outro. É possível a coleta para que se use um determinado serviço, mas essa coleta não necessariamente implica a possibilidade de tratamento destes dados. Dessa forma, tutela-se ainda mais a privacidade dos usuários.

Além de um direito em vida, a autodeterminação é também considerada após a morte do usuário. Não há uma legislação extensa sobre o assunto, nem uma doutrina uniforme. Porém, há que se ressaltar a necessidade de se tutelar o interesse do usuário até mesmo após a sua morte. Sobre isso, Bruno Torquato Zampier Lacerda (2016) conclui que deve ser concedida ao indivíduo a possibilidade de sua vontade, em vida, regular o futuro de suas informações pessoais após a sua morte. Em linha de pensamento similar, Juliana Evangelista de Almeida e Daniel Evangelista Vasconcelos Almeida (2013) defendem a necessidade de um testamento digital para que se definam os destinos dos ativos digitais.

> Com o advento da Internet é possível que alguns arquivos da pessoa, mesmo após a sua morte, sobrevivam e fiquem disponíveis a todos. Nos últimos anos o uso da Internet se intensificou. Em decorrência disso aumentou o número de arquivos digitais disponíveis para acesso. Como dito, tais arquivos possuem

[3] Disponível em <http://www.eugdpr.org/the-regulation.html>. Acesso em 10 ago. 2016.

> relevância jurídica e é interessante que o titular desses arquivos manifeste o seu interesse sobre o futuro de sua produção digital. O que se quer dizer é que é relevante se fazer um testamento digital. Os arquivos digitais após a morte do indivíduo são situações jurídicas a serem tuteladas pelo ordenamento, dado os centros de interesses que podem compor, como, por exemplo, direitos autorais, intimidade, privacidade, honra, entre outros. (ALMEIDA, J.; ALMEIDA, D., 2013)

A autodeterminação pode ser considerada a nova base para a privacidade na Internet, sendo o caminho pelo qual se consegue atribuir ao usuário o direito de controle. Como dito, não significa a criação de um novo direito, mas apenas a interpretação dos já existentes. Tanto a Diretiva Europeia de Proteção de Dados Pessoais, quanto a lei de dados pessoais no ordenamento jurídico brasileiro, trazem novas interpretações aos direitos já existentes, adequando o conteúdo destes à nova realidade fática, que se altera com as novas tecnologias.

Veja que a lei geral de proteção de dados pessoais consagrou tal direito, ao dispor que o mesmo é um fundamento para a proteção da pessoa no artigo 2º, inciso II. Mais que isso, é um requisito para que se tenha a coleta de dados pessoais, em conformidade com o artigo 7º, inciso I da lei. Por fim, conforme o artigo 8º, o consentimento deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. Há, pois, uma clara preocupação com o direito da autodeterminação informativa, respeitando, assim, a privacidade.

4.2 Direito de exclusão

Outra interpretação dada é o direito de exclusão, no qual qualquer informação do usuário é dele, atribuindo-lhe o direito de excluí-la. Esse direito é assegurado no inciso X do artigo 7º do Marco Civil da Internet. No dispositivo normativo é determinada a exclusão definitiva dos dados pessoais do usuário quando do término da

relação entre as partes, caso haja requerimento. Entretanto, este direito tem uma ressalva.

Pelo Marco Civil da Internet, os provedores de aplicação devem guardar as informações dos usuários pelo prazo de seis meses, conforme artigo 15 do Marco Civil da Internet. Ainda, conforme o artigo 13 do mesmo dispositivo normativo, os provedores de conexão devem guardar informações sobre o acesso pelo prazo de um ano.

Regulamentando a matéria, o Decreto 8.771 de 2016, determinou a exclusão dos dados pessoais tão logo decorrido estes prazos ou cessada a finalidade de seu uso[4]. Portanto, a informação é do usuário e não deve permanecer com os provedores.

Ocorre que a realidade fática não é essa, já que empresas lucram com as informações pessoais. Atualmente, é comum a prática de *mailing*, ou seja, o marketing direcionado pelo perfil do usuário (HIRATA, 2015). Ocorre que estas informações são vendidas por empresas (ATHENIENSE, 2017). Perceba que o valor de uma companhia pode ser determinado pelo seu potencial de dados coletados.

Veja que o Facebook Inc. comprou o WhatsApp no ano de 2014, pelo valor de vinte e dois bilhões de dólares. Ocorre que este último, naquele ano, gerou um faturamento de tão somente dois milhões e setecentos mil dólares, valor ínfimo se comparado com o de compra. Entretanto, o faturamento do Facebook, após a compra do App subiu em mais 59%, o que evidencia que a aquisição se deu em razão da possibilidade de uso de dados pessoais para a ampliação das receitas da rede social (PREJUÍZO, 2014). Daí decorre o direito

---

[4] Art. 13. Os provedores de conexão e de aplicações devem, na guarda, armazenamento e tratamento de dados pessoais e comunicações privadas, observar as seguintes diretrizes sobre padrões de segurança:
§ 2º Tendo em vista o disposto nos incisos VII a X do caput do art. 7º da Lei nº 12.965, de 2014, os provedores de conexão e aplicações devem reter a menor quantidade possível de dados pessoais, comunicações privadas e registros de conexão e acesso a aplicações, os quais deverão ser excluídos:
I - tão logo atingida a finalidade de seu uso; ou
II - se encerrado o prazo determinado por obrigação legal.

de exclusão, assegurando ao usuário a possibilidade de ser excluído da Internet. A lei geral de proteção de dados pessoais previu a possibilidade de exclusão de dados a requerimento do titular, conforme artigo 18, inciso VI.

4.3 Direito ao esquecimento

O direito ao esquecimento[5] tem origem no caso Soldatenmord von Lebach (SARLET, 2016). Na Alemanha, no ano de 1969, quatro soldados foram assassinados, sendo três réus condenados pelo crime, dois à prisão perpétua e outro à prisão de 06 anos. Este último, ao sair da prisão, tomou conhecimento que uma emissora de televisão faria uma reportagem especial sobre o crime, mostrando inclusive fotos dos criminosos. Assim, ele ajuizou uma ação pleiteando que não fosse exibido o programa. A corte alemã decidiu por impedir a exibição do programa, sob o fundamento de que não pode um fato se tornar um verdadeiro martírio na vida de uma pessoa. Há sim o direito de se noticiar fatos ocorridos no passado, mas desde que isso seja relevante. O direito de ser esquecido é de tamanha importância, que a diretiva da União Europeia, em sua última reforma, colocou-o como um direito de todos.

No ordenamento jurídico brasileiro tem-se o enunciado 531 do STJ, que dispõe que a tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento. Evidente que já se tem uma base para o direito ao esquecimento. Por mais que qualquer informação na rede seja perene, é dado aos usuários o direito de serem literalmente esquecidos pela rede, através da exclusão de seus dados.

---

[5] Em verdade, a corrente mais aceita no direito Europeu trabalha com o Direito de ser apagado/deletado (*right to be erase* ou *right to be delete*). O argumento é de que o esquecimento é subjetivo, não se pode impor que as pessoas esqueçam um fato, mas pode-se impor que um motor de busca apague um resultado. Sobre o tema, ver: BERNAL, P.A., 'A Right to Delete?', **European Journal of Law and Technology**, Vol. 2, No.2, 2011. Disponível em <http://ejlt.org/article/view/75/144>. Acesso em: 05 dez. 2016

Há uma diferença entre o direito ao esquecimento e o direito de exclusão. O último se refere à possibilidade de o usuário deletar os seus dados sob qualquer pretexto. Por sua vez, o direito ao esquecimento tem por base a possibilidade de o usuário requerer que dados sobre ele, pertencentes a terceiros, sejam excluídos. Assim, um se refere a dados próprios e o outro a dados de terceiros.

A grande dificuldade na era digital é a facilidade de como se copia um arquivo. Com apenas alguns cliques, é possível fazer uma cópia perfeita do arquivo original, o que torna uma árdua tarefa esquecer alguém na rede mundial de computadores.

Ante essa possibilidade de massificação das informações, na Europa já se defende o direito à desindexação. Ao invés de se determinar a exclusão do arquivo em si, se impõe uma obrigação aos motores de buscas, tais como Google e Yahoo, para que não mais exibam resultados de pesquisas.

O direito à desindexação surgiu no julgamento do caso da Agência Espanhola de Proteção de Dados, representando o cidadão espanhol Mario González, *versus* Google, em 2014 (O TRIBUNAL, 2015). Mario González pedia que o buscador Google removesse os resultados da busca de seu nome que remetia a uma antiga reportagem de 1998, que anunciava o leilão de sua casa por motivos de dívidas tributárias. No fim, o Google foi considerado como um controlador dos dados pessoais, pois realizava a indexação para os resultados, sendo julgado procedente o pedido.

Assim, pode-se requerer que os sites buscadores não mais associem o nome do usuário ao conteúdo (O TRIBUNAL, 2015). A Corte Europeia proferiu "sentença favorável a Mario González, advogado espanhol que exigia que o site de buscas Google apagasse o registro de seus dados pessoais, bem como os links para notícias do jornal La Vanguardia que continham aviso do Ministério do Trabalho daquele país sobre um leilão de imóveis realizado em 1998, para sanar dívidas de González." (O TRIBUNAL, 2015)

No Brasil, inicia-se um entendimento acerca da possibilidade de se determinar a desindexação do usuário. O caso se refere à uma

ação ajuizada por um Desembargador que pretendia que fosse retirado do Google resultados de pesquisa que ligassem seu nome à notícias que relatavam envolvimento do autor com improbidade. O pedido foi aceito, determinando sua desindexação, sendo assim ementado:

> EMENTA. CIVIL E PROCESSUAL CIVIL. AÇÃO DE OBRIGAÇÃO DE FAZER. PRETENSÃO DE EXCLUSÃO DA INTERNET DAS URL´S (LINKS) DE NOTAS QUE DESABONAM A CONDUTA DO AUTOR. NOTICIAS COM BASE EM PROCEDIMENTOS ADMINISTRATIVOS JULGADOS, SEM QUALQUER PUNIÇÃO AO INVESTIGADO E COM DECISÕES TRANSITADAS EM JULGADO. PEDIDO JULGADO IMPROCEDENTE NA PRIMEIRA INSTÂNCIA. APELO. JULGAMENTO ESTENDIDO (ART. 942 DO CPC). PROVIMENTO DO RECURSO. (4X1). SENTENÇA REFORMADA. AÇÃO PROCEDENTE. DECISÃO POR MAIORIA.
>
> 1. Não justifica a permanência por tempo indeterminado de notícias desabonadores à conduta do autor em razão de procedimentos administrativos funcionais, todos julgados, arquivados e com transito em julgado e, via dos quais não foi aplicada qualquer pena ao indiciado
>
> 3. A Jurisprudência pátria, por sua vez, tem assentado que "o princípio da dignidade da pessoa humana deve prevalecer em relação ao direito à informação e à liberdade de imprensa, de modo que a exclusão das informações consideradas ofensivas à honra e à imagem da agravada da ferramenta de buscas Google é medida que se impõe", mormente quando nada se apurou contra a conduta do investigado e cujos processos foram instruídos, julgados e arquivados.
>
> 4. O STJ, em recente julgado (datado de 19/03/18), reconheceu a possibilidade de se "[...] determinar que os provedores de busca retirem determinados conteúdos expressamente indicados pelos localizadores únicos (URL´S) dos resultados das buscas efetuadas pelos usuários"
>
> 5. Apelo provido para, reformando a sentença, julgar procedente o pedido autoral a fim de determinar que a ré/apelada (Google) se abstenha de exibir, nas pesquisas realizadas no seu buscador de internet, as notícias constantes dos links discriminados nos autos.
>
> 6. Decisão por maioria (4 x1). (TJPE. Apelação Cível 0040589-41.2016.8.17.2001, julgada pela 5ª Câmara Cível em 10/10/2018)

Ao se questionar o direito ao esquecimento, é necessário se trabalhar com o *Streisand effect*[6]. Tal fenômeno descreve a situação na qual, ao se tentar remover uma informação, o efeito é alastrar ainda mais esta, como uma espécie de publicidade negativa. Mike Masnick originalmente criou o termo em referência ao caso da atriz e cantora estadunidense Barbra Streisand que, no ano de 2003, processou o fotógrafo Kenneth Adelman e o website Pictopia.com, pleiteando que uma foto aérea de sua mansão fosse removida da coleção de 12.000 fotos da costa da Califórnia disponíveis no site. O argumento foi a sua privacidade que estaria sendo violada, entretanto, após a ação, a foto se tornou popular na Internet, com mais de 420.000 acessos ao site no mês seguinte.

Enquanto alguns usuários querem ser esquecidos pela Internet, outros querem ser lembrados, ou seja, indexados nos buscadores. O tema surgiu a partir dos casos dos sites Search King e Kinderstart, que nos anos de 2003 e 2006, respectivamente, ajuizaram ações contra o Google por terem seus nomes rebaixados nos resultados do mecanismo de buscas da companhia (LUDMER, 2017). Nos dois casos, o julgamento foi improcedente ao argumento de que a ordem de aparição nas buscas é estabelecida com base na liberdade de expressão.

Outro caso foi o da E-Ventures, companhia de SEO – "Search Engine Optimization" (conhecido em português como Otimização de Buscas), que ajuizou uma ação contra o Google por não aparecer mais nos resultados de buscas. O juiz julgou improcedente a ação, baseando-se mais uma vez no direito da livre expressão, depois de concluir que a E-Ventures violou a política de spam do Google (FLORIDA, 2017).

Nesse contexto, na Europa a Google foi multada em aproximadamente 9 bilhões de reais por "manipular os resultados do seu mecanismo de busca em favor dos produtos de seus parceiros

---

[6] Informação disponível em: <https://en.wikipedia.org/wiki/Streisand_effect>. Acesso em: 10 out. 2016.

na plataforma Google Shopping" (LUDMER, 2017). No caso, decidiu-se pela violação da neutralidade da rede, já que a companhia estava favorecendo parceiros comerciais.

A neutralidade da rede, um dos três pilares do Marco Civil da Internet, é o princípio que determina que todas as informações devem ser tratadas de igual maneira pela rede, não havendo qualquer tipo de distinção. O referido princípio está normatizado no artigo 9º do MCI, que dispõe que o "responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação." (BRASIL, 2017). Dessa forma, não pode um motor de buscas realizar a distinção do conteúdo a ser processado. Afirma-se que existe a neutralidade das buscas, como sendo uma derivação da neutralidade da rede (ODLYZKO, 2009).

Pode-se definir como um dos desdobramentos dos direitos da personalidade o direito de o usuário ser lembrado pelos motores de buscas, quer seja pessoa física ou jurídica. Há uma necessidade, em alguns casos, de se aparecer nos motores de buscas, razão pela qual pode-se considerar essa indexação como sendo um desdobramento do direito da personalidade do usuário.

4.4 Direito de acesso e modificação

No Brasil, os dados pessoais são atualmente tutelados por algumas leis esparsas, como, por exemplo, o Código de Defesa do Consumidor, que em seu artigo 43 normatiza sobre o direito que o consumidor tem de acessar os cadastros positivos sobre ele. O Código Civil de 2002, em seu artigo 21, traz uma proteção genérica à privacidade, o que, como visto, estende-se aos dados pessoais. Destacam-se, ainda, o Marco Civil da Internet e seu decreto regulamentador, a Lei do cadastro positivo (12414/11), Lei de acesso à informação pública (12532/11), Serviço de Atendimento ao Cidadão (dec. 5623/08), Decreto do cadastro único de programas

sociais do Governo Federal (dec. 6135/07) e o Decreto censo anual da educação (dec. 6425/08). Todas essas normas não possuem caráter amplo e genérico sobre o assunto.

Em suma, há no ordenamento jurídico brasileiro, determinação que garante ao usuário acesso às suas informações pessoais. Conforme artigo 43 do Código de Defesa do Consumidor - CDC, "O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes." (BRASIL, 1990). Tal disposição garante amplamente o direito de os usuários acessarem suas informações pessoais que constam nos provedores, já que se trata de uma relação de consumo.

A relação de consumo é aquela entre um fornecedor e um consumidor, ambos definidos nos artigos 3º e 2º do CDC, respectivamente. Em se tratando de um serviço na Internet, é evidente que o provedor é um fornecedor e o usuário um consumidor. Ante a essa relação consumerista, é possível se tutelar o direito de acesso em vista desta norma regulamentadora.

No mesmo sentido, a nova diretiva europeia de proteção de dados pessoais determina que os titulares de dados terão mais informações sobre como seus dados são processados. Ainda, a lei de proteção aos dados pessoais prevê em seu artigo 18, inciso II, o princípio do livre acesso, segundo o qual o titular tem a possibilidade de consulta gratuita aos seus dados pessoais, bem como de suas modalidades de tratamento.

Ocorre que existe, no mercado de consumo, uma prática denominada de *score* de crédito, que consiste em uma pontuação do indivíduo, feita com base em seus dados pessoais, que determinam o risco financeiro de um eventual contrato. Trata-se de um banco de dados positivo, previsto pelo CDC e na Lei 12.414/11, regulamentada pelo decreto 7.829/12. Sua finalidade é subsidiar a concessão de crédito, venda a prazo ou outra transação que importar risco financeiro. Assim, desde que atendidos os requisitos legais, a partir

do histórico de crédito, formado por dados pessoais, será mensurado e/ou concedido crédito ao consumidor. Para a formação do banco de dados, faz-se necessária a autorização prévia do potencial cadastrado por meio de consentimento informado através de documento próprio ou em cláusula contratual apartada, após, a anotação de qualquer dado não depende de autorização[7].

O acesso ao banco de dados do escore só será possível por aqueles que mantiverem ou pretenderem manter relação comercial ou creditícia com o cadastrado. Através da coleta desses dados, o gestor deste fornecerá aos consulentes um escore de pontuação do cadastrado, como forma de apoio na tomada de decisão na concessão do crédito, assim, quanto maior a pontuação, menor o risco na concessão do crédito e vice-versa.

Em novembro de 2014, através do Recurso Especial Nº 1.419.697 – RS, o relator Ministro Paulo de Tarso Sanseverino definiu escore de crédito como um sistema de pontuação de consumidores para fins de concessão de crédito. Essa pontuação é feita em uma escala de 0 a 1.000 pontos, e, quanto mais próximo do máximo, menor o risco de concessão de crédito. Para a realização dessa pontuação são utilizados dados dos consumidores, tais como adimplemento das obrigações, idade, sexo, estado civil, renda, número de dependentes, endereço – dados esses disponíveis, em muitos casos, na Internet. Na análise do caso, um determinado consumidor, em razão da pontuação obtida, mesmo não tendo inscrição negativa em cadastro de proteção de crédito, teve restringido o acesso ao crédito. Assim, requereu o cancelamento dos seus dados pessoais, bem como, indenização por dano moral *in re ipsa* pela restrição de crédito.

O Ministro Relator argumentou que o uso de dados pessoais sempre existiu, mesmo antes do advento da Internet. Entretanto,

---

[7] O STJ através do Recurso Especial Nº 1.419.697 entendeu não ser necessária a autorização do consumidor para a realização do escore de crédito, por não se tratar, esse serviço de banco de dados positivos, mas sim de uma classificação com a finalidade de se mensurar risco na concessão de crédito, ou seja, modelo estatístico.

com esta, há uma massificação no tratamento e processamento de informações. Assim, é possível o uso de dados para a criação de um *score* de crédito, desde que atendido os parâmetros legais, em especial o CDC e a Lei 12.414/11, sendo os critérios para a pontuação claros, objetivos e transparentes. Deve ser garantido ao consumidor o acesso a esses dados e aos critérios para a pontuação. Todavia, há aqui um conflito entre o segredo industrial e o direito de acesso. Isso porque essas informações podem revelar a forma e o algoritmo utilizado para a categorização do indivíduo, o que pode significar o maior patrimônio de uma companhia. Decidiu, ainda, o Relator, pela desnecessidade do consentimento prévio para o *score* de crédito, tendo em vista que se trata de uma metodologia de cálculo e não de um banco de dados positivo. Argumentou que são modelos estatísticos de análises que dispensam a autorização do consumidor.

No caso específico, o STJ entendeu que o fato de ser atribuída ao consumidor uma nota insatisfatória, não gera, por si, indenização por dano moral, enseja somente a retificação, caso não esteja de acordo com a realidade. Assim, garante-se ao consumidor a possibilidade de alterar o seu *score* de crédito apenas se houver erro neste.

Sedimentando a possiblidade de se manter um escore de crédito, o Superior Tribunal de Justiça - STJ - no dia 19 de outubro de 2015, publicou a súmula 550 que preceitua que "A utilização de escore de crédito, método estatístico de avaliação de risco que não constitui banco de dados, dispensa o consentimento do consumidor, que terá o direito de solicitar esclarecimentos sobre as informações pessoais valoradas e as fontes dos dados considerados no respectivo cálculo.". O que se observa é uma tendência em se permitir a categorização do ser através de um algoritmo. Evidente que o escore de crédito possui diversos benefícios, entretanto não se pode admitir uma redução da pessoalidade do ser através de um dado estatístico[8].

---

[8] Fala-se em Ditadura do Algoritmo, ou seja, a sua categorização por dados coletados que não podem ser modificados. Considera-se que "a redução do indivíduo a uma mera estatística, o que se denomina de escore de crédito, pode lhe retirar atributos inatos da pessoalidade. Ora, não se pode afirmar que

Uma consequência lógica do direito de acesso é a possibilidade de modificação destes dados pessoais. Isso é garantido no ordenamento jurídico brasileiro com o *habeas data*, remédio constitucional que possibilita o acesso e a modificação de dados pessoais constantes em órgão públicos. Conforme artigo 5º, inciso LXXII, será concedido *habeas data* 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" e para "a retificação de dados, quando não se prefira fazê-lo por processo sigiloso, judicial ou administrativo".

Tal remédio possibilita não só o acesso, mas também a modificação dos dados, desde que armazenados em entidades governamentais ou de caráter público. Contudo, não se tem um instrumento para a proteção deste direito em um âmbito privado. Não é atribuída ao indivíduo a possibilidade de retificar informações constantes em banco de dados particulares. Assim, os tribunais têm ampliado o conceito de banco de dados de caráter público, veja-se o entendimento do Tribunal de Justiça do Estado de Minas Gerais:

> EMENTA: HABEAS DATA. SERASA. SPC. ENTIDADES PRIVADAS. BANCOS DE DADOS DE CARÁTER PÚBLICO. LEGITIMIDADE PASSIVA AD CAUSAM.
> O habeas data é garantia (ação) constitucional, de natureza civil, de rito especial, isento de despesas judiciais e que tem como bem juridicamente tutelado a proteção da intimidade e da privacidade do autor, no que diz respeito a informações que sobre ele possam estar contidas em bancos de dados de caráter público, sejam estes integrantes de quaisquer dos Poderes (órgãos) do Estado ou da Administração Pública Indireta, ou mesmo pertencentes à iniciativa privada.
> O caráter público não está no fato do banco de dados integrar ou não o aparato estatal, mas na possibilidade de ser ele um depositário de informações generalizadas ou específicas sobre as pessoas físicas ou jurídicas, colhidas de terceiros e transmitidas

---

um indivíduo possa ter seus direitos reduzidos somente em razão do círculo social que este frequenta." (ALMEIDA,J.; ALMEIDA, D., 2016)

> também a terceiros, sem o conhecimento e/ou consentimento da pessoa cuja informação diga respeito.
> Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público (art. 43, § 4º, Código de Defesa do Consumidor). (MINAS GERAIS. Tribunal de Justiça, 2000)

No caso, definiu-se que o caráter público decorre do fato de os dados serem colhidos de terceiros e transmitidos sem autorização do titular, razão pela qual o SPC – Serviço de Proteção ao Crédito – e o SERASA - Centralização de Serviços dos Bancos, ambas pessoas jurídicas de direito privado, são partes legítimas para figurarem no polo passivo do Habeas Data. Assim, foi anulada a sentença que reconheceu a ilegitimidade passiva, determinando o processamento do feito no juízo de origem. No mesmo sentido é o parágrafo único do artigo 1º da Lei nº 9.507/97, que regula o direito de acesso a informações e disciplina o rito processual do habeas data. Conforme o dispositivo normativo,

> Parágrafo único. Considera-se de caráter público todo registro ou banco de dados contendo informações que sejam ou que possam ser transmitidas a terceiros ou que não sejam de uso privativo do órgão ou entidade produtora ou depositária das informações. (BRASIL, 1997)

É possível que o Habeas Data seja o remédio para assegurar o acesso e modificação de dados constantes em entidades privadas, sendo necessário que a informação seja transmitida a terceiros e que o uso não seja privativo. Assim, é possível se estender a interpretação da norma e atribuir à determinadas plataformas a legitimidade passiva em se tratando deste remédio constitucional. Entretanto, há a necessidade de se garantir o acesso mesmo em plataformas que não tenham o caráter público acima descrito. É preciso que se tutele a privacidade do usuário, possibilitando o acesso e consequente modificação de suas informações constantes em plataformas, mesmo que de caráter privado (DONEDA, 2009).

Com a aprovação da lei geral de dados pessoais, o direito de acesso ganha força. É expresso o direito de acesso à informações que o controlador eventualmente possuir. Indo além, é direito do titular ter acesso à revisão de decisões automatizadas com base em seus dados pessoais. Veja:

> Art. 20. O titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil pessoal, profissional, de consumo e de crédito ou os aspectos de sua personalidade.
> § 1º O controlador deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, observados os segredos comercial e industrial.
> § 2º Em caso de não oferecimento de informações de que trata o § 1º deste artigo baseado na observância de segredo comercial e industrial, a autoridade nacional poderá realizar auditoria para verificação de aspectos discriminatórios em tratamento automatizado de dados pessoais. (BRASIL, 2018)

Portanto, o titular de dados pessoais possui uma garantia de que suas informações serão corretamente utilizadas. Mais ainda, o titular pode solicitar a qualquer tempo correção de dados incompletos, inexatos ou desatualizados, bem como a portabilidade dos dados a outro fornecedor de serviço ou produto, mediante requisição expressa e observados os segredos comercial e industrial, de acordo com a regulamentação do órgão controlador. Assim, o titular torna-se o protagonista da determinação do uso de suas informações.

4.5 Direito de não ser conhecido

Outro desdobramento da privacidade é o direito de não ser conhecido, uma vertente da autodeterminação informativa. Um indivíduo tem o poder de decidir se faz ou não parte de uma rede

social, ou seja, se fornece seus dados pessoais. O MCI prevê isso no artigo 7º inciso IX, ao normatizar que é assegurado aos usuários o direito de "consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais". Interpretando tal dispositivo, tem-se a necessidade de uma política de privacidade e um aceite do usuário para que se faça o uso dessas informações.

No mesmo sentido, o Marco Civil em seu artigo 7º, inciso VII, normatiza o direito dos usuários ao não fornecimento a terceiros de seus dados pessoais, exceto se houver consentimento livre, expresso e informado. Esse consentimento, tratando-se de um contrato de adesão, é relativo. Isso porque, como se verá no próximo capítulo, o usuário, na maioria das vezes, sequer lê o contrato com o qual está aderindo. O Facebook assim dispõe em seus termos de uso:

> Quando você usa aplicativos, sites ou outros serviços de terceiros que utilizam ou são integrados aos nossos Serviços, eles podem receber informações sobre suas publicações ou compartilhamentos. Por exemplo, quando você joga com seus amigos do Facebook ou usa os botões Curtir ou Compartilhar em um site, o desenvolvedor do jogo ou o site pode coletar informações sobre as suas atividades no jogo, ou receber o comentário ou link do site compartilhado por você no Facebook. Além disso, quando você baixa ou usa serviços de terceiros, eles podem acessar seu Perfil Público, que inclui seu nome ou número de identificação de usuário, faixa etária e país/idioma, lista de amigos, bem como as informações que você compartilha com eles. As informações coletadas por esses aplicativos, sites ou serviços integrados está sujeita aos seus próprios termos e políticas. (FACEBOOK, 2016)

Percebe-se que o Facebook permite que um serviço de terceiro tenha acesso às informações sobre o usuário da plataforma. Além disso, em outra cláusula, o Facebook admite que compartilha as informações pessoais do usuário com o seu grupo de empresas. Assim dispõe o contrato: "Compartilhamos as informações que

temos sobre você com um grupo de empresas que fazem parte do Facebook." (FACEBOOK, 2016). Esse compartilhamento de dados pessoais fere o Marco Civil da Internet, além de fugir da finalidade da rede social.

O aplicativo "Lulu" foi um exemplo que evidenciou o quão prejudicial pode ser esse compartilhamento. Tal serviço permitia que as mulheres avaliassem sexualmente os homens que faziam parte de sua rede de amigos no Facebook, tudo isso de forma anônima. Muita discussão se formou, levando inclusive à instauração de um inquérito por parte do Ministério Público do Distrito Federal para que fosse apurada alguma irregularidade no caso, com base no argumento de que "o aplicativo no qual mulheres dão notas a homens de sua rede social evidencia ofensa a direitos existenciais de consumidores, particularmente à honra e à privacidade" (ALVES, 2016).

Trabalhou-se com o direito de não ser conhecido pela plataforma. Como os homens não aderiram aos termos de uso, eles não deveriam fazer parte daquela rede. Assim, apenas informações sobre os usuários que fossem fornecidas através de um consentimento informado poderiam ser coletadas.

Diversas foram as ações judiciais ajuizadas por homens contra o aplicativo, o que levou ao seu fim no ano de 2014, sem qualquer explicação para os usuários. Isso não impediu o julgamento de alguns processos que também tinham no polo passivo o Facebook, plataforma que cedeu os dados dos usuários ao aplicativo, sem a autorização expressa dos homens.

Um desses casos foi a apelação cível número 1000647-47.2014.8.26.0564, julgada pela 2ª Câmara de Direito Privado do Tribunal de Justiça do Estado de São Paulo em 20 de outubro de 2015. O caso teve a seguinte ementa:

> APELAÇÃO CÍVEL – Ação de indenização por danos morais – Sentença de procedência – Violação à honra do autor – Aplicativo "Lulu" – Ilegitimidade passiva – Inocorrência – No mérito, ocorrência de abalo moral indenizável - Valor da indenização

> fixado de forma razoável, no caso concreto – Recurso improvido. (SÃO PAULO, Tribunal de Justiça, 2015)

Trata-se de uma ação de indenização por danos morais ajuizada por um homem em face da "Luluvise Incorporation", empresa que possui o aplicativo "Lulu" e do Facebook. O juiz de primeira instância condenou os réus a ressarcirem o autor a importância de 20 mil reais em razão dos danos morais. O Facebook recorreu da decisão, argumentando que não possui legitimidade passiva, pois não é responsável pelo aplicativo tido como ofensivo. No mérito do recurso, argumentou que o autor consentiu com o uso de suas informações no momento em que aceitou os termos de uso da plataforma.

Sobre a preliminar arguida, o tribunal decidiu que não há ilegitimidade passiva do Facebook, pois este permitiu o compartilhamento de opiniões de caráter ofensivo à honra do autor, existindo solidariedade entre os réus. No mérito, argumentou o Relator que a parte autora teve as informações de seu perfil pessoal do Facebook capturadas sem o seu consentimento, servindo de avaliação pelo público feminino de forma anônima. O Relator rechaçou o argumento de que o autor teria anuído com essa cessão de dados pessoais quando aderiu à rede social, afirmando que se trata de um contrato de adesão. Assim, o tribunal, por unanimidade, negou provimento ao recurso, mantendo na íntegra a sentença.

O mesmo fundamento foi utilizado no Recurso Inominado 71005057401 da Quarta Turma Recursal do Tribunal de Justiça do Estado do Rio Grande do Sul, julgado em 19 de setembro de 2014. Veja-se trecho da decisão:

> E não é demais referir que o autor ao informar e autorizar a divulgação de seus dados no Facebook, não significa autorizar a utilização de forma irrestrita e que sejam utilizadas por qualquer um, mas apenas acesso aquelas pessoas para quem ele autoriza e quer compartilhar a sua vida. E com certeza não pretendeu nem mesmo compartilhar com aquelas mulheres, com quem nem pessoalmente se relacionou, e muito o mais ter a sua vida e pessoa

> avaliadas e de forma depreciativa, colocando em risco sua felicidade pessoal. (RIO GRANDE DO SUL. Tribunal de Justiça, 2014).

Foi decidido que a autorização para o uso das informações pelo Facebook não admite a utilização por terceiros. Tal conclusão decorre da aplicação do princípio da finalidade e da proteção da privacidade dos usuários, pois "todo indivíduo deve ter direito à proteção de sua propriedade e de sua privacidade." (PINHEIRO, 2016, p. 95). Houve uma interpretação da privacidade para o direito de não ser conhecido.

Apesar de toda a discussão sobre o aplicativo, ele voltou a funcionar em 2016 no Brasil (LOPES, 2016). Dessa vez, o cadastro e os dados utilizados não são oriundos do Facebook. Além do mais, os perfis disponíveis para a avaliação não são mais feitos automaticamente, é preciso que seja feito o cadastro prévio pela pessoa. Com isso, há um consentimento dos usuários em serem avaliados e avaliarem os outros, o que denota uma atenção à informação clara aos serviços prestados pelo aplicativo, com o respeito à privacidade dos demais usuários e o respeito ao direito de não ser conhecido.

5

Análise dos termos de uso e política de privacidade: regras gerais

As relações em meio digital são reguladas por contratos eletrônicos, os quais podem ser definidos como o negócio jurídico constituído por duas ou mais partes, com a finalidade de criar, extinguir, modificar, manter ou alterar um vínculo, tendo em vista um objeto, através de meio eletrônico. Esse tipo de contrato, muitas das vezes, é feito por adesão, sendo denominado, nesses casos, de termo de adesão digital.

A relação entre um provedor de aplicação e o usuário é feita através deste termo, por isso, afirma-se que é importante a investigação da validade deste tipo de avença. O atual estágio da sociedade, denominada de era da informação, na qual há uma vasta gama de informações sobre os usuários disponíveis na rede mundial de computadores, torna necessária a tutela destes e a proteção contra abusos feitos pelos fornecedores. Ressalta-se que a relação se amolda no conceito de consumo previsto no Código de Defesa do Consumidor.

Neste capítulo, discute-se a validade do termo de adesão digital, sendo feita uma análise sobre contratos eletrônicos, investigando os seus requisitos de validade e a forma como eles podem ser exteriorizados. Conforme se verá, o elemento vontade deixa de ser preponderante em uma relação jurídica com a massificação do consumo e a ruptura do liberalismo. Assim, afirma-se que a teoria clássica contratual entra em crise.

5.1 Contratos Eletrônicos

A relação entre um usuário e um provedor da Internet é uma relação de consumo. Assim, é preciso que se tenha uma maior proteção do usuário ante a sua vulnerabilidade. Nesse sentido, os contratos eletrônicos precisam ser interpretados de uma forma mais favorável ao consumidor (MARQUES, 2011).

Observe que não há como requisito de validade de um contrato a existência de uma avença escrita. Isso porque, conforme o artigo 104 do Código Civil brasileiro de 2002, são requisitos de validade dos contratos a capacidade, licitude do objeto e a forma, que pode ser obrigatória ou não proibida em lei. Portanto, não existe nenhuma obrigação de se ter um contrato eletrônico escrito, desde que não se faça o uso dos dados pessoais do usuário. Nesse caso, há a obrigação legal de um contrato escrito.

Isso se deve ao fato de que o artigo 7º, inciso VIII, alínea c, condiciona o uso de dados pessoais às finalidades que "estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de Internet" (BRASIL, 2014). Nesse sentido, apenas se um provedor fizer o uso de dados pessoais é que ele terá a obrigatoriedade de utilizar um termo de uso e uma política de privacidade.

Os termos de uso são os contratos eletrônicos feitos entre o usuário e o site, neles são previstas as condições às quais se está aderindo. Na sociedade da informação, os contratos feitos com provedores, tais como redes sociais, não são lidos. Experiência que comprova essa afirmação é a feita pelo aplicativo PC Pitstop no ano de 2005, por meio da qual foi colocada no meio dos termos de uso uma cláusula que prometia uma bonificação ao primeiro usuário que enviasse um *e-mail* requisitando a recompensa. Levou mais de 5 meses e mais de 3 mil downloads para alguém requerer o prêmio (ROMERO, 2016). Além disso, a Universidade de Stanford realizou uma pesquisa por meio da qual constatou que 97% dos usuários não leem os termos de uso (ROMERO, 2016).

Em um recente experimento, a Purple, uma companhia Inglesa especializada na oferta de acesso à Internet por conexão Wi-Fi em estabelecimentos privados, inseriu em seus termos de uso, uma cláusula pela qual os usuários concordavam em limpar banheiros sem qualquer remuneração[1]. Evidente que a companhia não irá – até mesmo por que essa cláusula é nula – executar a obrigação assumida pelos mais de 22 mil usuários que concordaram com a cláusula. Da mesma forma que o aplicativo PC Pitstop, a companhia inseriu uma bonificação para qualquer usuário que apontasse a cláusula, entretanto, apenas uma pessoa recebeu o prêmio. Esse experimento foi feito para a divulgação de que a Purple é a primeira rede de Wi-Fi público que cumpre nova Regulamentação de Proteção de Dados Gerais da Europa.

A natureza dessa avença é de um contrato de adesão feito em meio virtual, já que o conteúdo contratual vem em um tipo, o qual não se pode alterar substancialmente. O conceito de contrato de adesão encontra-se no artigo 54[2] do CDC (BRASIL, 1990). Trata-se daquela avença, cujo conteúdo o consumidor não pode discutir ou modificar substancialmente

Robert Cooter e Thomas Ulen (2007) defendem que há uma vantagem econômica no contrato de adesão, já que o risco e o preço são menores. Como se discute apenas o preço do negócio, é possível o fornecedor prever objetivamente os riscos e calcular melhor as despesas, significando um menor custo marginal do negócio.

---

[1]Informação disponível em: <http://gizmodo.uol.com.br/termos-de-servico-bizarro-wi-fi/>. Acesso em: 11 set. 2016.

[2] Art. 54. Contrato de adesão é aquele cujas cláusulas tenham sido aprovadas pela autoridade competente ou estabelecidas unilateralmente pelo fornecedor de produtos ou serviços, sem que o consumidor possa discutir ou modificar substancialmente seu conteúdo.

§ 1º A inserção de cláusula no formulário não desfigura a natureza de adesão do contrato.

§ 2º Nos contratos de adesão admite-se cláusula resolutória, desde que a alternativa, cabendo a escolha ao consumidor, ressalvando-se o disposto no § 2º do artigo anterior.

§ 3º Os contratos de adesão escritos serão redigidos em termos claros e com caracteres ostensivos e legíveis, cujo tamanho da fonte não será inferior ao corpo doze, de modo a facilitar sua compreensão pelo consumidor.

§ 4º As cláusulas que implicarem limitação de direito do consumidor deverão ser redigidas com destaque, permitindo sua imediata e fácil compreensão. (BRASIL, 1990)

Entretanto, do ponto de vista do consumidor, muitas vezes em tais contratos são inseridas cláusulas limitativas de direitos, o que pode gerar a nulidade, tendo em vista o disposto no Código Civil, conforme se verá adiante.

O CDC, visando tutelar o consumidor, normatiza que cláusulas restritivas devem ser escritas com destaque, permitindo a fácil identificação, conforme o artigo 54, §4º (BRASIL, 1990). Mais ainda, tratando-se de contrato de adesão, este deve ser escrito por inteiro em linguagem clara e de fácil compreensão, além da fonte ser de tamanho 12, no mínimo, de acordo com o §3º do mesmo dispositivo (BRASIL, 1990). Normas como essas têm o objetivo de proteger o consumidor de práticas abusivas (TARTUCE, 2012). Todavia, em alguns casos o usuário na Internet sequer sabe da existência de um termo de uso que regula a relação.

Existem dois tipos de contratos de adesão eletrônico, os chamados Click-wrap e o Browse-wrap[3] (LIMA, 2016). O contrato de Click-wrap é aquele por meio do qual o consumidor/usuário deve clicar na opção "Eu declaro que li e que concordo com os termos de uso e com a política de privacidade". Por sua vez, o contrato de Browse-wrap é aquele que regula a relação entre o provedor e o usuário sem que ao menos este tenha manifestado a sua intenção através do clique (KLEE, 2012). Este é utilizado em sites em que não é necessário um cadastro prévio para uso, mas que utilizam cookies[4], por exemplo. É feita a coleta de dados do usuário, com a autorização do termo de uso, o qual não foi disponibilizado realmente ao usuário, quer seja através de uma pop-up[5] ou através de um aviso no próprio site, por exemplo.

---

[3] Wrap é uma palavra de origem inglesa que significa embrulho. O intuito aqui é deixar claro que o contrato vem em um embrulho que deve ser clicado (Click-wrap) ou em um embrulho que é apenas navegado (Browse-wrap).

[4] Cookies é uma forma de comunicação entre o site e o usuário. Trata-se do armazenamento das preferências do usuário naquele determinado site. O seu objetivo é aperfeiçoar a navegação, tendo em vista ser possível traçar um perfil pré-determinado dos gostos do usuário.

[5] Pop-up é uma nova janela que abre no navegador ao se clicar em um link específico, ou, até mesmo, acessar um website.

O problema aqui é o imediatismo da sociedade da informação (PAESANI, 2013), que faz com que os usuários não leiam os termos de uso que regulam o serviço que estão usando. Sobre isso, assim conclui Cintia Lima:

> [...] a sociedade de informação pós-moderna busca, constantemente, a aceleração do tempo. Em outras palavras, na rede mundial de computadores, tudo deve acontecer muito rápido, sob pena de espantar os interessados. Neste contexto, insere-se uma nova prática contratual, em que o adquirente acessa a página na Internet do fornecedor, vinculando-se aos termos e condições de uso fixadas discretamente em um hiperlink no canto inferior do site. (LIMA, 2014, p. 130)

Nesse sentido, discute-se a validade destes contratos, tendo em vista a relativa ausência de expressão de vontade. Mais ainda, em se tratando de cláusulas restritivas, questiona-se como certificar que o usuário tenha conhecimento dos termos a que se vinculou.

5.2 A massificação dos contratos: crise contratual

Contrato é a exteriorização de um negócio jurídico, de forma que a "vontade é a nota característica que mais avulta no negócio jurídico. É a sua força propulsora" (FARIAS; ROSENVALD, 2007, p. 428). Tal conceito se enquadra na concepção clássica, quando se falava, mormente, em autonomia da vontade. Esta teoria entra em crise, mudando-se para a autonomia privada.

Como visto no capítulo 3, no auge do liberalismo, falava-se em autonomia da vontade, momento no qual os sujeitos determinavam as avenças, com a mínima intervenção estatal. Entretanto, o capitalismo e a revolução industrial fizeram com que acontecesse uma massificação dos contratos, mudando a forma como se negociava. Houve uma diminuição da vontade, que culminou na teoria preceptiva. Esta teoria ensina que "as obrigações oriundas dos contratos valem não apenas porque as partes as assumiram, mas

porque interessa à sociedade a tutela da situação objetivamente gerada, por suas consequências econômicas e sociais" (FIUZA, 2011, p. 94). Assim, passa-se de uma autonomia da vontade para uma autonomia privada, na qual não se tem na vontade uma lei máxima que deve sempre prevalecer, podendo um contrato ser revisto caso se tenha um abuso de uma das partes, por exemplo. Ademais, fala-se em boa-fé objetiva e função social do contrato, princípios capazes de relativizar os efeitos de um contrato. As relações entre indivíduos devem ser tuteladas para que o Estado garanta o equilíbrio entre eles. Não se trata de retirar a autonomia negocial, mas se protege o indivíduo contra abusos em relações privadas.

No mesmo sentido:

> É preciso aqui registrar, reiterando posição antes evidenciada à exaustão, que o elemento volitivo, fruto da autonomia da vontade e da autonomia privada, marca registrada do negócio jurídico, não mais assume caráter absoluto, sofrendo, sempre, as limitações decorrentes da ingerência de normas de ordem pública, notadamente constitucionais, por força da proteção destinada à pessoa humana, realçando sua necessária dignidade (art. 1º, III, CF/88). (FARIAS; ROSENVALD, 2007, p. 428).

Há uma mudança da valoração do elemento vontade, já que esse pode ser modificado em decorrência de abusos, relativizando os seus efeitos. Conforme afirma Enzo Roppo (2009),

> Existe, sem dúvida, na evolução da teoria e da disciplina dos contratos, uma tendência para a progressiva redução do papel e da importância da vontade dos contraentes, entendida como momento psicológico da iniciativa contratual: esta tendência, que podemos definir como <objectivação (sic) do contrato>, leva a redimensionar, sensivelmente, a influência que o elemento voluntarista exerce, quer em relação à definição geral do próprio conceito de contrato, quer em relação ao tratamento jurídico concreto de cada relação (ROPPO, 2009, p. 297)

Portanto, em uma relação contratual perde-se a preponderância do elemento vontade, razão pela qual, há contrato até mesmo quando feito por adesão, no qual não se discute o teor das cláusulas. Segundo Enzo Roppo (2009), há contrato em virtude da relação social que é modificada, sendo válido, pois o termo de adesão digital, o que não implica afirmar que todas as cláusulas ali inseridas sejam válidas.

Em se tratando de Direitos da Personalidade, como o caso do direito à imagem, estes não podem sofrer uma limitação sem que isso seja expressamente concordado pelo usuário, com base no disposto no artigo 11[6] do Código Civil de 2002 (BRASIL, 2002). Ademais, existem diversas previsões de nulidades de cláusulas contratuais, tanto no CDC, quanto no Marco Civil da Internet. Conforme normatiza o artigo 7º, inciso VI do Marco Civil, são asseguradas ao usuário "informações claras e completas constantes dos contratos de prestação de serviços" (BRASIL, 2014). Trata-se, pois, de um dever do provedor de serviço informar ao usuário como é que será regida a relação, através dos termos de uso, dando possibilidade ao consumidor/usuário de conhecer as regras do serviço. Frisa-se que o artigo 8º do mesmo dispositivo normativo traz hipóteses de nulidades de cláusulas dos termos de uso. Veja-se:

> Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à Internet.
> Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no caput, tais como aquelas que:
> I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela Internet; ou
> II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil. (BRASIL, 2014)

[6] Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.

Nesse sentido, caso exista uma cláusula que implique as hipóteses acima mencionadas, esta não terá validade. É uma forma de se tutelar o usuário ante aos termos de adesão, tendo em vista a falta de possibilidade de se escolher como vão ser tratados os dados pessoais, por exemplo.

Além do CDC e do Marco Civil, o Código Civil Brasileiro de 2002 possui duas normas que tratam do contrato de adesão, os artigos 423[7] e 424[8] (BRASIL, 2002). Tais normas trazem, respectivamente, o princípio da interpretação mais favorável ao aderente e da nulidade das cláusulas que tenham renúncia antecipada de direito resultante do negócio. Tais artigos normatizam que as cláusulas contratuais devem ser interpretadas de maneira mais favorável ao aderente, preservando, sempre que possível, a validade da avença.

Como os termos de uso dos serviços eletrônicos regulam aquela relação, neles são inseridas diversas condições para o uso, bem como das possibilidades de tratamento de dados pessoais, o que pode ferir a privacidade e a intimidade do usuário. Surge a necessidade de se certificar que o usuário anuiu com aquela cláusula restritiva em específico. Assim, o caminho mais apropriado, tratando-se de um contrato eletrônico, é fazer com que o usuário dê o consentimento em apartado para cada situação que implique uma limitação de seu direito, tal qual é feito no ordenamento jurídico Italiano para contratos de adesão feitos por escrito. O artigo 1341 do Código Civil Italiano assim dispõe:

> Art. 1341. Termos e Condições Gerais.
> Os termos e condições estabelecidos por um dos empreiteiros gerais são eficazes contra o outro, se, no momento da celebração do contrato estes os conheçam ou deveriam ter conhecido usando a diligência normal.

---

[7] Art. 423. Quando houver no contrato de adesão cláusulas ambíguas ou contraditórias, dever-se-á adotar a interpretação mais favorável ao aderente.

[8] Art. 424. Nos contratos de adesão, são nulas as cláusulas que estipulem a renúncia antecipada do aderente a direito resultante da natureza do negócio.

> Em qualquer caso, não têm nenhum efeito se não forem especificamente aprovadas por escrito, as condições que garantam, em favor de quem aderiu, limitação de responsabilidade, o direito de rescindir o contrato ou suspender a sua execução, ou impor sobre o outro empreiteiro, limitações ao direito de se opor, as restrições à liberdade contratual nas relações com terceiros, a extensão tácita ou renovação do contrato, cláusulas de arbitragem ou derrogações à competência do tribunal. (ITALIA, 2016, tradução nossa)[9]

Na Itália, existe uma obrigação de o fornecedor de bens ou serviços, tratando-se de cláusula restritiva, provar que o consumidor a leu, fazendo isso através de uma assinatura específica para aquela cláusula. Assim também deveria ser para os termos de adesão em meio digital. Caso se tenha uma cláusula que restrinja o direito do consumidor, este deve anuí-la através de uma pop-up[10], por exemplo. Desse modo, o fornecedor estaria cumprindo o seu dever de informar e o consumidor saberia, de forma clara, quais são as condições a que se sujeita.

Outra possibilidade é o projeto "Terms of Service; Didn't Read"[11], que em tradução livre seria "Termos de serviço: não os li". O referido projeto disponibiliza de maneira bem simplificada e intuitiva as regras que as principais plataformas utilizam em suas políticas de privacidade e termos de uso. Contudo, não existe a possibilidade de o usuário discordar das cláusulas, pois o referido projeto apenas informa as condições a que se submete. É melhor que isso seja feito pela própria plataforma, dando ao usuário a possibilidade de discordar (Opt-Out) de alguma cláusula restritiva,

---

[9] Art. 1341. Condizioni generali di contratto. Le condizioni generali di contratto predisposte da uno dei contraenti sono efficaci nei confronti dell'altro, se al momento della conclusione del contratto questi le ha conosciute o avrebbe dovuto conoscerle usando l'ordinaria diligenza. In ogni caso non hanno effetto, se non sono specificamente approvate per iscritto, le condizioni che stabiliscono, a favore di colui che le ha predisposte, limitazioni di responsabilità , facoltà di recedere dal contratto o di sospenderne l'esecuzione , ovvero sanciscono a carico dell'altro contraente decadenze , limitazioni alla facoltà di opporre eccezioni , restrizioni alla libertà contrattuale nei rapporti coi terzi , tacita proroga o rinnovazione del contratto, clausole compromissorie o deroghe alla competenza dell'autorità giudiziaria.

[10] Pop-up é uma janela que abre no navegador da Internet quando se acessa uma página na web ou algum link de redirecionamento.

[11] Disponível em: <https://tosdr.org/>. Acesso em: 11 ago. 2016.

quer seja proibindo o acesso a determinada informação, por exemplo, ou até mesmo optando pelo cancelamento do serviço.

Ademais, é preciso que se tenha em mente que um dos pilares do Marco Civil é a privacidade do usuário (BRANT, 2014). Fala-se no princípio da finalidade, o qual surge da preocupação com a coleta e tratamento de dados pessoais. Trata-se do princípio que determina que os dados pessoais devem ser utilizados com a finalidade para a qual foram coletados, impedindo a sua utilização para fins diversos do que o definido, ou seja, que haja tratamento secundário (MENDES, 2014). Portanto, os provedores não podem, à revelia dos usuários, realizar a coleta indiscriminada de dados pessoais.

Por isso, afirma-se que na modernidade o acesso aos bens de consumo é uma necessidade, portanto, o contrato é uma relação jurídica necessária e não mais voluntária. Fala-se em preceptivismo jurídico, em que o liberalismo perde força, fazendo com que o contrato tenha uma função social e deva ser protegido (FIUZA, 2011). "Assim, ser consumidor não é opção, bem como, por decorrência lógica, praticar atos de consumo ou atos necessários ao consumo (contratos), também não constituem fenômenos volitivos." (POLI; LORENTINO, 2016). Nesse sentido é que os contratos de adesão em meio eletrônico devem ser tutelados, pois não há uma relação de paridade entre os contratantes. Como visto, isso não importa em nulidade do contrato, o que pode acontecer é a declaração de nulidade de algumas das cláusulas da avença.

5.3 A abusividade e invalidade de cláusulas restritivas de direitos no termo de adesão digital

A principal característica do contrato de adesão é que não é possível alterar as cláusulas substanciais do contrato. Afirma-se que para os termos de adesão digital vigora o princípio da aceitação integral, segundo o qual não é possível discordar dos termos de uso ou política de privacidade. Isso gera o risco da invalidação do negócio jurídico.

> O risco da invalidação judicial está vinculado à inexistência de acordo mútuo sobre tais termos e condições, o que significa a própria inexistência do contrato em si, dependendo das circunstâncias do caso concreto. Além disso, a utilização de *hiperlink* para indicar a existência de um contrato, nos moldes atuais, anteriormente, descritos, não é aceito pelos tribunais, tendo em vista a dificuldade em percebê-los, constituindo, muitas vezes, uma prática desleal do proprietário do *site*. (LIMA, 2014)

No entanto, isso não implica invalidade do contrato, nem tampouco em validade absoluta de todas as cláusulas. Caso exista alguma cláusula abusiva ou restritiva de direitos, esta será considerada nula a depender do caso. Um exemplo de cláusula nula comumente encontrada nesses contratos é a que estabelece o domicílio para o ajuizamento de qualquer demanda pelo usuário. Veja-se, por exemplo, a que consta nos termos de uso do Facebook:

> Você resolverá qualquer reivindicação, causa de ação ou disputa (reivindicação) decorrente de ou relacionada exclusivamente à esta Declaração ou ao Facebook no tribunal distrital americano, para o distrito do norte da Califórnia, ou um tribunal estadual localizado no condado de San Mateo, e você concorda em submeter-se à jurisdição pessoal de tais tribunais com o propósito de pleitear todas essas reivindicações. As leis do estado da Califórnia regem esta Declaração, bem como as alegações que surjam entre você e nós, independentemente de conflitos nas disposições legais. (FACEBOOK, 2016)

Se aplicada a referida cláusula, um usuário brasileiro deveria ajuizar uma ação no estado da Califórnia nos Estados Unidos da América, onde se encontra a sede principal do Facebook. Entretanto, conforme o artigo 11 do Marco Civil da Internet (BRASIL, 2014), em qualquer operação de coleta, armazenamento, guarda e tratamento de registros de dados pessoais ou de comunicações por provedores de conexão e de aplicações de Internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente

respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros. Indo além, o Marco Civil da Internet normatiza em seu artigo 8º a nulidade de cláusula em um contrato de adesão que não ofereça como alternativa a adoção do foro brasileiro para a solução de controvérsias decorrentes de serviços prestados no Brasil.

Isso significa que quando a informação utilizada pelo Facebook provém de um usuário brasileiro, deverá ser aplicado o ordenamento jurídico deste país, ao contrário do que dispõe os termos de uso, o que implica a competência da jurisdição brasileira. Tal fato decorre dos artigos 101, inciso I do CDC (BRASIL, 1990) e do artigo 22 do Código de Processo Civil – CPC (BRASIL, 2015).

Por mais que o artigo 25 do CPC normatize que a autoridade brasileira não é competente quando houver cláusula de eleição de foro exclusivo estrangeiro em contrato internacional e que o artigo 22, inciso II do mesmo dispositivo normatiza que a autoridade judiciária brasileira possui competência concorrente para processar e julgar as ações decorrentes de relações de consumo, quando o consumidor tiver domicílio ou residência no Brasil (BRASIL, 2015), entende-se pela nulidade da cláusula.

Observe que o artigo 101 do CDC dispõe em seu caput e inciso I que a ação de responsabilidade civil do fornecedor de produtos e serviços pode ser proposta no domicílio do autor (BRASIL, 1990). Nesse sentido, por se tratar de uma relação de consumo a relação entre um usuário e um provedor (PINHEIRO, 2016), bem como o fato de se tratar de um contrato de adesão, deverá ser considerada nula de pleno direito a referida cláusula, podendo o usuário optar pelo seu domicílio para fins de fixação de competência, além da observância do ordenamento jurídico brasileiro para a aplicação do direito. No mesmo sentido é a lei para a proteção de dados pessoais, que, em seu artigo 3º, determina a vinculação à lei qualquer operação de tratamento ou coleta realizada no Brasil.

Veja que o Marco Civil prevê expressamente no artigo 8º a nulidade de cláusula que implique na renúncia do foro brasileiro

para a resolução de litígios decorrentes de serviços prestados no Brasil. Neste sentido, conclui-se pela nulidade de qualquer cláusula que vincule o usuário brasileiro à norma ou jurisdição de outro país. Nesse aspecto, tutela-se a vulnerabilidade do consumidor:

> Ainda, esta norma deriva do Princípio da vulnerabilidade do consumidor, positivado e ratificado internacionalmente. A autonomia da vontade, amplamente aceita nos casos de contratos internacionais, que permite que se apliquem leis distintas do foro competente, não faz sentido no caso dos contratos de consumo, até porque o Direito brasileiro adota como elemento de conexão a Lex loci contractus no art. 9º da LINDB; ou seja, aplica-se a Lei do país em que se constitui a obrigação. No contrato de consumo internacional eletrônico, deve-se considerar que o contrato de consumo se constituiu, mesmo que entre ausentes, no domicílio do consumidor brasileiro, por ser a norma mais favorável ao mesmo. (SALIB, 2013)

A autora Marta Luiza Leszczynski Salib (2013), escreveu sobre o tema sob a égide do Código de Processo Civil de 1973. Naquele diploma não se tinha a previsão expressa de observância do domicílio do consumidor em contratos internacionais, ainda que concorrente. Assim, a doutrina discutia se havia a possibilidade de se aplicar a jurisdição brasileira a um contrato feito entre ausentes no qual o fornecedor era domiciliado no exterior. A autora, à época, concluiu pela submissão à jurisdição brasileira após expor normas de proteção ao consumidor.

> Além disso, defendemos ainda o afastamento da aplicação do art. 9º, §2º da LINDB para entender que as obrigações contraídas pelo consumidor na Internet devem ser vistas como concluídas em seu domicílio; sendo assim, aplica-se a Lei do seu domicílio nos casos em que litigar com fornecedor estrangeiro. Isso porque, mesmo entendendo este contrato como entre ausentes, aplicar a Lei do foro do proponente (no caso, o fornecedor, como prevê o art. 9º da LINDB), seria afastar a jurisdição do consumidor, que não teria noção dos seus direitos pela Lei estrangeira, até porque a maioria dos contratos assinados virtualmente pelo consumidor é de adesão. Assim sendo, entendemos que as lides consumeristas

> oriundas do comércio eletrônico internacional devem ser propostas e dirimidas no domicílio do consumidor. (SALIB, 2013)

Atualmente, o CPC de 2015 pacificou o entendimento de que nesse tipo de contrato, a jurisdição brasileira é concorrente. Nesse sentido, conclui-se pela nulidade de qualquer cláusula que vincule o usuário brasileiro à norma ou jurisdição de outro país.

Outro exemplo de cláusula nula de pleno direito que comumente é inserida nos termos de adesão digital é a que trata da cessão de dados para terceiros. O Marco Civil em seu artigo 7º, inciso VII, normatiza o direito dos usuários ao não fornecimento a terceiros de seus dados pessoais, exceto se houver consentimento livre, expresso e informado. Esse consentimento, tratando-se de um contrato de adesão, é relativo. Isso porque, como já exposto, o usuário usualmente sequer lê o contrato ao qual está aderindo.

Apesar disso, há o compartilhamento de informações entre plataformas. No capítulo 4.5, trabalhou-se com o caso do aplicativo Lulu, o qual é um exemplo de que essa regra não é seguida. Na era do Big Data, as informações pessoais dos usuários são cedidas a terceiros, quer seja a título gratuito quer seja oneroso. Veja que as informações pessoais podem ser compradas por menos de oito centavos de dólar[12], e serão utilizadas para mapear os gostos dos usuários.

Não obstante, é comum encontrar nos termos de uso disposições que permitem o compartilhamento de dados. Em 2016, o Ministério Público Federal no Piauí ajuizou ação civil pública, com pedido de liminar, contra o Google, alegando que este faz scaneamento não autorizado de e-mails dos usuários do aplicativo Gmail, o que fere a legislação brasileira (PIAUÍ, 2016). A ação teve como base o Inquérito Civil Público nº 1.27.000.001406/2015-03, instaurado para investigar violação à privacidade de usuários.

---

[12] Disponível em: <http://www2.camara.leg.br/atividade-legislativa/comissoes/comissoes-permanentes/cdc/noticias/rodrigo-martins-venda-de-dados-pessoais-na-Internet-e-perigoso-e-pode-levar-a-abusos>. Acesso em: 10 set. 2016.

Foi noticiado que o Google analisa o conteúdo dos e-mails enviados por meio do seu aplicativo Gmail, com objetivos comerciais. O Ministério Público argumentou pela violação do art. 7º, inciso IX do Marco Civil da Internet, que exige consentimento expresso e destacado do usuário para tratamento de seus dados pessoais. Por sua vez, a plataforma argumentou que os usuários concordam com essa prática, ao aceitarem os termos de uso e política de privacidade. O argumento do Ministério Público é que em se tratando de cláusula restritiva de direito, essa não tem validade, mormente em um contrato de adesão (PIAUÍ, 2016).

Na ação foi requerida tutela de urgência para que a plataforma suspendesse a análise do conteúdo dos e-mails em todo o território brasileiro. Contudo, o pedido foi indeferido no dia 30 de junho de 2017 com base na contestação apresentada pelo réu. Atualmente, o processo encontra-se em fase de conhecimento, não tendo sido proferida sentença de mérito (BRASIL, 2017).

Sobre o compartilhamento dos dados pessoais, dispõe a lei para a proteção dos dados pessoais em seu artigo 7º, §5º que:

> § 5º O controlador que obteve o consentimento referido no inciso I do caput deste artigo que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Nesse sentido, será necessário o consentimento do titular para que seja feito o compartilhamento. Como a Internet não tem barreiras, discute-se ainda a possibilidade de transferência internacional de dados, sendo que a lei geral para a proteção de dados pessoais reservou um capítulo para tratar da matéria. Entre as disposições, há a regra geral de que o compartilhamento só será feito para países que garantam nível de proteção equiparado ao brasileiro, permitindo algumas exceções, tais como necessidade de investigação, proteção à vida ou a transferência resultar de acordo de cooperação internacional.

Outra cláusula comumente encontrada é a que determina a renúncia a algum tipo de sigilo, por exemplo o bancário. O Spotify, plataforma de *streaming* de música, assim determina em seu termo de uso:

> Concorda que, ao aceitar essa política de privacidade, onde for aplicável e na medida permitida pela lei aplicável, você renuncia expressamente aos seus direitos previstos nessas leis de sigilo bancário com referência ao spotify, a qualquer empresa no grupo spotify e a quaisquer parceiros de negócios e prestadores de serviços confiáveis, que poderão estar localizados fora do seu país de residência.[13]

Trata-se de uma renúncia não informada que fere inclusive a legislação brasileira sobre o sigilo bancário, qual seja, a Lei Complementar nº 105, de 10 de janeiro de 2001, a qual normatiza em seu artigo 1º que "As instituições financeiras conservarão sigilo em suas operações ativas e passivas e serviços prestados". Assim, entende-se que a referida cláusula é nula de pleno direito, eis que coloca o usuário em risco (ALMEIDA, 2016).

Várias condutas adotadas por plataformas são prejudiciais aos usuários, contudo faltam mecanismos de tutela específicos para coibir os abusos das grandes companhias. Mesmo que se tenha um ordenamento interno que possibilite uma proteção, haverá a falta de um mecanismo internacional, isso porque o fenômeno Internet é transnacional. Assim, é importante que se tenha uma cooperação internacional determinando o bom uso da Internet.

5.4 Venire Contra factum proprium

Como o termo de uso se trata de um contrato, a ele se aplica o princípio da boa-fé objetiva. O referido princípio é positivado no ordenamento jurídico brasileiro nos artigos 113 (função

[13] Informação disponível em: <https://www.spotify.com/br/legal/end-user-agreement/>. Acesso em: 10 set. 2017.

interpretativa), 422 (função integrativa) e 187 (função restritiva), todos do Código Civil (BRASIL, 2002). Conforme Carlos Roberto Gonçalves:

> O princípio da boa-fé exige que as partes se comportem de forma correta não só durante as tratativas como também durante a formação e o cumprimento do contrato. Guarda relação com o princípio do direito segundo o qual ninguém pode beneficiar-se da própria torpeza. Recomenda ao juiz que presuma a boa-fé, devendo a má-fé, ao contrário, ser provada por quem a alega. Deve este, ao julgar demanda na qual se discuta a relação contratual, dar por pressuposta a boa-fé objetiva, que impõe ao contratante um padrão de conduta, o de agir com retidão, ou seja, com probidade, honestidade e lealdade, nos moldes do homem comum, atendidas as peculiaridades dos usos e costumes do lugar. (GONÇALVES, 2011, p. 700)

As partes devem agir sempre com probidade na execução contratual, bem como adotar uma postura de lealdade para com o contratante. Assim sendo, a boa-fé objetiva resulta da análise do padrão do homem médio e os usos e costumes locais. Por isso, afirma-se que é em vão a tentativa de se cunhar uma definição fechada deste princípio, pois, em cada individualidade, haverá um significado distinto (FARIAS; ROSENVALD, 2007).

Diversos são os desdobramentos da boa-fé objetiva. Um deles é *venire contra factum proprium*, também conhecida como teoria dos atos próprios.

> Na tradução literal, *venire contra factum proprium* significa vir contra um fato próprio. Ou seja, não é razoável admitir-se que uma pessoa pratique determinado ato ou conjunto de atos e, em seguida, realize conduta diametralmente oposta. (GAGLIANO; PAMPLONA FILHO, 2011, p. 118)

Pela teoria dos atos próprios, o contratante não pode ter uma conduta contraditória na execução do contrato, ou seja, deve manter um padrão esperado de comportamento. Conforme afirma

Anderson Schreiber (2005), há necessidade de se tutelar a confiança dos contratantes gerada pelo comportamento do outro, em conformidade com o princípio da solidariedade social.

> O princípio da solidariedade social, protegido como objetivo da República brasileira no artigo 3º da Constituição de 1988, impõe a consideração da posição alheia também na atuação privada. O *nemo potest venire contra factum proprium*, concebido como uma vedação ao comportamento incoerente dirigida à tutela da confiança, não é outra coisa senão um instrumento de realização deste valor constitucional. Há, em outras palavras, direta vinculação entre a solidariedade social e o princípio de proibição ao comportamento contraditório. (SCHREIBER, 2005, p. 101)

Isso tem relevante influência na análise dos termos de uso de um serviço de Internet. Questiona-se a possibilidade de se proteger um usuário por uma ação que ele mesmo tomou, ou seja, proteger a pessoa dela mesma.

A título exemplificativo, será abordado o caso do adolescente Nissim Ourfali. No ano de 2012, um vídeo postado pelo pai do adolescente se espalhou pela Internet, sendo assistido por inúmeras pessoas. O referido vídeo era um convite feito à família para o seu Bar Mitzvah, uma cerimônia judaica que marca o início da adolescência (JUSTIÇA..., 2016).

O que era para ser apenas um convite aos familiares, rapidamente tomou conta das redes sociais, pois o vídeo possuía diversas passagens cômicas:

> O vídeo de Nissim feito por uma produtora mostrava o jovem, ao som da música do One Direction, falando em português sobre sua família e suas atividades favoritas - ele faz referências a lugares como a praia da Baleia. O vídeo foi feito para o Bar Mitzvah do garoto, uma cerimônia que insere o jovem judeu como um membro pleno da comunidade judaica. (JUSTIÇA..., 2016).

Logo após o vídeo ter se espalhado, o pai apagou o original, entretanto, já havia diversos outros disponíveis para acesso. Em

verdade, é possível encontrar o vídeo com muita facilidade na Internet, basta que se pesquise o nome do Nissim Ourfali em qualquer motor de buscas, tal como o Google.

Ante a dificuldade em retirar o conteúdo da Internet, Nissim Ourfali, assistido por seus pais, ajuizou uma ação contra o Google, requerendo a retirada de todo e qualquer vídeo que "apresentassem o nome, a voz ou a imagem do jovem e estivessem disponíveis no YouTube, no Orkut e no Blogger (redes sociais da empresa)" (GOOGLE, 2016a).

Foi requerida medida liminar para a retirada do conteúdo, a qual foi deferida. Entretanto, o pedido foi julgado improcedente pelo Juiz de primeira instância. Assim sendo, foi feito um recurso para o Tribunal de Justiça do Estado de São Paulo. A 9ª câmara de direito privado do Tribunal de Justiça do Estado de São Paulo deu provimento ao recurso do Nissim, determinando a retirada de todo e qualquer conteúdo relacionado ao vídeo do Google.

O processo tramita sob segredo de justiça, o que impede o conhecimento de mais detalhes sobre o caso. Entretanto, em nota divulgada pelo Google, este afirmou que "a decisão do Tribunal de Justiça de São Paulo não observou a jurisprudência pacífica do STJ sobre a matéria, que reconhece a necessidade de indicação das URLs[14] - Uniform Resource Locator - específicas do conteúdo para que seja possível fazer a remoção" (GOOGLE, 2016a). Assim, há um erro na decisão, pois não foi indicado o endereço do conteúdo a ser retirado, o que já era o entendimento consolidado no STJ, definido em 2013, no Recurso Especial 1.396.417, além de ser a disposição legal do Marco Civil da Internet em seu artigo 19, §1º (GOOGLE, 2016a).

Analisando o caso sob o prisma da teoria dos atos próprios, deve-se questionar a possibilidade de imputação ao Google do ato ilícito, tendo em vista que o vídeo ofensivo foi colocado pelo próprio

[14] URL - Uniform Resource Locator, em tradução livre, significa localizador padrão de recursos. A sigla designa o endereço a ser digitado no navegador para que se chegue a determinado conteúdo.

usuário à disposição de todos. Mais ainda, conforme os termos de uso da plataforma, o usuário permite que outros reproduzam o trabalho, podendo inclusive distribuí-lo. Veja-se:

> Para fins de esclarecimento, Você mantém todos os direitos de propriedade sobre seu Conteúdo. Entretanto, ao enviar o Conteúdo ao YouTube, Você, pelo presente, cede ao YouTube licença mundial, não exclusiva, isenta de royalties, passível de ser sublicenciada e transferida, para usar, reproduzir, distribuir, preparar trabalhos derivados, exibir e executar o Conteúdo em conexão com o Serviço e YouTube (e de seus sucessores e afiliadas), inclusive, mas sem se limitar a atividades de promoção e redistribuição parcial ou total do Serviço (e trabalhos derivados) em qualquer formato de mídia e através de qualquer canal de mídia. Você também cede a todos os usuários do Serviço uma licença não-exclusiva para acessar o seu Conteúdo por meio do Serviço, e para usar, reproduzir, distribuir, exibir e executar tal Conteúdo conforme permitido pelas funcionalidades do Serviço e de acordo com estes Termos de Serviço. (GOOGLE, 2016b, grifo nosso)

Por mais que se trate de um contrato de adesão, não se vislumbra sob essas circunstâncias um vício que anule a referida cláusula, importando em um dever da plataforma indenizar o usuário. Isso porque foi ele quem fez com que o vídeo fosse disponibilizado na Internet, momento em que já saberia da possibilidade de ser acessado por qualquer pessoa. Ora, como o usuário teve o intuito de tornar público o vídeo, não pode, agora, após gerar essa expectativa de comportamento no provedor de serviço, requerer uma reparação pela repercussão que o caso tomou. O pai de Nissim sabia, desde o princípio, que, ao disponibilizar o vídeo no *YouTube*, o público alvo se tornaria indeterminado. Assim, não pode agora ir contra o próprio ato. Evidente que a análise do caso perpassa por outro aspecto, qual seja, o direito de ser esquecido pela Internet, abordado no tópico 5.1.3. Dessa forma, trabalha-se, também, com a teoria dos atos próprios.

6

Análise específica dos termos de uso e política de privacidade das redes sociais

Conforme Fernando Velloso (2014), rede social é uma estrutura composta por pessoas ou organizações, conectadas por um ou vários tipos de relações que partilham valores e objetivos comuns. Assim, qualquer plataforma que tem como objetivo a conexão de pessoas é considerada uma rede social. Como visto no tópico 2.2, na Web 3.0, as redes sociais são de suma importância, pois representam a nova forma de relacionamento online.

Nesse sentido, o contrato feito entre o usuário e a plataforma pode ser visto como necessário. Tal afirmação decorre da constatação de que a avença entre usuário e plataforma é feita por adesão, além de que estar em uma rede social, em alguns casos, é imprescindível, visto que as relações interpessoais são afetadas pela Internet (TUTOR, 2015).

Diversas cláusulas destes contratos são nulas de pleno direito se analisadas sob o prisma do ordenamento jurídico brasileiro ou sobre diretivas internacionais, como as europeias. O objetivo deste capítulo é a análise dos termos de uso das mais populares redes sociais[1], mostrando algumas nulidades encontradas nestes. Foram eleitos o Facebook, Instagram e Google, este último representa o YouTube, rede social de compartilhamento de vídeos. Serão confrontadas as cláusulas tidas como abusivas frente ao

---

[1] Informação disponível em <https://www.oficinadanet.com.br/post/16064-quais-sao-as-dez-maiores-redes-sociais>. Acesso em 15 out. 2017.

ordenamento jurídico brasileiro e diretivas europeias de proteção de dados pessoais.

6.1 Facebook

O Facebook é atualmente a maior rede social, com aproximadamente 1,9 bilhão de usuários ativos, praticamente um terço da população mundial. É raro encontrar alguém que não tenha perfil na plataforma. Atualmente, a Facebook INC., companhia que administra a rede social, possui também o Instagram, Facebook Menseger e WhatsApp. Em verdade, as maiores companhias detentoras de redes sociais são o Facebook INC. e a Google[2].

Através do Facebook o usuário cadastra um perfil, inserindo nele informações pessoais, tais como nome, idade, localização, gênero, interesses, entre outras. Além disso, é facultado ao usuário inserir uma foto de perfil, a qual será visível para todos na Internet. Essas informações são inseridas livremente pelo usuário, pois filiar-se a rede é facultativo, mas a vinculação aos termos de uso e política de privacidade é obrigatória.

Como já visto no tópico 5.3, há nos termos do Facebook cláusula de eleição de foro, a qual é nula de pleno direito. Entretanto, analisar-se-ão, nos próximos tópicos, algumas outras cláusulas que também ensejam a nulidade.

6.1.1 Cláusula de Propriedade Intelectual

Conforme a cláusula 2 dos termos de uso do Facebook, o usuário cede os direitos patrimoniais de toda a sua criação, permitindo que a plataforma dela utilize para qualquer fim, sem a necessidade de o remunerar. Entretanto, há a manutenção do

---

[2] Informação disponível em <http://www.bbc.com/portuguese/geral-40205922>. Acesso em 15 out. 2017

usuário como autor da criação. Nesse ponto, é necessário se explicar a natureza dúplice dos direitos autorais.

Conforme Leonardo Poli (2008), os Direitos Autorais têm um aspecto pessoal e outro material, daí decorrendo a têm natureza jurídica dúplice. O primeiro é extrapatrimonial e refere-se ao vínculo personalíssimo entre o autor e obra. O segundo é patrimonial e refere-se ao direito do autor em explorar economicamente a criação. Nesse sentido, o primeiro é indisponível e o segundo disponível.

Os Direitos Morais do autor[3] são um desdobramento dos direitos da personalidade, razão pela qual são intransmissíveis e irrenunciáveis, ou seja, não são transmitidos para terceiro, nem são disponíveis. Ademais, são absolutos, ou seja, oponíveis *erga omnes*, além de não serem atingidos pelo instituto da prescrição ou decadência. Por fim, prevalecem em eventuais conflitos com outros direitos subjetivos.

Em contrapartida, enquanto um desdobramento dos direitos reais, os direitos patrimoniais do autor são transmitidos, quer seja a título gratuito, quer seja oneroso. Desta feita, é possível se transmitir a exploração comercial de uma obra, mas não a autoria. Ressalta-se a independência entre os Direitos Morais e Patrimoniais do autor.

Dessa maneira, acredita-se que os perfis em redes sociais se tratam de obras e, como tais, são tuteladas pelo Direito Autoral.

---

[3] Os direitos morais do autor são normatizados pelo artigo 24 da Lei de Direitos Autorais. Art. 24. São direitos morais do autor:
I - o de reivindicar, a qualquer tempo, a autoria d a obra;
II - o de ter seu nome, pseudônimo ou sinal convencional indicado ou anunciado, como sendo o do autor, na utilização de sua obra;
III - o de conservar a obra inédita;
IV - o de assegurar a integridade da obra, opondo-se a quaisquer modificações ou à prática de atos que, de qualquer forma, possam prejudicá-la ou atingi-lo, como autor, em sua reputação ou honra;
V - o de modificar a obra, antes ou depois de utilizada;
VI - o de retirar de circulação a obra ou de suspender qualquer forma de utilização já autorizada, quando a circulação ou utilização implicarem afronta à sua reputação e imagem;
VII - o de ter acesso a exemplar único e raro da obra, quando se encontre legitimamente em poder de outrem, para o fim de, por meio de processo fotográfico ou assemelhado, ou audiovisual, preservar sua memória, de forma que cause o menor inconveniente possível a seu detentor, que, em todo caso, será indenizado de qualquer dano ou prejuízo que lhe seja causado. (BRASIL, 1998)

Como se sabe, todo o conteúdo do perfil digital é fruto da criação do espírito humano e tem um aspecto da personalidade deste. Entretanto, salienta-se que, em um mesmo perfil, é possível que se tenha mais de um autor, como no caso de comentários em fotos, publicações de mensagens na página de amigos dentre outras interações. Assim sendo, cada perfil pode ter uma série de autores.

Analogicamente, é como se fosse uma biografia, só que em meio informático. Embora não tenha um caráter patrimonial, configura-se como Direito Autoral, pois como visto, são autônomos os Direitos Morais do autor e os Direitos Patrimoniais deste. Ressalta-se que o ordenamento jurídico brasileiro adotou a teoria dualista dos Direitos Autorais, ou seja, há separação entre os Direitos Morais e Patrimoniais do autor. Dessa forma, observa-se que os Direitos Patrimoniais são disponíveis, já os Direitos Morais do autor, como faceta de sua personalidade, são indisponíveis.

Ao concordar com os termos de uso do Facebook o usuário cede, gratuitamente, os direitos patrimoniais, mantendo-se como autor. Entretanto, trata-se de renúncia inválida juridicamente se analisado sob a ótica do ordenamento jurídico brasileiro, especificamente o artigo 424 do Código Civil brasileiro, que, conforme visto, normatiza a nulidade de cláusulas que estipulem renúncia antecipada a direito resultante do negócio.

Portanto, a referida cláusula do Facebook é nula de pleno direito, ao estipular que:

> Para conteúdos protegidos por leis de direitos de propriedade intelectual, como fotos e vídeos (conteúdo IP), você nos concede especificamente a seguinte permissão, sujeita às suas configurações de privacidade e de aplicativos: você nos concede uma licença global não exclusiva, transferível, sublicenciável, livre de royalties para usar qualquer conteúdo IP publicado por você ou associado ao Facebook (Licença IP). Essa Licença IP termina quando você exclui seu conteúdo IP ou sua conta, exceto quando seu conteúdo é compartilhado com outras pessoas e este não é excluído por elas. (FACEBOOK, 2016)

Em verdade, o Facebook mantém o usuário como autor originário e o coloca como derivado, porém não fica determinado como serão distribuídos os possíveis ganhos econômicos. Logo, havendo direito resultante de alguma publicação na rede social, entende-se que ao usuário deve ser garantido o direito moral e patrimonial sobre ela.

6.1.2 Transferência internacional de dados pessoais

Além da coleta dos dados pessoais, há a transferência destes para o processamento de informações, conforme a cláusula 16.1, a qual dispõe que "Você concorda em ter seus dados pessoais transferidos para e processados nos Estados Unidos." (FACEBOOK, 2016). Assim, é preciso que se investigue acerca da legalidade dessa cláusula.

O estudo a respeito da transferência internacional de dados pessoais é importante na medida em que o avanço tecnológico proporciona uma interação fácil entre o mundo. Desde o ano de 1980, quando a Organização para a Cooperação e Desenvolvimento Econômico – OCDE – publicou as "Diretrizes sobre Proteção da privacidade e o Fluxo Transnacional de Informações Pessoais"[4], há uma preocupação com a transnacionalidade no tratamento de dados pessoais. Ocorre que as diretrizes não são vinculativas, sendo consideradas *soft law*, ou seja, não vinculam os Estados membros da OCDE. Já no ano de 1995, veio o primeiro instrumento normativo com caráter vinculativo, a Diretiva 95/46/EC da União Europeia[5]. No referido instrumento há no artigo primeiro uma norma que assegura que os Estados membros da União Europeia devem assegurar que as legislações internas estejam em conformidade com a diretiva.

---

[4] Disponível em:<http://www.oecd.org/sti/ieconomy/15590254.pdf>. Acesso em: 10 set. 2016.

[5] Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 05 out. 2016.

A Diretiva Europeia estabelece o sistema geográfico de proteção de dados pessoais em seu artigo 4º, que assim normatiza:

> Artigo 4º
> Direito nacional aplicável
> 1. Cada Estado-membro aplicará as suas disposições nacionais adoptadas por força da presente diretiva ao tratamento de dados pessoais quando:
> a) O tratamento for efetuado no contexto das atividades de um estabelecimento do responsável pelo tratamento situado no território desse Estado-membro; se o mesmo responsável pelo tratamento estiver estabelecido no território de vários Estados-membros, deverá tomar as medidas necessárias para garantir que cada um desses estabelecimentos cumpra as obrigações estabelecidas no direito nacional que lhe for aplicável;
> b) O responsável pelo tratamento não estiver estabelecido no território do Estado-membro, mas num local onde a sua legislação nacional seja aplicável por força do direito internacional público;
> c) O responsável pelo tratamento não estiver estabelecido no território da Comunidade e recorrer, para tratamento de dados pessoais, a meios, automatizados ou não, situados no território desse Estado-membro, salvo se esses meios só forem utilizados para trânsito no território da Comunidade.
> 2. No caso referido na alínea c) do nº 1, o responsável pelo tratamento deve designar um representante estabelecido no território desse Estado-membro, sem prejuízo das ações que possam vir a ser intentadas contra o próprio responsável pelo tratamento. [6]

No supracitado artigo é estabelecido que mesmo os Estados estrangeiros que se situem fora do bloco da União Europeia devem respeitar a diretiva. Assim, fica assegurado o modelo geográfico, que é o modelo que se admite a transferência internacional de dados pessoais apenas quando o país destinatário respeitar a legislação do país onde o dado foi coletado.

---

[6] Disponível em: <http://ec.europa.eu/justice/policies/privacy/docs/95-46-ce/dir1995-46_part1_pt.pdf>. Acesso em: 05 out. 2016.

Existem dois modelos básicos de transferência internacional de dados pessoais, quais sejam, o geográfico e o organizacional. O modelo organizacional possibilita a transferência para qualquer país, sendo atribuída à companhia a responsabilidade por qualquer violação de privacidade ou ilícito derivado do ato. Há quem defenda que o modelo organizacional, por ser descentralizado, respeita o princípio da governança.

Com a informatização das produções humanas é possível universalizar o saber, deixando com que esse não seja mais concentrado. Isso porque "Quanto mais o digital se afirma como um suporte privilegiado de comunicação e colaboração, mais essa tendência à universalização marca a história da informática." (LÉVY, 1999, p. 112). Esse é o papel fundamental que a rede mundial de computadores deve realizar, qual seja, universalizar o acesso ao conhecimento.

Para tanto, é necessário que a Internet continue a ser um fenômeno descentralizado, pautado pela sua Governança. Isso significa dizer que a atuação dos diversos atores na Internet tem o potencial de promover a Rede, para que se tenha um desenvolvimento sustentável e inclusivo.

Governança da Internet é a atuação conjunta dos diversos atores (Governo, sociedade civil, iniciativa privada, universidades, entre outros) no direcionamento do uso da rede. A Internet é um fenômeno transnacional, não possuindo barreiras físicas. Até então, foi construída de maneira a se dissociar de normas legais dos Estados, não havendo imposição de uma norma de um país sobre outro. Isso significa que as regras e os costumes são definidos pelos próprios atores que atuam na Internet. Daí decorre a importância da Governança da Internet, pois garante o uso cada vez mais livre e sem censura, tendo em vista a atuação multissetorial dos atores na formação das normas, princípios, usos e costumes.

Atribuir a uma companhia o controle dos dados pessoais pode, por um lado, respeitar o princípio da governança das redes, porém, por outro lado, pode significar uma restrição de privacidade,

já que em um determinado país pode não haver proteção à este direito. Em verdade, é possível se pensar em um sistema híbrido, por meio do qual se permita a transferência apenas para países que respeitem certas normas fundamentais de proteção de privacidade, bem como que a companhia se responsabilize sobre qualquer ato decorrente desta transferência.

O Marco Civil da Internet, em seu artigo 11, normatiza que deverá ser observada a legislação brasileira em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais, desde que pelo menos um dos terminais esteja localizado no Brasil, ou seja, estando o usuário ou provedor sediado no Brasil, deverá ser respeitado o ordenamento jurídico desse país. O §2º do citado artigo normatiza que se aplica a regra às atividades realizadas por companhias estrangeiras desde que ofertadas para o público brasileiro ou que integrem grupo econômico no qual faça parte companhia com sede no território brasileiro.

Entende-se que o Brasil adotou nesse artigo o sistema geográfico, tendo em vista a vinculação com o ordenamento jurídico pátrio quando a coleta dos dados ocorrer neste território. No entanto, com a aprovação da lei geral para a proteção de dados pessoais, há uma relativização da regra, ao prever que a transferência é permitida para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao dispositivo normativo. Assim dispõe o artigo 33:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei; (BRASIL, 2018)

Portanto, a regra descrita na lei é compatível com o sistema geográfico, porém não vincula a plataforma à legislação brasileira, é exigido tão somente proteção em nível equiparável. Existem ainda

outras hipóteses de transferência, estabelecidas nos incisos II a VI do artigo 33, a saber:

> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
> a) cláusulas contratuais específicas para determinada transferência;
> b) cláusulas-padrão contratuais;
> c) normas corporativas globais;
> d) selos, certificados e códigos de conduta regularmente emitidos;
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
> V - quando a autoridade nacional autorizar a transferência;
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei. (BRASIL, 2018)

O inciso III traz a regra sobre a transferência no caso de cooperação judicial para investigação[7]. Já no inciso IV há a previsão de transferência no caso de proteção ao titular dos dados. Os incisos V a VII se referem às hipóteses nas quais há intervenção de entidades, no caso de autorização, compromisso assumido em acordo internacional e necessidade de execução de política pública.

[7] Sobre o tema ver http://www.indexlaw.org/index.php/revistadgnt/article/view/1487

O inciso VII é um paradoxo dentro da legislação, pois parece normatizar o sistema organizacional de transferência ao estabelecer que esta é permitida "quando o titular tiver fornecido o seu consentimento para a transferência, com informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos." Ao longo deste trabalho, discorreu-se sobre a ausência de consentimento nos termos de uso e políticas de privacidade. Seria um paradoxo acreditar que o consentimento em uma política de privacidade é capaz de representar a vontade do titular do dado pessoal.

O artigo 34 da lei estabelece critérios para identificar o nível de proteção, sendo eles:

> I - as normas gerais e setoriais da legislação em vigor no país de destino ou no organismo internacional;
> II - a natureza dos dados;
> III - a observância dos princípios gerais de proteção de dados pessoais e direitos dos titulares previstos nesta Lei;
> IV - a adoção de medidas de segurança previstas em regulamento;
> V - a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados pessoais; e
> VI - outras circunstâncias específicas relativas à transferência. (BRASIL, 2018)

Acredita-se que o sistema jurídico não é mais organizacional como é disposto no Marco Civil da Internet, mas sim híbrido, com a possibilidade de transferência pela companhia, desde que respeitadas normas fundamentais de proteção de dados pessoais. Evidente que em se tratando de conflito de normas, prevalecerá a norma mais especial, já que esta revoga a lei geral. Há autores que defendem que o Marco Civil deverá prevalecer sobre a norma de proteção de dados pessoais.

> Sob essa hierarquia, as normas do Marco Civil prevaleceriam em todos os casso envolvendo consentimento na Internet, mesmo que haja casos em que o modelo proposto pela Lei de Proteção de Dados seria mais adequado (i.e, temas envolvendo a proteção de

> dados e o consentimento online). (INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE, 2017).

Respeitada a opinião, acredita-se que em se tratando de Internet, o Marco Civil seria a lei geral, sendo as demais leis especiais, como a de proteção de dados pessoais. Trata-se de um microssistema mais específico que a própria Internet, sendo que inclusive o Marco Civil menciona que a legislação específica irá regulamentar a proteção de dados pessoais. No que se refere à proteção de dados pessoais, a lei geral de proteção de dados pessoais deve prevalecer em detrimento das normas do Marco Civil da Internet em caso de conflito. Portanto, com a promulgação desta lei, o Brasil deixou de ser um país de modelo geográfico, adotando um modelo híbrido de proteção de dados pessoais.

No que se refere a transferência internacional de dados pessoais, tem-se que, com base no Marco Civil da Internet, a cláusula do Facebook é nula de pleno direito, eis que não vincula o tratamento e transferência à legislação brasileira. Contudo, com a promulgação da lei para a proteção de dados pessoais pode ser que a cláusula seja válida, desde que respeitados os critérios para a transferência, o que até o momento não é possível saber, haja vista a falta de transparência com o tratamento dos dados pessoais.

Ressalta-se que o modelo híbrido constante da lei geral de proteção de dados pessoais atribui uma responsabilidade objetiva à companhia que realizar o tratamento dos dados pessoais, isso em conformidade com os artigo 42 e 43.

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.
>
> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;

> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.

A Responsabilidade Civil é a subsunção de uma pessoa, humana ou jurídica, a uma obrigação de reparar o dano outrora causado, ou nas palavras de Carlos Roberto Gonçalves (2011), é uma garantia da restituição ou compensação do bem sacrificado.

Nesse sentido, conforme lecionam Pablo Stolze e Rodolfo Pamplona (2012), a Responsabilidade Civil pressupõe a atividade danosa de alguém. A responsabilidade civil pressupõe a existência de 4 elementos, quais sejam: a) Conduta omissiva ou comissiva; b) Dano; c) Nexo de Causalidade; e d) Culpa *latu sensu*. Trata-se da chamada Responsabilidade Civil Subjetiva que é a regra geral adotada pelo Código Civil de 2002, conforme artigos 186 e 927.

Por outro lado, há ainda a responsabilidade civil objetiva, que se refere aos casos em que não é necessária a caracterização da culpa. A delimitação de tal instituto encontra-se no parágrafo único do artigo 927, que normatiza que: "Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem." (BRASIL, 2002).

> A responsabilidade que se baseia na culpa do autor do ilícito denomina-se subjetiva, por ter como base o elemento subjetivo, culpabilidade. Já a responsabilidade sem culpa recebe o nome de responsabilidade objetiva, por se basear apenas na ocorrência do dano. Exemplo seria o abuso de direito, que dispensa a culpa para sua configuração. Uma pessoa pode abusar de direito, como o direito de dirigir em baixa velocidade, sem agir com culpa ou dolo. (FIUZA, 2011, p. 333)

No caso da transferência internacional de dados, a companhia será responsabilizada independentemente da culpa, o que torna a reparação do usuário mais fácil. Dessa forma, no caso de algum dano sofrido, haverá uma facilidade na reparação do dano em decorrência da desnecessidade do elemento culpa.

6.1.3 Coleta de dados pessoais

Questão preocupante é a coleta dos dados pessoais. Afirma-se que o Facebook sabe mais da vida do usuário do que esse fornece ativamente[8]. Na política de privacidade da rede, a mesma informa que coleta informações fornecidas pelo usuário, além de dados sobre como ele utiliza os serviços. Isso é necessário para o funcionamento da rede e não causa, a priori, violação do ordenamento jurídico brasileiro.

A plataforma coleta informações da rede de contatos, através da agenda do telefone celular. Essas informações podem dizer respeito tanto a um usuário quanto a um não usuário. Por exemplo, caso o usuário A tenha um endereço de e-mail secundário não fornecido a plataforma, mas o usuário B, também tenha salvo esta informação em sua agenda de contatos, a plataforma irá sincronizar essa informação, sem que o usuário A tenha fornecido ativamente. Essas informações podem dizer respeito inclusive a um não usuário, o que será objeto do capítulo 7.3.

Além disso, são colhidas informações sobre o dispositivo informático que é utilizado para acessar a plataforma. Por fim, são utilizadas informações recebidas de parceiros externos.

Quanto à coleta de dados, entende-se que, pelo princípio da finalidade, normatizado no artigo 7º, inciso VIII, do MCI, ela só é permitida para fins que a justifiquem. Assim, caso alguma dessas informações coletadas não seja necessária ao funcionamento da rede, este ato será nulo. Não se trata de nulidade da cláusula, pois

---

[8] Disponível em <http://www.bbc.com/portuguese/geral-40067569?ocid>. Acesso em 10 set. 2016.

para o funcionamento de uma rede social é importante que se tenha o cruzamento de informações entre usuários. Dessa forma, é necessário que se investigue o ato da coleta em si, pois se trata de uma cláusula necessária ao funcionamento da rede. Entretanto, não significa que, uma vez coletado o dado, o Facebook poderá utilizá-lo de forma indiscriminada.

6.1.4 Uso indiscriminado de algoritmos para definição do si eletrônico

Um dos princípios norteadores da privacidade na era digital é a autodeterminação afirmativa, pela qual pode-se interpretar que o usuário tem direito de ser reconhecido enquanto pessoa. Ocorre que as principais redes reduzem o perfil a um mero dado, utilizando algoritmos para a definição do sujeito.

No ano de 2016, ocorreu as eleições presidenciais dos Estados Unidos da América, que elegeu o presidente Donald Trump. Nessas eleições, iniciou-se a discussão sobre como as redes sociais podem influenciar no resultado, sendo que o Facebook foi acusado de favorecer a eleição do presidente[9]. Tudo isso se deve ao uso indiscriminado de algoritmos. “Na opinião de especialistas, o conteúdo do news feed é "calculado" por um algoritmo levando em conta os interesses do usuário e isso pode criar uma espécie de "bolha" que deixa de fora diferenças de opinião.”[10].

Em verdade, o Facebook direciona o conteúdo da plataforma com base nos gostos do usuário, mas esse processo não é transparente. Assim consta na política de privacidade:

> Podemos oferecer nossos Serviços, personalizar conteúdo e fazer sugestões usando essas informações para entender como você usa e interage com nossos Serviços, com as pessoas ou elementos a que

---

[9] Informação disponível em: <http://www.bbc.com/portuguese/internacional-37950265?ocid>. Acesso em: 10 set. 2017.

[10] Informação disponível em: <http://www.bbc.com/portuguese/internacional-37950265?ocid>. Acesso em: 10 set. 2017.

> você está conectado e pelos quais se interessa, dentro e fora dos nossos Serviços. (FACEBOOK, 2016)

Assim, é preciso que se tenha um processo transparente no uso de algoritmos, ante aos princípios do Direito do Consumidor. Dentre os direitos do consumidor está o de informação adequada e clara sobre os serviços. Dessa maneira, defende-se o dever de o Facebook informar sobre como é formado o conjunto de informações ao usuário.

6.1.5 Compartilhamento de informações pessoais

O MCI normatiza em seu artigo 7º, inciso VII que é assegurado ao usuário o direito de "não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de Internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei". Interpretando-se a disposição normativa, tem-se que não é permitido o compartilhamento de informações pessoais pelo Facebook, salvo se o usuário consentir expressamente.

Como já visto, em se tratando de um termo de adesão digital, não se fala em vontade livre nem em consentimento informado. Assim, entende-se nula a cláusula do termo de privacidade do Facebook que permite o compartilhamento de informações com as empresas do grupo econômico, bem como com parceiros comerciais.

> Compartilhando com as empresas do Facebook.
> Compartilhamos as informações que temos sobre você com um grupo de empresas que fazem parte do Facebook. Saiba mais sobre nossas empresas.
> Compartilhando com parceiros e clientes terceiros
> Trabalhamos com empresas terceirizadas que nos ajudam a fornecer e a melhorar nossos Serviços ou com empresas que usam anúncios e produtos relacionados, o que possibilita a operação de nossas empresas e o fornecimento de serviços gratuitos para pessoas do mundo inteiro. (FACEBOOK, 2016)

Nesse sentido, é preciso que se tenha efetivamente o consentimento informado e isso não pode ser depreendido a partir da simples adesão ao termo de uso e/ou política de privacidade. Dessa forma, como os termos de uso e política de privacidade não são sequer lidos, entende-se que não é lícito o compartilhamento, tratando-se de cláusula nula de pleno direito.

6.2 Instagram

O Instagram é uma rede social por meio da qual o usuário realiza o upload de fotos e vídeos possibilitando que seus amigos visualizem, curtam e comentem a respectiva publicação. Atualmente, o Instagram pertence ao Facebook Inc., mesma companhia que administra os serviços do Facebook.

Tratando-se de um termo de adesão digital, o contrato que rege o serviço do Instagram dispõe em seu preambulo que "se você não concorda com todos esses Termos de Uso, não acesse ou use o Serviço" (FACEBOOK, 2013) confirmando o princípio da aceitação integral.

6.2.1 Cláusula de Propriedade Intelectual

O Instagram, assim como o Facebook, possui uma cláusula restritiva de direitos no que tange à propriedade intelectual. Veja-se:

> O Instaram não reivindica a propriedade de nenhum Conteúdo que você publica no Serviço ou através dele. Em vez disso, você concede ao Instaram, por meio deste, uma licença global, não exclusiva, sublicenciável, sem royalties e totalmente paga de uso do Conteúdo que você publica no Serviço ou através dele, sujeito à Política de Privacidade do Serviço, disponível em http://instagram.com/legal/privacy/, incluindo, entre outras, as seções 3 ("Compartilhamento de suas informações"), 4 ("Como nós armazenamos suas informações") e 5 ("Suas escolhas sobre suas informações"). Você pode escolher quem visualiza seu Conteúdo e

> atividades, incluindo suas fotos, conforme descrito na Política de Privacidade. (FACEBOOK, 2013)

Assim como no Facebook, aqui o usuário cede todos os direitos patrimoniais do autor por tempo indeterminado à plataforma, o que pode significar uma renúncia à faceta patrimonial do Direito Autoral. Portanto, pelo mesmo motivo exposto no tópico 6.1.1, a referida cláusula é nula de pleno direito.

6.2.2 Transferência internacional de dados pessoais

Além da coleta dos dados pessoais, há a transferência destes para o processamento de informações.

> As suas informações coletadas através do Serviço podem ser armazenadas e processadas nos Estados Unidos ou em qualquer outro país em que o Instagram, suas Afiliadas ou Provedores de Serviço mantenham instalações.
> O Instagram, suas Afiliadas ou Provedores de Serviço podem transferir informações que coletamos sobre você, incluindo informações pessoais, através de fronteiras e do seu país ou jurisdição para outros países ou jurisdições ao redor do mundo. Se você se encontra na União Europeia ou em outras regiões com leis que regem a coleta e uso de dados que possam ser diferentes da lei dos Estados Unidos, observe que nós podemos transferir informações, incluindo informações pessoais, para um país e jurisdição que não tem as mesmas leis de proteção de dados que a sua jurisdição.
> Ao se registrar no Serviço e utilizá-lo, você concorda com a transferência de informações para os Estados Unidos ou para qualquer país em que o Instagram, suas Afiliadas ou Provedores de Serviço mantenham instalações e com o uso e divulgação de informações sobre você conforme descrito nesta Política de Privacidade.
> Nós usamos meios de proteção comercialmente aceitáveis para ajudar a manter protegidas as informações coletadas através do Serviço e tomamos medidas razoáveis (como a solicitação de uma senha exclusiva) para verificar sua identidade antes de conceder a você acesso à sua conta. Entretanto, o Instagram não pode garantir a segurança de nenhuma informação transmitida por você para o

> Instagram ou garantir que esta informação no Serviço não possa ser acessada, divulgada, alterada ou destruída.
> Solicitamos que você faça sua parte para nos ajudar. Você é responsável por manter sigilo sobre sua senha exclusiva e as informações de sua conta e por controlar o acesso a emails entre você e o Instagram, o tempo todo. Suas configurações de privacidade também podem ser afetadas por alterações que os serviços de mídia social que você usa para se conectar ao Instagram fazem em seus serviços. Nós não somos responsáveis pela funcionalidade, privacidade ou medidas de segurança de qualquer outra organização. (FACEBOOK, 2013)

Como já discutido no tópico 6.1.2, atualmente o MCI adota o sistema geográfico para a transferência internacional de dados pessoais, o que torna nula a referida cláusula. Entretanto, com a aprovação da lei para a proteção de dados a referida cláusula poderá ser considerada válida, desde que se respeitem os princípios fundamentais de proteção à privacidade.

6.2.3 Coleta de dados pessoais

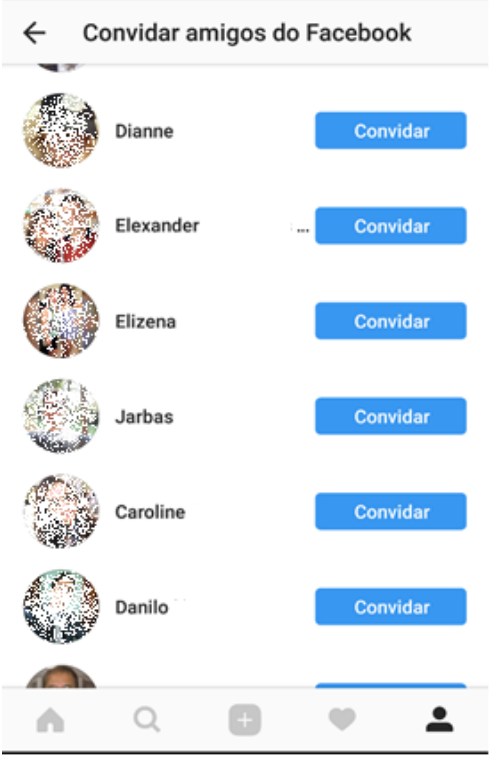
Uma cláusula que chama atenção é a coleta de dados de pessoas que sequer fazem parte da plataforma, ou seja, não se vinculam aos termos de uso e política de privacidade do Instagram. Assim dispõe o contrato:

> Nós usamos ferramentas de análise de terceiros para nos ajudar a medir o tráfego e as tendências de uso do Serviço. Essas ferramentas coletam informações enviadas pelo seu dispositivo ou pelo nosso Serviço, incluindo as páginas da Web que você acessa, extensões e outras informações que nos ajudam a melhorar o Serviço. Nós coletamos e usamos essas informações de análise com informações de análise de outros Usuários, de forma que elas não podem ser usadas razoavelmente para identificar qualquer Usuário específico individualmente. (FACEBOOK, 2013)

A plataforma admite a coleta de dados de terceiro através do dispositivo informático do usuário. Evidente que para uma rede

social funcionar, é necessário haver uma ligação entre amigos por meio da plataforma, no entanto, isso não autoriza a coleta indiscriminada de dados pessoais. Assim, quando um serviço disponibiliza uma ferramenta de convidar amigos que não fazem parte da rede, já existe um perfil pré-criado, bastando ao indivíduo publicá-lo. Veja na imagem a seguir que, ao utilizar a ferramenta de convidar um amigo para se juntar a rede, já há o nome e a foto da pessoa. Não é possível mensurar todas as informações que a plataforma possui sobre um não usuário.

Figura 1: Exemplo de perfis prontos no Instagram



Fonte: print sreen do Instagram na aba “convidar amigos do facebook”.[11]

[11] As imagens foram borradas com programa de edição de imagens e os sobrenomes ocultados para se proteger a privacidade dos usuários.

Evidente que na imagem acima foi utilizada a ferramenta de convidar um usuário do Facebook, razão pela qual presume-se que a foto e o nome foram retirados daquela plataforma. Mesmo nessa hipótese, ainda assim a coleta dessa informação foi feita sem a autorização expressa do não usuário. Veja ainda, que a plataforma Facebook também possui uma ferramenta semelhante, mas que possibilita o convite de não usuário da rede.

Figura 2: Exemplo de perfis prontos no Facebook

Fonte: print sreen da plataforma facebook. [12]

Na figura acima se constata que a plataforma cria um perfil para a usuária Érica. Este perfil ficará oculto, até que a mesma aceite os termos de uso e política de privacidade do Facebook. Com o aceite, o perfil será publicado, sendo utilizadas informações sobre o usuários que já foram coletadas antes mesmo deste ser um usuário.

No que tange à cláusula do Instagram, entende-se que a mesma é nula de pleno direito, pois um usuário está autorizando a coleta de dados sobre um não usuário que sequer tem conhecimento dos termos de uso. Como os dados pessoais refletem a personalidade do indivíduo, não é dado a terceiros o direito de cessão sobre essas informações. Não se quer afirmar que o usuário por meio do qual o Instagram fez a coleta dos dados praticou um ato ilícito, pois este

[12] O Email e o sobrenome foram ocultados para se proteger a privacidade da usuária.

não tem a possibilidade de evitar que isso aconteça. Por sua vez, a plataforma possui meios de evitar que sejam coletados dados de não usuários. Não é respeitado o direito de não ser conhecido, interpretação do direito à privacidade.

6.2.4 Uso indiscriminado de algoritmos para definição do si eletrônico

Assim como no Facebook, há o uso indiscriminado de algoritmos para o fornecimento de conteúdo direcionado ao usuário. Inclusive, a plataforma admite que utiliza algoritmo para direcionar marketing aos usuários.

> Além de alguns dos usos específicos de informações que descrevemos nesta Política de Privacidade, nós podemos usar as informações que recebemos para:
> [...]
> fornecer informações e conteúdo personalizados para você e outros, o que pode incluir anúncios online ou outras formas de marketing. (FACEBOOK,2013)

Da mesma forma que o Facebook, defende-se o dever de informação clara e adequada ao consumidor, que, muitas das vezes, não sabe porque lhe é mostrado determinado conteúdo. Não significa que não é permitido o uso de algoritmo para determinar o conteúdo da rede social, pois isso pode inclusive ser benéfico ao usuário, que irá visualizar conteúdo de acordo com seus interesses. No entanto, há a possibilidade de se controlar o pensamento do usuário, como demonstrado no tópico 6.1.4, razão pela qual é preciso cautela no tratamento dos dados pessoais.

6.2.5 Compartilhamento de informações pessoais

Como visto, o MCI normatiza em seu artigo 7º, inciso VII é direito do usuário o não fornecimento de seus dados pessoais a

terceiros. Entretanto, assim como o Facebook, o Instagram também não cumpre a legislação brasileira. Além de possibilitar o compartilhamento de informações com empresas do grupo econômico, a plataforma disponibiliza dados pessoais como 'ferramentas como cookies, arquivos de log e identificadores de dispositivo e dados de localização, com organizações de terceiros que nos ajudam a fornecer o Serviço a você" (FACEBOOK, 2013). Portanto, terceiros recebem informações pessoais dos usuários e, além disso, podem realizar a análise das informações para o direcionamento de propaganda, já que "essas informações permitem que redes de anúncio terceirizadas, entre outras coisas, forneçam propaganda direcionada que elas acreditam que seja de maior interesse para você". (FACEBOOK, 2013)

Dessa forma, acredita-se que o termo de adesão digital do Instagram é nulo neste ponto, tendo em vista que o Marco Civil da Internet não possibilita que sejam compartilhados dados pessoais com terceiros, a não ser que exista um consentimento informado do titular da informação. Até mesmo porque estas informações fogem ao princípio da finalidade, já que o único objetivo é a divulgação com parceiros para que seja feita propaganda direcionada.

6.3 Google

Google é uma empresa tecnológica que hospeda uma série de serviços online. O principal produto é o site de buscas www.google.com.br, o mais conhecido e visitado site do mundo[13]. A empresa foi fundada em 1996 por Larry Page e Sergey Brin, à época estudantes de Doutorado da Universidade de Stanford. Foi criado por eles um mecanismo que possibilitava a busca e indexação de sites de conteúdo na Internet, nascendo assim o que é conhecido

[13] Informação disponível em: <https://www.alexa.com/siteinfo/google.com>. Acesso em 10 set. 2016.

hoje como Google. Atualmente é a maior empresa de mídia eletrônica do mundo.[14]

O Google possui 72 tipos de serviços e produtos, dentre os quais destacam-se o Gmail[15], sistema Android[16], Waze[17], Google Maps[18], Google Drive[19] e YouTube. Este último é uma rede social de compartilhamento de vídeos, por meio do qual os usuários podem realizar o upload de gravações feitas ou simplesmente assistir vídeos de terceiros. Cada serviço possui um termo de uso específico, portanto este trabalho irá analisar tão somente o termo de adesão digital do YouTube, o que não implica validade absoluta dos demais termos. No que se refere à política de privacidade, existe um único documento que vale para todos os serviços Google.

6.3.1 Cláusula de Propriedade Intelectual

Assim como os demais serviços evidenciados neste trabalho, o YouTube possui uma cláusula restritiva de direitos, por meio da qual há uma cessão dos direitos patrimoniais do autor. Entretanto, por mais que não conste expressamente nos termos de uso, o YouTube possui uma regra para o compartilhamento de receitas feitas por anúncios pagos.

Ao enviar um vídeo para a plataforma, o usuário cede todos os direitos patrimoniais daquela exibição ao YouTube, porém existem empresas que compram anúncios para serem exibidas antes ou durante aquele vídeo. Assim, toda vez que um usuário qualquer assiste a um vídeo que tenha anúncios, ele gera renda ao YouTube, que reparte essa quantia com os titulares das contas.

---

[14] Informação disponível em: http://exame.abril.com.br/tecnologia/google-lidera-lista-com-principais-grupos-de-midia-do-mundo/. Acesso em: 15 set. 2017.
[15] Serviço de e-mail.
[16] Sistema operacional de smartphone.
[17] Navegador GPS.
[18] Sistema de mapas.
[19] Sistema de armazenamento em nuvem.

O cálculo feito pela rede social utiliza um algoritmo, do qual não se tem conhecimento. Entretanto, estima-se que existe um cálculo aproximado para cada mil visualizações do vídeo anúncio.

> CPM (abreviação de "custo por mil") é o valor que o anunciante paga ao YouTube a cada mil views monetizados de um vídeo. Sabe-se que o valor do CPM varia muito, o tempo todo, e o YouTube não é transparente em relação aos critérios. Tudo entra na conta: desde o valor que o anunciante se dispõe a pagar até a relevância dos canais de veiculação. Por isso não há uma tabela de valores. Mas a média é 1 dólar e pouco por mil views. (BARGAS, 2017)

Assim, há realmente uma cessão sobre os direitos patrimoniais do autor pelo vídeo enviado ao YouTube, mas a plataforma remunera parcialmente o usuário do valor que é arrecado com anúncios. Essa remuneração é indireta, ou seja, não reflete o ganho real que a plataforma teve com o vídeo, porém é uma forma de estimular os usuários a monetizarem a conta.

A cláusula restritiva do termo de adesão digital do YouTube é nula de pleno direito, mesmo com essa remuneração indireta. O correto seria remunerar o autor pelo uso comercial da obra, caso houvesse. Contudo, o dano patrimonial é minimizado pela divisão dos lucros com anúncios.

6.3.2 Renúncia e Limitação de Responsabilidade Civil

Em seu termo de adesão virtual, o YouTube estipula uma cláusula por meio da qual se exime de qualquer responsabilidade pelos conteúdos de sua rede social. Discute-se aqui a responsabilidade civil por ato de terceiro, já que assim está disposto nos termos de uso:

> Você concorda que o uso do serviço será por sua conta e risco exclusivos, até o limite permitido por lei. O Youtube, seus executivos, diretores, funcionários e representantes negam qualquer responsabilidade, expressa ou implícita, relacionada ao

serviço e ao uso dele por você. o Youtube não garante nem se responsabiliza pela precisão ou integralidade do conteúdo de seu site ou do conteúdo de qualquer site ligado ao seu, e não assume qualquer obrigação ou responsabilidade por quaisquer (i) erros, equívocos ou imprecisões de conteúdo, (ii) danos pessoais ou materiais, de qualquer natureza, que resulte do seu acesso e do uso do nosso serviço, (iii) qualquer acesso ou uso de nossos servidores protegidos e/ou toda e qualquer informação pessoal e/ou financeira ali armazenada que não tenham sido autorizados, (iv) qualquer interrupção ou cessação da transmissão de e para o nosso serviço, (iv) quaisquer bugs, vírus, cavalos-de-tróia ou afins que possam ser transmitidos para ou através do nosso serviço por qualquer terceiro, e/ou (v) quaisquer erros ou omissões em qualquer conteúdo ou qualquer perda ou dano de qualquer natureza sofrido como resultado do uso de qualquer conteúdo ou e-mail enviado, transmitido ou de outra forma disponibilizado através do serviço. o Youtube não garante, endossa, defende ou assume responsabilidade por qualquer produto ou serviço divulgado ou oferecido por terceiros através do serviço ou de qualquer hyperlink do serviço, ou exibido em qualquer banner ou outro tipo de publicidade, e o Youtube não participará nem será de nenhuma forma responsável por monitorar qualquer transação entre você e provedores terceirizados de produtos ou serviços. Como se faz na compra de um produto ou serviço por qualquer meio ou em qualquer ambiente, você deve usar o bom senso e ser cauteloso sempre que for necessário.

Em nenhuma circunstância o Youtube, seus executivos, diretores, funcionários ou representantes serão responsabilizados por qualquer dano direto, indireto, incidental, especial, punitivo ou imprevisto resultante de quaisquer (i) erros, equívocos ou imprecisão de conteúdo, (ii) danos pessoais ou materiais , de qualquer natureza, resultante do seu acesso e do uso do nosso serviço, (iii) qualquer acesso ou uso dos nossos servidores protegidos e/ou de toda e qualquer informação pessoal e/ou financeira ali armazenada que não tenha sido autorizado, (iv) qualquer interrupção ou cessação de transmissão de ou para o nosso serviço, (iv) qualquer bug, vírus, cavalos-de-troia ou afins que possam ser transmitidos para ou através do nosso serviço por quaisquer terceiros, e/ou (v) quaisquer erros ou omissões em qualquer conteúdo ou qualquer perda ou dano de qualquer natureza sofrido em consequência do uso de qualquer conteúdo ou

> e-mail enviado, transmitido ou de qualquer outra forma disponibilizado através do serviço, seja por responsabilidade, contrato, ofensa ou qualquer outra hipótese legal, e independentemente de a empresa ser alertada sobre a possibilidade de tais danos à limitação de responsabilidade acima descrita será aplicada na medida máxima permitida por lei na jurisdição competente.
> Você reconhece especificamente que o Youtube não será responsabilizado pelo conteúdo ou pela conduta difamatória, ofensiva ou ilegal de quaisquer terceiros e que o risco de prejuízo ou dano resultante dos mesmos recai inteiramente sobre você. (GOOGLE, 2017, grifo nosso)

O Marco Civil da Internet possui uma seção específica para tratar da responsabilidade por ato de terceiro, qual seja, a Seção III, intitulada de "Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros". Tratando-se de provedor de conexão, este não será responsabilizado por conteúdo gerado por terceiros, conforme disposto no artigo 18[20] da Lei. Não há que se responsabilizar o provedor de conexão, uma vez que este não possui qualquer controle sobre a informação contida na rede. A discussão paira sobre o provedor de conteúdo.

Conforme o artigo 19[21] do Marco Civil, o Provedor de Aplicações[22] somente poderá ser responsabilizado por conteúdo de terceiros após uma ordem judicial específica para, dentro de seus limites, tornar indisponível o conteúdo. Neste ponto é importante salientar que a responsabilidade surge, via de regra, após o descumprimento da ordem judicial, como se essa fosse a fonte da

---

[20] Art. 18. O provedor de conexão à Internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros. (BRASIL, 2014)

[21] Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de Internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário. (BRASIL, 2014)

[22] O Marco Civil utiliza a nomenclatura de Provedor de Aplicações em vez de Provedor de Conteúdo. A diferença entre os tipos de provedores é feita pela doutrina, sendo que o Marco Civil trata apenas de provedor de aplicação.

obrigação principal, sendo o seu descumprimento a fonte da obrigação de reparar o dano. Ou seja, pune-se a inércia do provedor em não retirar o conteúdo ofensivo. Além do caput, o artigo 19 possui quatro parágrafos que detalham como é a responsabilidade por ato de terceiros.

Prioriza-se a liberdade de expressão ao se exigir ordem judicial para a retirada de conteúdo. Isso porque não se concede ao provedor a autonomia para julgar se um conteúdo é ofensivo ou não. O que se faz é atribuir ao poder judiciário a tarefa de analisar o teor do suposto ilícito, após a requisição de alguém, para que, após, o provedor seja notificado e torne o conteúdo indisponível.

A indisponibilidade do conteúdo será feita dentro dos limites técnicos do serviço e em prazo hábil concedido pelo judiciário. Certo é que será necessária a indicação do endereço (URL), conforme determina o parágrafo primeiro[23] do artigo 19.

Evidente que a responsabilização do provedor só será possível após a notificação judicial, não bastando apenas a ocorrência do dano. Assim, é necessária uma ordem judicial para que se retire um conteúdo ofensivo da Internet. Ante a necessidade de dilação probatória e a complexidade da causa, via de regra, o processo judicial tramitará sob o rito do procedimento comum. Entretanto, existe a exceção prevista no parágrafo terceiro[24] do dispositivo legal. Tratando-se de conteúdo atentatório à honra, à reputação ou aos direitos de personalidade, a ação poderá ser ajuizada sob o rito dos Juizados Especiais.

Tratando-se dos casos supramencionados poderá existir a possibilidade de urgência no pedido. Assim, o parágrafo quarto[25]

---

[23] § 1º A ordem judicial de que trata o caput deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

[24] § 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na Internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de Internet, poderão ser apresentadas perante os juizados especiais.

[25] § 4º O juiz, inclusive no procedimento previsto no § 3o, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na Internet, desde que presentes os

admite a antecipação dos efeitos da tutela desde que presente prova inequívoca do fato, verossimilhança da alegação e fundado receio de dano irreparável ou de difícil reparação.

A responsabilidade do provedor só existirá em razão da não retirada do conteúdo, não tendo qualquer responsabilidade perante este. Tanto o é que o artigo 20[26] do Marco Civil normatiza que, se o provedor tiver o contato do usuário que causou o dano, deverá comunicar a ele o motivo da retirada. Assim se garante a liberdade de expressão e o acesso ao contraditório, tendo em vista que o usuário poderá exigir que se mantenha o conteúdo, caso entenda que não é ofensivo, devendo provar isso judicialmente.

Nesse sentido, o artigo 21[27] normatiza que o provedor de aplicações possui responsabilidade subsidiária, ou seja, só é responsabilizado se não retirar o conteúdo. Como já enfatizado, é necessária uma ordem judicial para que se determine a retirada, entretanto existe a exceção que é quando o conteúdo apresentar nudez ou ato sexual privado. Nesses casos, basta a notificação pelo usuário ou representante.

A preocupação do legislador, nesse caso, é com a volatilidade das informações na Internet. Uma vez que quando algo é disponibilizado na rede, perde-se o controle. Assim, quanto antes se

---

requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação. (BRASIL, 2014)

[26] Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de Internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de Internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização. (BRASIL, 2014)

[27] Art. 21. O provedor de aplicações de Internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo. (BRASIL, 2014)

retirar o conteúdo, menor será a chance de se espalhar. Evidente que, conforme o parágrafo único[28] do artigo 21 do MCI, a notificação deverá conter os elementos que permitam identificar o dano.

Portanto, a regra geral do Marco Civil quanto ao conteúdo ofensivo gerado por terceiro é o sistema conhecido como *Judicial Notice and Take Down*, que exige uma ordem judicial para a retirada, com a responsabilidade subsidiária do provedor. Além deste sistema, existe também o *Notice and Take Down*, que é a responsabilização com apenas a notificação extrajudicial, o que é aplicado no ordenamento jurídico brasileiro para casos com nudez explícita ou que contenham ato sexual privado. É necessário que se discutam ambos os casos para que se analise a temática da responsabilidade civil por ato de terceiros.

A jurisprudência brasileira, no que se refere à retirada de conteúdo e consequente responsabilidade civil dos provedores de aplicação, em um primeiro momento, foi construída com base na responsabilidade objetiva, aplicando-se ou a regra do parágrafo único do artigo 927 do Código Civil ou a regra do CDC, qual seja, também da responsabilidade independentemente do elemento culpa. Nesse sentido, conforme afirmam Ronaldo Lemos, Carlos Affonso Pereira de Souza e Sérgio Branco Vieira Junior (2010), a ausência de legislação específica implicava tal regramento.

Sobre a responsabilidade objetiva, Marcelo Leonardi (2005) afirma que dois são os argumentos para a aplicação da responsabilidade objetiva. São eles: a dificuldade de encontrar o responsável e a natureza econômica. Entretanto, o próprio autor rechaça tais argumentos, visto que a responsabilidade objetiva geraria um dever de vigilância contínua, que muitas vezes pode ser impossível fática e tecnicamente. Assim, Vainzof (2014) afirma que esse dever poderia acarretar em censura prévia, pois muitos conteúdos poderiam ser retirados sem um regramento claro.

---

[28] Parágrafo único. A notificação prevista no caput deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido. (BRASIL, 2014)

Todavia, ainda antes da vigência do Marco Civil, a regra construída pelo STJ foi a da responsabilidade civil do provedor de serviço por ato de terceiro, calcada no *Notice and Take Down*. Isso significa que bastava a notificação extrajudicial do provedor para que surgisse para este o dever de retirar o conteúdo ofensivo, sob pena de responsabilização. Sobre a regra, cita-se o acórdão 1402104/RJ julgado pela quarta turma do STJ em 27/05/2014.

> Este Tribunal Superior, por seus precedentes, já se manifestou no sentido de que: I) o dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site por usuário não constitui risco inerente à atividade desenvolvida pelo provedor da Internet, porquanto não se lhe é exigido que proceda a controle prévio de conteúdo disponibilizado por usuários, pelo que não se lhe aplica a responsabilidade objetiva, prevista no art. 927, parágrafo único, do CC/2002; II) a fiscalização prévia dos conteúdos postados não é atividade intrínseca ao serviço prestado pelo provedor no Orkut.
> 2. A responsabilidade subjetiva do agravante se configura quando: I) ao ser comunicado de que determinado texto ou imagem tem conteúdo ilícito, por ser ofensivo, não atua de forma ágil, retirando o material do ar imediatamente, passando a responder solidariamente com o autor direto do dano, em virtude da omissão em que incide; II) não mantiver um sistema ou não adotar providências, que estiverem tecnicamente ao seu alcance, de modo a possibilitar a identificação do usuário responsável pela divulgação ou a individuação dele, a fim de coibir o anonimato. (BRASIL. Superior Tribunal de Justiça, 2014)

Assim, até a vigência do Marco Civil bastava a notificação extrajudicial do usuário para que originasse a obrigação de retirada de conteúdo ofensivo. Não havia a responsabilidade pelo controle do conteúdo, mas tão somente pela retirada após a solicitação do usuário. Tal regra é comum em outros países, como por exemplo os integrantes da União Europeia e os Estados Unidos (DIXON, 2009).

Com esse sistema é possível minorar os danos a um usuário, tendo em vista que o sistema extrajudicial é de certo mais célere do que um sistema judicial. Entretanto, existe a possibilidade de se

limitar a liberdade de expressão dos usuários. Isso decorre do fato de que o provedor é quem irá realizar a análise do que é ofensivo ou não. O problema é estabelecer quais serão os parâmetros utilizados. A depender do caso, é possível que um conteúdo que não seja ofensivo seja retirado, ao passo que um conteúdo ofensivo pode não ser retirado devido à análise do provedor.

Por isso, afirma-se que o sistema *Judicial Notice and Take Down* garante a liberdade de expressão. Nesse sentido, havendo um dano, que, conforme Leonardo Poli "é a lesão de um interesse juridicamente protegido, contra a vontade do prejudicado" (POLI, 2009, p. 581), deverá o sujeito passivo acionar o judiciário para que solicite a retirada do conteúdo da Internet, salvo as exceções previstas no ordenamento jurídico brasileiro.

Claro que a melhor saída para se coibir a existência de conteúdos ofensivos é a educação dos usuários. Tanto o é que o Marco Civil, em seu artigo 26, normatiza ser um dever a inclusão em todas as esferas e níveis de ensino a capacitação para o uso seguro, consciente e responsável da Internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Entretanto, em pesquisa realizada pela Federação do Comércio de São Paulo (2016), demonstrou-se que a maioria das escolas (95,6%) do Estado de São Paulo não possui a disciplina Educação Digital em suas grades curriculares. Ainda, apenas 4,75% das escolas privadas adotaram a disciplina que o artigo 26 do Marco Civil da Internet se refere. Entre as escolas públicas, a porcentagem cai para apenas 1%, sendo que 83% das instituições de ensino não sabem o que é o Marco Civil da Internet. Além disso, 65,9% das instituições afirmaram que não há a intenção de incluir a nova disciplina na grade curricular. Ao invés de se tentar reparar o dano, é melhor evitar a ocorrência deste, o que perpassa pelos planos da educação.

Dentre as políticas e diretrizes da União Europeia está a retirada de conteúdos ofensivos através de notificação extrajudicial.

Assim, pode o usuário do Facebook requerer diretamente à plataforma a retirada do conteúdo, invocando para si o uso da diretiva Europeia, o que deverá ser atendido pelo provedor.

Como visto, nos termos de uso do YouTube há uma cláusula que retira totalmente a responsabilidade da plataforma. Porém, com base no Marco Civil da Internet, casos que envolvam nudez ou ato sexual privado atraem a responsabilidade para a plataforma com a simples notificação extrajudicial. Portanto, em um primeiro momento a cláusula é válida, visto que não existe responsabilidade pelo controle das informações postadas pelos usuários, porém, a depender do tipo de conteúdo, a simples notificação atrai para a plataforma a responsabilidade, que como visto é subsidiária.

6.3.3 Coleta, tratamento, uso e transferência de dados pessoais

A coleta, tratamento uso e transferência de dados pessoais é regulamentada pela política de privacidade do Google. O serviço oferecido pelo Google evoluiu junto com a Internet, o que proporciona uma análise de quais informações eram coletadas pela plataforma no início e quais são hoje.

Na primeira política de privacidade feita pelo Google, datada de 4 de janeiro de 2001[29], as informações coletadas eram basicamente as fornecidas ativamente pelo usuário. Havia a coleta de informações de log de conexão, tais como endereço IP, local e hora da conexão, porém não havia o uso de informações coletadas sem que o usuário soubesse. Isso mudou com o advento das redes sociais, momento em que se começou a cruzar cada vez mais as informações pessoais.

A primeira atualização da política de privacidade do Google foi feita em 14 de outubro de 2005, logo após a criação do Orkut, primeira rede social da companhia, criada no fim de 2004. Com a

[29] Informação disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/archive/20010104/>. Acesso em 10 set. 2017

atualização, a plataforma passou a utilizar informações obtidas pela comunicação dos usuários dentro da própria plataforma. Veja-se:

> Informação de Arquivo – Quando você usa os serviços do Google, os nossos servidores automaticamente registram a informação que o seu browser envia sempre que você visita um site da web. Estes registros do servidor podem incluir informação, tal como solicitação da web, idioma do browser, data e hora de sua solicitação e um ou mais cookies que podem identificar o seu browser. [30]

Após essa atualização, diversas pequenas mudanças foram feitas, até que em 3 de outubro de 2010, com o uso da tecnologia GPS – Global Position System – em dispositivos domésticos, a plataforma iniciou a coleta destas informações. Assim foi disposto nos termos de uso:

> O Google oferece serviços com base em localidades, como o Google Maps e o Google Latitude. Caso você use esses serviços, o Google pode receber informações sobre sua localização real (como sinais de GPS enviados por um aparelho celular) ou seu local aproximado (como um ID do celular). [31]

Já em 1 de março de 2012 a companhia ampliou ainda mais o espectro de informações coletadas. Além das já expostas, passou-se a coletar informações do dispositivo, isso em virtude do aumento da capacidade de processamento dos smartphones. Assim está disposto nos termos de uso:

> Podemos coletar informações específicas do dispositivo (como seu modelo de hardware, versão do sistema operacional, identificadores exclusivos de produtos e informações de rede móvel, inclusive número de telefone). O Google pode associar seus

---

[30] Informação disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/archive/20051014/>. Acesso em 10 set. 2017

[31] Informação disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/archive/20101003/>. Acesso em: 10 set. 2017

> identificadores de dispositivo ou número de telefone com sua Conta do Google. [32]

A última atualização da política de privacidade foi feita em 17 de abril de 2017. O termo é elucidativo e abarca diversas dúvidas que o usuário possa vir a ter. Na atual versão, seis produtos do Google possuem regras específicas, que podem ser acessadas em apartado, são eles o Google Chrome[33] e Chrome OS[34], Play Livros[35], Payments[36], Fiber, Project Fi[37]. e o G Suite for Education[38]. Os demais serviços são regulados pela política geral de privacidade.

No uso dos dados pessoais, existe uma condição que pode ser considerada nula de pleno direito, qual seja, a que possibilita a alteração de informações feita pela plataforma mediante a coleta de dados passiva do usuário. Veja-se:

> Podemos usar o nome que o usuário fornece em seu Perfil do Google em todos os serviços que oferecemos e que exijam uma Conta do Google. Além disso, podemos substituir seus nomes antigos associados com sua Conta do Google de modo que o usuário esteja representado de maneira consistente em todos nossos serviços. Se outras pessoas já tiverem o e-mail ou outras informações que identifiquem o usuário, nós podemos mostrar-lhes estas informações do Perfil do Google que são publicamente visíveis (como nome e foto). (GOOGLE, 2017)

Conforme disposto acima, o Google poderá alterar as informações sobre usuário mediante a coleta de informações sem que o mesmo tenha fornecido ativamente, ou seja, não é respeitado o princípio do livre consentimento e direito do usuário de modificar suas informações pessoais. Mais que isso, a plataforma poderá

---

[32] Informação disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/archive/20120301/>. Acesso em: 10 set. 2017

[33] Navegador de Internet.

[34] Navegador de Internet.

[35] Serviço de leitura de E-books.

[36] Serviço de pagamento digital.

[37] Um projeto do Google para o fornecimento de redes WiFi

[38] Plataforma voltada para o ensino

cruzar informações de usuários, coletando informações sobre pessoas que sequer utilizam algum serviço da companhia.

Assim como os demais serviços evidenciados neste trabalho, o Google pode "processar as informações pessoais do usuário em um servidor localizado fora do país em que este vive" (GOOGLE, 2017). Portanto, há também a transferência internacional de dados pessoais, que, conforme visto, fere o Marco Civil da Internet.

7

Os shadow profiles e a violação dos direitos de personalidade dos usuários e dos não usuários das redes sociais

Ao se utilizar a Internet, a privacidade deveria ser uma preocupação constante dos usuários. Entretanto, estes não têm o hábito de ler os termos de uso, não que isso tenha algum efeito na proteção de sua privacidade, pois nada poderá ser modificado. Mas existe a possibilidade de, conhecendo a política de privacidade, o usuário decida a forma como irá utilizar a rede.

Existem maneiras de se conscientizar quanto à privacidade na rede. Uma delas é o projeto "Terms of Service; Didn't Read"[1], que em tradução livre seria "Termos de serviço: não os li". O referido projeto disponibiliza de maneira bem simplificada e intuitiva as regras que as principais plataformas utilizam em suas políticas de privacidade e termos de uso.

A privacidade deve ser uma preocupação pelo fato de que atualmente os usuários não são meros expectadores da Internet, ao contrário, tornam-se cada vez mais atores, participando efetivamente da construção da rede. Isso ocorre em razão do que se denomina de Web 2.0 (O'REALLY, 2005). O referido fenômeno caracteriza a Internet como uma rede a ser alimentada tanto pelos provedores quanto pelos usuários.

---

[1] Informação disponível em: <https://tosdr.org/>. Acesso em: 10 ago. 2016.

Como visto, o Facebook, por exemplo, possui muito mais conteúdo postado pelos usuários do que fornecido pela plataforma. Conforme (LEVERAGE, 2014), a cada segundo os usuários compartilham aproximadamente um milhão de links.

É evidente a importância que as redes sociais têm na vida das pessoas, tendo em vista o aumento constante no uso destas. Mais ainda, por ser um fenômeno recente, ainda não se tem uma cultura sólida formada a respeito do uso da Internet, o que leva a um mau uso da ferramenta.

Importante demonstrar que, quanto à política de privacidade, vigora o princípio da aceitação integral, ou seja, não é possível discordar com os termos de uso ou política de privacidade. Dentre as principais regras do Facebook, principal rede social em operação, estão as que permitem a coleta de todas as informações que o usuário fornece sobre ele e sobre outros; coleta de informações sobre o usuário fornecidas por terceiros; coleta de algumas informações que o usuário não fornece à plataforma; e a coleta de informações sobre redes e conexões.

O usuário, muitas vezes, não sabe exatamente quais as suas informações que o provedor possui. Assim, cada vez mais se caminha para um consentimento afirmado, ou seja, mais do que clicar em "Eu declaro que li e concordo com os termos de uso e a política de privacidade" de cada provedor, é preciso que o usuário tenha o conhecimento de forma clara e objetiva ao que estará exposto caso utilize o serviço, dando a ele o controle sobre suas informações pessoais. Dessa maneira, estará tutelada a privacidade do usuário na rede mundial de computadores.

Em verdade, quando um provedor de conteúdo utiliza um dado pessoal, geralmente é para venda e/ou marketing. Fala-se hoje em ditadura do algoritmo. Todos têm uma reputação digital, ou seja, são avaliados de acordo com os seus próprios hábitos. Isso pode influenciar em diversas esferas da vida do usuário. Veja que já há o registro de uma patente pelo Facebook que objetiva a concessão de

empréstimo com base nos amigos que se tem na rede (JUNQUEIRA, 2015).

Evidente que a privacidade remonta a ideia do "Right to be let alone", ou seja, o Direito de ser deixado só. Mas é difícil se afirmar o que é íntimo e o que é privado na rede, tratando-se de uma diferenciação teórica (LEORNADI, 2011). Assim, não se diz que a informação deva ser mantida em segredo para que garanta ao usuário a sua privacidade. No Direito Digital, conforme Stefano Rodotà (2014), a privacidade remonta ao direito de seguir a própria informação onde quer que ela esteja e de se opor a qualquer interferência. Fala-se no governo de si, ou seja, a possibilidade de se afirmar na rede.

No que diz respeito aos *Shadow Profiles*, tal prática foi conhecida através do caso Max Schrems vs. Facebook. Em 2011, o estudante de direito austríaco Max Schrems apresentou uma reclamação contra o Facebook após ter solicitado uma cópia *off-line* de todos os seus dados (COMPLAINT, 2016). Foi constatado que a rede social possuía muito mais informação do que ele havia fornecido. Ou seja, era mantido um perfil sombrio, que não aparecia para ele, mas que a rede sabia da existência para classificar o usuário de acordo com seus hábitos e gostos.

Andrew Noyes, gerente de relações públicas do Facebook, ao responder a acusação, negou veemente que mantinha perfis sombras, ao argumento de que:

> Nós podemos enviar e-mails para seus amigos, convidando-os a entrar no Facebook. Mantemos endereço de e-mail e nome para que você saiba quando eles se juntam o serviço dos convidados. Esta prática é comum entre quase todos os serviços que envolvem convites de compartilhamento de documentos para o planejamento do evento. A afirmação de que o Facebook está fazendo algum tipo de perfil sombrio é simplesmente errado, além disso, o Facebook oferece mais controle do que outros serviços, permitindo que as pessoas a eliminar o seu endereço de e-mail do Facebook ou recusar convites que recebem.

> Além disso, como parte de oferecer às pessoas os serviços de mensagens, que permitem que as pessoas possam eliminar mensagens que recebem na sua caixa de entrada e mensagens que enviam. No entanto, as pessoas não podem excluir uma mensagem que enviar a partir de caixa de entrada do destinatário ou uma mensagem que você recebe de pasta enviadas do remetente. Esta é a maneira que cada serviço de mensagens trabalha. Achamos que é também consistente com as expectativas das pessoas. Estamos ansiosos para fazer esses e outros esclarecimentos à DPA irlandês. (LOCKE, 2016, tradução nossa)[2]

Como visto, afirma-se que "o Facebook está mapeando a população em uma conexão social com ou sem a ajuda do usuário" (RUTHRUFF, 2016, tradução nossa)[3]. Nesse contexto, observa-se o que se denomina big data, ou sociedade da informação.

7.1 A tutela da privacidade na era da ausência da privacidade

Com o avanço da Internet, cada vez mais os usuários têm a sua vida privada exposta, sem que isso implique violação à privacidade, em vista de que a informação foi fornecida ativamente por estes. Entretanto, ao se trabalhar com a ideia de um perfil sombrio, é necessário que se repense a tutela da informação pessoal que não foi fornecida ativamente pelo usuário, porém captada pela plataforma.

---

[2] Tradução de: "We enable you to send e-mails to your friends, inviting them to join Facebook. We keep the invitees' e-mail address and name to let you know when they join the service. This practice is common among almost all services that involve invitations--from document sharing to event planning--and the assertion that Facebook is doing some sort of nefarious profiling is simply wrong. In addition, Facebook offers more control than other services by enabling people to delete their e-mail address from Facebook or to opt-out of receiving invites.
Also, as part of offering people messaging services, we enable people to delete messages they receive from their inbox and messages they send from their sent folder. However, people can't delete a message they send from the recipient's inbox or a message you receive from the sender's sent folder. This is the way every message service ever invented works. We think it's also consistent with people's expectations. We look forward to making these and other clarifications to the Irish DPA."

[3] Tradução de: "Facebook is mapping the human population one social connection at a time with or without your help."

Para isso, propõe-se uma leitura sob a teoria de Stefano Rodotà (2010), em seu livro "La vida y las reglas: Entre el derecho y el no derecho". Rodotà (2010) afirma que se vive em uma sociedade saturada de lei, na qual o direito está presente em âmbitos desnecessários e ausente em âmbitos necessários. A partir dessa afirmação, ele mostra um aspecto histórico, qual seja, em sociedades antes dominadas exclusivamente por regras religiosas, a lei era imposta, imutável. Com a ruptura, passando a um estado laico, a lei passa a ser fruto da atividade humana, o que faz dela autônoma. Aqui cabe inclusive citar a reflexão de Kelsen (2006) sobre o sistema estático e dinâmico de ordenamentos. Para o referido autor, um sistema normativo pode ser estático ou dinâmico, a depender da derivação de conteúdo da norma pressuposta fundamental. Havendo derivação de conteúdo da norma pressuposta fundamental, estar-se-á diante de um sistema estático, no qual a mudança normativa será quase nula. Por sua vez, não havendo derivação de conteúdo, mas tão somente de validade formal, estar-se-á diante de um sistema dinâmico, que aceita mudanças ao longo do tempo. Enquanto que em relações pautadas pela religião não há (ou quase não há) mutação de normas por haver derivação de conteúdo, o mundo do direito clama por mudança. Isso porque as relações sociais são reguladas pelo direito e elas mudam constantemente. Rodotà (2010) afirma que o modelo laico tem o direito como único remédio social, o que se contrapõe a um modelo de religião.

Nesse sentido, constata-se que o Direito está condicionado por novas realidades e tenta proteger o indivíduo dos abusos do Estado, o que o leva a ser autoritário, pois "Não há nada no mundo que o direito não queira tocar" [4] (RODOTÀ 2010, p. 33, tradução nossa). Mais ainda, nada humano pode ser considerado estranho ao direito.

Esse positivismo entra em crise, não no sentido pejorativo da palavra, mas no sentido de mudança, com a constatação de que o Direito deixa de ser um instrumento de defesa e passa a ser um

[4] Tradução de: "No hay nada em el mundo que ele derecho no quiera tocar, disciplinar, poseer."

instrumento de agressão. Assim, o direito passa a ter um limite, qual seja, a pessoa humana. Com a constatação de que se regulam coisas que não deveriam ser do direito, questiona-se se a ausência deste remeteria a um vazio. Rodotà afirma que não, o não direito não remete a um vazio. Essa visão da autonomia privada não se trata de um retrocesso, na verdade, é uma mudança de intervenção pública para privada, até mesmo porque "um vazio no direito pode defini-lo melhor do que a sua presença."[5] (RODOTÀ 2010, p. 39, tradução nossa).

Com esse apanhado geral, percebe-se que há sim um limite para o Direito, qual seja, a pessoa humana, sendo que não se pode considerar que o não direito remete a um vazio. Partindo dessa premissa, Rodotà define o Direito como "um aparato simbólico que estrutura a organização social quando se sabe que algumas de suas normas estão destinadas a não serem aplicadas" [6] (RODOTÀ, 2010, p. 60, tradução nossa).

O direito pode ser visto como um instrumento de pacificação, utilizado em último caso, o que o Rodotà (2010) afirma ser aplicado ao Direito Penal, a "reserva de código". Um direito mínimo não supõe necessariamente uma diminuição do controle da atividade do indivíduo. Na ótica do penal, ele afirma existirem alternativas, tais como o ressarcimento da vítima, substituição por uma sanção administrativa. A mesma lógica é a que Rodotà afirma se aplicar à desregulação, que não se identifica como uma menor quantidade de regras jurídicas, mas uma menor quantidade de regras públicas, que deixa aos particulares a liberdade para determinar sua atividade, ou seja, uma maior autonomia privada. Analisando a teoria de Rodotà (2010), tem-se que a falta de uma norma jurídica não implica a falta de proteção do ser humano, pois com a crise do positivismo e a repersonificação do Direito Privado, este passou a ser o pilar central do ordenamento jurídico.

---

[5] Tradução de: "Hay ausências que, como em la vida, pesan muho más que las presencias."

[6] Tradução de: "El derecho es um aparato simbólico que estrutura la organización soal incluso cuando se sabe que algunas de sus normas están destinadas a no ser aplicadas."

Situações que antes não eram imaginadas não clamam necessariamente a criação de uma nova norma para que se tutele os interesses do indivíduo. Como visto no capítulo 4, basta que se faça uma interpretação dos conteúdos da privacidade para que se tenha a proteção do usuário na Internet.

7.2 O *Shadow Profile* do usuário

Todo usuário de uma rede social precisa concordar com os termos de uso e política de privacidade para que possa utilizar os serviços oferecidos pela plataforma. Com isso, ainda que não tenha um consentimento livre, esclarecido e informado, o usuário aceita que seus dados pessoais sejam coletados. Toda informação coletada pela plataforma que não seja fornecida ativamente pelo usuário compõe o seu *shadow profile*. É como se existisse um perfil do usuário visível apenas para a plataforma e seus parceiros comerciais, por meio do qual é definido o padrão daquela pessoa. Haveria violação da privacidade do usuário?

Como visto, a nova leitura do direito de privacidade importa, dentre outros contornos, o direito de autodeterminação, pelo qual se garante que o usuário tenha poder de controle sobre os seus dados pessoais, garantindo que ele possa se abster do uso de suas informações em determinadas maneiras. Em verdade, a análise feita ao longo deste trabalho evidenciou que o usuário, na maioria das vezes, sequer lê os termos que regulam a relação. Além disso, o usuário não tem poder de controle sobre sua informação, visto que as companhias utilizam os dados pessoais destes para os mais diversos fins, tais como marketing e direcionamento de conteúdo com base em algoritmos.

Na denúncia feita por Max Schrems (COMPLAINT, 2016), foi constado que a plataforma havia coletado diversas informações de seus dispositivos, tais como e-mail secundário e número de telefone. Essas informações foram repassadas após o estudante austríaco ter requerido uma cópia offline de suas informações. Questiona-se

quais seriam as informações que a plataforma possui e que sequer foram repassadas ao usuário.

Falta transparência no tratamento de dados pessoais, razão pela qual é necessário que se tenha um mecanismo de defesa para que se tutele a privacidade do usuário. Evidente que não é necessária uma legislação sobre o assunto, porém, caso uma norma estabelecesse um programa de transparência, ter-se-ia a possibilidade de controlar ainda mais o uso desenfreado de dados pessoais.

Uma mudança significativa seria a inserção na lei para a proteção de dados pessoais de uma norma estabelecendo que o dado coletado pertence ao usuário e não à plataforma, sendo que se pode ter apenas uma cessão de direitos temporária para o tratamento destes. Dessa forma, o usuário poderia ter total controle sobre suas informações, já que os dados dela extraídos lhe pertenceriam.

Outra mudança a ser pensada é a criação de uma agência reguladora para a regulamentação do mercado que tenha o tratamento de dados pessoais. Agência reguladora é uma pessoa jurídica de Direito público interno, geralmente constituída sob a forma de autarquia especial ou outro ente da administração indireta, cuja finalidade é regular e/ou fiscalizar a atividade de determinado setor da economia de um país.

Com a criação de uma agência reguladora, as companhias sofreriam fiscalização, por meio da qual haveria a possibilidade de identificar falhas e ilegalidades na coleta, uso, armazenamento e tratamento de dados pessoais. Em verdade, a tutela individual da proteção da privacidade, no atual patamar da sociedade, não se revela eficaz para a proteção deste direito, posto que os usuários muitas das vezes não têm acesso aos reais usos das informações coletadas.

7.3 O *Shadow Profile* do não usuário

Além das informações de um usuário, uma plataforma coleta dados sobre não usuários, razão pela qual quando uma pessoa

recebe um convite para integrar determinada rede social, já há um *pré-perfil*, bastando que se faça a ativação dele. Ao receber um convite do usuário A, o não usuário recebe a informação de que, além de A, os usuários B, C e D, que são seus amigos na vida real, também fazem parte da rede. Como poderia a plataforma saber que aqueles indivíduos também são amigos na vida real? Isso só é possível através da coleta e processamento de informações do não usuário, criando-se uma espécie de perfil, sendo que para sua ativação basta que a pessoa faça a adesão aos termos de uso e política de privacidade. Isso se denomina *shadow profile* do não usuário, um perfil sombrio que já existe para a plataforma, bastando a ativação da pessoa para que ele seja publicado.

A essência de qualquer rede social é a conexão de pessoas e, para isso, na Internet se faz necessária a coleta de uma vasta gama de informações sobre contatos para o bom funcionamento da plataforma. Assim, não se trata de uma violação de direitos à coleta de informações da agenda de contatos de um usuário para que se faça a conexão entre ele e seus amigos que já existem na plataforma. Porém, isso não pode servir como uma forma de a rede social angariar mais consumidores, realizando o registro de informações de não usuários, fazendo uma rede de conexão destes e enviando convites para que estes ativem os perfis que já vão estar praticamente prontos.

Trata-se do direito de não ser conhecido. Ora, se uma pessoa não se registrou em uma rede social, não é permitido que uma plataforma qualquer faça a guarda de informações sobre essa pessoa. Pelo atual estágio da tecnologia, um usuário possui sobre um não usuário informações como nome, e-mail, telefone, data de aniversário e fotos, as quais são armazenas na agenda de contatos do seu smartphone, fazendo com que a plataforma acesse tais informações. O avanço da tecnologia é exponencial, razão pela qual não se sabe quais informações serão armazenadas sobre os contatos no futuro. Assim, o risco de se permitir a coleta dessas informações é alto.

Um questionamento que se pode ter é a possível violação de privacidade de uma pessoa que não utiliza uma determinada rede social caso algum usuário faça o upload de uma foto daquela. Nesse caso, entende-se que não há qualquer violação de privacidade puramente pelo ato de a rede social ter uma foto de um não usuário em um perfil de um usuário, pois a simples veiculação de uma fotografia por terceiro não é caracterizador de um ilícito civil indenizante[7]. É necessário que se tenha interesse econômico na divulgação, conforme Súmula 403 do STJ, que dispõe que "Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais". Evidente que o não usuário possui o direito de ajuizar uma ação pleiteando a retirada deste conteúdo, utilizando o seu direito de esquecimento e de apagamento, tendo em vista se tratar de um ato ilícito, que conforme Leonardo Macedo Poli (2009), é todo ato antijurídico, ainda que não seja indenizante. Felipe Braga Netto (2003) classifica os ilícitos segundo a eficácia destes:

> a) Ilícito indenizante: é todo ilícito cujo efeito é o dever de indenizar. Não importa o ato que está como pressuposto normativo. Se o efeito é reparar, in natura ou in pecunia, o ato ilícito praticado, estaremos diante de um ilícito indenizante.
> b) Ilícito caducificante: é todo ilícito cujo efeito é a perda de um direito. Também aqui não importa os dados de fatos aos quais o legislador imputou eficácia. Importa, para os termos presentes, que se tenha a perda de um direito como efeito de um ato ilícito. Sendo assim, teremos um ilícito caducificante.
> c) Ilícito invalidante: é todo ilícito cujo efeito é a invalidade. Se o ordenamento dispôs que a reação pelo ato ilícito se daria através da negação dos efeitos que o ato normalmente produziria, em virtude da invalidade, o ato é invalidante, que engloba tanto a nulidade quanto a anulabilidade.

---

[7] Diferente da súmula, Anderson Schereiber (2011) leciona que a imagem e a honra são direitos distintos. Assim, a simples violação do direito de imagem já gera o dever de indenizar, independente da finalidade econômica da divulgação. Para o autor, não é necessário que com a violação da imagem se atinja também a honra do titular, tendo em vista a autonomia dos bens jurídicos tutelados.

> d) Ilícito autorizante: é todo ilícito cujo efeito é uma autorização. Assim, em razão do ato ilícito, o sistema autoriza que a parte prejudicada pratique determinado ato, geralmente em detrimento do ofensor. (BRAGA NETTO, 2003, p. 101)

Portanto, nem todo ato ilícito é indenizante, o que faz com que a súmula do STJ não implique na validade da publicação de fotografia sem a autorização do titular em rede social. Sobre a inclusão de fotos de um não usuário na Internet, acredita-se que se trata de um ilícito invalidante, já que o efeito é a exclusão dos dados pessoais coletados sem autorização.

7.4 A informação como meio de exploração e a sua valorização na sociedade

A Internet deve ser livre, sem a interferência do Estado no sentido de retirar do usuário a sua liberdade de se manifestar. Entretanto, o que acontece é um aumento da vigilância para que se garanta a privacidade dos usuários. Trabalha-se com a teoria do utilitarismo de Jeremy Bentham e John Stuart Mill (BITTAR, ALMEIDA, 2016), segundo a qual se afirma que as ações são boas quando tendem a promover a felicidade e más quando tendem a promover o oposto da felicidade, existindo o princípio do bem-estar máximo. Assim, "o aumento do vigilantismo leva a esse perigoso senso de que não importam mortos, feridos, ou direitos revogados, tudo é colateral para se alcançar o resultado, a justiça está apenas nos olhos que observam fixos o monitor" (PINHEIRO, 2016, p. 482). Portanto, é preciso que se garanta a privacidade dos usuários, sem que isso implique uma máxima intervenção estatal.

Alvin Tofler (1980) classifica a informação como o bem mais valioso da sociedade moderna. Evidente que a informação pessoal é hoje muito importante, já que é possível construir um perfil de consumo através de pesquisas de gostos. O que se quer afirmar é que o aumento da capacidade de processamento de dados pessoais faz com que os usuários sejam classificados como um mero dado

estatístico, atribuindo-lhes características de consumo, fornecendo informação à medida que a plataforma julgue necessário.

Admitir essa categorização dos indivíduos mediante algoritmos pode propiciar um panorama perigoso. A China, por exemplo, planeja avaliar todos os cidadãos com uma nota, por meio da qual serão concedidos diversos serviços. O país iria atribuir a nota com base nos serviços tomados. (CHINA..., 2016)

Planeja-se até o ano de 2020 realizar uma categorização dos cidadãos chineses através de uma nota. Entretanto, antes de implementar o projeto em nível nacional, a China concedeu uma licença a oito grandes companhias para criarem sistemas e algoritmos para os escores de crédito social (BOTSMAN, 2017).

Uma das companhias autorizadas é a Sesame Credit, a qual pertence ao Ant Financial Services Group, afiliada da Alibaba, uma das maiores companhias de comércio eletrônico do mundo. A referida companhia vende produtos de seguros e fornece empréstimos a pequenas e médias empresas, admitindo "que julga as pessoas pelos tipos de produtos que compram" (BOTSMAN, 2017, tradução nossa)[8]. Existem cinco fatores que influenciam na avaliação, quais sejam, o histórico de crédito, cumprimento de obrigações pretéritas, informações pessoais como endereço e número de telefone, comportamento e relações interpessoais.

Com base nas avaliações feitas pelo governo chinês, possivelmente "pessoas com baixas classificações terão velocidades mais lentas na Internet; acesso restrito a restaurantes e perda do direito de viajar." (BOTSMAN, 2017, tradução nossa)[9]. Com o referido sistema, as pessoas serão reduzidas a uma nota que irá determinar quais tipos de serviços se poderão ter acesso.

> As pontuações influenciarão no aluguel de uma pessoa, sua capacidade de obter seguro ou um empréstimo e até mesmo

[8] Tradução de: "Admits it judges people by the types of products they buy"

[9] Tradução de: "People with low ratings will have slower Internet speeds; restricted access to restaurants and the removal of the right to travel"

> benefícios de previdência social. Cidadãos com escores baixos não serão contratados por certos empregadores e serão proibidos de obter alguns empregos, inclusive no serviço civil, no jornalismo e nas áreas jurídicas, onde é claro que você deve ser considerado confiável. Os cidadãos de baixa avaliação também serão restritos quando se trata de se inscrever ou de seus filhos em escolas privadas de alto pagamento. Não se está fabricando essa lista de punições. É a realidade que os cidadãos chineses enfrentarão. (BOTSMAN, 2017, tradução nossa)[10]

Existe um exemplo na arte que retrata os perigos da categorização do indivíduo com base em nota: o episódio "Nosedive", primeiro da terceira temporada da série Black Mirror.

O episódio conta a história de Lacie Pound, uma mulher no auge da juventude que vive em um mundo onde as pessoas podem avaliar popularidades com cinco estrelas. Lacie, mora com seu irmão Ryan que tem um índice de aprovação baixo e não se preocupa com isso, ao contrário de sua irmã, que possui um índice 4.2 e deseja aumentá-lo para que possa conseguir um financiamento imobiliário em uma vizinhança melhor. A fim ser capaz de ter recursos para viver lá, Lacie deveria possuir uma avaliação de 4.5 ou acima. Lacie é amiga de infância de Naomi, uma influenciadora que possui um índice de 4.8. Naomi convidou Lacie para ser madrinha de seu casamento, que seria realizado em sua ilha particular, em meio do seu círculo social de classificação alta. Lacie acredita que se ela entregar um discurso de honra perfeito, sua classificação será elevada até os 4.5 que ela precisa. Na sua casa, antes de entrar no táxi com destino ao aeroporto, Lacie tem uma discussão com seu irmão e perde pontos na avaliação, que custaram a impossibilidade de viajar para a ilha de avião. Importante argumentar que tudo na

---

[10] Tradução de: "Scores will influence a person's rental applications, their ability to get insurance or a loan and even social-security benefits. Citizens with low scores will not be hired by certain employers and will be forbidden from obtaining some jobs, including in the civil service, journalism and legal fields, where of course you must be deemed trustworthy. Low-rating citizens will also be restricted when it comes to enrolling themselves or their children in high-paying private schools. I am not fabricating this list of punishments. It's the reality Chinese citizens will face."

sociedade era baseado na pontuação, desde os preços até as condições especiais. Lacie optou por alugar um veículo para viajar durante nove horas, porém ao ficar sem combustível teve que pedir carona. Ela consegue uma carona de uma motorista de caminhão que revela que também estava obcecada com classificações até que seu marido não recebeu um tratamento de câncer vital porque ele tinha uma avaliação de 4.3 ao invés de um 4.4. No caminho até a ilha, muitos acontecimentos fazem com que a avaliação de Lacie caia para 2,6, razão pela qual Naomi liga para ela dizendo não ser mais bem-vinda ao casamento. Lacie persiste e decide ir de qualquer maneira e se infiltra na ilha, já que sua classificação é muito baixa para entrar oficialmente e bloqueia a recepção de casamento. Lacie é presa e tem a tecnologia para ser classificada confiscada.[11]

A série traz reflexões de como a avaliação que os usuários têm pode ser vital para a manutenção de contratos. Observe que a realidade não é muito distante da ficção, já que o Facebook patenteou (JUNQUEIRA, 2015) uma ferramenta de concessão de crédito com base no círculo de amigos, assim como o Serasa que possui uma ferramenta de cadastro positivo para a avaliação de risco do consumidor, o chamado *credit score*.

Atualmente existe um serviço que utiliza a avaliação do indivíduo para a tomada de decisões, o Uber. O Uber é uma companhia que presta serviços de transporte particular de passageiros, ligando um motorista cadastrado a um passageiro também cadastrado. Ao finalizar uma corrida, os usuários podem se avaliar, atribuindo uma nota de 1 a 5.

Todos os usuários do Uber possuem uma nota com base na avaliação dos demais usuários. Com base nas últimas 500 avaliações é feita uma média, chegando-se à pontuação. Caso seja motorista, há uma média mínima de avaliação para cada cidade, sendo que se

[11] Informações sobre o enredo do filme foram retiradas da enciclopédia livre: Wikipédia. Disponível em: https://pt.wikipedia.org/wiki/Nosedive. Acesso em: 15 set. 2017

o motorista obtiver uma média de avaliação inferior à da cidade, ele poderá ser excluído do serviço. Veja-se:

> O que leva você a perder o direito de acesso à sua conta? Existe uma média mínima de avaliação em cada cidade. Isso acontece, porque existem diferenças culturais na forma como pessoas em diferentes cidades avaliam umas às outras. Nós o informaremos quando sua avaliação estiver chegando perto desse limite e você também receberá material com informações sobre como melhorar a qualidade que o ajudarão a se aperfeiçoar. Entretanto, se a sua avaliação média continuar caindo, você poderá perder o acesso à sua conta. (UBER, 2017)

O mesmo ocorre com o passageiro que é avaliado pelo serviço. Ao solicitar uma viagem é exibida a sua nota, sendo que o motorista poderá recusá-lo em virtude da avaliação negativa. Percebe-se que há uma categorização do ser com base em uma avaliação feita por terceiros, o que é determinante para o uso do aplicativo Uber. Não é explícito nos termos de uso do serviço se um passageiro pode ser excluído da plataforma em decorrência de sua baixa nota de avaliação.

A reputação digital é de suma importância na sociedade atual, podendo significar a contratação de serviços, o que é exemplificado na vida real pelo Uber e na ficção, pela série Black Mirror. Além disso, a reputação digital pode representar o acesso a determinadas oportunidades de trabalho. Veja que a atriz brasileira Natália Rodriguez não foi contratada para uma atuação em razão do baixo número de seguidores no Instagram. O contratante havia dito que a mesma poderia ser indicada para uma vaga de trabalho, mas que para isso, a atriz deveria comprar seguidores no Instagram, o que evidenciou a necessidade de uma reputação digital para o trabalho na vida real (MÜLLER, 2017)

Portanto, a informação é hoje muito importante para a sociedade, e, no futuro, a classificação do eu digital poderá ser a essência do indivíduo, já que as relações têm se tornado cada vez mais digitais.

> Diante das novas tecnologias que marcam a modernidade, a naturalidade que outrora definia a essencialidade da espécie humana se desintegrou. A cada dia que passa vivenciamos processos de incorporação de tecnologias à naturalidade, de forma que um eu eletrônico surge e evidencia a extensão da própria pessoalidade. (SÁ, MOUREIRA, 2017)

Maria de Fátima Freire de Sá e Diogo Luna Moureira (2017) defendem a existência de um "eu" que se projeta em um corpo virtual. O artigo em questão traz uma análise sobre o filme "Her", o qual conta a história de um programa de computador com características que se assemelham às de uma pessoa. Discutem, assim, a possibilidade de atribuição de pessoalidade ao eu digital. Segundo os autores, a tecnologia faz com que seja possível a realidade virtual, ou seja, o corpo construído fora do "eu". A tecnologia traz muita celeuma e necessita-se de muita cautela, porém, se utilizada de forma correta trará benefícios, em vez de apenas violação a direitos e garantias individuais.

Os dados pessoais são hoje uma moeda de troca valiosa, daí a preocupação com a proteção da privacidade dos usuários e não usuários. Veja o exemplo capitaneado pelo grupo Pão de Açúcar, uma rede de supermercados. O referido grupo, pensando em como aumentar a receita, desenvolveu um aplicativo de descontos, por meio do qual disponibiliza ofertas e descontos direcionados para cada consumidor. A companhia que fabrica o produto é que arca com o desconto ou promoção, cabendo ao grupo Pão de Açúcar tão somente fornecer os dados pessoais dos usuários.

> A moeda de troca do Pão de Açúcar era um tesouro que estava enterrado debaixo de uma camada de algoritmos: o grupo abriu para a indústria toda a base de dados de seus programas de fidelidade.
> Os fornecedores têm acesso ao perfil de quem consome (e de quem ignora) seus produtos, e podem fazer ofertas 'nichadas'. (VIRI, 2017)

O grupo Pão de Açúcar diz que o modelo traz um sistema de fidelidade mais efetivo, já que o marketing é direcionado aos consumidores que têm o perfil para aquele determinado tipo de produto. Veja que um grupo de supermercado conseguiu aumentar suas vendas somente com base nos dados cadastrados pelos próprios usuários. Com a coleta indiscriminada de dados pessoais pelas redes sociais, gerando o *shadow profile*, será possível se categorizar ainda mais os usuários e até mesmo os não usuários. Em determinada medida, essa categorização é benéfica, pois pode gerar um desconto em produtos, como no caso do grupo Pão de Açúcar, mas, por outro lado, pode gerar efeitos negativos, como, por exemplo, o rebaixamento do escore de crédito com base em hábitos sociais ou círculo de amizades, com a consequente negativa de contratação com base em informações das quais o usuário sequer saberá da existência.

A valoração dos dados pessoais reflete o que se denomina de capitalismo da vigilância. O termo foi cunhado por Shoshana Zuboff (2015), professora de direito da universidade de Havard. Segundo a autora, as informações pessoais podem refletir a maneira como o consumidor se comporta, o que gera uma expectativa de comportamento em determinadas companhias. Assim, o valor de um negócio pode ser representado pelo potencial de coleta de dados pessoais.

> O lucro, por sua vez, não está somente na intermediação, mas em um conjunto de práticas de rastreio, vigilância, armazenamento, processamento e apropriação privada de dados. São elas que permitem o melhoramento dos serviços das plataformas e a constituição de novos produtos informacionais, que servem a todo um conjunto de atores do mercado capitalista. (EVANGELISTA, 2015)

Hal Varian (apud DANAHER, 2016), chefe de economia do Google, propõe quatro características principais para o capitalismo da vigilância. São elas:

1. A direção através de mais e mais extração de dados e analise.
2. O desenvolvimento de novas formas contratuais usando monitoramento computacional e automação
3. O desejo de personalizar e customizar os serviços oferecidos para os usuários de plataformas digitais
4. O uso de infraestrutura tecnológica para executar experimentos futuros em seus usuários e consumidores. (DANAHER, 2016)

Não é estranho observar notícias nas quais se afirma que os dados pessoais[12] são o petróleo do século XXI (THE WORLD'S..., 2017). A valoração da informação e o seu potencial merece ser estudado pela sociedade. É preciso que se tutele a privacidade dos usuários e dos não usuários, freando a coleta indiscriminada de dados pessoais. Não é porque um termo de uso autoriza a coleta que isso deve ser considerado válido. Entende-se que a existência dos *shadow profiles* viola a privacidade da pessoa e, consequentemente, seu direito de personalidade.

[12] Veja que existem diversas notícias de venda de banco de dados em mercados ilegais. Disponível em <http://m.folha.uol.com.br/mercado/2017/10/1929596-banco-de-dados-com-milhoes-de-telefones-custa-r-200-em-sao-paulo.shtml?mobile>. Acesso em 26 set. 2017

8

Conclusão

A investigação mostrou que as TICs evoluíram ao longo da história, e que a Internet pode ser considerada um bem essencial, cujo acesso pode ser considerado direito fundamental. Assim, é importante que se resguarde os usuários, tendo em vista que inclusive direitos da personalidade podem ser manifestados e, consequentemente, violados na rede.

Vive-se hoje na era denominada de Web 3.0, na qual o usuário deixa de ser um mero expectador e passa a ser o principal ator do processo de criação de conteúdo. Foi a partir da Web 2.0 que o provedor de informação passou a ser um usuário, o qual utiliza o provedor de conteúdo para a difusão daquela. As redes sociais são hoje amplamente utilizadas, sendo que conforme pesquisas, a maior delas, o Facebook, tem hoje aproximadamente 1,9 bilhão de usuários ativos. Daí decorre a importância da tutela da personalidade dos usuários.

A pesquisa evidenciou que hoje a informação possui um valor significativo, razão pela qual as maiores companhias em atividade do mundo são empresas de base tecnológica. O valor gerado por estas companhias é fruto de uma segmentação de mercado, feita através da coleta indiscriminada de dados pessoais, o que possibilita a existência de *Shadow Profiles*. Concluiu-se que existem duas vertentes de *Shadow Profiles*. A primeira consiste nos dados sobre um usuário que são coletados sem o consentimento expresso ou até mesmo conhecimento do usuário e a segunda se refere às informações de quem sequer faz parte da plataforma.

Investigou-se a respeito da formação história dos direitos da personalidade, momento em que se evidenciou a existência de uma cláusula geral de proteção, com um rol não taxativo de tutela. Apesar de a doutrina distinguir as espécies existentes dos direitos da personalidade, esses direitos estão em perene expansão, com surgimento de novas situações fáticas que clamam tutela jurídica. Assim, conclui-se pela possibilidade de proteção de novas situações jurídicas não previstas em lei.

Como a Internet alterou a realidade fática, novas situações antes inimagináveis surgiram, nascendo a necessidade de tutela. Essa proteção não necessita de criação de novas normas. Como visto, é possível se trabalhar com as teorias da interpretação para se alcançar uma proteção eficaz dos direitos da personalidade.

Em uma concepção clássica, a privacidade é vista como o direito de ser deixado só. Ao trabalhar com esse direito remonta-se à ideia de que o indivíduo possui aspectos na sua vida que devem ser respeitados, facultando-lhe a exclusão do outro. Contudo, na Internet sempre haverá interação com alguém, nem que seja um provedor. Assim, é necessária uma releitura do direito à privacidade.

A pesquisa evidenciou que na rede mundial de computadores é correto se afirmar que a privacidade é respeitada quando o usuário tem controle sobre suas informações pessoais. Assim, a privacidade deve ser lida como o direito de controlar as próprias informações, ou, como defendido, a autodeterminação informativa.

Entre as novas interpretações do direito à privacidade evidenciadas nesse trabalho, tem-se o direito de autodeterminação, que é reflexo da doutrina do *Self determination*, sendo a possibilidade de o usuário controlar suas informações pessoais. Ocorre que os usuários muitas vezes não sabem quais dados pessoais estão sendo coletados e sequer como são utilizados.

A investigação mostrou que um reflexo desse controle das informações pessoais é o direito de exclusão, que deve ser dado a todo usuário. Tal direito se difere do direito ao esquecimento ao passo que o segundo se refere a informações que estão na rede, mas

que pertencem a terceiros. Caso um titular tenha um perfil em uma rede social criado e mantido por ele, deve lhe ser facultado o direito de excluí-lo a qualquer momento e a isso se denomina direito de exclusão.

Quanto ao direito ao esquecimento, evidenciou-se o que se denomina de *streissand effect*, um paradoxo para o direito. Quando alguém solicita a exclusão de uma informação com base no direito ao esquecimento é possível que o efeito da tutela pretendida seja reverso, fazendo com que cada vez mais pessoas tenham conhecimento sobre aquele fato. Assim, por mais que se tenha uma base sólida para o direito ao esquecimento, é necessária cautela na sua aplicação.

O estudo mostrou ainda que se trabalha com o direito a desindexação, que é o direito de solicitar a retirada de resultados dos motores de buscas, tal como o Google. A medida pode ser mais eficaz, tendo em vista que as informações são comumente acessadas através de motores de busca, o que faz com que se tenha uma maior efetividade na medida pretendida.

Outro desdobramento da privacidade é o direito de acesso e modificação dos dados. Afirmou-se ser um direito de todos ter acesso aos dados em poder dos provedores, podendo, inclusive, modificá-los.

Por fim, o presente trabalho trouxe o direito de não ser conhecido, uma proposta para se proibir a existência de *Shadow Profiles*. Afirmou-se que é um direito do indivíduo não ser conhecido por uma plataforma, o que acontecerá com a proibição da coleta indiscriminada de dados pessoais.

Trabalhou-se com o caso do aplicativo Lulu, que coletava dados através do Facebook, cadastrando perfis de homens para serem avaliados por mulheres anonimamente. Diversas ações judiciais foram ajuizadas e, como visto, julgadas procedentes para que fosse determinada a exclusão dos dados e, em alguns casos, a condenação em indenização por danos morais.

Tal direito é normatizado no Marco Civil da Internet, ao ser regulado o direito dos usuários ao não fornecimento a terceiros de seus dados pessoais, exceto se houver consentimento livre, expresso e informado. Quando se fala em consentimento, em verdade esse não existe, tendo em vista a natureza do contrato que regula a relação.

A investigação mostrou que a relação entre um provedor de aplicação de Internet e um usuário é regulada por um termo de adesão digital, que é um contrato de adesão. Como característica principal, estes termos têm a aceitação integral, ou seja, ou se aceitam todos os termos ou não se utiliza o serviço desejado.

Tal fato evidencia a relativização do elemento vontade nas relações entre usuários e provedores. A ideia de autonomia da vontade deve ser revisitada, pois não mais reflete a ordem principiológica moderna. Fala-se em preceptivismo jurídico, teoria segundo a qual além de interessarem aos contraentes, os contratos possuem um efeito em toda a sociedade, e a esta também interessa o adimplemento da avença. Assim, houve uma crise após o auge do liberalismo, acompanhada da massificação das relações jurídicas, com uma objetivação do contrato. Mostrou-se que as relações são necessárias, não mais voluntárias, o que não significa a ausência de vontade. Há o elemento voluntarista, entretanto este não é mais o preponderante, tutelando-se a confiança das partes.

Com base na análise documental feita, evidenciou-se a teoria da autonomia privada, que melhor reflete essa tutela da confiança. Há limites sobre a vontade dos contratantes, como, por exemplo, os princípios da boa-fé objetiva e da função social do contrato.

A investigação mostrou que existem dois tipos de termos de adesão digital, quais sejam, o *Click-Wrap* e o *Browse-Wrap*. O primeiro é aquele no qual o usuário deve clicar em alguma caixa ou botão para concordar com o contrato, aceitando os seus termos. Por sua vez, o segundo tipo é aquele quando se navega em um *Web Site* sem que se tenha aceitado os termos com um click, mas estando vinculado a este simplesmente por estar utilizando aquele serviço.

Percebe-se que o elemento vontade não é o preponderante dessa relação. Conforme a investigação mostrou, isso não implica invalidade da avença, pois rompeu-se com o paradigma de necessidade de se tutelar a vontade.

No entanto, este estudo mostrou que é possível se falar em invalidade de determinadas cláusulas contratuais. Isso porque não se pode ter, por exemplo, renúncia antecipada ao direito resultante da natureza do negócio em um contrato de adesão. O contrato continua válido, mas, existindo uma cláusula que implica renúncia, por exemplo, apenas esta será invalidada. Há primazia da continuidade da relação contratual, pois, como visto, o adimplemento interessa a toda sociedade. Portanto, a análise da validade deve ser feita em cada cláusula em apartado e, conforme evidenciado, deverá ser observado o ordenamento jurídico brasileiro, em especial o Marco Civil da Internet, Código Civil de 2002, Código de Defesa do Consumidor e Código de Processo Civil de 2015. Assim, cláusulas comumente inseridas em termos de adesão digital são consideradas inválidas, tais como as que determinam a eleição de foro e a cessão de dados a terceiros.

Outro aspecto estudado neste trabalho diz respeito à proteção contra o comportamento contraditório, teoria conhecida como *venire contra factum proprium* ou teoria dos atos próprios, a qual é um desdobramento da boa-fé objetiva. De acordo com tal princípio, uma parte não pode assumir um comportamento em uma relação contratual e posteriormente ir contra essa postura.

Trabalhou-se com o caso do Nissim Ourfali, no qual um vídeo cômico foi colocado na Internet pelo próprio pai do adolescente, vindo a ser divulgado por diversas pessoas. Posteriormente, foi ajuizada uma ação contra o Google, requerendo a retirada do vídeo. Com base na teoria dos atos próprios, não se pode falar em qualquer dano praticado pelo provedor, pois sabia-se que, ao inserir o vídeo na plataforma Youtube, ele poderia ser acessado e compartilhado por qualquer pessoa, ou seja, a parte adotou um comportamento no início da relação, o de divulgar o vídeo, e, posteriormente, requereu

a retirada deste. Não se discute a possibilidade jurídica do direito ao esquecimento, é evidente que há hipótese de o vídeo ser retirado com base neste instituto.

A investigação trabalhou com a análise específica de termos de uso e política de privacidade de três plataformas, quais sejam, Facebook, Instagram e Google. Discutiu-se a validade de algumas cláusulas controvertidas e concluiu-se que a renúncia a direitos de propriedade intelectual, por exemplo, é inválida.

O trabalho evidenciou que o Google, nos primeiros termos de uso e políticas de privacidade, não coletava informações além das fornecidas ativamente pelos usuários. Entretanto, isso mudou ao longo dos anos e, em 2005 após a criação do *Orkut*, primeira rede social da plataforma. Com o avanço da tecnologia novas alterações foram feitas, o que leva à conclusão de que ocorreram mudanças com a Web 2.0.

A investigação trouxe uma análise a respeito da violação de direitos da personalidade com a existência do que se denominou de *Shadow Profile*. Tendo como marco teórico Stefano Rodotà, concluiu-se que a falta de uma norma jurídica não implica a falta de proteção do ser humano, pois, com a crise do positivismo e a repersonificação do Direito Privado, este passou a ser o pilar central do ordenamento jurídico. Assim, é possível a tutela da personalidade mesmo com o advento de uma nova realidade fática.

Concluiu-se que a existência de *Shadow Profile* viola direitos da personalidade tanto do usuário quanto do não usuário. Foi proposta a criação de uma agência reguladora para a regulamentação do mercado que tenha o tratamento de dados pessoais. Através dessa agência, as plataformas sofreriam uma fiscalização sem que isso implicasse perda de liberdade de expressão. Estado Democrático de Direito não pressupõe a ausência de controle, pelo contrário, é necessária a intervenção pontual para que se defenda os indivíduos de abusos, como os que ocorrem com os *Shadow Profiles*.

Como visto, a informação pode ser utilizada como um meio de exploração. A valoração dos dados pessoais reflete o que se denomina de capitalismo da vigilância, segundo o qual o valor de um negócio pode ser representado pelo potencial de coleta de dados pessoais. Portanto, é necessário que se repense a tutela da privacidade na Internet o que não necessita exclusivamente da criação de novas normas, pois as que já existem são satisfatórias para a proteção dos direitos da personalidade do usuário e do não usuário. Normas como a lei de proteção de dados pessoais trarão uma proteção eficaz para novas situações na Internet. Entretanto, mais do que a edição de leis, se faz necessária a criação de mecanismos eficientes capazes de frear a coleta e uso indiscriminado de dados pessoais.

Referências

ALMEIDA, Juliana Evangelista de. Responsabilidade Civil dos Provedores de Serviço de Internet. **Revista de Direito Privado**. São Paulo: Revista do Tribunais, v.62, p.97-116, 2015.

ALMEIDA, Juliana Evangelista de; ALMEIDA, Daniel Evangelista Vasconcelos. Os Direitos de Personalidade e o Testamento Digital. **Revista de Direito Privado**, São Paulo, ano 14, vol. 53, p. 179 – 200, jan./mar., 2013.

ALMEIDA, Juliana Evangelista de; ALMEIDA, Daniel Evangelista Vasconcelos. A ditadura do algoritmo e a proteção da pessoa humana: uma análise do controle do Si eletrônico. **Revista de Direito Privado:** RDPriv, São Paulo, v. 17, n. 69, p. 29-43, set. 2016.

ALMEIDA, Rafael. **Em nova política de privacidade, spotify exige que usuários brasileiros renunciem ao direito de sigilo bancário**. 22 dez. 2016. Disponível em: http://www.b9.com.br/69182/social-media/em-nova-politica-de-privacidade-spotify-exige-que-usuarios-brasileiros-renunciem-ao-direito-de-sigilo-bancario/. Acesso em: 20 ago. 2017.

ALVES, Cida. Ministério Público Abre Inquérito contra aplicativo Lulu e Facebook. **Folha de São Paulo**. Disponível em: <http://www1.folha.uol.com.br/cotidiano/2013/12/1379824-ministerio-publico-abre-inquerito-contra-aplicativo-lulu-e-facebook.shtml>. Acesso em: 14 nov. 2016.

AMARAL, Francisco. **Direito Civil:** introdução. 7. ed. ver. atual. e aum. Rio de Janeiro: Renovar, 2008.

ATHENIENSE, Alexandre. Empresas vendem dados do consumidor na Internet. **JusBrasil**. 5 fev. 2011. Disponível em: https://alexandre-atheniense.jusbrasil.com.br/noticias/2556744/empresas-vendem-dados-pessoais-do-consumidor-na-Internet. Acesso em: 20 ago. 2017.

ASCENÇÃO, José Oliveira. O “Fundamento do Direito”: Entre o Direito Natural e a Dignidade da Pessoa. In: SÁ, Maria de Fátima Freire de; MOUREIRA, Diogo Luna; ALMEIDA, Renata Barbosa. **Direito Privado**: Revisitações. Belo Horizonte: Arraes Editores, 2013. p. 1-16.

BARGAS, Diego. **Quanto o Youtube paga por pageview**. 19 set. 2017. Disponível em: http://mundoestranho.abril.com.br/cotidiano/quanto-o-youtube-paga-por-pageview/. Acesso em: 20 ago. 2017.

BITTAR, Carlos Alberto. **Direito de Autor**. 4. ed. Rio de Janeiro: Forense Universitária, 2003.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. Rio de Janeiro: Forense Universitária, 1999.

BITTAR, Eduardo C. B.; ALMEIDA, Guilherme Assis de. **Curso de Filosofia do Direito**. 12ª Ed. São Paulo: Atlas, 2016.

BONAVIDES, Paulo. **Curso de Direito Constitucional**. 31. ed. São Paulo: Malheiros, 2016.

BOTSMAN, Rachel. Big data meets Big Brother as China moves to rate its citizens. **WRED**. Disponível em: <http://www.wired.co.uk/article/chinese-government-social-credit-score-privacy-invasion>. Acesso em: 21 out. 2017.

BRAGA NETTO, Felipe Peixoto. **Teoria dos ilícitos civis**. Belo Horizonte: Del Rey, 2003.

BRANT, Cássio Augusto Barros. **Lições Preliminares de Propriedade Intelectual**. Belo Horizonte: Edição do Autor, 2012.

BRANT, Cássio Augusto Barros. **Marco Civil da Internet:** comentários sobre a Lei 12.965/2014. Belo Horizonte: Editora D’Plácido, 2014.

BRANT, Cássio Augusto Barros. **O microssistema do direito tecnodigital**. Belo Horizonte, 2016. Disponível em: <http://www.biblioteca.pucminas.br/teses/Direito_BrantCAB_1.pdf>.

BRASIL, Ministério da Justiça. **Pensando o direito**. Disponível em: <http://pensando.mj.gov.br/dadospessoais/texto-em-debate/anteprojeto-de-lei-para-a-protecao-de-dados-pessoais/>. Acesso em: 04 set. 2017.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil.** Promulgada aos 5 de outubro de 1988. Brasília: Senado, 1998.

BRASIL. Decreto Nº 8.771 de 11 de maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na Internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. **Diário Oficial da União**. Brasília, 11 maio. 2016.

BRASIL. Lei Nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. **Diário Oficial da União**. Brasília, 10 jan. 2002.

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

BRASIL. Superior Tribunal de Justiça. Processo 1402104/RJ, Rel. Ministro Raul Araújo. **Diário de Justiça**, Brasília 18 jun. 2014.

BRASIL. LEI Nº 8.078, DE 11 DE SETEMBRO DE 1990. Dispõe sobre a proteção do consumidor e dá outras providências. **Diário Oficial da União**. Brasília, 12 set. 1990.

BRASIL. Lei Nº 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, 13 nov. 1997.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). **Diário Oficial da União**. Brasília, 15 ago. 2018.

BRASIL. Tribunal Regional Federal. Andamento do Processo N. 25463-45.2016.4.01.4000 - Ação Civil Pública - 03/07/2017 do Trf-1. **Diário Oficial da União**. 30 jun. 2017. Disponível em: https://www.jusbrasil.com.br/diarios/documentos/474357638/andamento-do-processo-n-25463-4520164014000-acao-civil-publica-03-07-2017-do-trf-1?ref=topic_feed. Acesso em: 20 ago. 2017.

BRIGGS, Asa; BURKE, Peter. **1921 – Uma História social da mídia:** de Gutenberg à Internet Tradução de Maria Carmelita Pádua Dias. 2 ed. ver. e ampl. Rio de Janeiro: Zahar, 2006

CHAVES, Christian Frau Obrador. A Luta Contra o Terrorismo e a Proteção de Dados Pessoais: Análise Crítica de um Precedente do Tribunal Constitucional Alemão (Bundesverfassungsgericht). **Direitos fundamentais & justiça**, v. 12, p. 284-293, 2010. Disponível em:<https://www.google.com.br/url?sa=t&rct=j&q=&esrc=s&source=web&cd=1&ved=0ahUKEwjVjcS5ozWAhVMRyYKHb8DDCIQFggnMAA&url=http%3A%2F%2Fwww.agu.gov.br%2Fpage%2Fdownload%2Findex%2Fid%2F5211353&usg=AFQjCNFmr2NBOlwBrv04sT61FvTIiSBmAw>. Acesso em: 04 de set. 2017.

CHINA planeja avaliar cidadãos adotando notas para cada pessoa. **Estúdio I.** Globo News. 26 out. 2016. Disponível em: http://g1.globo.com/globo-news/estudio-i/videos/t/todos-os-videos/v/china-planeja-avaliar-cidadaos-adotando-notas-para-cada-pessoa/5404962/. Acesso em: 30 set. 2017

COELHO, Fábio Ulhoa. **Manual de Direito Comercial:** direito de empresa. 23. ed. São Paulo: Saraiva, 2011.

COMPLAINT. **Europe versus Facebook**. Disponível em: <http://europe-v-facebook.org/Compalint_02_Shadow_Profiles.pdf>. Acesso em: 08 jun. 2016.

COOTER Robert; ULEN, Thomas. **Law and Economics.** Pearson: Addison Wesley, 2007.

CORTE ALEMÃ julga Internet como serviço essencial. **Mundo Positivo**. 25 jan. 2013. Disponível em: <http://www.mundopositivo.com.br/noticias/brasil/20138626-corte_alema_julga_Internet_como_servico_essencial.html> Acesso em: 25 jan. 2015.

COUTO E GAMA, André. **Direito Civil**: Sistema dos Direitos da Personalidade. Belo Horizonte: Editora D'Plácido, 2014.

CRIADO, Miguel Ángel. **O que o seu celular revela sobre você**. Disponível em: <http://brasil.elpais.com/brasil/2016/05/16/tecnologia/1463385894_263250.html?id_externo_rsoc=TW_CM>. Acesso em: 08 jun. 2016.

CUPIS, Adriano de. **Os direitos da personalidade**. Lisboa: Morais, 1961.

DANAHER, John. The Logic of Surveillance Capitalism. **Algocracy and the Transhumanist Project.** 21 mar. 2016. Disponível em <https://ieet.org/index.php/IEET2/more/danaher20150625 >. Acesso em: 9 fev. 2017.

DEBORD, Guy. **A sociedade do Espetáculo. 2003**. Paráfrase em português: Railton Souza Guedes. Disponível em: https://www.marxists.org/portugues/debord/1967/11/sociedade.pdf. Acesso em: 20 ago. 2017.

DIXON, A. Liability of users and third parties for copyright infringement on the Internet: overview of international developments. In: STROWEL, A. (ed.).**Peer-to-Peer File Sharing and Secondary Liability in Copyright Law.** Edward Elgar, 2009, p. 2-42.

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

DONEDA, Danilo. Iguais mas separados: o Habeas Data no ordenamento jurídico brasileiro e a proteção de dados pessoais. **Cadernos da Escola de Direito e Relações Internacionais (UniBrasil).** Vol. 9, p. 14-32, 2009.

DONEDA, Danilo. Privacidade, vida privada e intimidade no ordenamento jurídico brasileiro. Da emergência de uma revisão conceitual e da tutela de dados pessoais. In: **Âmbito Jurídico**, Rio Grande, XI, n. 51, mar 2008. Disponível em: <http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2460>. Acesso em 15 out 2017.

EVANGELISTA, Rafael. **A estranha lógica do capitalismo de vigilância**. 25 ago. 2015. Disponível em: http://www.oplanob.org/?p=687. Acesso em: 20 ago. 2017.

FACEBOOK. **Política de dados**. 2016. Disponível em <https://www.facebook.com/privacy/explanation> Acesso em: 19 ago. 2016.

FACEBOOK. **Termos de uso** (Instagram). 2013. Disponível em: https://www.facebook.com/help/instagram/478745558852511. Acesso em: 19 ago. 2016.

FARIAS, Cristiano Chaves de; ROSENVALD, Nelson. **Direito Civil:** Teoria Geral**.** 6. ed. Rio de Janeiro: Lumen Juris, 2007.

FERNANDES, Bernardo Gonçalves. **Curso de Direito Constitucional.** 6. ed. Salvador: Editora JusPodivm, 2014.

FERREIRA, Aurélio Buarque de Holanda. **Novo Aurélio Século XXI:** o dicionário da língua portuguesa. 3.ed. rev. e ampl. Rio de Janeiro: Nova Fronteira, 1999.

FIUZA, César. **Direito civil**: Curso Completo. 15. ed. Belo Horizonte: Del Rey, 2011.

FLORIDA, USA, Fort Myers District. **Case No: 2:14-cv-646-FtM-29CM. E-VENTURES WORLDWIDE, LLC v. GOOGLE, INC.** 19 ago. 2016. Disponível em: http://cases.justia.com/federal/districtcourts/florida/flmdce/2:2014cv00646/303931/104/0.pdf?ts=1471684860. Acesso em: 20 ago. 2017.

GAGLIANO, Pablo Stolze; PAMPLONA FILHO, Rodolfo. **Novo Curso de Direito Civil**. São Paulo: Saraiva, 2011.

GANDELMAN, Henrique. **De Gutenberg à Internet: direitos autorais na era digital**. 4ª Ed. Ampliada e atualizada. Rio de Janeiro: Editora Record, 2001.

GONÇALVES, Carlos Roberto. **Direito Civil Brasileiro** – Contratos e atos unilaterais. Vol. 3. São Paulo: Saraiva, 2011.

GOOGLE é obrigado a excluir todos os vídeos de Nissim Ourfali do YouTube. **CONJUR**. 2016a. Disponível em: http://www.conjur.com.br/2016-mar-15/google-obrigado-excluir-videos-nissim-ourfali-youtube Acesso em: 15 jul. 2016.

GOOGLE. **Termos de Serviço**. 2016b. Disponível em: <https://www.youtube.com/static?gl=BR&template=terms&hl=pt > Acesso em: 19 ago. 2016.

GOOGLE. **Políticas de privacidade**. Disponível em: <https://www.google.com/intl/pt-BR/policies/privacy/>. Acesso em: 20 ago. 2017.

HIRATA, Thaís. Sites que vendem dados pessoais são alvo de investigação no Ministério Público. **Folha de São Paulo.** 29 jul. 2015. Disponível em: http://www1.folha.uol.com.br/mercado/2015/07/1662078-sites-que-vendem-dados-pessoais-sao-alvo-de-investigacao-no-mp.shtml. Acesso em: 20 ago. 2017.

INSTITUTO DE REFERÊNCIA EM INTERNET E SOCIEDADE (IRIS). **Policy Paper:** Transferência Internacional de dados no PL 5276/16. 2017. Disponível em: http://irisbh.com.br/policy-paper-sobre-a-transferencia-internacional-de-dados-no-projeto-de-lei-5-2762016/. Acesso em: 10 set. 2017.

ITALIA. **Codice Civile**. 2016. Disponível em <http://www.studiocataldi.it/codicecivile/>. Acesso em: 14 nov. 2016.

JÁ ouviu falar em fazenda de likes sim elas existem. **Uol notícias**. 21 jun. 2017. Disponível em: https://tecnologia.uol.com.br/noticias/redacao/2017/06/21/ja-ouviu-falar-em-fazenda-de-likes-sim-elas-existem.htm. Acesso em: 20 ago. 2017.

JENKINS, Henry, **Cultura da Convergência**. São Paulo: Aleph, 2008.

JUNQUEIRA, Daniel. Patente do Facebook usa seus amigos para provar ou rejeitar empréstimos. **Gizmodo**. 7 ago. 2015. Disponível em: <http://gizmodo.uol.com.br/patente-facebook-emprestimo/>. Acesso em: 20 ago. 2017.

JUSTIÇA determina que Google tire do ar vídeos sobre garoto**. Globo. G1**, 2016. Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/03/nissim-ourfali-justica-determina-que-google-tire-do-ar-videos-sobre-garoto.html> Acesso em: 15 jul. 2016.

KELSEN, Hans. **Teoria pura do direito.** 7. ed. São Paulo: Martins Fontes, 2006.

KLEE, Antonia Espíndola Longoni. O diálogo das fontes nos contratos pela Internet: do vínculo contratual ao conceito de estabelecimento empresariam virtual e a proteção do consumidor. In: MARQUES, Claudia Lima. **Diálogo das Fontes**: Do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012. p. 399-450.

LACERDA, Bruno Torquato Zampier **A tutela dos bens tecnodigitais**: possíveis destinos frente à incapacidade e morte do usuário. Belo Horizonte, 2016. Disponível em < http://www.sistemas.pucminas.br/BDP/SilverStream/Pages/pg_ConsItem.html>. Acesso em: 04 set. 2017.

LACERDA, Bruno Torquato Zampier **Bens Digitais**. São Paulo: Editora Foco, 2017.

LAZARO, Christophe; LE MÉTAYER, Daniel. Control over Personal Data: True Remedy or Fairy Tale? (June 1, 2015). **SCRIPT-ed**, Vol. 12, No. 1, June 2015. Disponível em: https://ssrn.com/abstract=2689223. Acesso em: 04 set. 2017.

LEMOS, Ronaldo; SOUZA, Carlos Affonso Pereira de; VIEIRA JUNIOR, Sérgio Branco. Responsabilidade civil na Internet: uma breve reflexão sobre a experiência brasileira e norte-americana. **Revista de Direito da Comunicações = Communications Law Review,** São Paulo, v. 1, n. 1, p. 80-98, jan./jun. 2010.

LEONARDI, Marcel. **Responsabilidade civil dos provedores de serviço de Internet.** São Paulo: Juarez Oliveira, 2005.

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

LEVERAGE, Social Media Comparison **Infographic**, 28 de abril de 2014. Disponível em: https://leveragenewagemedia.com/blog/social-media-infographic/. Acesso em: 20 ago. 2017.

LÉVY, Pierre. **Cibercultura**. São Paulo: Editora 34, 1999.

LIMA, Cíntia Rosa Pereira De. Contratos de Adesão Eletrônicos (*Shrink-wrap e Click-wrap)* e os termos de condições de uso (*Browse-wrap*). IN: LIMA, Cíntia Rosa Pereira De; Nunes, Lydia Neves Bastos Telles. **Estudos Avançados de Direito Digital.** Rio de Janeiro: Elsevier, 2014.

LIMA, Cíntia Rosa Pereira De. **O Ônus de Ler o Contrato no Contexto da "Ditadura" dos Contratos de Adesão Eletrônicos**. 2016. Disponível em: <http://publicadireito.com.br/artigos/?cod=981322808aba8a03>. Acesso em: 18 ago. 2016.

LOCKE, Laura. **Facebook Ireland accused of creating 'shadow profiles' on users, nonusers**. Disponível em <http://www.cnet.com/news/facebook-ireland-accused-of-creating-shadow-profiles-on-users-nonusers/>. Acesso em: 08 jun. 2016.

LOPES, Renan. Com tantos processos judiciais, como o app Lulu conseguiu voltar ao Brasil?. **Gizmodo.** Disponível em <http://gizmodo.uol.com.br/lulu-volta-ao-brasil/>. Acesso em:14 nov. 2016.

LUDMER, Eduardo**.** O direito de ser lembrado**. Jota Info.** 11 ago. 2017. Disponível em**:** https://jota.info/artigos/o-direito-de-ser-lembrado-11082017. Acesso em: 20 ago. 2017.

MAIORIA das escolas paulistas não oferece a disciplina Educação Digital. **Fecomercio/SP**. Disponível em: <http://www.fecomercio.com.br/NoticiaArtigo/Artigo/12905> Acesso em: 15 jul. 2016.

MARICHAL, Jose. De volta à névoa: o futuro do Facebook. **PoliTICs**, junho de 2013. Disponível em: <https://www.politics.org.br/edicoes/devolta-%C3%A0-n%C3%A9voa-o-futuro-do-facebook>. Acesso em: 26 jan. 2017.

MARQUES, Cláudia Lima. **Contratos no Código de Defesa do Consumidor:** o novo regime das relações contratuais. 6. ed. atual. e ampl. São Paulo: Revista dos Tribunais, 2011.

MARTINS, Fran. **Curso de Direito Comercial:** direito de empresa. vol 1. 37. ed. Rio de Janeiro: Editora Forense, 2014.

MAYER-SCHÖNBERGER, Viktor. Generational development of data protection in Europe. In: AGRE, Philip E.; ROTENBERG, Marc. **Technology and privacy**: the new landscape. Cambridge: Mit, 2001.

MENDES, Laura Schertel. **Privacidade, proteção de dados e defesa do consumidor linhas gerais de um novo direito fundamental**. São Paulo: Saraiva, 2014.

MENDONÇA, Fernanda Graebin. **O Direito à Autodeterminação Informativa:** A (des)Necessidade de Criação de um Novo Direito Fundamental Para a Proteção de Dados Pessoais no Brasil. Disponível em http://www.egov.ufsc.br/portal/conteudo/o-direito-%C3%A0-autodetermina%C3%A7%C3%A3o-informativa-desnecessidade-de-cria%C3%A7%C3%A3o-de-um-novo-direito. Acesso em: 04 set. 2017.

MINAS GERAIS, Tribunal de Justiça. **Apelação Cível 2.0000.00.310192-2/000,** Relator(a): Des.(a) Maria Elza, Relator(a) para o acórdão: Des.(a) , julgamento em 02/08/2000, publicação da súmula em 15/08/2000.

MÜLLER, Leonardo. Atriz diz que perdeu papel por não ter seguidores o suficiente no Instagram. **Tecmundo**. Disponível em: <https://www.tecmundo.com.br/cultura-geek/121926-atriz-diz-perdeu-papel-nao-ter-seguidores-suficiente-instagram.htm>. Acesso em: 21 out. 2017.

NAVES, Bruno Torquato de Oliveira; SÁ, Maria de Fátima Freire de. **Direitos da Personalidade**. Belo Horizonte: Arraes Editores, 2017.

O TRIBUNAL da UE endossa o 'direito ao esquecimento' na Internet. **El País**. Madri, 13. Maio 2014. Disponível em: http://brasil.elpais.com/brasil/2014/05/12/sociedad/1399921965_465484.html Acesso em: 20 abr. 2015.

O'REILLY, Tim. **What is Web 2.0.** 2005. Disponível em <http://www.oreilly.com/pub/a/web2/archive/what-is-web-20.html>. Acesso em: 20 abr. 2015.

ODLYZKO, Andrew. Network Neutrality, Search Neutrality, and the Never-ending Conflict between Efficiency and Fairness in Markets. **Review of Network Economics**, 8(1), 2009. Disponível em: https://www.degruyter.com/view/j/rne.2009.8.issue-1/rne.2009.8.1.1169/rne.2009.8.1.1169.xml. Acesso em: 16 ago. 2017.

ORWELL, George. **1984**. São Paulo: Companhia Das Letras, 2009.

PAESANI, Liliana Minardi. **O Direito na Sociedade da Informação III:** a evolução do Direito Digital. São Paulo: Atlas, 2013.

PERSONAL details of nearly 200 million US citizens exposed. **BBC**. Disponível em <http://www.bbc.com/news/technology-40331215>. Acesso em 04 set. 2017.

PREJUÍZO do facebook com whatsapp chega a us$ 232 milhões em 6 meses. **Globo.com**. 29 out. 2014. Disponível em: http://g1.globo.com/tecnologia/noticia/2014/10/prejuizo-do-facebook-com-whatsapp-chega-us-232-milhoes-em-6-meses.html. Acesso em 04 de set. 2017.

PIAUÍ. Procuradoria da República. **MPF/PI ajuíza ação contra Google por descumprir normas de proteção de dados.** 10 nov. 2016 Disponível em: http://www.mpf.mp.br/pi/sala-de-imprensa/noticias-pi/mpf-pi-ajuiza-acao-contra-google-por-descumprir-normas-de-protecao-de-dados. Acesso em: 04 set. 2017.

PINHEIRO, Patrícia Peck. **Direito Digital.** 6. ed. São Paulo: Saraiva, 2016.

POLI, Leonardo Macedo. **Direito Autoral:** parte geral. Belo Horizonte: Del Rey, 2008.

POLI, Leonardo Macedo. Ato Ilícito. In: FIUZA, César (org.). **Curso Avançado de Direito Civil.** Rio de Janeiro: Forense, 2009.

POLI, Leonardo Macedo; LORENTINO, Sérgio Augusto Pereira. Autonomia dos Consumidores nos Contratos. In: **CONPEDI**; 2015, v. 1, p. 208-226. Disponível em: <http://www.conpedi.org.br/publicacoes/66fsl345/852e718s/vMLdSzDuxS7mH7ff.pdf>. Acesso em: 15 jul. 2016.

REALE, Miguel. **Lições Preliminares de Direito.** 27ª Ed. São Paulo: Saraiva, 2009.

RECUERO, Raquel. Rede social. In: AVORIO, A.; SPYER, J. (Org.). **Para entender a Internet**. versão rev. e ampl., 2015. Disponível em: < http://paraentender.com/sites/paraentender.com/static/pdf/livro.pdf >. Acesso em: 15 jul. 2016.

RHETT, Jones. 22 mil pessoas concordaram limpar banheiros por acesso Wi-fi porque elas não leram os termos. **Gizmodo Brasil.** 16 jul. 2017.

RIO GRANDE DO SUL. Tribunal de Justiça do Rio Grande do Sul. Processo 71005057401, Rel. Desembargadora Gisele Anne Vieira de Azambuja. **Diário de Justiça,** Brasília, 23 set. 2014.

RODOTÀ Stefano. **La vida y las reglas:** Entre el derecho y el no derecho. Madrid, Espanha: 2010.

RODOTÀ, Stefano. **A vida na sociedade da vigilância.** A privacidade hoje. Organização, seleção e apresentação de Maria Celina Bodin de Moraes. Rio de Janeiro: Renovar, 2008.

RODOTÁ, Stefano. **Il mondo nellarete: quali i diritti, quali i vincoli**. Roma: Laterza, 2014.

RODOTÀ, Stefano. Por que é necessária uma Carta de Direitos da Internet?. Tradução de Bernardo Diniz Accioli de Vasconcellos e Chiara Spadaccini de Teffé. **Civilistica.com**. Rio de Janeiro, a. 4, n. 2, jul.-dez./2015. Disponível em: http://civilistica.com/wp-content/uploads/2015/12/Rodota%CC%80-trad.-de-Teffe%CC%81-e-Vasconcellos-civilistica.com-a.4.n.2.20152.pdf. Acesso em: 10 jul. 2016

ROMERO, Luiz. Não li e concordo**. Super Interessante**. 2016. Disponível em <http://super.abril.com.br/tecnologia/nao-li-e-concordo>. Acesso em: 22 ago. 2016.

ROPPO, Enzo. **O Contrato**. Coimbra: Almedina, 2009.

ROUSSEFF, Dilma. **Discurso da Presidenta da República, Dilma Rousseff, na abertura do Debate Geral da 68ª Assembleia-Geral das Nações Unidas - Nova Iorque/EUA.** Disponível em: http://www2.planalto.gov.br/acompanhe-o-planalto/discursos/discursos-da-presidenta/discurso-da-presidenta-da-republica-dilma-rousseff-na-abertura-do-debate-geral-da-68a-assembleia-geral-das-nacoes-unidas-nova-iorque-eua. Acesso em: 10 jul. 2016.

RUTHRUFF, Austin. **You Might Have an Invisible Facebook Account Even if You Never Signed Up**. Disponível em: <http://www.groovypost.com/news/facebook-shadow-accounts-non-users/>. Acesso em: 08 jun. 2016.

SÁ, Maria de Fátima Freire de; MOUREIRA, Diogo Luna. O Direito e as Dimensões Semânticas da Pessoalidade: Reflexões sobre 'Her', conectada e Desintegrada. In: VIEIRA, Tereza Rodrigues; CARDIN, Valéria S.Galdino; GOMES, Luiz.G.do Carmo. (Org.). **Bioética & Cinema.** 2.ed. Maringá, PR: Miraluz, 2017, v. 1, p. 199-215.

SALIB, Marta Luiza Leszczynski. **A tutela do consumidor brasileiro no mercado eletrônico internacional.** 2013. 157f.Dissertação (Mestrado). PucGoiás. Goiânia, 2013. Disponível em: http://tede2.pucgoias.edu.br:8080/bitstream/tede/2666/1/MARTA%20LUIZA%20LESZCZYNSKI%20SALIB.pdf. Acesso em: 04 set. 2017

SÃO PAULO. Tribunal de Justiça. Processo 1000647-47.2014.8.26.0564, Desembargador José Carlos Ferreira Alves. **Diário de Justiça,** Brasília, 20 out. 2015.

SARLET, Ingo Wolfgang. **Do caso Lebach ao caso Google vs. Agencia Espanhola de Proteção de Dados.** Disponível em <http://www.conjur.com.br/2015-jun-05/direitos-fundamentais-lebach-google-vs-agencia-espanhola-protecao-dados-mario-gonzalez> Acesso em: 15 jul. 2016.

SCHREIBER, Anderson. **Direitos da Personalidade.** São Paulo: Atlas, 2011.

TARTUCE, Flávio. A teoria geral dos contratos de adesão no Código Civil. Visão a partir da teoria do diálogo das fontes. In: MARQUES, Claudia Lima. **Diálogo das Fontes:** Do conflito à coordenação de normas do direito brasileiro. São Paulo: Revista dos Tribunais, 2012. p. 205-232.

TEFFÉ, Chiara Spadaccini de; MORAES, Maria Celina Bodin de. Redes sociais virtuais: privacidade e responsabilidade civil. Análise a partir do Marco Civil da Internet. **Revista Pensar**. VOl. 22, nº. 1, 2017. Disponível em: <http://periodicos.unifor.br/rpen/article/view/6272>. Acesso em: 04 set. 2017

THE WORLD'S most valuable resource is no longer oil, but data. **The Economist**. 6 maio 2017. Disponível em: https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource. Acesso em: 04 set. 2017

TOFFLER, Alvin. **The Third Wave**. New York: Bantam Books, 1980.

TUTOR, Aranzazu Bartolomé. **Los Derechos de la Personalidad del Menor de Edad su Ejercicio en el Ámbito Sanitario Y en las Nuevas Tecnologías de Información.** Espanha: Aranzadi, 2015.

UBER. **Termos de Serviço**. 2017. Disponível em: <https://www.uber.com/legal/community-guidelines/br-pt/> Acesso em: 19 out. 2017.

VAINZOF, Rony. Da Responsabilidade Civil por Danos Decorrentes de Conteúdo Gerado por Terceiros. In: **Marco Civil da Internet** – lei 12.965/2014**,** São Paulo: Editora Revista dos Tribunais, p. 177-207, 2014.

VELLOSO, Fernando**. Informática**: Conceitos Básicos. 9. ed. Rio de Janeiro: Elsevier Campus, 2014.

VIEHWEG, Theodor. **Tópica e Jurisprudência**. Tradução Tércio Sampaio Ferraz Jr. Brasília: Departamento de Imprensa Nacional, 1979.

VIRI, Nathalia. Pão de Açúcar descobre um tesouro nos algoritmos. **Brazil Journal.** 28 jul. 2017. Disponível em: http://braziljournal.com/pao-de-acucar-descobre-um-tesouro-nos-algoritmos. Acesso em: 04 set. 2017

ZUBOFF, Shoshana. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization (April 4, 2015). **Journal of Information Technology**. n. 30, p. 75–89. doi:10.1057/jit.2015.5. Disponível em: https://ssrn.com/abstract=2594754. Acesso em: 04 set. 2017.