IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO CIVIL CONTEMPORÂNEO

CÉSAR AUGUSTO DE CASTRO FIUZA

MARIA CREUSA DE ARAÚJO BORGES

HELENA NASTASSYA PASCHOAL PITSICA

D597

Direito civil contemporâneo [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: César Augusto de Castro Fiuza; Maria Creusa De Araújo Borges; Helena Nastassya Paschoal Pitsica – Florianópolis: CONPEDI, 2021.

Inclui bibliografia
ISBN: 978-65-5648-426-6
Modo de acesso: www.conpedi.org.br em publicações
Tema: Constitucionalismo, desenvolvimento, sustentabilidade e smart cities.

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Direito civil. 3. Contemporâneo. IV Encontro Virtual do CONPEDI (1: 2021 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

IV ENCONTRO VIRTUAL DO CONPEDI

DIREITO CIVIL CONTEMPORÂNEO

Apresentação

No presente livro, são tratados vários temas. O interessante é que perpassa por todos eles, direta ou indiretamente, a ideia de responsabilidade civil. O Direito Civil Contemporâneo pode ser visto sob dois prismas. Primeiramente, como sinônimo de Direito Civil Constitucional; em segundo lugar, como Direito Civil dogmático, visto sob a ótica do Direito Privado e da autonomia privada. Nos textos que compõem este livro, pode-se verificar ambas as vertentes. Espera-se que o leitor possa tirar bom proveito.

A IDENTIDADE DIGITAL DO USUÁRIO DA INTERNET E A RESPONSABILIDADE CIVIL DECORRENTE DA VIOLAÇÃO DA PRIVACIDADE

THE DIGITAL IDENTITY OF THE INTERNET USER AND THE CIVIL LIABILITY ARISING FROM THE VIOLATION OF PRIVACY

Jaqueline Da Silva Paulichi
Valéria Silva Galdino Cardin

Resumo

Neste artigo serão apresentados alguns conceitos acerca da identidade digital do usuário da internet e das redes sociais. Serão analisados os conceitos de responsabilidade civil, assim como a importância da proteção dos dados no âmbito de proteção da privacidade. A lei geral de proteção de dados traz a possibilidade de responsabilidade civil dos agentes de tratamento dos dados pessoais na internet. Assim, analisar-se-á as hipóteses de responsabilidade civil decorrente da violação do dever de proteger a privacidade dos usuários. Utilizou-se o método hipotético-dedutivo para este artigo, baseando-se na análise de artigos e doutrinas, bem como do estudo da LGPD.

Palavras-chave: Identidade digital, Privacidade, Direitos da personalidade

Abstract/Resumen/Résumé

In this article, some concepts about the digital identity of the internet user and social media will be presented. The concepts of liability will be analyzed, as well as the importance of data protection within the scope of privacy. The general data protection law brings the possibility of liability of agents processing personal data on the Internet. Thus, the hypotheses of liability arising from the violation of the duty to protect the privacy of users will be analyzed. The hypothetical-deductive method was used for this article, based on the analysis of articles and doctrines, as the study of the LGPD.

Keywords/Palabras-claves/Mots-clés: Digital identity, Privacy, Personality rights

1 INTRODUÇÃO

Neste trabalho será apresentado o conceito de identidade digital e a sua relevância na atualidade, levando em consideração a cibercultura e o direito à privacidade. A identidade digital não possui o mesmo sentido que a identidade pessoal, pois na esfera digital é possível que o indivíduo edite suas informações, demonstrando a forma como deseja ser representado no ambiente cibernético.

A identidade digital do sujeito surge após a coleta de inúmeras informações que são coletadas ao longo de sua vida, criando um mosaico de dados que constituem uma personalidade da *internet*. A personalidade digital é constituída pelos algoritmos que realizam a coleta de dados de acordo com as buscas que a pessoa realiza nas plataformas de pesquisa.

Dessa forma, o objetivo geral deste artigo é apresentar o conceito de identidade digital e como esse processo pode violar a privacidade do sujeito, causando danos à intimidade, à honra e a violação dos seus direitos da personalidade. Também será analisada a possibilidade de responsabilizar civilmente a pessoa que faz o uso inadequado dos dados para proteger a privacidade dos usuários.

O texto está estruturado em cinco itens, em que inicialmente se discute acerca do conceito de identidade digital, apresentando os seus contornos jurídicos. Em seguida, serão analisados os conceitos e requisitos da responsabilidade civil e, posteriormente, as situações em que decorre a violação dos direitos da personalidade, mais especificamente, o direito à privacidade.

Por fim, para esta pesquisa foi utilizado o método hipotético-dedutivo, por meio da leitura e fichamento de artigos científicos e textos de doutrinadores que tratam do tema proposto.

2 DA IDENTIDADE DIGITAL

A tecnologia é uma condicionante das relações socioculturais, em decorrência de possibilitar à população conhecer e assimilar novas linguagens, costumes e signos, o que pode levar a uma espécie de inteligência coletiva. (LEVY, 1999)

Além disso, a sociedade digital gera a possibilidade de convívio com outras pessoas, culturas, costumes e, por essa razão, o ambiente virtual possui linguagem própria que é absorvida pelas pessoas. A hiperconectividade ao redor do mundo gera inúmeros dados produzidos e um certo aprofundamento das informações coletadas, devido aos dispositivos que

estão conectados à *internet* 24 horas por dia. (MAGRANI, 2018. p.21)

Comprende-se que a identidade também está inserida no rol dos direitos da personalidade, pois faz parte do aparato do ser humano, conforme leciona Maria Helena Diniz: "O direito da personalidade é o direito da pessoa de defender o que lhe é próprio, como a vida, a identidade, a liberdade, a imagem, a privacidade, a honra, etc." (2017, p.119-120). Dessa maneira, pode-se afirmar que a identidade digital é um desdobramento dos direitos da personalidade e, consequentemente, possui proteção jurídica.

Os perfis das redes sociais possibilitam que as pessoas se comuniquem com o restante do mundo, independente da língua utilizada, gerando uma espécie de imortalidade no *cyberspace* (RUARO, SARLET, 2021. p.198). Dessa maneira, a identidade digital demonstra uma realidade da modernidade, pois através da conexão do usuário é possível que os algoritmos captem dados essenciais do sujeito, como as suas preferências pessoais, anúncios que visita, redes sociais que mais interage, *sites* de compras e lazer, jogos *online*, dados da face e da voz, dentre outros.

Ricardo de Jesus Machado explica acerca da imersão da sociedade no contexto da cibercultura:

> As sociedades do início do século XXI estão imersas no contexto tecnocultural da microinformática em que mesmo os analfabetos funcionais ou digitais fazem parte da imensa rede digital que conecta pessoas e dados e que transforma dados em identidades individuais e coletivas (MACHADO, 2016. p.108).

Com a captação de todos esses dados, tem-se a singularização da pessoa e, consequentemente, a sua identidade digital, que será formada pelas informações em que o próprio sujeito fornece aos sistemas de inteligência artificial, os rastros digitais que deixa quando usa a *internet.* (RUARO, SARLET, 2021. p.198)

Na rede mundial de computadores é possível encontrar páginas pessoais ou ainda páginas das redes sociais em que o sujeito cria uma nova "persona". A identidade digital abrange os modos de ser da pessoa, como a forma de se expressar, o uso de apelidos, avatares, gírias e *emoticons*, considerando uma maneira de manifestação da personalidade do sujeito. (RECUERO, 2009)

A manifestaçao da identidade digital está ligada à cibercultura, pois entende-se que o ser digital realiza diversas ações na *internet*, como as transações comerciais, as conversas com amigos, o estabelecimento de laços afetivos, a busca por conhecimento e informações, além de adquir bens, dentre outros, possibilitando a criação da identidade digital. (NEGROPONTE, 2003) A cibercultura é a expressão de um novo universo "diferente das formas culturais que

vieram antes dele no sentido de que ele se constrói sobre a indeterminação de um sentido global qualquer" (LEVY, 1999. p.20).

Valéria Galdino Cardin e Juliana L. Mazaro definem a identidade virtual como a

> [...]evolução natural para a pessoa, principalmente, aquelas que já nascem inseridas em uma sociedade altamente digital, móvel e tecnológica, assim como, podem ser construídas por aqueles que agregam ao seu conteúdo indentitário já constituído os novos signos, símbolos e costumes da cibercultura (2020).

O usuário das redes sociais expressa sua personalidade pelo espaço virtual, constituindo-se como uma extensão da sua vida cotidiana. Assim, tem-se uma espécie do "eu estendido", que pode ser visualizado como outra denominação da identidade digital. Neste sentido, as mídias sociais se configuram como uma espécie de auto apresentação para aqueles que se utilizam das redes sociais (BELK, 2013).

A Lei Geral de Proteção de Dados traz a previsão de anonimização das informações, sendo um meio para evitar a captação de dados pelos formulários *online*. Sob essa perspectiva, defende-se que deve haver o uso ético das tecnologias da inteligência artificial. Jacob Turner trata desse tema ao questionar como as tecnologias de realizam escolhas éticas (2019).

Acrescente-se que grande parte dos *sites* disponíveis na *internet* lucram com a captação de dados, dificultando o trabalho com a anonimização dos dados dos usuários. Outra questão relevante é a limitação do uso da identidade digital da pessoa para enviar a ele inúmeras publicidades, seja por meio das redes sociais, seja durante a navegação em *sites* na *internet*.

Existe, de fato, um direito à privacidade na rede? Pode-se pensar que não existiria um direito à privacidade na rede quando se analisar os *logins* efetuados pelas redes sociais ou páginas identificadoras, como o caso do Google. Então, caso a pessoa deseja navegar na *internet* de forma anônima, deverá "deslogar" de suas páginas, ou ainda, utilizar um navegador no modo "espião" ou "anônimo".

A discussão quanto à proteção do direito à privacidade iniciou em 1890 com a publicação do artigo *"The Right to Privacy"*, publicado na Revista da Universidade de Harvard. No referido texto, o direito à privacidade foi tratado como o *"right to be let alone"* (SCHREIBER: 2014; p.136-137).

Modernamente, a privacidade pode ser conceituada como o direito que o sujeito possui de impedir que estranhos se intrometam em sua vida privada e familiar, impedindo que tenham acesso à informações, possuindo também o direito de impedir que estas sejam divulgadas indevidamente. (BASTOS: 1989; p.63)

A privacidade compreende o ato intelectual de expressar por escritos os fatos que podem ser descritos por qualquer outro meio, se apresentando como uma das vertentes do direito de estar só. (WARRENS BRANDEIS: 1890; p.205)

Na década de 1960, houve uma mudança do cenário quanto ao direito à privacidade, decorrente das novas tecnologias e dos meios inovadores de processamento de informações. Tal fato resulta no uso dos dados da população nas mais variadas formas, como a análise e concessão de crédito em instituições financeiras, planos de saúde, vagas de emprego, etc.

Dessa forma, a privacidade em sua concepção moderna possui um sentido mais amplo que o direito à intimidade, abrangendo diversos setores e aspectos do ser humano, como as suas características físicas, dados acerca da sua saúde, crenças pessoais, filosóficas e religiosas, dentre outras. Logo, o direito à privacidade irá abranger o controle da coleta e utilização das próprias informações pessoais. (SCHREIBER, 2014)

A privacidade não pode ser confundida com a intimidade, eis que a primeira diz respeito as questões externas do ser humano, como o recinto do seu lar, a conta telefônica, o modo de viver, etc., enquanto a segunda trata do foro íntimo, como os segredos, as relações íntimas, a orientação sexual, dentre outras. (DINIZ, 2005)

A teoria das esferas diferencia o conteúdo do direito à privacidade, diferenciando-o da intimidade e do sigilo. Dessa forma, na esfera do direito à privacidade existem outras duas subdivisões, no qual a primeira trata da intimidade e a segunda trata do sigilo. A esfera da intimidade seria uma espécie de intermediária com o direito ao sigilo. (FERRAZ JUNIOR, 1992)

Tércio Sampaio Ferraz Jr. explica sobre o conteúdo do direito aqui debatido explicando que:

> A privacidade é regida pelo princípio da exclusividade, cujos atributos principais são a solidão (o estar-só), o segredo, a autonomia. Na intimidade protege-se sobretudo o estar-só; na vida privada, o segredo; em relação à imagem e à honra, a autonomia. A privacidade tem, pois, a ver com a inviolabilidade do sigilo. (FERRAZ JUNIOR, 1992)

A privacidade possui os seus atributos, "[...] no recôndito da privacidade se esconde, pois, em primeiro lugar, a intimidade. A intimidade não exige publicidade, porque não envolve os direitos de terceiros. O problema da aplicação da teoria das esferas é que não há uma explicação acerca da ligação entre o sigilo e a privacidade (FERRAZ JUNIOR: 1992; p.54).

O direito à privacidade já ganhou novos contornos jurídicos em decorrência das inovações tecnológicas:

> Com o desenvolvimento da tecnologia, passa a existir um novo conceito de privacidade, sendo o consentimento do interessado o ponto de

> referência de todo o sistema de tutela da privacidade, direito que toda pessoa tem de dispor com exclusividade sobre as próprias informações, nelas incluindo o direito à imagem.[1]

O comércio eletrônico cresce de maneira exponencial e assim as empresas de publicidade que atuam na *internet* se utilizam de técnicas que influenciam o usuário:

> Cada vez mais, os usuários da *Internet* subvertem-se em consumidores, sendo uma clara amostra de tal afirmação o crescimento exponencial do comércio eletrônico. No Brasil, o *e-commerce* acumula taxas de crescimento significativas, tendo faturado a quantia expressiva de R$ 44,4 bilhões no ano de 2016. Assim, cresce, em igual importância, os anúncios publicitários *on-line* para induzir o usuário ao consumo (BIONI, 2021).

É por esse motivo que as empresas de publicidade se utilizam de tecnologias que buscam identificar até mesmo quais produtos o sujeito está disposto a adquirir.

As empresas de publicidade se utilizam da identidade digital do usuário para vender cada vez mais produtos e serviços, de modo personalizado. Cite-se o caso do grande conglomerado de empresas da *internet* o "*Facebook*". A referida empresa é proprietária de outras redes sociais muito conhecidas, como o *Whatsapp* e o *Instagram*. No entanto, a rede social "*Whatsapp*" é uma rede de troca de mensagens, não havendo espaço para publicidade. Então, qual seria o modo de monetização da respectiva rede?

A monetização ocorre com a captação dos dados pessoais de seus usuários durante as mensagens trocadas. Note-se que o conglomerado "*Facebook*" se utiliza das informações inseridas nas suas redes sociais para otimizar a experiência do usuário durante a navegação, através do cruzamento dos dados. Essa "otimização" da experiência do usuário ocorre através de anúncios publicitários.

Bruno Bioni explica sobre a política da empresa:

> [...] em 2015, a (nova) política de privacidade do WhatsApp concretizou a cogitada reversão do seu modelo de negócio. Agora, os dados dos seus usuários são compartilhados entre o grupo de empresas do *Facebook* para "aprimorar as experiências" dos seus serviços, especialmente com relação aos "anúncios e produtos no *Facebook* (2021).

Essa publicidade direcionada aos consumidores demonstrou ser mais eficaz, e assim, as empresas de tecnologias passaram a se utilizar das informações que os próprios usuários

[1] STJ, REsp 1168547/RJ, 4ª T, Rel. Min. Luis Felipe Salomão, j. 11/05/2010, v.u., DJe 07/02/2011

repassam nos formulários *online*. Muitos desses dados proporcionam acesso aos serviços gratuitos, que é uma forma eficaz de captação (BIONI, 2021).

Dessa maneira, percebe-se que os registros de navegação criam um retrato das preferências dos usuários ou, em outras palavras, a sua identidade digital. Assim, a publicidade passa a ser atrelada ao perfil comportamental do consumidor, pois "sabe-se o que ele está lendo, quais os tipos de *websites* acessados, enfim, tudo aquilo em que a pessoa está efetivamente interessada" (BIONI, 2021).

O perfil comportamental do consumidor é utilizado pelas empresas de tecnologia e de inteligência artificial para realizar o direcionamento da publicidade. O grande problema dessa prática é que os consumidores ficam desprotegidos quanto ao número excessivo de publicidade que recebem diariamente, nas mais diversas plataformas digitais. Defende-se que essa prática necessita de limites para que não haja violação aos direitos da personalidade, como a privacidade, a intimidade, o sigilo, a imagem, a voz, ao direito autoral, dentre outros.

3 DOS FUNDAMENTOS DA RESPONSABILIDADE CIVIL

No que diz respeito à responsabilidade civil, cumpre dizer que ela faz parte do direito das obrigações, tendo em vista que é resultante de um ato ilícito que é cometido, gerando a obrigação de reparar o dano. As obrigações que surgem a partir do ato ilícito são constituídas por meio de ações ou omissões – sejam elas culposas ou dolosas – praticadas pelo agente, sendo que a partir delas surge a obrigação de indenizar ou ressarcir os prejuízos que foram causados.

Segundo Judith Martins-Costa, a responsabilidade civil "significa ingressar num vasto e fascinante universo (...) no qual se emaranham aspectos do mais profundo significado ético atinente à própria condição humana" (2003, p.92).

A responsabilidade civil se fundamenta em três pressupostos e conforme a teoria clássica, são: o dano, a culpa do autor do dano e o nexo de causalidade entre o fato e o dano. "Na etiologia da responsabilidade civil, estão presentes três elementos, segundo a doutrina subjetivista: a ofensa a uma norma preexistente ou o erro de conduta, um dano e o nexo de causalidade entre uma e outra" (STOCCO, 2007. p.151).

Não havendo prova do dano, não há que se falar em responsabilidade civil. E, no que diz respeito ao dano, esse pode ser de cunho moral ou material ou ambos. Dessa forma, caso não se tenha a efetiva comprovação do dano, não há o dever de indenizar. Vale dizer que a responsabilidade objetiva também conta com uma cláusula geral que está elencada no parágrafo único do art. 927 do supracitado código, sendo aqueles casos que em razão do risco do ato

praticado haverá a responsabilidade objetiva (Teoria do Risco). Pode-se citar como exemplo: as empresas que tratam de material radioativo.

Contudo, não é qualquer risco que pode ser caracterizado segundo o que preconiza o parágrafo único do artigo 927 do Código Civil, pois, se houvesse a consideração de todo e qualquer risco como a possibilidade de responsabilidade objetiva, existiria uma banalização da responsabilidade objetiva (STOCCO, 2007. p.154).

Nesse contexto, somente os riscos excepcionais, extraordinários e fora do comum podem ser enquadrados como responsabilidade objetiva, de acordo com as regras estabelecidas pelo Código Civil. Hodiernamente, a responsabilidade objetiva divide-se entre a teoria do risco e a teoria do dano objetivo, sendo que as duas atingiram o objetivo do dever de indenizar independente de culpa (STOCCO, 2007. p.156).

O uso excessivo do perfil comportamental do consumidor e dos usuários das mídias sociais, para o envio das mais variadas publicidades, gera um dano, mesmo que não seja de fácil percepção. O usuário possui a autonomia para escolher não ver determinadas publicidades, ou ainda para optar em não utilizar as redes sociais. No entanto, essa publicidade irá gerar o dever de indenizar quando demonstrar o abuso, contrariar os bons costumes, se apresentar de modo excessivo nas redes ou outras formas que violam a lei.

Nos termos da teoria do dano objetivo, havendo um dano, independentemente de culpa, este deve ser ressarcido. Atualmente, há uma tendência em substituir o conceito de responsabilidade pelo de reparação, a culpa pelo risco, a responsabilidade subjetiva pela responsabilidade objetiva, contudo, deve-se tomar cuidado com as referidas substituições para que não haja erros na responsabilização de pessoas físicas e jurídicas.

No direito pátrio, para se falar em responsabilidade, deve existir culpa, conforme preceitua a teoria subjetiva, prevista no art. 186 do Código Civil. Assim, para haver a efetiva reparação de um dano, deve-se, necessariamente, comprovar a culpa do agente que a cometeu, pressupondo que esse ato seja ilícito.

Porém, não se pode ignorar que o Código Civil adota outras teorias, como a responsabilidade objetiva prevista nos artigos 936, 937 e 938, que tratam da responsabilidade do dono de animal, do edifício e daquele que habita o imóvel, dentre outros. Nos termos do que dispõe a teoria do risco, se alguém exerce atividade que naturalmente possui algum risco de

danos para terceiros e ocorrendo este, o causador do dano, mesmo que isento de culpa será responsabilizado. (TARTUCE, 2015).

A lei impõe que, em certos casos, o dever de reparar é independente da prova de culpa e, quando isso ocorre, a responsabilidade será definida como objetiva, necessitando apenas do nexo de causalidade e do dano. Nesta, não há a necessidade de se comprovar a culpa do agente, pois a responsabilidade estará fundada no risco, sendo a culpa irrelevante para configurar o dever de indenizar. Contudo, ainda é necessário que se comprove o nexo de causalidade entre o fato e o dano, a fim de saber quem deu causa ao dano, pois, caso contrário, mesmo sendo objetiva, não haverá o dever de indenizar (TARTUCE, 2015).

Dessa maneira, a violação dos dados digitais do sujeito pode ensejar a responsabilidade civil, pois informações pessoais e íntimas ficam a mercê dos *softwares* que captam os dados. Por exemplo, cite-se os casos em que os dados de milhões de usuários são colocados à venda em fóruns da *internet*, com a intenção de vender produtos e serviços ou ainda com a intenção de demonstrar o quanto é frágil a proteção desses *sites*.

O número excessivo de anúncios recebidos por celular, pelas redes sociais e durante a navegação do usuário demonstram a fragilidade do sistema. Assim, a responsabilidade civil pode ocorrer durante o uso de uma rede social ou de um *site* que solicite as informações pessoais da pessoa. O mais comum é a clonagem do cartão de crédito e a compra de produtos e serviços de forma indevida, necessitando, então, que os provedores forneçam melhores condições para proteger a privacidade dos dados dos seus usuários. Quando se tratar dos dados de inúmeros usuários das redes, tem-se o dano quanto aos interesses difusos, devendo haver a tutela pelos órgãos competentes.

4 A PROTEÇÃO AO DIREITO À PRIVACIDADE NA CAPTAÇÃO DE DADOS

Os dados pessoais dos consumidores são considerados ativos digitais na economia da informação. Assim, “os dados pessoais dos cidadãos converteram-se em um fator vital para a engrenagem da economia da informação” (BIONI,2020 p.10). Consequentemente, existe um mercado que se sustenta com a extração desses dados e os padroniza. Ressalte-se que os usuários sempre confirmam o consentimento quando se trata de dados pessoais.

O consumidor deixou de ter uma posição passiva, e neste diapasão o sujeito tem participação ativa fornecendo os seus próprios dados pessoais, transformando-se na figura da

pessoa que consome e também produz o seu bem de consumo, conforme as suas predileções, o seu padrão de consumo, a sua posição geográfica, e os locais que mais gosta de frequentar.

Bruno Bioni realiza uma reflexão acerca do tema:

> O consumidor deixa, portanto, de ter uma posição meramente passiva no ciclo do consumo. Ele passa a ter uma participação ativa, que condiciona a própria confecção, distribuição e, em última análise, a segmentação do bem de consumo, transformando-se na figura do *prosumer*. O consumidor não apenas consome (*consumption*), mas, também, produz o bem de consumo (*production*): *prosumer* (BIONI, 2020. p.13).

Pode-se citar como exemplo o aplicativo Waze, que permite ao usuário marcar os locais que frequenta e utiliza de sua geolocalização. Empresas como Microsoft, Apple e Google têm investido nesta forma de IA:

> i) o patenteamento da tecnologia de direcionamento de anúncios com base em emoções; ii) a implementação de um sistema de processamento de movimentos (M7), o qual identifica os deslocamentos dos usuários para precisar o estado mental deles no momento de interação com o celular; iii) projeção de um sistema para detectar sorrisos e outras expressões faciais de quem assiste a vídeos no YouTube (BIONI, 2020. p. 18).

Uma das formas de ilustrar a captação de dados é o caso de uma empresa americana que utiliza dados para identificar consumidoras que estão grávidas. Assim, a equipe da empresa conseguiu verificar qual o perfil do consumidor que adquire uma determinada lista de produtos próprios das pessoas que já estão esperando bebês, e isso permitiu que a empresa realizasse a previsão acerca da gravidez, o período da gestação. etc., direcionando produtos específicos conforme a fase gestacional da usuária. Ocorre que existem os casos em que a mulher perde o bebê e continua a receber informações e anúncios publicitários relativos à gravidez, bem como anúncios de outros produtos relacionados ao tema, sem que a pessoa saiba ao menos que está grávida (BIONI, 2020).

O mesmo sistema também é utilizado para pessoas que colocam sintomas de doenças no sistema de busca do Google e, assim, logo após os anúncios relacionados à doença, ou ainda possíveis diagnósticos lhe são dispostos em suas redes.[2]

[2] Um dos exemplos mais citados para ilustrar *Big Data* é o da ação por parte da varejista americana Target para identificar consumidoras grávidas. A gravidez é uma fase da vida na qual tais consumidoras consomem uma infinidade de produtos, sendo, por isso, tal informação estratégica.

Em 2018, a empresa *Cambridge Analytica (*empresa de análise de dados) utilizou-se de dados de mais de 50 milhões de usuários do *Facebook*, que foram coletados através de testes psicológicos, para fazer propaganda política. A referida empresa participou de grandes campanhas eleitorais como a do *Brexit* no Reino Unido e a campanha de Donald Trump. Após o escândalo do uso e tratamento indevido dos dados de milhões de usuários, iniciou-se o debate acerca da proteção dos dados pessoais (SCHREIBER, 2021).

O avanço tecnológico, o uso excessivo das redes sociais como meio de comunicação, o fornecimento de informações pessoais, quando são preenchidos os formulários *online*, auxiliam na captação de todos esses dados pessoais. Ocorre que, nem sempre o usuário percebe que tais informações podem ser utilizadas de maneira inadequada, seja para venda a terceiros, ou ainda para a conversão em publicidades.

A Lei Geral de Proteção de Dados (LGPD) prevê no art. 2º que a proteção de dados pessoais possui como fundamentos o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, de informação, de comunicação, de opinião, a inviolabilidade da intimidade, da honra, da imagem, o desenvolvimento econômico tecnológico, a inovação, a livre iniciativa, a livre concorrência, a defesa do consumidor e os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Dessa forma, o direito à privacidade dos usuários deve ser resguardado durante o tratamento dos seus dados, assim como a necessidade de que saibam para qual finalidade seus dados estão sendo captados. A lei supracitada possui o objetivo de conferir aos cidadãos um maior controle e autonomia dos dados pessoais, necessitando que a pessoa forneça seu consentimento para a captação e tratamento de seus dados. A LGPD foi elaborada com a finalidade de evitar que as informações sejam utilizadas de modo abusivo.

O art. 42 da Lei prevê: "O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual

---

A equipe de análise da Target conseguiu verificar que tal perfil de consumidoras adquiria uma determinada lista de produtos. Isso permitiu não só prever o estado de gravidez, mas, também, o período de gestação para, daí, lhes direcionar produtos de acordo com a respectiva fase da gravidez.
Dessa forma, os algoritmos dos bancos de dados foram programados para estabelecer tal correlação, segmentando, dentre as milhares de consumidoras, aquelas com tal perfil para fins de ação publicitária.
A eficiência da tecnologia em questão foi comprovada quando um pai furioso entrou no estabelecimento comercial de tal empresa, acusando-a de incentivar a sua filha adolescente a engravidar. Passados alguns dias, o gerente da loja, preocupado em perder o cliente, ligou para o furioso pai. Este último, acanhado do outro lado da linha, informou que tinha tomado conhecimento de fatos até então ignorados: a sua filha estava grávida, desculpando-se pelo ocorrido. (BIONI, 2020. P.36)
Revista Veja. Entenda... Op.cit., p.71. Nesse mesmo sentido: MAYER-SCHONEBERGER, Viktor; CUKIER, Kenneth. *Big data*

ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo". A partir da análise do referido dispositivo, pode-se perceber que a LGPD abrange não apenas as lesões realizadas no âmbito individual, mas também aquelas realizadas coletivamente, mesmo porque inúmeras pessoas não procuram o Poder Judiciário ao descobrir que os seus dados foram violados.

O artigo supramencionado trata da responsabilidade objetiva, fundamentado na teoria do risco, que determina que toda pessoa que exerça alguma atividade e que possa gerar danos deverá repará-los, caso haja os requisitos da responsabilidade civil, disciplinado no parágrafo único do art. 927 do Código Civil.

Ainda, no art. 43 existe a previsão da exclusão da responsabilidade, quando o ato for realizado por terceiros, recaindo a responsabilidade civil ao encarregado, se este for o terceiro envolvido ou ainda um *cyber* criminoso (MELLO, 2019).

Os direitos da personalidade são violados por diversas maneiras, desde a venda de dados de clientes que fizeram financiamentos e empréstimos até a recusa do cadastro da pessoa com base na pontuação de sistemas que não estão acessíveis aos cidadãos (SCHREIBER, 2014). Ao realizar um cadastro em um *site*, ou até mesmo em uma loja, o consumidor não está autorizando que estes dados sejam vendidos a terceiros. Significa apenas que o seu consentimento é para aquele ato (SCHREIBER, 2014). Ocorre que nem sempre as empresas se utilizam desses dados apenas para o seu cadastro interno, e que muitas vezes essas informações são vendidas a terceiros. Pelas regras de interpretação dos negócios jurídicos, deve-se levar em conta que o consumidor anuiu apenas com o repasse de seus dados para aquela empresa específica.

No campo militar, fala-se em robôs soldados que são capazes de tomar decisões autônomas acerca do uso de armas letais. No campo financeiro, também existem inteligências artificiais que decidem quando comprar e quando vender ações na bolsa de valores. A *internet* das coisas - ou IOT - é o meio mais propício para a difusão do sistema de inteligência artificial e para a captação de dados pessoais de seus usuários. Gustavo Tepedino trata do fenômeno da *internet of things (internet* das coisas), que é um campo que difunde os sistemas de inteligência artificial. (TEPEDINO, SILVA, 2019).

Em relação à responsabilidade civil e ao dano indenizável, questiona-se se o usuário ou programador de inteligência artificial pode ser isentado da responsabilidade civil sob o argumento de que os sistemas são autônomos e adotaram condutas imprevisíveis. Questiona-se também acerca do modo de aprendizado da máquina, em que está ainda está na fase de melhoramento e do conhecimento de suas possibilidades decisórias.

Ressalte-se que a responsabilidade será sempre contratual, em que o usuário, ao anuir com aquela forma de inteligência artificial, seja com o uso de tecnologias vestíveis ou ainda com o uso de aplicativos da *internet*, estará assinando um contrato de adesão. Note-se que os usuários raramente leem os termos do contrato de adesão ou os termos de serviço, pois, na maioria das vezes, a ferramenta a ser utilizada solicita de seus usuários alguns dados pessoais, que não lhe custam um centavo. E assim, a inteligência artificial é alimentada com os dados pessoais dos usuários.

Gustavo Tepedino e Rodrigo G. Silva abordam acerca dos critérios de imputação da responsabilidade:

> Ainda, no que diz respeito aos critérios de imputação: o regime de responsabilidade será subjetivo ou objetivo? Se subjetivo, pode-se associar a maior autonomia do sistema de inteligência artificial à menor reprovabilidade da conduta do usuário? Podem incidir regularmente as causas excludentes de ilicitude? Se objetivo o regime de responsabilidade, qual exatamente haveria de ser seu fundamento? (TEPEDINO, SILVA, 2019).

Os autores também questionam se essa responsabilidade seria objetivo-subjetiva ou ainda, quando for subjetiva, se poderia ser associada com a autonomia do sistema de inteligência artificial (TEPEDINO, SILVA, 2019).

A União Europeia, já preocupada com a responsabilidade civil decorrente do uso dos meios de inteligência artificial, estabelecendo a Diretiva 2010/40/EU do Parlamento Europeu, que estabelece “um quadro para a implantação de sistemas de transporte inteligentes no transporte rodoviário, inclusive nas interfaces com outros modos de transporte”.

A LGPD prevê a proteção especial dos dados sensíveis, no qual o seu tratamento ocorrerá apenas nas hipóteses previstas de modo expresso na lei. Na GDPR não existe equivalência em relação a este dispositivo. A LGPD prevê que os dados sensíveis podem ser tratados independentemente do consentimento nas hipóteses em que for indispensável para a execução pela administração pública prevista em alguma lei ou regulamento, ou ainda, para a garantia da prevenção à fraude e à segurança do titular nos processos de identificação e autenticação de cadastro em sistemas eletrônicos.

A lei europeia proíbe o tratamento dos dados sensíveis, porém estabelece algumas exceções como os dados que se tornam públicos pelo titular e os dados relativos a atuais membros de fundações associações organizações sem fins lucrativos, desde que o tratamento seja para fins legítimos e com medidas de segurança apropriadas.

De acordo com o art. 11 da LGPD, o tratamento[3] de dados pessoais sensíveis só poderá ocorrer nas hipóteses em que: o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas. Podendo ser dispensado o consentimento nos casos previstos em lei.[4]

Com relação ao tratamento de dados de menores, a LGPD prevê a necessidade de consentimento dos responsáveis legais para o tratamento dos dados pessoais para todos aqueles que forem menores de 18 anos, conforme a previsão do estatuto da criança e do adolescente. Enquanto isso, a lei europeia, GDPR, aceita o consentimento dos maiores de 16 anos.

Em relação à política de proteção de dados, a lei brasileira tratou de implementar um programa de governança em privacidade como a faculdade aos controladores dos dados, ou seja, pode ser que estes controladores não realizem tal programa. Já a Lei Europeia atribuiu aos controladores dos dados a obrigação para adotar medidas técnicas e de organização que sejam adequadas para assegurar o tratamento de dados em conformidade com a legislação.

Aos representantes das empresas de tratamento de dados, a lei brasileira prevê que a empresa estrangeira será intimada de todos os atos processuais na pessoa do seu agente ou representante que tem estabelecimento no Brasil. Dessa forma, pode-se inferir que empresas estrangeiras que não possuem estabelecimento, representantes, ou escritórios situados no país não estarão sujeitos às penalidades decorrentes da LGPD.

A partir dessa premissa, pode-se perceber uma lacuna na lei e a possibilidade de que empresas estrangeiras passem a disponibilizar no país seus serviços, porém com as suas sedes, representantes e demais escritórios em países vizinhos, para que não sejam penalizadas quanto ao tratamento indevido dos dados pessoais e dados sensíveis[5]. Já a GDPR prevê aplicabilidade

---

[3] O tratamento dos dados pessoais está previsto no art. 5º da LGPD, inc. X:- tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

[4] a) cumprimento de obrigação legal ou regulatória pelo controlador; b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos; c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis; d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ; e) proteção da vida ou da incolumidade física do titular ou de terceiro; f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais.

[5] A definição de dado pessoal sensível está no Art. 5º da LGPD, inc. II: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

na figura do controlador ou do processador de dados em quaisquer estados membros da União Europeia.

Quanto à responsabilidade civil, a lei brasileira prevê como excludente de responsabilidade a ausência de envolvimento da pessoa física ou jurídica com o tratamento dos dados, ou ainda, mesmo quando houver dano e o tratamento for realizado em conformidade com a legislação e, por fim, quando os agentes comprovarem que o dano é decorrente de culpa exclusiva do titular dos dados ou ainda quando a culpa for exclusiva de terceiros.

Ressalte-se que pode ser feita a essa última hipótese ocorre quando as empresas se utilizam da culpa exclusiva de terceiros com a indicação de *sites* que são disponibilizados no país, porém tem sede em outros países em que não são abrangidos pela lei geral de proteção de dados brasileira.

Por sua vez, a lei européia prevê apenas como excludente de responsabilidade quando a pessoa física ou jurídica não estiver envolvida com tratamento de dados, ou ainda quando for realizado conforme a previsão da legislação e, dessa forma, não haverá responsabilização quanto aos agentes responsáveis pelo tratamento dos dados pessoais.

Com relação aos dados que os usuários permitem que o *site* os utilize, a lei brasileira aplica a regras gerais de consentimento, transparência e direito de objeção dos titulares desses dados. Já A GDPR estabelece previsões específicas, ou seja, o titular dos dados que verificar que estes foram violados tem a possibilidade de se opor a essa violação e o tem direito de se opor ao tratamento dos dados pessoais.

No Brasil, por exemplo, quando se tratar de dados anonimizados, estes podem ser utilizados para a padronização e serem utilizados por meio da inteligência artificial de análise preditiva e, posteriormente, serem vendidos para empresas que tenham interesse naquelas informações (desde que sejam anonimizadas).

A lei brasileira também não prevê a exigência de contrato formal entre o usuário e o controlador ou a pessoa que irá realizar o tratamento desses dados, enquanto a lei europeia por sua vez, prevê que haja o contrato ou ato jurídico equivalente. Dessa forma, o direito à privacidade deve ser protegido de maneira abrangente, desde o início da captação desses dados, até o final do tratamento pela empresa detentora, devendo ser apagado após o uso. Existem inúmeras formas de se requerer que os dados sejam apagados ou ainda a tutela por dano moral e material decorrente do uso abusivo destes. No entanto, nem sempre a pessoa entende que há violação dos dados mais básicos como a violação de um direito.

Nem todos os atos realizados rotineiramente na *internet* deveriam ser captados pelos sistemas de inteligência artificial, eis que se trata de aspectos íntimos do ser humano. Ainda se

questiona: como se dará a valoração da violação dos dados de apenas uma pessoa? Judicialmente, existirá algum modo de indenizar o consumidor apenas em decorrência da violação de suas informações?

A privacidade do usuário é violada constantemente por meio da captação de seus dados de navegação e a transformação desses em informações para a compra de produtos e serviços. Assim, não só a personalidade é violada, mas também o poder de decisão acerca da compra do produto, já que o consumidor é bombardeado de publicidades constantemente. Não há como se precisar exatamente qual o âmbito de captação desses dados. É por esse motivo que a Lei Geral de Proteção de Dados prevê o tratamento ético dos dados, mas isso depende da aplicação e fiscalização da lei e não apenas de sua formalização.

5 CONCLUSÃO

A Lei Geral de Proteção de Dados possui como princípio fundamental a proteção à privacidade de seus usuários, a necessidade de consentimento livre e esclarecido, dentre outros. O respeito ao direito à privacidade e seus desdobramentos ocorre por meio do consentimento do usuário ao clicar em *sites*, anúncios, redes sociais, jogos, dentre outros.

Ocorre que, mesmo com a necessidade de consentimento do usuário para tratamento de suas informações, é possível que empresas repassem os dados pessoais a outras, ou ainda que haja o uso indevido desses dados.

Um dos exemplos mais comuns é a venda de banco de informações de consumidores de estabelecimentos bancários a empresas de empréstimos, ou ainda, o uso dos dados dos consumidores no mercado, como meio de pontuar o crédito, em que aqueles que já tenham o histórico de débitos e pendências financeiras possuem uma pontuação menor e, consequentemente, terão acesso dificultado a empréstimos e outros serviços bancários.

Na era da tecnologia, as empresas de publicidade que atuam pela *internet* se utilizam da identidade digital do sujeito, que se utilizam dos dados mais básicos, como a localização do usuário, o tempo que passa analisando *sites* e redes sociais, os anúncios que clica, os jogos que gosta e até mesmo a forma de se comunicar nas redes sociais. Tudo isso gera a sua identidade digital e, consequentemente, empresas direcionam seus anúncios publicitários para que consigam vender cada vez mais produtos e serviços.

Os contratos eletrônicos, que são realizados constantemente pelos usuários, por já estarem escritos e se classificarem como contratos de adesão, recebem tratamento consumerista. No entanto, a grande discussão acerca dos “termos e condições” dessas redes sociais é se estas

realmente tratam do interesse do usuário, e se o aplicativo ou rede social irá cumprir com os termos elencados. Outra questão relevante é se o usuário realmente lê o termo de adesão, ante a possibilidade de captação de dados pessoais, como acesso a câmera, contatos de telefone, acesso as redes sociais, dentre outros.

Nem todos os usuários leem os termos e condições do aplicativo que instala em seus *smartphones*, gerando a facilidade de captação indevida de dados. Os programas que são instalados nos computadores e celulares quase sempre estão vinculados a uma conta pessoal do *google* ou do *facebook*, realizando assim o cruzamento das informações do usuário. Outro aspecto a ser notado é de que a maioria dos aplicativos pedem acesso a câmera do dispositivo móvel, contatos, e demais dados pessoais para que se tenha acesso à todas as funções do aplicativo. Por estes motivos que se faz necessário a pesquisa acerca do uso das redes sociais e possíveis soluções para a invasão de privacidade e violação dos direitos da personalidade ante a identidade digital do sujeito.

O direito à privacidade e seus desdobramentos, como a intimidade, o sigilo, o segredo, etc., são os direitos comumente violados quando ocorre o uso indevido das informações pessoais, gerando a responsabilidade civil de empresas que realizam o tratamento desses dados. Enquanto não havia previsão legal acerca da responsabilidade dessas empresas, a insegurança jurídica era maior, levando a injustiças. Muitas empresas que não possuem sede no Brasil se beneficiavam pela ausência de legislação a respeito dos dados pessoais, o que mudou consideravelmente após o advento da LGPD.

Assim, com a Lei Geral de Proteção de Dados, espera-se que as empresas atuem de maneira ética ao captar e tratar os dados pessoais, pois, caso não ocorra o respeito aos preceitos estabelecidos em lei, poderá ocorrer a responsabilidade civil do agente.

REFERÊNCIAS

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 1989.

BELK, R. *Extended self in a digital world. Journal of Consumer Research,* v. 40, n. 3, 2013.

BIONI, Bruno Ricardo *Proteção de Dados Pessoais: a função e os limites do consentimento*. Rio de Janeiro: Forense, 2021.

BITTAR, Carlos Alberto. Os direitos da personalidade. Saraiva, São Paulo: 2013.

CARDIN, Valéria Silva Galdino. MAZARO, Juliana Luiza. *Identidade Cultural Cyber E Identidade Virtual: A Construção De Novos Direitos Da Personalidade Pela Cibercultura*. Conpedi. Grupo de Trabalho Direito, Governança e Novas Tecnologias I apresentados no II Encontro Virtual do CONPEDI. Direito, governança e novas tecnologias I [Recurso eletrônico on-line] organização CONPEDI Coordenadores: Aires Jose Rover; Danielle Jacon Ayres Pinto; Fabiano Hartmann Peixoto; José Renato Gaziero Cella – Florianópolis: CONPEDI, 2020.

DINIZ, Maria Helena. *Curso de direito civil brasileiro: Teoria Geral do Direito Civil*. São Paulo: Saraiva, 2005.

FERRAZ JUNIOR, Tércio Sampaio. *Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado.* Cadernos de direito constitucional e ciência política, ano 1. São Paulo: Revista dos Tribunais, 1992.

LEVY, Pierre. *Cibercultura.* São Paulo. 34, 1999.

MACHADO, Ricardo de Jesus. "*Eu digital": identidade e audiovisualidades na web. In: FLICHY, P. et al. Redes digitais: um mundo para os amadores. Novas relações entre mediadores, mediações e midiatizações*. Brazil, South America: Brasil, 2016. ISBN 978-85-8384-045-9. Disponível em: https://www.ufsm.br/editoras/facos/redes-digitais/ Acesso em: 02 set. 2021.

MAGRANI, Eduardo. *A internet das coisas*. Rio de Janeiro: FGV Editora, 2018.

MARTINS-COSTA, Judith. *Comentários ao Novo Código Civil*. Rio de Janeiro: Forense, 2003.

MELLO, Luan Maia de. *Agentes de Tratamento de dados pessoais*. *In:* FEIGELSON, Bruno. SIQUEIRA, Antonio Henrique Albani (coord). *Comentários À Lei Geral De Proteção De Dados Lei 13.709/2018.* Revista dos Tribunais, São Paulo: 2019.

SIQUEIRA, Antonio Henrique Albani. *Coleção Direito e novas tecnologias: Comentários à lei geral de proteção de dados.* Revista dos Tribunais: São Paulo, 2019.

NEGROPONTE, Nicholas. *Vida digital*. São Paulo: Companhia das letras, 2003.

RECUERO, Raquel. *Redes sociais na internet*. Porto Alegre: Sulinas, 2009.

RUARO, Regina Linden. SARLET, Gabrielle Bezerra Sales. *O direito fundamental à proteção de dados sensíveis no sistema normativo brasileiro: uma análise acerca das hipóteses de tratamento e da obrigatoriedade do consentimento livre, esclarecido e informado sob o enfoque da lei geral de proteção de dados (lgpd) – lei 13.709/2018*. In: Tratado de proteção de dados pessoais. DONEDA, Danilo... [et al.] Rio de Janeiro: Forense, 2021.p.198

SCHREIBER, Anderson. *Direitos da personalidade*. São Paulo: Atlas, 2014.

SCHREIBER, Anderson. *Responsabilidade Civil na lei Geral De Proteção de Dados Pessoais.* in. Danilo Doneda ... [et al.]. – Rio de Janeiro: Forense, 2021.

STOCO, Rui, *Tratado de Responsabilidade Civil*. São Paulo: RT, 2007.

TARTUCE, Flávio. *Direito Civil 2:* Direito das Obrigações e Responsabilidade Civil. São Paulo: Método, 2015.

TEPEDINO, Gustavo; SILVA, Rodrigo da Guia. *Desafios da inteligência artificial em matéria de responsabilidade civil. Revista Brasileira de Direito Civil* – RBDCivil, Belo Horizonte, v. 21, p. 61-86, jul./set. 2019

TURNER, Jacob. *Robot Rules: Regulating Artifcial Intelligence*. PALGRAVE PACMILLAN. London Uk. 2019. ISBN 978-3-319-96234-4 https://doi.org/10.1007/978-3-319-96235-1.

WARREN, Samuel D.; BRANDEIS, Louis, D. *Right to privacy*. Harvard Law Review. Vol.IV, Dec.15.1890, No. 05. Disponível em: https://www.cs.cornell.edu/~shmat/courses/cs5436/warren-brandeis.pdf Acesso em: 17.fev.2021