



**COOKIES E DIREITOS DA PERSONALIDADE: DESAFIOS SOBRE A
APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**

*COOKIES AND PERSONALITY RIGHTS: CHALLENGES ABOUT THE GENERAL DATA
PROTECTION LAW APPLICABILITY*

Micaela Mayara Ribeiro¹

Zulmar Fachin²

Resumo: Este artigo é uma reflexão sobre “cookies”. Tem por objetivo analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais no uso dos *cookies*, frente à possibilidade de eles guardarem dados pessoais ilicitamente. Considera que os *cookies*, compreendidos como um arquivo que armazena informações do usuário durante a visita em páginas da *web*, podem violar direitos da personalidade. Adota-se o método dedutivo, utilizando livros, artigos científicos e normas do ordenamento jurídico brasileiro. O estudo revela que, embora signifique um avanço legislativo, a Lei Geral de Proteção de Dados, é insuficiente para evitar a violação a direitos da personalidade.

Palavras-chave: Privacidade; internet; preferências; violação; direitos da personalidade

Abstract: This article is a reflection on “cookies”. The objective is to analyze the General Data Protection Law applicability in the use of cookies, since there is a possibility that they may store data unlawfully, violating personality rights. Consider that cookies, understood as a file that stores information during the user's visit the web, may violate personality rights. The deductive method is adopted, using books, scientific articles and norms of the legal system to scrutinize the research. The study reveals that the General Data Protection Law, although it represents a legislative advance, is insufficient to avoid the violation of personality rights.

Keywords: Privacy; internet; preferences; violation; personality rights

¹ Graduada em Direito pela Universidade Cesumar – UniCesumar. Pós-graduada em Advocacia no Direito Digital e Proteção de Dados pela Escola Brasileira de Direito – EBRADI. Mestranda em Ciências Jurídicas pela Universidade Cesumar – UniCesumar. Bolsista Taxa PROSUP – CAPES. Advogada. E-mail: micaela-mayara@hotmail.com. ORCID - 0000-0002-6881-2748.

² Doutor em Direito Constitucional (UFPR). Mestre em Direito (UEL). Mestre em Ciência Política (UEL). Bacharel em Direito (UEM). Licenciado em Letras (UniCesumar). Professor na UEL e no Programa de Doutorado e Mestrado em Ciência Jurídica na Universidade Cesumar - UniCesumar. Coordenador do Programa de Mestrado Profissional em "Direito, Sociedade e Tecnologias" da Escola de Direito das Faculdades Londrina. Membro eleito da Academia Paranaense de Letras Jurídicas. Presidente do IDCC - Instituto de Direito Constitucional e Cidadania. Pesquisador do Instituto Cesumar de Ciência, Tecnologia e Inovação. Bolsista Produtividade em Pesquisa do ICETI. E-mail: zulmarfachin@uol.com.br. ORCID - 0000.0001.5514.5547.





1 INTRODUÇÃO

Todos os usuários que navegam na internet já se depararam, em diversas oportunidades, com o uso dos chamados “cookies”. O objetivo da pesquisa é analisar a aplicabilidade da Lei Geral de Proteção de Dados Pessoais no uso dos *cookies*, diante da possibilidade de violação de direitos da personalidade.

Com a entrada em vigor da Lei Geral de Proteção de Dados, os provedores de aplicações passaram a necessariamente compartilhar com o titular quais serão as informações ali colhidas e de forma transparente, informando, ainda, quais são os *cookies* realmente necessários para uma melhor navegação e quais serão utilizados com fins publicitários, cedendo ao usuário a opção de permitir ou não essa coleta de dados e para qual fim.

Os *cookies* são percebidos tão logo se visita algum site. Ocorre que, com a gama de sites visitados ao longo do dia, muitas vezes os visitantes não se atentam na possibilidade de alterar essas preferências, aceitando a opção que o site disponibiliza de imediato e essa seleção pode conter autorização para obtenção de dados com o propósito de impulsionar o consumo, por exemplo, traçando o perfil de consumo do usuário e direcionando a publicidade que melhor interessa à determinada pessoa.

Nesse contexto, as normas da Lei Geral de Proteção de Dados e do Marco Civil da Internet não são bastantes para proteger os direitos do consumidor, acarretando violação aos seus direitos da personalidade.

O problema da pesquisa está assim formulado: como o uso da ferramenta de *cookies* pode se tornar algo prejudicial ao usuário da internet, violando direitos da personalidade?

A pesquisa considera a hipótese de que as leis vigentes não são suficientes para abarcar questões atinentes à era tecnológica em ascensão, em especial os *cookies*, que, muito embora possam ter utilidade prática, podem, também, acarretar violações a direitos da personalidade.

Utilizou-se o método dedutivo, com pesquisa em livros, artigos científicos, legislações e demais documentos relevantes ao desenvolvimento da temática.

O objetivo geral da pesquisa é analisar as normas vigentes no ordenamento jurídico brasileiro aplicáveis ao tema, bem como posições doutrinárias e informações obtidas em artigos desenvolvidos no Brasil exterior a fim de discorrer se a norma jurídica já existente seria suficiente para regulamentar o uso desses arquivos que são armazenados no disco rígido do computador, carregando determinados dados do indivíduo que navega na internet, e que tem por um dos objetivos, personalizar o acesso do internauta.

O objetivo específico, por sua vez, é esclarecer de forma breve e acessível, o que são os *cookies*, quais mudanças ocorreram com o advento da Lei Geral de Proteção de Dados e os riscos de violação de direitos da personalidade caso as disposições da norma não sejam atendidas.

A importância do tema estudado se vislumbra na impossibilidade de que qualquer página seja acessada sem a presença de mecanismos de acolhimento de dados, tornando a navegação sem deixar rastros de preferências quase impraticável. Existir e consumir na era atual tem se tornado uma espécie de fomento para a internet e os riscos disso não podem ser ignorados.

Ao final, a pesquisa resultou na inefetividade da existência de diversas normas se não somadas à conscientização e conhecimento do próprio usuário acerca da importância de averiguar a finalidade do acolhimento de seus dados antes de ceder seu consentimento.

2 COOKIES E A FINALIDADE DOS TEXTOS ARMAZENADOS NOS NAVEGADORES

Cookie é um pequeno arquivo baseado em texto fornecido ao usuário por um site visitado, que ajuda a identificá-lo para aquele site, sendo também usado para manter as informações de estado conforme o usuário navega por diferentes páginas em um site ou retorna ao site posteriormente.

Para Xavier Pacheco, os *cookies* são textos colocados no navegador do usuário:

Cookies são basicamente textos que o servidor Web pode colocar no navegador do cliente. Eles são transferidos via cabeçalho HTTP. À medida que o usuário visita várias páginas dentro de um site ou aplicação Web, o servidor (examina) o conteúdo desses cookies (PACHECO, 2005, p. 825).



Em outras palavras, diversas informações reconhecidas enquanto o internauta navega na internet são armazenadas em pequenos arquivos de texto, permanecendo salvas durante a navegação, de uma forma que facilita acesso posterior, sem necessidade de percorrer o mesmo caminho diversas vezes para se chegar a um mesmo local.

São, na verdade, ferramenta para personalizar páginas *web* e permitir que acessos futuros do usuário ao site sejam personalizados, possibilitando a reativação quando o usuário retornar à mesma página, identificando informações coletadas na visita anterior e aplicando no acesso posterior (NETO, 2018, p. 1501).

Existem diversos tipos de *cookies*. Cada um tem finalidade distinta e guardam diferentes dados do usuário. Dentre eles, destacam-se os *Cookies* de primeira ou terceira pessoa, ou em inglês, *cookies de first e third party*.

Os *cookies* de primeira pessoa (*cookies first-party*) são gerados pelo próprio domínio, ou seja, o site que o usuário visita. Nesse caso, são coletadas muitas informações, tais como o nome de usuário, senhas, preferências de idioma, meio de pagamento escolhido para compra e produtos em um carrinho de compras.

Em um primeiro momento, é possível crer que, na realidade, guardar essas informações pode ser relativamente útil e pode até mesmo facilitar a rotina dos usuários de forma significativa. Isto porque, ao fechar a aba ou navegador, não será necessário que o site solicite ao usuário o preenchimento de suas informações sempre que regressar, podendo fazer sugestões de produtos com base nas suas preferências e, em geral, oferecer uma melhor experiência de navegação.

Se alguém passar o dia todo pesquisando promoções em determinada plataforma de *marketplace* sem ter efetuado o *login* em uma conta específica, inserindo no carrinho vários produtos de lojas distintas e, de alguma forma inesperada, e o navegador seja encerrado, as preferências sobre as lojas visitadas e os produtos inseridos no carrinho ficarão salvas para acesso posterior, graças ao uso dos *cookies*,

Por sua vez, os *cookies* de terceira pessoa (*cookies third-party*) são criados por um domínio de terceiros e na maioria dos casos sua função está ligada à publicidade digital. E é esse tipo de *cookie* que tem causado maior discussão acerca da privacidade dos usuários.

Basta pensar no seguinte questionamento: determinada pessoa se sentiria confortável se alguém sentasse ao seu lado olhando para a tela do seu computador o tempo todo, vendo

todo o conteúdo acessado e tomando conhecimento sobre sua intimidade? Para uma grande maioria, a resposta seria não. Contudo, ao clicar em “aceitar”, a utilização de *cookies* enquanto acessa alguma página da internet, sem ao menos verificar o que se está aceitando, é exatamente isso que o usuário autoriza.

A dificuldade enfrentada nos tempos atuais tem sido encontrar um equilíbrio entre proteger a privacidade do usuário e, ao mesmo tempo, lhe dar mais controle, de modo a conferir-lhe maior autonomia para decidir se gostaria ou não de receber determinada publicidade.

Seguindo sobre os tipos de *cookies*, os estritamente necessários permitem a navegação e utilização das aplicações, bem como acessar a áreas seguras do site. Sem eles, a aplicabilidade pode não funcionar corretamente.

Enquanto que os *cookies* analíticos coletam dados estatísticos anônimos com a finalidade de analisar a utilização do site e seu respectivo desempenho, por exemplo, quantas visualizações o site já teve, por qual meio o usuário chegou ao site.

Já os *cookies* de funcionalidade são utilizados para assegurar a disponibilização de funcionalidades adicionais do site ou para guardar as preferências definidas pelo usuário ao navegar na internet, sempre que utilizar o mesmo dispositivo, como por exemplo, país, URL da primeira página da sessão e ID da sessão.

Por fim, os *cookies* de publicidade direcionam anúncios em função dos seus interesses, ajudando a medir o sucesso de aplicações e a eficácia da publicidade de terceiros. Essa espécie de *cookie*, por guardar informações mais específicas do usuário, traçando um perfil de consumo, por exemplo, deve ser tratada com maior atenção.

Vale ressaltar que, embora ainda seja permitido o uso dessa espécie de *cookie*, é necessário que o *website* disponha de forma expressa se utilizam ou não *cookies* de publicidade e, ainda, faculte ao internauta a opção de aceitar ou rejeitar o uso. Não parece adequado lançar uma informação genérica, como por exemplo, de que “Ao clicar em “Aceitar todos os cookies”, concorda com o armazenamento de cookies no seu dispositivo para melhorar a navegação no site, analisar a utilização do site e ajudar nas nossas iniciativas de marketing”, sem ao menos disponibilizar a opção ao internauta de rejeitar tal armazenamento ou a possibilidade de analisar as opções.



É justamente em razão de informações genéricas que o usuário aceita o direcionamento de *marketing* sem mesmo se atentar, de modo que uma navegação diária em sítios eletrônicos que deveria ser algo acessível, simples e até mesmo prazeroso, torna-se algo estressante em razão da quantidade colossal de anúncios direcionados que surgem na tela, tornando muitas vezes o uso da internet algo desagradável.

Não bastasse as espécies de *cookies* já existentes, com os avanços tecnológicos surgem novas modalidades objetivando a manutenção das sessões dos internautas (NETO; CARMO; SCARMANHÃ, 2018). Dentre eles, estão os *cookies de flash* e os *evercookies*. Os *cookies de flash* possuem “algumas vantagens em relação ao espaço de armazenamento de dados e a forma de comunicação com o servidor”, de forma que esta nova tecnologia permite a “implementação proprietária, não permitindo a manipulação dos seus objetos pelos navegadores, sendo necessária a instalação de uma aplicação para a exclusão de dados”. Assim, os usuários normalmente deixam suas informações valiosas nestes objetos por muito tempo, gerando mais um problema para segurança destes dados (QUEIROZ, 2011). Contudo, os *evercookies* são os mais danosos, por usarem técnicas de persistência. Nesse sentido, mesmo que o usuário venha a apagar as informações, o *evercookie* possibilita recuperá-las.

De acordo com informações disponíveis na Cartilha de segurança do Comitê Gestor da Internet no Brasil (2012), alguns dos riscos relacionados ao uso de *cookies* podem ser: (i) compartilhamento de informações: antes do advento da Lei Geral de Proteção de Dados, era comum e desenfreado o compartilhamento de informações entre sites, de modo a conferir uma publicidade direcionada ao usuário; (ii) exploração de vulnerabilidades: é possível que alguns *cookies* armazenem informações técnicas sobre o computador do usuário, tais como o sistema operacional, hardware e programas instalados, aumentando as chances de exploração de eventual vulnerabilidade do computador em um eventual ataque virtual; (iii) autenticação automática: são as famosa opções “permanecer conectado” ou lembrar esta senha”. Essa prática pode ser considerada arriscada quando usada em computadores de terceiros ou com algum *malware*, pois os *cookies* podem ser coletados e permitirem que outras pessoas se autenticem como se fosse o próprio usuário; (iv) coleta de informações pessoais: referente ao preenchimento de formulários online pelo usuário. Aqui são coletados por atacantes ou códigos maliciosos e indevidamente acessados, caso não estejam criptografados.



Como melhor se explanará a frente, com a entrada em vigor da LGPD, certa autonomia está sendo cedida ao usuário para que ele decida sobre quais dados permite a coleta e tratamento.

3 A APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS E O USO DE *COOKIES*

O crescente uso por provedores de aplicação e conteúdo é algo que deveria causar desconforto em qualquer pessoa. A regulamentação desse espaço virtual em que tais mecanismos são utilizados não é específica, de modo que a saída para preencher lacunas eventualmente existentes e que envolvem o ciberespaço tem sido o uso da analogia e dos institutos jurídicos tradicionais (FACHIN, 2021, p. 9).

Foi nesse sentido que surgiu a Lei Geral de Proteção de Dados (Lei n. 13.709/18), a qual entrou em vigor em 14 de agosto de 2020. Em síntese, a lei brasileira objetiva assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, por meio de práticas transparentes e seguras, garantindo direitos fundamentais.

Vale mencionar, outrossim, que dados pessoais usualmente já nascem, são coletados, utilizados e descartados diretamente por meios digitais, de forma dinâmica. Todavia, a Lei também se aplica ao tratamento de dados em estado físico ou *off-line*, que possam ou não migrar, posteriormente, para o meio digital ou *on-line* (MALDONADO, 2019, p. 23).

Por meio da aplicação de multas altíssimas que podem chegar a até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluído os tributos, e por meio da publicização da infração (BRASIL, 2018), a LGPD busca garantir que todos os dados pessoais coletados pelos agentes de tratamento tenham o devido tratamento, evitando, assim, o vazamento de dados que podem comprometer a vida pessoal e/ou profissional dos indivíduos.

Entretanto, as sanções administrativas previstas nos artigos 52, 53 e 54 da referida lei (BRASIL, 2018), tiveram sua entrada em vigor apenas em 1.º de agosto de 2021, o que, certamente, propiciou maior prazo para adequação dos interessados aos termos da lei.

De todo modo, além de outras sanções e do impacto financeiro, convém mencionar sobre o impacto na imagem do agente que não tratou os dados coletados de forma adequada,



uma vez que vazados os dados dos titulares, a credibilidade da pessoa jurídica ou do provedor de aplicações despencará em níveis incontroláveis, levando em conta que àqueles que tiveram seus dados vazados, não sentirão mais confiança naquele que não tratou seus dados adequadamente.

Destaca-se que, para buscar dar efetividade ao fundamento da autodeterminação informativa, a LGPD dispõe sobre os direitos dos titulares, entre eles: de obter do controlador a confirmação da existência de tratamento; de ter acesso aos seus dados; da correção de dados incompletos, inexatos ou desatualizados; da anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com a lei; da portabilidade dos dados a outro fornecedor de serviço ou produto; da revogação do consentimento; da eliminação dos dados pessoais tratados com o consentimento do titular; da informação das entidades públicas e privadas com as quais o controlador realizou uso compartilhado de dados; da informação sobre a possibilidade de não fornecer consentimento e sobre as consequências dessa negativa, entre outros (MALDONADO, 2019, p. 30).

Surgiu, então, essa possibilidade de que os titulares optem por consentir ou não com o tratamento dos dados, limitando, por consectário, a coleta de informações por meio dos *cookies*. E é por este viés que se destaca, adiante, a aplicabilidade da Lei Geral de Proteção de Dados Pessoais quando se trata do uso dos *cookies*.

O que a LGPD prevê especificamente sobre os *cookies*? Há, nesse ponto, grande lacuna. Contudo, ao tratar sobre os *cookies*, mecanismo pelo qual se coletam dados e informações de determinado internauta, mostra-se necessário o aprofundamento do estudo sobre aplicabilidade da referida lei.

Sabe-se que a LGPD disciplinou o tratamento de dados pessoais, inclusive nos meios digitais, a fim de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A lei definiu como dado pessoal a informação relacionada à pessoa natural identificada ou identificável, adotando o conceito expansionista de dado pessoal (BRASIL, 2018, art. 5). A lei, contudo, não define especificamente o que seria uma pessoa identificada ou identificável, de modo que se mostra necessário recorrer ao conceito basicamente genérico.

Dizer que uma pessoa é identificada significa apontar diretamente a alguém, sabendo desde logo quem ela é. Já quando se diz que uma pessoa é identificável, significa que só será

possível saber de quem se trata por meio da junção de mais de uma informação até que se identifique alguém.

Considerando, outrossim, que a LGPD abrange não só aspectos físicos, mas também digitais, bem como do intuito de lucro ou caritativo da atividade desenvolvida, cabível, portanto, a discussão sobre sua aplicabilidade no que diz respeito ao uso de *cookies* para coleta de dados e preferências de determinado indivíduo.

Vale ressaltar que nem todos os dados guardados pelos *cookies* são pessoais, entretanto, pode se tornar um dado pessoal a partir do momento em que o usuário cede alguma informação ainda que sem perceber, como por exemplo, cadastrar o e-mail em algum site, tornando-se identificável.

Alguns estudiosos como De Hert e Gutwirth (2008) e Zuiderveen Borgesius (2016), entendem que *cookies* com identificadores únicos devem ser vistos como dados pessoais e alguns deles, por serem sensíveis, estão “relacionadas a características da personalidade do indivíduo e às suas escolhas pessoais” (FALEIROS JÚNIOR, 2019, p. 214-215).

Por outro lado, a LGPD não será diretamente aplicada em razão da ausência de dados pessoais aptos a identificar o usuário, se este visita determinado site em guia anônima e sem efetuar o *login* em alguma conta ou ceder qualquer outra informação. Veja-se que nesse caso não serão colhidos quaisquer dados pessoais do usuário, vez que não foi cedida qualquer informação que pudesse identificá-lo.

De acordo com o Suporte do Google Chrome³, com a navegação privada, o histórico de navegação e as informações inseridas nos formulários não são salvos. Os *cookies*, por sua vez e os dados do site são mantidos enquanto a navegação está ativa, sendo excluídos quando o modo de navegação anônima ou a aba/janela é fechada. Desde o início, é possível bloquear cookies de terceiros quando uma nova janela anônima é aberta.

Melhor dizendo, em uma navegação privada, os dados são anônimos e seria contraditório utilizar o termo “dado anonimizado pessoal”, pois, se anonimizado, ele perde a característica de ser pessoal. Contudo, se faz necessária uma ressalva quanto a possibilidade de que o usuário se torne identificável ao fornecer mais de uma informação que em conjunto, possam torná-lo identificável, como o *login* em um serviço da *Web*, como por exemplo, o

³ Informações extraídas do site “Ajuda do Google Chrome”. Disponível em: <https://support.google.com/chrome/answer/95647?hl=pt-BR&co=GENIE.Platform%3DDesktop>. Acesso em: 13 abr. 2022.



Gmail. Em suma, apenas nos casos em que o usuário seja, portanto, identificado ou identificável, caberá a aplicação da Lei Geral de Proteção de Dados Pessoais.

Seguindo a mesma linha, mas neste momento quanto à anuência do titular, disciplina a referida lei, as formas de consentimento pelo titular consideradas válidas, quais sejam a manifestação por escrito ou por outro meio que demonstre a manifestação de vontade do titular (BRASIL, 2018, art. 8).

A norma jurídica, ao fixar como uma das formas de consentimento “outro meio que demonstre a manifestação de vontade do titular”, de certa forma, ampliou a possibilidade de que àqueles que necessitam do consentimento expresso do internauta, inovassem a fim de obter algum meio para registrar essa manifestação de vontade.

E é por este motivo que a maioria dos domínios utiliza *pop-ups* colocados de forma estratégica no início da visita do site e que certamente incomode o usuário caso não exare imediatamente seu “consentimento” acerca do uso dos *cookies*. Com isso, as plataformas estariam, em tese, seguras e adequadas às normas vigentes, vez que colheram a autorização do titular de algum modo.

Martin Degeling et al (2019) ao realizar uma pesquisa acerca dos mecanismos de segurança da *web* e o atendimento das regras da GDPR, concluiu pela existência de mais de um meio para obtenção de consentimento do titular dos dados. Um deles seria o *AutoAccept*, que identifica automaticamente o consentimento com o uso dos *cookies* se o usuário “rolar” a tela ou clicar em algum link que remova o aviso sobre os *cookies*.

Contudo, se essa manifestação de vontade foi consciente ou não é outro assunto que merece maior atenção, vez que, em tese, a norma deixou aberta a possibilidade de que a autorização seja obtida por escrito ou por outro meio e os *pop-ups*, por ora, se enquadram nesse requisito por deixarem registrada, de algum modo, a autorização e preferência do titular.

4 ADEQUAÇÃO DOS PROVEDORES DE APLICAÇÃO E DE CONTEÚDO EM RELAÇÃO À LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS FRENTE AOS DIREITOS DA PERSONALIDADE

Neste item, será analisada a possibilidade de adequação dos provedores de aplicação e dos provedores de conteúdo às disposições da LGPD, tendo em vista a proteção e,

eventualmente, a violação de direitos da personalidade, instituídos com o objetivo de defender os valores existenciais do homem (LUZ SEGUNDO, 2020).

Nesse contexto, tem se identificado inúmeras dificuldades em relação ao desafio de regular as relações intersubjetivas no âmbito da internet. A imposição de normas legisladas por parte dos Estados nacionais não tem se mostrado a melhor forma de regular tais relações (FACHIN, 2021, p. 11).

Lawrence Lessig (2009) sustenta a necessidade de que as quatro modalidades de regulação sejam compreendidas em uma perspectiva integradora, de modo que se possa aproveitar cada uma delas para regular o ciberespaço, visto que todas impõem deveres e asseguram direitos.

Quando se visita um site, principalmente plataformas de vendas, normalmente o que aparece primeiro é um *pop-up* forçando o visitante a escolher alguma opção para que essa ferramenta suma de alguma forma. O que costuma aparecer é algo como: “Este site utiliza alguns cookies para controle de sessão, verificar seu uso em nosso site e para marketing. Você pode aceitar todos ou configurar quais deseja compartilhar. Deseja aceitar, rejeitar ou visualizar as preferências?”⁴. Muitas vezes, na pressa ou até mesmo por falta de conhecimento técnico, o usuário acaba por aceitar a opção sem ao menos consultar as preferências e remover os *cookies* que não lhe agradam.

Um estudo recente realizado por Manuel Batista et. al (2021, p. 75-92), com uma amostra composta por cidadãos portugueses, com idade entre os 20 e 34 anos, considerados população jovem com maior utilização da Internet em Portugal, atestou que numa escala ordinal, de 1 a 7, foi possível verificar que, em relação ao conhecimento sobre os *cookies*, os valores médios estão em torno de cinco, o que demonstra um nível razoável de conhecimento por parte dos inquiridos. Na mesma pesquisa, desta vez sobre estarem ou não indiferentes ao fato de serem rastreados, houve a percepção de que, em uma escala ordinal, na qual 1 significa muito incômodo ao ser rastreado, e 7 elevada indiferença ao ser rastreado, o valor mediano ficou em torno de 3. Essa análise certamente demonstra que os inquiridos ficam incomodados com o rastreamento, contudo, isso não inibe a aceitação aleatória dos *cookies*.

É muito comum pesquisar sobre determinado produto em alguma plataforma e, na sequência, aparecerem inúmeros anúncios sobre o mesmo produto ou similares em redes

⁴ Exemplo extraído da plataforma Dafiti. Disponível em: <https://www.dafiti.com.br/>. Acesso em: 13 abr. 2022.



sociais ou outros sites visitados posteriormente. Isso ocorre porque os *cookies* de publicidade foram aceitos pelo usuário quando adentrou no site e, sem checar as preferências, aceitou as preferências sugeridas pelo próprio site.

Neste sentido, algo que chama a atenção é que o *pop-up* que trata sobre a autorização ou não do uso de determinados *cookies*, em sua maioria, está localizado estrategicamente em locais do site que em alguns casos tornam impossível a navegação e identificação do conteúdo sem aceitar ou recusar as preferências.

Essa colocação dos *pop-ups* sobre a preferência dos *cookies*, na realidade, foi uma determinação da Diretiva de Privacidade Eletrônica (e-Privacy Directive 2009/136/EC), conhecida como “Lei dos cookies”, vez que exige o consentimento dos usuários finais para a colocação de *cookies* e tecnologias semelhantes para armazenar e acessar informações nos equipamentos dos usuários.

Mais especificamente, o art. 5.º, § 3.º da Diretiva, determina que o armazenamento de dados no equipamento de um usuário só pode ser feito se o usuário receber informações sobre como esses dados são usados e o usuário tiver a possibilidade de negar essa operação de armazenamento.

Essa concessão de oportunidade ao usuário para que identifique quais dados serão coletados e sua finalidade pode ser também considerado uma adequação à Lei Geral de Proteção de Dados Pessoais, e a colocação de *pop-ups* é modo a coagir o usuário a consentir ou não com o seu uso.

Constantemente, ao visitar os provedores de aplicação, é possível identificar o uso da política de *cookies*, seguida da solicitação de consentimento do usuário para seu tratamento, o que demonstra que, em um contexto geral, os provedores de conteúdo e aplicação estão se adequando à Lei Geral de Proteção de Dados Pessoais de forma a afastar a responsabilização em caso de vazamento de dados ou violação da privacidade do titular.

Cumpra mencionar, inclusive, que alguns provedores têm anunciado o fim do uso dos *cookies* de *third-party* a fim de assegurar melhor conformidade à Lei Geral de Proteção de Dados, garantindo maior transparência e menos individualização, como é o exemplo do navegador Google Chrome que anunciou o fim do uso dos *cookies* de terceira pessoa em 2023 (NOBREGA, 2021).

Em que pese a aparente adequação ao uso de *cookies*, alguns resultados do estudo de Ayenson e outros (2011, p. 13-14)₂ demonstram que as tecnologias verificadas nos *cookies*

possuem uma capacidade de disseminação e de operação que extrapolam as habilidades de usuários comuns de conexão. Com isso, ainda que o usuário controle os *cookies* de seu próprio navegador, é possível que ele não consiga lidar com certas estratégias de armazenamento e de coleta de dados pessoais na rede e permaneça incessantemente monitorado no plano virtual.

Explicitando de outra forma, o estudo realizado por Ayenson constatou a existência de uma técnica de reaparecimento, ou *respawning*, de *cookies* que foram deletados. Por meio dessa técnica, as informações gravadas sobre as páginas visitadas pelo navegador (cache) são espelhadas por meio de um identificador específico, chamado de ETag. Deste modo, ainda que o usuário opte por bloquear ou deletar os *cookies* HTTP, flash ou HTML5, eles poderão reaparecer para rastrear a navegação.

Em outras palavras, alguns *cookies* se valem de um recurso inerente ao funcionamento do navegador para reaparecerem quando forem deletados, e para se livrar desse recurso, seria necessária a realização de uma limpeza do cache de navegação a cada site visitado, sendo que nem o modo de navegação anônimo seria capaz de blindar os seus dados contra o rastreamento (OLIVEIRA, SILVA, 2019, p. 297-310).

A Lei Geral de Proteção de Dados Pessoais, em razão da constante inovação digital, não regulamentou com precisão casos como esse em que mesmo deletados, as informações se perpetuam por outros meios, prevendo, apenas, as hipóteses⁵ em que os dados pessoais deverão ser eliminados e as hipóteses em que a conservação está autorizada (art. 16).

O que se vê, na realidade, é o fortalecimento da mídia digital, caminhando em constante evolução para a readequação de acordo com o crescimento do uso intensivo de dados pessoais, respeitando, em sua maioria, a privacidade dos internautas. Contudo, a evolução é algo constante e a readequação também deve ser, de modo que, em breve, novas diretrizes deverão surgir a fim de manter a privacidade e o acesso à tecnologia em níveis harmônicos.

É alarmante tomar conhecimento de que em uma era quase que completamente digital, muitos ainda não se preocupam com a violação à privacidade do internauta,

⁵ Dentre as hipóteses de eliminação dos dados pessoais previstas no art. 16 da LGPD, estão inseridas as seguintes: (i) cumprimento de obrigação legal ou regulatória pelo controlador; (ii) estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais; (iii) transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta lei; e (iv) uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados.



importando-se apenas em manter operante o sistema que trouxe à empresa certa riqueza. Contudo, o investimento em se adequar às normas vigentes jamais pode ser considerado algo oneroso ou inútil, dado que as consequências da adequação certamente serão positivas e proveitosas e as consequências da não adequação, possivelmente catastróficas para os envolvidos.

Até este ponto do estudo, buscou-se esclarecer como a Lei Geral de Proteção de Dados Pessoais pode ser aplicada aos *cookies* e a necessidade de que os provedores de aplicação e conteúdo se adequem às normas desta lei. Entretanto, caso esses provedores não se ajustem a referida lei e também até mesmo a outras normas vigentes, existe certo risco de que acarretem ofensa à direitos da personalidade do usuário.

Os direitos da personalidade, no entendimento de Carlos Alberto Bittar (2014, p. 37), são direitos reconhecidos à pessoa humana tomada em si mesma e em suas projeções na sociedade, previstos no ordenamento jurídico exatamente para a defesa de valores inatos no homem, como a vida, a higidez física, a intimidade, o segredo, o respeito, a honra, a intelectualidade e outros tantos.

Esses direitos são considerados direitos subjetivos e essenciais a uma pessoa que possui atributos que remetem à condição humana, ao homem vivo. São direitos oponíveis a todos (PONTES DE MIRANDA, 1974, p. 5-6). Para Adriano de Cupis, esses direitos essenciais constituem a medula da personalidade da pessoa, de modo que se eles não existissem, a pessoa não existiria como tal (2008, p. 24).

O Código Civil também preceitua sobre os direitos da personalidade, oferecendo diretrizes jurídicas mais específicas para solucionar questões práticas envolvendo tais direitos. Referido código estabelece que tais direitos são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária (BRASIL, 2018, art. 11). Neste sentido, ele protege o direito à vida (art. 15), o direito à integridade do corpo (arts. 13 e 14), o direito ao nome (arts. 16 e 18), incluindo a proteção do pseudônimo (art. 19), o direito à honra, à imagem (arts. 17 e 20) e o direito à vida privada (art. 21).

A Constituição Federal, por seu turno, deixa expresso quais são os relaciona diversos direitos da personalidade, tais como, a liberdade de expressão (art. 5, inciso IX), a honra, a intimidade, a vida privada e imagem das pessoas (art. 5, inciso X), inviolabilidade do domicílio (art. 5, inciso XI), inviolabilidade de correspondência (art. 5, inciso XII). A

violação de qualquer um desses direitos enseja o dever de indenizar por dano material, moral ou à imagem.

Neste sentido, questão importante é analisar como é possível que tais direitos sejam violados, em especial durante o uso da internet. Relembre-se que os *cookies*, objeto do presente estudo, são arquivos que armazenam informações e preferências do usuário a fim de facilitar a navegação. Dentre tais informações, pode ser coletado o nome de usuário, senhas, preferências de idioma, meio de pagamento escolhido para compra, produtos em um carrinho de compras e constantemente o marketing digital tem usado essas informações para encontrar seus públicos e direcionar melhor suas campanhas.

A questão que deve ser ponderada é se a privacidade e intimidade dos usuários são preservadas com a coleta dessas informações. O uso de determinados *cookies* pode ser comparado com uma pessoa sentada ao lado da pessoa observando atentamente tudo o que ela está acessando, seus gostos de consumo e até mesmo venda.

É como se nos dias atuais não seja possível dar ao menos um passo sem deixar algum dado por onde passa. A privacidade do usuário, então, se mostra ameaçada por suas preferências acabarem escancaradas em uma vitrine digital.

Imagine que uma mulher desconfia de uma gravidez e passa a pesquisar curiosidades sobre gestação e alguns itens para bebês. Ao longo da navegação, ela aceita todos os *cookies* durante as visitas a diversos sites, como por exemplo, blogs de instrução para alimentação adequada durante a gestação, *marketplace* de roupas e acessórios de bebê, entre outros. Ao aceitar todos os *cookies*, é possível que os provedores de aplicação tenham guardado as preferências da mulher possivelmente grávida para personalizar anúncios conforme sua preferência. Ocorre que o computador pelo qual foram realizadas as buscas é compartilhado entre a mulher e seu marido, o qual acaba descobrindo que a esposa está grávida ao acessar sites aleatórios e repetidamente receber anúncios sobre produtos para grávidas e bebês.

As hipóteses de desfecho para essa situação hipotética são diversas, mas o que se quer ponderar nesse momento é se houve a violação da privacidade pelo provedor de aplicação que usou dos *cookies* para personalizar os anúncios. A verdade é que não há como lançar uma culpa exclusiva ao site se ele tomou as medidas adequadas para obter consentimento do titular para tratar e utilizar os dados obtidos durante a navegação.



Ao clicar imediatamente em algo que visivelmente atrapalha sua navegação, como os *pop-ups* acerca da política de privacidade e uso de *cookies*, o usuário acaba se vinculando em uma extensa cadeia de direitos e deveres econômicos, obrigando também suas informações personalíssimas sensíveis, porquanto seu *click* concederá presunção de permissão para o empresário digital fazer tratativas, tais como coleta, guarda e partilha de dados pessoais (COUTO, 2021, p. 86).

A Lei Geral de Proteção de Dados Pessoais preceitua que o consentimento pode ser obtido por qualquer meio que demonstre a manifestação de vontade do titular (BRASIL, 2018, art. 8). Desse modo, considerando a hipótese de uma mulher que supõe estar grávida e navega pesquisando produtos para bebês aceitou o uso de *cookies*, seja por *pop-ups* colocados de forma estratégica no início da visita do site ou de outra forma, cedeu expressamente o consentimento para o uso de suas informações, ainda que pudessem ensejar à descoberta de algo que era apenas vivo em sua intimidade.

Se a situação fosse diversa, como por exemplo, a navegação em janela anônima ou fosse realmente impossível guardar informações sobre o objetivo de suas buscas (o que francamente, é praticamente impossível na era atual), bem como inexistisse qualquer tipo de consentimento, haveria a possibilidade de se discutir acerca da violação da privacidade do usuário. É por esse motivo em especial que os direitos da personalidade devem ser protegidos e, com o maçante uso de ferramentas para alavancar o consumismo exacerbado, essa proteção se torna cada vez mais necessária.

Todavia, não basta a criação de normas para regular os fatos que podem ocorrer envolvendo a internet. Deve-se, principalmente, conscientizar as pessoas enquanto titulares de dados pessoais, a fim de que se mantenham informadas sobre a prevenção de algum atentado a seus direitos da personalidade.

5 CONCLUSÃO

Com a expansão da sociedade e disseminação da tecnologia, propagou-se também a possibilidade de coleta de dados de inúmeras formas. Dentre tais meios, surgiu o uso dos *cookies*, os quais muitas vezes tornam a navegação em um site muito mais rápida, acessível e prazerosa ao usuário. Todavia, até o surgimento de dispositivos jurídicos que regulavam a

coleta e o uso de informações, referido mecanismo era utilizado, em especial, como uma estratégia desenfreada de *marketing*.

A Lei Geral de Proteção de Dados Pessoais colaborou significativamente com a limitação dessa coleta de dados, proporcionando, de certo modo, maior autonomia ao usuário para escolher quais dados podem ser tratados e para qual finalidade. É por essa e outras razões que os *cookies* de terceira pessoa estão sendo cada vez menos utilizados.

Em que pese os provedores de aplicação e de conteúdo tenham se adaptado para colher o consentimento do usuário e se enquadrar à LGPD, é difícil saber se essa manifestação de vontade é sempre consciente ou não, vez que a utilização de *pop-ups* na navegação, na verdade, faz com que o internauta aceite a utilização dos *cookies* apenas para que aquela janela que atrapalha sua navegação desapareça imediatamente e não necessariamente porque está literalmente concordando com as disposições do site.

Conclui-se, portanto, que a imposição de multa no caso de descumprimento dos termos da Lei Geral de Proteção de Dados Pessoais, certamente, foi um ponto relevante para a adequação dos provedores de conteúdo no que se refere à coleta e tratamento de dados pessoais dos usuários, evitando a violação a direitos da personalidade. Entretanto, referida lei e as demais normas vigentes ainda não podem ser consideradas suficientes para evitar incidentes de violação de direitos da personalidade.

É importante reconhecer que não basta apenas a conscientização daqueles que coletam e tratam dados, mas também daqueles que os fornecem. A rotina acelerada e automatizada do usuário, buscando sempre o imediatismo, por muitas vezes acaba por limitá-lo a essa consciência sobre o uso dos *cookies*, o que motiva os domínios a utilizar de *pop-up* e outros meios aptos no intuito de captar a atenção para que exare um consentimento, ainda que seja com um “click”, ainda que não saiba expressamente do que se trata.

Não só o Direito deve acompanhar a constante evolução da tecnologia e sua aplicabilidade no cotidiano nas pessoas, mas também, e principalmente, as pessoas enquanto titulares de dados pessoais, devem buscar se manter informados sobre a prevenção de algum atentado bem como a proteção de seus direitos da personalidade.

É certa a necessidade de incentivo de políticas de conscientização dos usuários de internet acerca da necessidade de uma breve leitura acerca de quais tipos *cookies* são utilizados durante o acesso a uma determinada página, uma vez que mesmo sem parecer, os



cookies também são considerados coletores de dados pessoais e podem ferir a privacidade e/ou intimidade de alguém.

REFERÊNCIAS

Autoridade Nacional de Proteção de Dados. **Sanções Administrativas: o que muda após 1º de agosto de 2021?** Jul. 2021. Disponível em: <https://www.gov.br/anpd/pt-br/assuntos/noticias/sancoes-administrativas-o-que-muda-apos-1o-de-agosto-de-2021>. Acesso em: 04 mar. 2022.

AYENSON, Mika D. et al. **Flash Cookies and Privacy II: Now with HTML5 and ETag Respawning**. Social Science Research Network. Publicado em 30 jul. 2011. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=1898390. Acesso em: 04 mar. 2022.

BATISTA, Manuel et al. **Aceitação do Aviso de cookies e criação de publicidade direcionada: uma decisão consciente ou falta de informação?** RISTI, Porto, n. 43, p. 75-92, set. 2021. Disponível em: http://scielo.pt/scielo.php?script=sci_arttext&pid=S1646-98952021000300075&lng=pt&nrm=iso. Acesso em: 10 abr. 2022.

BITTAR, Carlos Alberto. **Os Direitos da Personalidade**. 8ª edição. São Paulo. Editora Saraiva, 2015, p. 37.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**. Brasília-DF. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm#art65. Acesso em: 04 mar. 2022.

Comitê Gestor da Internet no Brasil. **Cartilha de Segurança para Internet**. Cert.br. São Paulo. 2012. Disponível em: <https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em: 04 mar. 2022.

COUTO, José Henrique de Oliveira. **Ausência de consentimento esclarecido do consumidor para tratamento de dados pessoais sensíveis: abordagem à luz da *clickwrap***. SKEMA Business School e CONPEDI. 2021, p. 83-90. Disponível em: <http://site.conpedi.org.br/publicacoes/b3vv7r7g/xb85z780/2JjyN6oV3CQhQkA6.pdf>. Acesso em: 13 abr. 2022.

CUPIS, Adriano de. **Os direitos da personalidade**. 2ª edição. Quorum Editora, 2008, p. 24.

DE HERT, P. et. al. **Regulating profiling in a democratic constitutional state**. In Hildebrandt M., & Gutwirth S. (eds), *Profiling the European Citizen*, Springer. 2008, p. 271-302.



Europe. **Directive 2009/136/EC of the European Parliament and of the Council of 25 November 2009.** Disponível em <https://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=OJ:L:2009:337:0011:0036:en:PDF>. Acesso em: 04 mar. 2022.

FACHIN, Zulmar. **Desafios da Regulação do ciberespaço e a proteção dos Direitos da Personalidade.** Revista Jurídica (FURB). v. 25, n. 56, jan./abr. 2021.

FALEIROS JÚNIOR, José Luiz de Moura. **A tutela jurídica dos dados pessoais sensíveis à luz da Lei Geral de Proteção de Dados.** In: João Victor Rozatti Longhi. Estudos Essenciais de Direito Digital. Uberlândia: Laboratório Americano de Estudos Constitucionais Comparados, 2019, p. 214-215.

Google Chrome. **Como a navegação privada funciona no Chrome.** Disponível em: <https://support.google.com/chrome/answer/7440301>. Acesso em: 04 mar. 2022.
LESSING, Lawrence. **The Code version 2.0.** Cambridge, Basic Books, 2006.

LUZ SEGUNDO, Elpídio Paiva. **Direitos da personalidade: quo vadis?.** Revista de Direito da Faculdade Guanambi, Guanambi, v. 7, n. 01, e280, jan./jun. 2020. Disponível em: <http://revistas.faculdadeguanambi.edu.br/index.php/Revistadedireito/article/view/280>. Acesso em: 16 abr. 2022.

MALDONADO, Viviane Nóbrega. BLUM, Renato Ópice. **LGDP - Lei Geral de Proteção de Dados Comentada.** São Paulo: Revista dos Tribunais, 2019.

MARTIN, Degeling. et. al. **We Value Your Privacy ... Now Take Some Cookies: Measuring the GDPR's Impact on Web Privacy.** Proceedings. 2019. Network and Distributed System Security Symposium. Disponível em: <https://arxiv.org/abs/1808.05096>. Acesso em: 12 abr. 2022.

PONTES DE MIRANDA, Francisco Cavalcanti. **Tratado de direito privado.** 4. ed. São Paulo: RT, 1974. t. 7, p. 5-6.

NETO, Mário Furlaneto. CARMO Júlio César Lourenço. SCARMANHÃ. Bruna de Oliveira da Silva Guesso. **Cookies: Vulnerabilidade do Direito à Privacidade nos meios digitais no âmbito da legislação brasileira.** 2018. Disponível em: https://www.cidp.pt/revistas/rjlb/2018/4/2018_04_1491_1517.pdf. Acesso em: 04 mar. 2022.

NOBREGA, Cristiano. **O fim dos cookies third-party: tudo que você precisa saber neste momento.** 2021. IAB Brasil. Disponível em: <https://iabbrasil.com.br/artigo-o-fim-dos-cookies-third-party-tudo-que-voce-precisa-saber-neste-momento/>. Acesso em: 04 mar. 2022.

OLIVEIRA, J. V.; SILVA, L. A. **“É de Comer?” Cookies de Navegador e os Desafios à Privacidade na Rede.** R. Tecnol. Soc., Curitiba, v. 15, n. 37, p. 297-310, 2019. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/8419/6309>. Acesso em: 04 mar. 2022.





PACHECO, Xavier. **Guia do desenvolvedor de Delphi for .NET**. São Paulo: Pearson Makron Books, 2005, p. 825.

PADÍN, Sebastián Garcia. **Cookies first-party e third-party: quais as diferenças?** Publicado em 8 de abril de 2021. IAB Brasil. Disponível em: <https://iabbrasil.com.br/artigo-cookies-first-party-e-third-party-quais-as-diferencas/>. Acesso em: 04 mar. 2022.

QUEIROZ, Anderson Apolônio Lira. **A invasão de privacidade na Internet: um modelo de boas práticas e uma proposta interativa de proteção da privacidade por meio dos cookies**. Dissertação (Mestrado). Universidade Federal de Pernambuco, Recife, 2011. Disponível em: <https://repositorio.ufpe.br/handle/123456789/1298>. Acesso em: 04 mar. 2022.

SOARES, João Bruno. **LGPD e Cookies o que você precisa saber!** Publicado em abril de 2021. AdOpt. Disponível em: <https://goadopt.io/blog/cookies-e-lgpd/>. Acesso em 04 mar. 2022.

Support Microsoft. **Descrição de cookies**. Disponível em: <https://support.microsoft.com/pt-br/topic/descri%C3%A7%C3%A3o-de-cookies-ad01aa7e-66c9-8ab2-7898-6652c100999d>. Acesso em: 04 mar. 2022.

ZUIDERVEEN BORGESIU, Frederik. J. **Singling out people without knowing their names—behavioural targeting, pseudonymous data, and the new data protection regulation**. *Computer Law & Security Review*. 2016. V. 15, p. 256-271.