



COOKIES E A VIOLAÇÃO DE DIREITOS FUNDAMENTAIS NO MEIO DIGITAL

Vitor Hugo Crellis Costa¹

RESUMO: o presente artigo tem por objetivo analisar o uso das ferramentas digitais, conhecidas como *cookies*, suas funções e tipos, e a partir da luz da legislação brasileira debater quanto a invasão de privacidade, uso e armazenamento de dados pessoais e seus reflexos na sociedade tecnológica. O método abordado será o método dialógico, do qual há uso da interdisciplinaridade para se chegar à tese.

Palavras-chave: Cookies; privacidade; direito digital; direito fundamental.

1 INTRODUÇÃO

Muito se debate sobre os dados pessoais na internet, a violação de direitos fundamentais em virtude de terceiros, seus usos e associações com os chamados *cookies*. Usado por muitos sites principalmente por questões de alcance e personalização de anúncios, esses arquivos reúnem informações pessoais do cliente e vendem aos controladores.

Há de se entender primeiramente o que são esses arquivos, suas funções e tipos, para posteriormente ter um parecer acerca da legislação brasileira e a proteção de direitos fundamentais e os dados do usuário.

No presente artigo foi usada a metodologia dialógica, no qual é usado a interdisciplinaridade entre os campos da informática e tecnologia e o direito, com uso de livros, artigos científicos e normas do ordenamento jurídico brasileiro.

2 COOKIES: CONCEITO, FUNÇÃO, TIPOS

Inicialmente, é necessário entender o que são *cookies*, sua função no meio digital e quais os principais tipos, para posterior entendimento da sua influência na vida e nos dados pessoais do usuário.

¹ Discente do 1º ano (2º termo) do curso de Direito, do Centro Universitário Antonio Eufrásio de Toledo de Presidente Prudente. vitorcrellis@live.com

2.1 Conceito

Os *Cookies* são pequenos arquivos, usados como ferramentas por sites para a identificação do visitante, recolhendo informações pessoais do usuário, seja para uma navegação personalizada de acordo com o perfil dele, seja para facilitar o transporte de dados, de maneira que fique mais rápida sua navegação.

Para Lessig (2006, p. 07; 48), os *cookies* foram indispensáveis para o desenvolvimento da internet, principalmente no quesito comercial. Em 1994, a empresa Netscape desenvolve uma ferramenta que gravaria no computador do usuário informações acerca do site que ele havia visitado. Essa ferramenta, o *cookie*, é responsável por fazer o operador do site identifique o usuário e personalize conforme seu acesso.

Segundo Xavier Pacheco (2005, p.825):

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.

Deste modo fica definido o conceito de *cookies* na internet e a sua necessidade para algumas áreas, contudo até onde essa necessidade pode ir e ultrapassar? Esse assunto será debatido nos próximos tópicos.

2.2 Função

A principal função desses arquivos são salvaguardar informações sobre o indivíduo que acessa determinada página, para assim facilitar o uso, dando ao sujeito uma experiência personalizada ou maior velocidade para navegar. Em grande parte, os *cookies* salvam informações pessoais, como o histórico da pessoa, e-mail, senhas e outros dados para serem usados durante sua experiência. Por exemplo, no uso do histórico para verificar os interesses da pessoa e oferecê-la possíveis produtos para a compra, estratégia muito usada hoje em dia no marketing digital.

Para Neto, Carmo e Scarmanhã (2018, p. 1501) os *cookies* têm a seguinte função:

A análise de comportamento de consumidores em websites tem sido utilizada para conhecer o comportamento dos consumidores enquanto ferramenta para tornar o modelo de negócio eletrônico mais rentável, de modo que para que isto seja possível, foi necessário a criação e a inclusão de informações de controle de estado nas comunicações entre clientes e servidores

Segundo o Comitê Gestor de Internet no Brasil (2012), algumas funções dos *cookies* podem apresentar riscos ao usuário, tais como: compartilhamento de informações, exploração de vulnerabilidade, autenticação automática, coleta de informações pessoais, coleta de hábitos de navegação.

2.3 Tipos

Aqui ficam definidos os tipos de *cookies* e a utilização única de cada um, de maneira a aprofundar o conhecimento do leitor acerca de cada um deles.

2.3.1 Cookies de Sessão

Os *cookies* de sessão são arquivos temporariamente criados na memória do computador do usuário, eles não coletam tantas informações como em outros casos. São chamados também de *cookies* temporários por durarem somente enquanto há utilização no site.

Esse tipo de arquivo é muito usado em sites de compras, quando o usuário ao separar seus pedidos, estes ficam salvos para a posterior finalização do pedido.

De acordo com Palmer (2008), caso algum mecanismo, site ou até mesmo hacker consiga interagir com esse tipo de *cookie*, ele comprometerá sua segurança e sigilo, de maneira que mesmo o arquivo sendo apagado, ele estará registrado por alguma plataforma ou terceiro

2.3.2 Cookies Persistentes

São os *cookies* mais usuais pelos sites, estes ficam salvos por dias, meses ou até mesmo anos dependendo de como a plataforma o utilizar. Esse armazena dados para uso posterior ou como forma de personalizar o serviço,

“No lado negativo, as empresas podem usar *cookies* persistentes para rastrear o usuário. Ao contrário dos *cookies* de sessão, eles registram informações sobre seus hábitos de navegação durante todo o tempo em que estão ativos” (KINAST, Priscilla, 2019).

Segundo Toubiana, Narayanan e Boneh (2010), alguns sites tem sistemas de *cookies* que funcionam não propriamente com a decisão do usuário, mas sim de acordo com seu comportamento durante a navegação, de maneira que sorrateiramente os dados, preferências e escolhas do usuário fossem registradas e usadas.

2.3.3 Cookies Primários

Cookies primários, também chamados de *first-party* em inglês, são gerados pelo próprio site, sendo este responsável pelo domínio das informações. Estes gravam informações sobre quais páginas foram visitadas, as preferências do usuário, e-mails, senhas, dados em sites, todas essas informações ficam guardadas no HD da máquina, até que os *cookies* expirem ou o próprio usuário os apague.

Estes *cookies* são responsáveis pelo hospedeiro guardar informações das quais o usuário está utilizando em seu site. Por exemplo, ao entrar em uma loja online, o sujeito faz o cadastro, escolhe os produtos, dos quais são mandados para a área “meu carrinho” e acidentalmente fecha a página, ao fazer o uso de *cookies*, o site consegue retornar todo o caminho já percorrido pelo usuário

2.3.4 Cookies de Terceiros

Os *cookies* de terceiros, também chamados de *third-party* em inglês, são arquivos desenvolvidos e em domínio de terceiros afim de rastrear e registrar a atividade do usuário on-line, nesse tipo há uma formação de um banco de dados robusto e fiel ao usuário. Geralmente, são usados por redes de marketing e publicidade na intenção de aumentar suas vendas e alcance.

São estes tipos de *cookies* que geram a devida problemática, já que não se tem o conhecimento de por onde os dados do usuário passam, de maneira que o terceiro, desconhecido, tem acesso a seus dados pessoais, e-mail, senhas, preferências, histórico do navegador.

Queiroz e De Queiroz (2010), explicam esse tipo de *cookie*:

Estes *cookies* se originam de relacionamentos entre diversos domínios e serviços oferecidos entre eles; são web sites que mantêm relação comercial com o *site* utilizado pelo usuário, estes *cookies* são criados e manipulados por provedores terceiros a relação estabelecida entre o cliente e o provedor.

De fato, os *cookies* têm sua importância e uso nos vários mecanismos dos navegadores, influenciando diretamente a vida do usuário, facilitando e aprimorando sua experiência na internet. Contudo, ainda deve ser debatido o controle, armazenamento e análise de seus dados pessoais, afinal de contas, é uma violação direta a relação de privacidade e dados pessoais, sendo que muitos consentem com os *cookies* mesmo sem saber o que são ou para o que servem.

3 A LEGISLAÇÃO BRASILEIRA E A PROTEÇÃO AOS DADOS PESSOAIS

Devido à grande evolução tecnológica, a repercussão dos *cookies* na sociedade e sua relação com a violação do direito à privacidade e uso de dados pessoais, a legislação brasileira passou a limitar esses mecanismos por meio de leis, dentre elas o Marco Civil da Internet e a Lei Geral de Proteção de Dados Pessoais.

Segundo Bodin de Moraes (2012, p. 5) os direitos da personalidade não são estáticos e imutáveis, mas sim se transformam e ampliam de acordo com a evolução da sociedade e suas transformações sociais, surgem novas instâncias quanto ao direito da personalidade do cidadão, a ponto que nem o legislador pode prevê-las para garantir seus direitos positivados, sendo assim uma categoria aberta. Diante disso, há uma necessidade de que a lei comece a abarcar os dados pessoais na internet para que se tenha uma adequação nos tempos atuais, de forma que proteja a integridade moral, a imagem e a privacidade do usuário.

Diante da complexidade da obtenção de dados pessoais, Zarsky (2006) faz uma comparação entre a obtenção desses dados de maneira física, no mundo real, e a maneira virtual, através de navegadores e com uso dos *cookies*. No mundo real, os dados são transmitidos após o término da transação, enquanto no digital, eles são expostos a todo o tempo de navegação.

De acordo com Manuel Castells (1999, p. 70):

O que deve ser guardado para o entendimento da relação entre a tecnologia e a sociedade é que o papel do Estado, seja interrompendo, seja promovendo, seja liderando a inovação tecnológica, é um fator decisivo no processo geral, à medida que expressa e organiza as forças sociais dominantes em um espaço e uma época determinados.

Em face do exposto, surge a necessidade de uma proteção em relação ao compartilhamento de dados pessoais, principalmente em vista de terceiros que manipulam e vendem esses dados para empresas que necessitam do perfil do usuário. Diante disso, o Estado passou a criar determinadas leis que regulam o uso, compartilhamento e armazenamento de dados pessoais, tendo como principal ponto a proteção da privacidade do usuário, de sua imagem e moral.

3.1 Marco Civil da Internet

O Marco Civil da Internet (Lei 12965/14) foi o primeiro documento que legislou sobre a regulamentação da internet no Brasil, com o objetivo de estabelecer princípios, garantias, direitos e deveres. Como dito no “Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil”. (BRASIL, 2014).

No quesito de proteção de dados pessoais e privacidade do usuário a referida lei diz:

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:
II - proteção da privacidade;
III - proteção dos dados pessoais, na forma da lei;
VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei; (BRASIL, 2014)

Logo a lei exerce influência direta sobre os dados e a privacidade do cidadão, podendo este responsabilizar o controlador do determinado site caso esses princípios sejam feridos, contudo a lei ainda é muito vaga, de maneira que a mesma não indica as formas de indenização de que o usuário poderá receber. Por exemplo, determinado site ao pegar a informação para análise do usuário, acaba por espalhá-la rede a fora, ao julgar pela lei o controlador tem a obrigação de retirar as informações que vazaram, contudo, como fica a imagem do usuário diante da rápida disseminação no meio digital? Será que o simples fato de apagar essas informações fará tudo voltar ao normal? Para essa pergunta a lei se pauta no artigo 7:

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; (BRASIL, 2014)

Ademais, retomando o uso de *cookies* e sua influência direta a violação de privacidade do cidadão, o artigo 7, incisos VII, VIII e IX, apresentam soluções para esse problema:

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais; (BRASIL, 2014)

Diz Cavalcanti (2021, p. 105) sobre a captação de informações do usuário:

Note-se que tal determinação legal advinda do MCI desde 2014 já demonstrava a necessidade de haver comunicação clara e inequívoca ao usuário da web acerca da captação de suas informações, expondo-se, inclusive, as finalidades de tal tratamento.

O Marco Civil da Internet foi uma importante lei para o uso da internet no Brasil, assegurando aos usuários o direito a proteção a imagem, a moral, dados pessoais, sigilo de suas informações (reforçando essa garantia presente no artigo 5, XII, da Constituição Federal de 1988). Contudo ainda havia a necessidade da complementação dessa lei, diante disso, foi criada a Lei Geral de Proteção de Dados (LGPD).

3.2 Lei Geral de Proteção de Dados Pessoais

Antes de adentrarmos na lei brasileira, precisamos entender uma lei internacional que influenciou totalmente a criação da Lei Geral de Proteção de Dados Pessoais. O Regulamento Geral sobre a Proteção de Dados (RGPD), em inglês *General Data Protection Regulation* (GDPR), surgiu com base na discussão da União Europeia em 2012, sobre os dados pessoais de seus cidadãos usados nas relações comerciais. A RGPD concede aos usuários gerenciarem seus dados pessoais requisitados por sites e organizações digitais. O regulamento foi publicado em 27 de abril de 2016, entrando em vigor em 2018.

Nesse sentido, o Brasil cria a Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/18, entrando em vigor em 14 de agosto de 2020. A lei tem como principal ponto a proteção dos usuários e de seus dados pessoais, assegurando a liberdade, privacidade e livre desenvolvimento da personalidade (BRASIL, 2018).

Como consta a lei:

Art. 2º A disciplina da proteção de dados pessoais tem como fundamentos:
I - o respeito à privacidade;
II - a autodeterminação informativa;
III - a liberdade de expressão, de informação, de comunicação e de opinião;
IV - a inviolabilidade da intimidade, da honra e da imagem;
VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Desse modo, os direitos sobre os dados pessoais começam a ganhar mais poderes, de maneira que o cidadão está legalmente protegido em casos de disseminação de informações pessoais feitas por terceiro.

Segundo a lei (2018):

Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
I - mediante o fornecimento de consentimento pelo titular;
II - para o cumprimento de obrigação legal ou regulatória pelo controlador;
(BRASIL, 2018)

Como visto o fornecimento de dados pessoais do usuário só pode ser feito mediante consentimento ou obrigação legal. Deste modo boa parte das páginas on-line que usam *cookies* adotaram medidas para adquirir o consentimento do usuário, dentre uma das medidas feitas está o uso de *pop-ups*, pequenos avisos que surgem na tela, normalmente com termos genéricos do tipo: “Este site utiliza *cookies* para melhor desempenho e utilização do usuário. Verificar políticas de privacidade ou

aceitar o uso”. Tal medida é legal, contudo deve se levar em conta o grau de conhecimento do usuário que muitas vezes desconhece o que são *cookies* e para o que servem.

Tal medida pode ser considerada uma arquitetura de consentimento, tendo em vista o desconhecimento técnico do usuário, além de, ao se ler os termos de privacidade é utilizada uma linguagem jurídica e de difícil entendimento, de maneira que muitas vezes a pessoa acaba aceitando sem ler ou sem entender. Vale ressaltar também o incômodo que esses avisos geram, fazendo com que, mais uma vez, o usuário aceite mesmo sem saber ou realmente consentir.

Uma outra forma de consentimento mostrada pela experiência de Martin Degeling et al. (2019) foi o meio de *AutoAccept* em que o usuário ao efetuar a simples rolagem da página, já é considerada uma forma de consentimento.

A respeito disso a LGPD diz:

Art. 8º O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular.

§ 3º É vedado o tratamento de dados pessoais mediante vício de consentimento.

§ 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. (BRASIL, 2018)

Tais maneiras, em especial a do experimento, são vícios de consentimento, ora, como o usuário pode consentir sem saber do que se trata ou como pode ele saber que a simples interação com a página já ativa mecanismos para o armazenamento de seus dados, portanto nulas.

Diante do descumprimento das medidas impostas, é dito:

Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: [\(Vigência\)](#)

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R\$ 50.000.000,00 (cinquenta milhões de reais) por infração;

III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência; (BRASIL, 2018)

Logo, tem-se que os domínios que descumprem tal lei serão multados em até 2%, um valor alto dependendo do quanto é faturado pelo domínio, já que grande parte dos sites na internet tem uma origem pequena e amadora. Vale-se também do recurso da imagem do controlador, já que se tem a publicização do ocorrido, prejudicando sua imagem e possível perda de público.

3.3 Constituição Federal de 1988

Valendo-se de direitos fundamentais, a Constituição (1988) diz:

Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:

X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal; [\(Vide Lei nº 9.296, de 1996\)](#)

Diante disso, a Constituição ressalva os direitos fundamentais, trazendo ao campo digital, esses direitos recaem especificamente aos dados pessoais do usuário, de maneira que eles devem ser protegidos para a proteção da intimidade, vida privada, honra e imagem, como consta no inciso X. Quanto a divulgação de dados pessoais por terceiros, o direito recai sobre o inciso XII, quanto a inviolabilidade do sigilo a correspondência e comunicações, de maneira há uma interceptação de terceiro enquanto o usuário fornece seus dados ao domínio.

4 CONCLUSÃO

Diante do presente artigo, vê-se que o uso de *cookies* e seus processos, armazenamento, investigação do perfil do usuário, como seu histórico, procura de produtos e serviços, preferências, e-mail e até senha, foram de grande relevância a sociedade digital, em específico nas áreas de marketing e publicidade em que há a criação de um perfil de consumidor tão fiel quanto o original. O fato é que grande parte desses dados são obtidos através do uso de *cookies* de terceiros, de modo que o

usuário não tenha total consciência de quem está usufruindo de seus dados, para onde estes vão ou qual a exata utilidade dele para o referido arquivo. Muitos desses dados são “vendidos” a grandes lojas digitais para maior alcance e venda de seus produtos, contudo essa venda é feita sem o real consentimento do usuário.

Mediante a problemática o Google se prontificou, em sua página Suporte do Google Chrome indica que com o uso da página anônima, os dados, histórico, contas, entre outras informações não são salvas, quanto aos *cookies* seu uso vira de sessão, sendo que ao fechar o navegador eles são automaticamente excluídos. Vale ressaltar também a iniciativa do Google de acabar com os *cookies* de terceiros em 2024, consultando mais privacidade e proteção ao usuário.

Como dito, medidas destacadas na Lei Geral de Proteção de Dados Pessoais como multa e a publicidade do fato ocorrido são medidas que acabam por gerar grande prejuízo tanto para a imagem do domínio, quanto o prejuízo econômico, efetivando a perda de público e grande perda de dinheiro a depender do faturamento da pessoa jurídica de direito privado.

Contudo deve ser destacado a necessidade de políticas de implementação para o conhecimento do usuário sobre a utilização de *cookies*, sua influência no meio digital e, principalmente, no recolhimento de dados pessoais e sua violação a direitos fundamentais.

Deste modo pode se ter uma maior consciência acerca dos direitos fundamentais, sua importância e relevância no atual meio digital, cuja a tendência é um crescimento desenfreado, mediante a isso cabe maior ampliação e destinação da legislação para assegurar um ambiente seguro no meio digital.

REFERÊNCIAS

ALMENARA, Igor. **Google adia fim dos cookies no Chrome para 2024**. CanalTech, 2022. Disponível em: <https://canaltech.com.br/internet/google-adia-fim-dos-cookies-no-chrome-para-2024-221779/>. Acesso em: 13 set. 2022.

BITTAR, Eduardo C B. **Metodologia da pesquisa jurídica: teoria e prática da monografia para os cursos de direito**. São Paulo: Editora Saraiva, 2022. E-book. ISBN 9786553622470. Disponível em: <https://integrada.minhabiblioteca.com.br/#/books/9786553622470/>. Acesso em: 10 set. 2022.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidência da República, 2022. Disponível em:

http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 13 set. 2022.

BRASIL. **Lei Federal nº. 12.965/2014**, “Marco Civil da Internet no Brasil”. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 13 set. 2022.

BRASIL. **Lei n. 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados (LGPD)**. Brasília, DF. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 13 set. 2022.

BODIN DE MORAES, Maria Celina. **Ampliando os direitos da personalidade**. Academia.edu, 2012. Disponível em: [https://www.academia.edu/9689598/Ampliando os direitos da personalidade](https://www.academia.edu/9689598/Ampliando_os_direitos_da_personalidade). Acesso em: 11 set. 2022.

CANDIDO, João Pedro; ARAÚJO, Tayná; RIBEIRO, William. **HISTÓRICO DA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)**. Advocatta, 2022. Disponível em: <https://advocatta.org/historico-da-lei-geral-de-protecao-de-dados-lgpd/#:~:text=A%20Lei%20Geral%20de%20Prote%C3%A7%C3%A3o%20de%20Dados%20passou%20por%20um,e%20tratamento%20de%20seus%20dados>. Acesso em: 13 set. 2022.

CAVALCANTI, Mario Filipe. **COOKIES PARA QUEM? ENTRE O ESCAMBO DIGITAL E OS DIREITOS À PRIVACIDADE E PROTEÇÃO DE DADOS**. Revista Acadêmica da Faculdade de Direito do Recife – ISSN: 2448-2307, 2021. Disponível em: <https://periodicos.ufpe.br/revistas/ACADEMICA/article/view/249887>. Acesso em: 7 set. 2022.

CASTELLS, Manuel. **A Sociedade em rede**. São Paulo: Paz e Terra, 1999. Disponível em: <https://globalizacaoeintegracaoregionalufabc.files.wordpress.com/2014/10/castells-m-a-sociedade-em-rede.pdf>. Acesso em: 11 set. 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: 11 set. 2022.

GOOGLE. **Limpar, ativar e gerenciar cookies no Chrome**. Disponível em: <https://support.google.com/chrome/answer/95647?hl=pt-BR&co=GENIE.Platform%3DAndroid>. Acesso em: 13 set. 2022.

KINAST, Priscilla. **7 tipos de cookies do navegador**. Oficina da Net, 2019. Disponível em: <https://www.oficinadanet.com.br/internet/24798-7-tipos-de-cookies-do-navegador>. Acesso em: 10 set. 2022.

LESSIG, Lawrence. **Code (version 2.0)**. Nova Iorque: Basic Books, 2006. ISBN-10: 0-465-03914-6. ISBN-13: 978-0-465-03914-2.

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: 14 set. 2022.

MICROSOFT. **Resumo do Regulamento Geral sobre a Proteção de Dados**. Microsoft, 2022. Disponível em: <https://docs.microsoft.com/pt-br/compliance/regulatory/gdpr>. Acesso em: 13 set. 2022.

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: 9 set. 2022.

OLIVEIRA, Jordan V.; SILVIA, Lorena A. **“É de Comer?” Cookies de Navegador e os Desafios à Privacidade na Rede**. R. Tecnologia e Sociedade, Curitiba, v. 15, n. 37, p. 297-310. 2019. Disponível em: <https://periodicos.utfpr.edu.br/rts/article/view/8419>. Acesso em: 7 set. 2022.

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

PALMER, Chris. **Secure Session Management With Cookies for Web Applications**. San Francisco – CA, 2008. Disponível em: <https://crypto.stanford.edu/cs142/papers/web-session-management.pdf>. Acesso em: 9 set. 2022

QUEIROZ, Anderson A.L.; DE QUEIROZ, Ruy J.G.B. **A Invasão de Privacidade na Internet: um Modelo de Boas Práticas e uma Proposta Interativa de Proteção da Privacidade por Meio dos Cookies**. 2011. Dissertação (Mestrado). Programa de Pós-Graduação em Ciência da Computação, Universidade Federal de Pernambuco, Recife, 2011. Disponível em: <https://repositorio.ufpe.br/handle/123456789/1298>. Acesso em: 7 set. 2022.

RIBEIRO, Micaela M.; FACHIN, Zulmar. **COOKIES E DIREITOS DA PERSONALIDADE: DESAFIOS SOBRE A APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS**. Revista de Direito, Inovação, Propriedade Intelectual e Concorrência. 2022. Disponível em: <https://www.indexlaw.org/index.php/revistadipic/article/view/8838>. Acesso em: 7 set. 2022.

Sem autoria definida. **GDPR: o que é e qual a diferença em relação à LGPD?**. Cátedra, 2021. Disponível em: <https://idcatedra.com.br/2021/08/gdpr-o-que-e-e-qual-a-diferenca-em-relacao-a-lgpd/>. Acesso em: 13 set. 2022.

TOUBIANA, Vincent; NARAYANAN, Arvind; BONEH, Dan; NISSENBAUM, Helen F.; BAROCAS, Solon. **Adnostic: Privacy Preserving Targeted Advertising**. 2010. Proceedings Network and Distributed System Symposium, March 2010. Disponível em: <https://ssrn.com/abstract=2567076>. Acesso em: 10 set. 2022.

ZARSKY, Tal. **Online Privacy, Tailoring and Persuasion.** Privacy and Technologies of Identity - A Cross-Disiplinary Conversation, 2006. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=946428. Acesso em: 12 set. 2022.