

Análise da obtenção de consentimento para coleta de dados em sites de e-commerce: um olhar da Ciência da Informação

Daiane Marcela Piccolo

Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP) – Marília-SP, Brasil

Elaine Parra Affonso

Faculdade de Tecnologia de Presidente Prudente (Fatec); Centro Estadual de Educação Tecnológica Paula Souza (CEETEPS) – SP, Brasil

Ricardo César Gonçalves Sant'Ana

Universidade Estadual Paulista Júlio de Mesquita Filho (UNESP) – Marília-SP, Brasil

ORIGINAL

Resumo

Objetivo. A lei Geral de Proteção de Dados, aprovada no Brasil, estabelece restrições ao coletar informações online que possam ser usadas para identificar indivíduos, na qual o consentimento na coleta de dados emerge como determinação para proteção da privacidade. Nesse cenário, este artigo tem como objetivos analisar as práticas de obtenção de consentimento do usuário em relação à coleta de dados.

Método: A metodologia constituiu de uma pesquisa exploratória de caráter qualitativo; pesquisa documental por meio de análise de documento jurídico em leis e regulamentos, a fim de identificar e descrever como os sites implementam práticas de obtenção de consentimento dos usuários em relação à coleta de dados. A abordagem adotada foi a pesquisa multicase utilizando para o estudo os 10 sites de e-commerce mais acessados no mês de março de 2022, segundo o ranqueamento do E-commerce Brasil. Para análise das práticas adotadas pelos sites, buscou-se as diretrizes propostas na Lei Geral de Proteção de Dados aprovada no Brasil. A coleta foi realizada no mês de abril de 2022.

Resultado: Observou-se que 6 (seis) dos sites analisados obtém consentimento para a coleta de dados por meio de avisos de cookies, predominando mensagens breves, mencionando apenas a melhoria da experiência do usuário e link para a política de privacidade e sem oferecer opções de personalização, dificultando a compreensão completa da coleta de dados.

Conclusões: O consentimento informado nos sites, influenciado pelas regulamentações de proteção de dados, como o GDPR na Europa e a LGPD no Brasil, tem sido abordado principalmente por meio de avisos de cookies, frequentemente limitados a um simples botão de "OK" ou "concordo", resultando em deficiências na explicitação dos tipos de cookies e opções de configuração. Essas lacunas podem gerar uma falsa sensação de controle por parte dos usuários e levar a riscos a proteção da privacidade.

Palavras-chaves:

Coleta de dados. Consentimento. Política de Privacidade. Privacidade. Proteção de Dados Pessoais.

Consent to data collection: privacy policies and data collection notices

Abstract

Objective: The General Data Protection Law, approved in Brazil, establishes restrictions on the privacy of online information that can be used to identify individuals, in which consent to data collection emerges as a determination to protect privacy. In this scenario, this article aims to analyze the practices of providing user consent in relation to data collection.

Method: The methodology consisted of exploratory qualitative research; documentary research through legal document analysis of laws and regulations in order to identify and describe how websites implement practices for obtaining user consent in relation to data collection. The approach adopted was multi-case research used to study the 10 most accessed e-commerce sites in March 2022, according to the E-commerce Brasil ranking. To analyze the practices adopted by websites,

look for the guidelines proposed in the General Data Protection Law approved in Brazil. The collection was carried out in April 2022.

Result: It was observed that 6 (six) of the websites analyzed obtain consent for data collection through cookie notices, predominantly brief messages, mentioning only the improvement of user experience and a link to the privacy policy and without offering customization options, making it difficult to fully understand the data collection.

Conclusions: Informed consent on websites, influenced by data protection regulations such as GDPR in Europe and LGPD in Brazil, has been addressed mainly through cookie notices, often limited to a simple "OK" or "OK" button. I agree", resulting in deficiencies in explaining the types of cookies and configuration options. These gaps can generate a false sense of control on the part of users and pose risks to privacy protection.

Keywords:

Data collection. Consent. Privacy Policy. Privacy. Protection of Personal Data.

Análisis del consentimiento para la recolección de datos en sitios de comercio electrónico: una mirada a la Ciencia de la Información

Resumen

Objetivo. La Ley General de Protección de Datos, aprobada en Brasil, establece restricciones a la recolección de información en línea que pueda ser utilizada para identificar individuos, en la cual el consentimiento en la recolección de datos surge como una determinación para proteger la privacidad. En este contexto, este artículo pretende analizar las prácticas de obtención del consentimiento de los usuarios en relación con la recogida de datos.

Método: La metodología consistió en una investigación exploratoria cualitativa; una investigación documental mediante el análisis de documentos legales en leyes y reglamentos con el fin de identificar y describir cómo los sitios web implementan prácticas para obtener el consentimiento del usuario en relación con la recogida de datos. El abordaje adoptado fue un estudio de casos múltiples utilizando los 10 sitios de comercio electrónico más visitados en marzo de 2022, según el ranking E-commerce Brasil. Para analizar las prácticas adoptadas por los sitios, se utilizaron las directrices propuestas en la Ley General de Protección de Datos aprobada en Brasil. Los datos se recogieron en abril de 2022.

Resultados: Se observó que 6 (seis) de los sitios web analizados obtienen el consentimiento para la recolección de datos a través de avisos de cookies, predominantemente mensajes breves, que mencionan únicamente la mejora de la experiencia del usuario y un enlace a la política de privacidad y sin ofrecer opciones de personalización, lo que dificulta la plena comprensión de la recolección de datos.

Conclusiones: el consentimiento informado en los sitios web, influido por normativas de protección de datos como el GDPR en Europa y la LGPD en Brasil, se ha abordado principalmente a través de avisos de cookies, a menudo limitados a un simple botón "OK" o "aceptar", lo que provoca deficiencias a la hora de explicar los tipos de cookies y las opciones de configuración. Estas lagunas pueden crear una falsa sensación de control por parte de los usuarios y conllevar riesgos para la protección de la privacidad.

Keywords:

Recogida de datos. Consentimiento. Política de privacidad. Protección de datos. Protección de datos personales.

1. Introdução

O sujeito participante do ciberespaço¹ torna-se alvo de indesejáveis coletas de dados que podem ocorrer em diversos momentos e, indubitavelmente, sem que o titular tenha conhecimento sobre a coleta de seus dados, atividade que, posteriormente, pode resultar em tratamento e disponibilização dos dados. Proporcionar conhecimento em relação aos dados coletados requer estratégias, tais como as políticas de privacidade, termos de uso dos dados e solicitação de consentimento do usuário, tornando-se esses fundamentais para minimizar a insciência dos usuários em relação a coleta de seus dados nos ambientes digitais.

Sarlet e Caldeira (2019) abordam a importância do consentimento, especialmente no contexto da internet, como um processo de conhecimento (gnosiológico). Eles enfatizam que esse processo envolve o conhecimento prévio

¹ Conceituado por Lévy (2008, p. 17) como novo meio de comunicação que surge da interconexão mundial de computadores, sendo esse espaço representado pela infraestrutura material da comunicação digital, pelo universo oceânico de informações e os usuários que participam desse universo.

e claro sobre aspectos como pertinência, finalidade, adequação, tempo de coleta, armazenamento, tratamento e transmissão dos dados. Essas informações devem ser comunicadas de maneira clara, precisa, apropriada e suficiente para permitir ao consentidor a tomada de decisão informada. Essa abordagem visa garantir que o consentimento concedido possibilite ao indivíduo renunciar, alterar, utilizar, ceder, disponibilizar ou recusar seus dados conforme sua vontade.

Com aprovação da Lei 13.709 de 2018 no Brasil e do Regulamento (UE) 679 de 2016 do Parlamento Europeu e Conselho - *General Data Protection Regulation* (GDPR), o consentimento nas questões vinculadas a coleta de dados como meio de proteção da privacidade tem se tornado aspecto relevante para que vários segmentos atendam a esses regulamentos. No entanto, questões relacionadas ao consentimento já são recorrentes na área da saúde, e de acordo com Pithan (2012) tem sido entendido como um processo de comunicação recíproca entre médico e paciente, para que esses possam decidir se desejam ou não se submeter a um tratamento ou procedimento diagnóstico.

Ganha importância crescente a necessidade de fundamentar regulamentações e leis de privacidade na abordagem do consentimento. Essa abordagem se apoia na premissa de que o consentimento de um indivíduo confere legitimidade a qualquer coleta de dados e seu subsequente uso (Choi; Jeon; Kim, 2019).

Sant'Ana (2016) ao abordar sobre o Ciclo de Vida dos dados (CVD) enfatiza que a fase de Coleta está relacionada com atividades de planejamento, a fim de verificar como os dados serão obtidos, filtrados e organizados, assim, é possível definir sua estrutura, formato e meios de descrição a ser utilizada. A fase de coleta no CVD apresenta fatores como privacidade, integração, qualidade, direitos autorais, disseminação e preservação dos dados.

Esta pesquisa aborda questões cruciais no âmbito da ciência da informação, que se concentra na compreensão, organização, recuperação e uso da informação em diferentes contextos. A partir do momento em que o sujeito participante do ciberespaço se torna vulnerável a indesejáveis coletas de dados sem seu conhecimento prévio, a pesquisa entra em um território diretamente relevante para a ciência da informação.

Primeiramente, a pesquisa aborda a questão da conscientização e compreensão do usuário em relação à coleta de dados em ambientes digitais. A falta de clareza nas políticas de privacidade e a abstração em relação ao processo de coleta de dados são temas centrais que a ciência da informação busca abordar. A ciência da informação se preocupa em garantir que os usuários tenham conhecimento e compreensão adequados sobre como seus dados estão sendo coletados, tratados e utilizados, a fim de capacitar sua tomada de decisão informada e proteger sua privacidade digital

Além disso, é destacado a importância do consentimento informado como um elemento fundamental na proteção da privacidade e dos direitos dos usuários. O consentimento nas questões relacionadas à coleta de dados é discutido como um processo de comunicação recíproca entre os usuários e as entidades coletoras, refletindo os princípios de transparência e autonomia fundamentais na ciência da informação. A ciência da informação busca estabelecer diretrizes e regulamentações que garantam que o consentimento seja obtido de maneira clara, precisa e suficiente, alinhando-se com as preocupações éticas e legais relacionadas à proteção de dados pessoais.

A pesquisa investiga, ainda, as práticas de consentimento adotadas pelos sites de e-commerce, demonstrando uma preocupação com a aplicação prática dos princípios de privacidade de dados em contextos específicos. Ao utilizar as diretrizes da Lei Geral de Proteção de Dados, a pesquisa se alinha com os esforços para traduzir os princípios legais em práticas concretas que protejam os direitos e interesses dos usuários.

Portanto, esta pesquisa apresenta forte aderência à Ciência da Informação, pois aborda questões essenciais relacionadas à privacidade de dados, transparência, consentimento informado e ética na coleta e uso de informações digitais, contribuindo para o avanço do conhecimento e práticas nesse campo interdisciplinar

Nesse contexto, esta pesquisa tem o objetivo identificar e descrever como os sites estão abordando a questão da obtenção de consentimento para coleta de dados levando em consideração o seguinte questionamento: quais práticas de consentimento foram adotadas em sites para que o usuário concorde com a coleta de seus dados?

O estudo teve como amostra os 10 sites de e-commerce mais acessados no Brasil no mês de março de 2022, segundo a classificação do E-commerce Brasil. A escolha de sites de e-commerce para o estudo, foi devido ao

crescimento dessa área no período da pandemia da COVID-19. Para a análise das práticas adotadas pelos sites, para obter o consentimento na coleta de dados, utilizou-se das diretrizes propostas na Lei Geral de Proteção de Dados aprovada no Brasil.

Este trabalho está estruturado da seguinte forma: os procedimentos metodológicos são explanados na seção 2, na seção 3 encontra-se a revisão bibliográfica sobre os conceitos e especificidades do consentimento para proteção de dados pessoais. Os resultados são apresentados na seção 4 e, as considerações finais na seção 5.

2. Procedimentos metodológicos

Esta pesquisa adota uma abordagem exploratória e qualitativa para investigar as práticas de obtenção de consentimento dos usuários em relação à coleta de dados nos sites de e-commerce. A coleta foi realizada no mês de abril de 2022.

A escolha do método multicaso proporcionou uma análise detalhada e comparativa de diferentes contextos, permitindo uma compreensão mais ampla das práticas de consentimento. Os casos foram selecionados com base nos 10 sites de e-commerce mais acessados no Brasil, conforme ranking do E-commerce Brasil, garantindo uma amostra representativa do cenário nacional.

A coleta de dados envolveu uma pesquisa documental por meio da análise de regulamentações de proteção de dados, como o GDPR na Europa e a Lei Geral de Proteção de Dados no Brasil e, parte das políticas de privacidade dos sites selecionados para o estudo. Além disso, foram observadas e descritas as informações disponibilizadas nos avisos de cookies dos sites, relacionadas a coleta de dados por meio do consentimento do usuário.

A análise comparativa permitiu identificar padrões, semelhanças e diferenças nas práticas de consentimento entre os diferentes sites. Para sistematizar os resultados, foi elaborado quadro com informações detalhadas sobre as práticas de obtenção de consentimento, incluindo os tipos de cookies utilizados e as opções de gerenciamento oferecidas aos usuários.

É importante ressaltar que esta pesquisa não tem como objetivo discutir aspectos legais e eventuais consequências para os casos que estariam infringindo a legislação. No entanto, espera-se que os resultados obtidos neste estudo possam subsidiar futuros estudos desenvolvidos no campo da Ciência da Informação sobre a responsabilidade de profissionais da informação e em especial bibliotecários, bem como questões relacionadas a motivação para participação, seja nas atividades de controle, vigilância ou mesmo acompanhamento, inclusive motivando novas pesquisas.

3. O consentimento para proteção de dados pessoais: conceitos e especificidades

No Brasil a lei específica para proteção de dados pessoais foi sancionada em 16 de agosto de 2018, a denominada Lei 13.709/18 - Lei Geral de Proteção de Dados Pessoais (LGPD), que: [...] dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (Brasil, 2018).

Para fins da LGPD, o termo consentimento é definido no artigo XII como “manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada” (BRASIL, 2018). Ressalta-se que na presente lei, o termo tratamento é conceituado como “toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução [...]” (Brasil, 2018).

A LGPD segue diretrizes do Regulamento (UE) 2016/679 do Parlamento Europeu e do *General Data Protection Regulation* (GDPR), que entrou em vigor em maio de 2018 e, em relação ao consentimento, o GDPR declara que:

O consentimento do titular dos dados deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito, como por exemplo mediante uma declaração escrita, inclusive em formato eletrônico, ou uma declaração oral (União Europeia, 2016).

Ao analisar o termo de consentimento nos regulamentos, observou-se que se alinha com as seguintes situações: manifestação/vontade livre; informada, específica e inequívoca.

A existência de consentimento livre só é válida “se o titular dos dados puder exercer uma verdadeira escolha e não existir nenhum risco de fraude, intimidação, coação ou consequências negativas importantes se o consentimento for recusado” (União Europeia, 2014, p.60), apontando, assim, para o posicionamento da legislação europeia no sentido de que a manifestação não seja livre se o titular não puder dar seu consentimento de modo separado para as diferentes operações de tratamento de dados pessoais (União Europeia, 2014). Desta forma, qualquer elemento de pressão ou influência inadequada que impede um titular de dados de exercer seu livre arbítrio, tornará o consentimento inválido (Machado, 2023).

O elemento "livre" implica em escolha real do titular dos dados e deve ser dado de forma voluntária (GDPR, 2016). Como regra geral, o GDPR prescreve que se o titular dos dados não tiver escolha real, sentir-se obrigado a consentir, sofrer qualquer tipo de pressão, intimidação, ou consequências negativas, e se não consentir, então o consentimento não será válido (GDPR, 2016).

Caso o consentimento seja agrupado como uma parte inegociável dos termos e condições, presume-se que não tenha sido dado livremente. Assim, o consentimento não será considerado livre se o titular dos dados não puder recusar ou retirar seu consentimento sem prejuízo (Machado, 2023).

O consentimento deverá ser informado, isto é, torna-se necessário fornecer ao titular informações suficientes para contribuir com a tomada de decisão. Assim, é necessário dispor de uma descrição rigorosa e facilmente compreensível do objeto do consentimento, das consequências do consentimento, como também de sua recusa (União Europeia, 2014).

O titular dos dados deve possuir informações suficientes antes de tomar sua decisão, dessa forma, a suficiência ou insuficiência das informações fornecidas poderá ser determinada caso a caso, considerando que a linguagem utilizada deve ser adaptada aos titulares das informações. Importante destacar que, questões de acessibilidade e visibilidade das informações são elementos importantes na determinação desta decisão (União Europeia, 2014; Brasil, 2018).

Deve ser informado, ainda, sobre o seu direito de retirar o consentimento a qualquer momento, visto que, a retirada deve ser tão fácil quanto dar consentimento. No § 5º do artigo X da LGPD fica regulamentado que: “O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação” (Brasil, 2018).

A revogação do consentimento deve ser tão fácil quanto a sua concessão, e os titulares devem ser informados claramente sobre o seu direito de retirar o consentimento a qualquer momento. Em suma, o consentimento continua a ser um elemento central nas regulamentações de proteção de dados, mas agora está sujeito a condições que refletem a ênfase na autonomia do titular dos dados e na transparência no tratamento de dados pessoais.

A *European Data Protection Board* (EDPB) entende que pelo menos as seguintes informações são necessárias para obter o consentimento válido: a identidade do controlador; o propósito de cada uma das operações de processamento para as quais se busca o consentimento; quais dados serão coletados e utilizados; a existência do direito de retirada do consentimento; informações sobre o uso dos dados para tomada de decisão automatizada, quando necessário, e; os possíveis riscos de transferência de dados devido à ausência de uma decisão de adequação e de salvaguardas adequadas (European Data Protection Board, 2020).

Colesky, Hoepman e Hillen (2016) atrelam o consentimento informado como uma estratégia para que o titular tenha controle em relação aos seus dados, pois, para que aconteça o tratamento de dados pessoais seria necessário ter o consentimento explícito e dado de forma livre pelo titular. Desta forma, o consentimento informado está vinculado à autonomia, que concede liberdade individual ao escolher, e está associado à

privacidade, autodomínio, escolha livre, liberdade de escolha e aceitação da responsabilidade pelas escolhas (Faden, Beauchamp, 1986).

Spencer, Van Haneghan e Baxter (2021) ao abordar sobre questões de controle e autodeterminação proporcionadas pelo consentimento informado, ressalta que a autonomia da pessoa é uma pré-condição e, uma consequência do consentimento, o que confere ao titular dos dados influência no processamento dos seus dados.

O consentimento deve ser inequívoco, pois requer uma declaração ou um ato afirmativo claro e não pode ser implícito devendo sempre ser realizado por meio de um *opt-in*² ou uma declaração, para que não haja equívocos quanto o consentimento realizado pelo titular dos dados (GDPR, 2016)

Raposo (2018) esclarece que o consentimento inequívoco é aquele que foi prestado mediante uma manifestação do titular ou uma clara ação afirmativa, isso significa que o titular deve saber exatamente a finalidade para que está autorizando o uso de seus dados, por exemplo, quando realiza o *download* de um aplicativo para celular.

O consentimento tem de ser dado sempre de forma inequívoca, o que significa que não devem existir dúvidas razoáveis de que a pessoa em causa pretendia comunicar a sua permissão para o tratamento dos seus dados. O consentimento deduzido da mera inércia, por exemplo, não constitui um consentimento inequívoco. Quando esteja em causa o tratamento de dados sensíveis, o consentimento tem de ser obrigatoriamente explícito e inequívoco (União Europeia, 2014, p.60)

De acordo com Bioni (2020), o consentimento mantém sua importância central nos regulamentos, mas está começando a ser sujeito a limitações e condições para se alinhar com a autonomia do titular nesse cenário. Agora, é interpretado como um consentimento "livre, informado, inequívoco, explícito e/ou específico", refletindo a ênfase significativa atribuída ao consentimento nesses regulamentos.

A LGPD também aborda que o consentimento será específico para ser válido e, esta característica está intrinsecamente ligada à qualidade das informações fornecidas sobre o objeto do consentimento. No § 1º do artigo IX da referida lei é determinado que: "Na hipótese em que o consentimento é requerido, esse será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou abusivo ou não tenham sido apresentadas previamente com transparência, de forma clara e inequívoca." (Brasil, 2018).

Caso estejam previstas novas operações de tratamento ou alterações que não poderiam razoavelmente ter sido previstas quando o titular dos dados deu inicialmente o seu consentimento, é necessário pedir-lhe novamente o seu consentimento (União Europeia, 2014).

O consentimento assume uma função crucial nas regulamentações, visando conceder aos usuários o controle sobre seus dados para garantir a proteção de sua privacidade. Simultaneamente, são estabelecidos requisitos para que os detentores de dados informem os usuários sobre a coleta de dados, incluindo detalhes sobre seus direitos (Strycharz et al., 2021).

No contexto dos sites, o GDPR determina que o consentimento poderá ser dado mediante a validação de caixa de seleção, quando, por exemplo, se visita um web site, ou qualquer outro meio que deixa explícito que o titular dos dados aceita o tratamento que será realizado com seus dados. Ainda, ao abarcar sobre o consentimento na fase de coleta de dados em sites web, é regulamentado que o silêncio, a pré-validação ou a omissão não deverão configurar-se como consentimento (União Europeia, 2016).

O consentimento, no contexto da Lei Geral de Proteção de Dados (LGPD), é definido como uma manifestação livre, informada e inequívoca, em que o titular concorda com o tratamento de seus dados pessoais para uma finalidade específica (Brasil, 2018). Esse tratamento abrange uma série de operações, incluindo coleta, produção, recepção, classificação, utilização, acesso e reprodução dos dados. Inspirada no Regulamento Geral de Proteção de Dados (GDPR) da União Europeia, a LGPD estabelece diretrizes claras para o consentimento, exigindo que seja dado por meio de uma declaração positiva, clara e específica.

Interessante sublinhar que as questões vinculadas ao consentimento não são abordadas apenas na fase de coleta de dados no GDPR, mas busca abranger todas as atividades de tratamentos de dados, desta forma,

2 Reter/revogar o consentimento, optando pela exclusão (Densmore, 2019)

quando o tratamento tem várias finalidades, o titular deverá estar ciente sobre o consentimento para todos os possíveis fins.

Portanto, o consentimento deve ser livre, informado e inequívoco: Livre, o que implica que o titular dos dados tenha a capacidade de exercer uma verdadeira escolha, sem qualquer forma de coerção ou influência indevida. Informado, ou seja, o titular dos dados deve receber informações suficientes para tomar uma decisão consciente, incluindo a descrição precisa do objeto do consentimento e as consequências de aceitá-lo ou recusá-lo. Específico, aplicando-se apenas à finalidade determinada para a qual foi concedido.

3.1 Medidas para promover o consentimento em sites

Uma estratégia para minimizar questões voltadas à quebra de privacidade tem sido o uso de consentimento informado em ambientes digitais. Em 1998, a *Federal Trade Commission* baseada nas *Fair Information Practice Principles* (FIPPs)³ propôs cinco princípios básicos de proteção de privacidade, e dentre os princípios expõe sobre a escolha e consentimento do titular em relação aos dados, tal como o direito de escolher entre opções a forma como seus dados podem ser usados, regulamentando os regimes de *opt-in* ou *opt-out*. O regime *opt-in* requer que o titular confirme a permissão da coleta e/ou uso dos dados, enquanto o regime *opt-out* requer afirmações para impedir a coleta ou uso desses dados nos ambientes digitais (Federal Trade Commission, 1998)

No entanto, quando o ambiente é online, a *Privacy Online: A Report to Congress* ao descrever os *Fair Information Practice Principles Generally* enfatiza que o consentimento pode ser exercido clicando em caixas de diálogo, que indica a decisão do titular em relação à coleta, uso e compartilhamento de seus dados, ainda, esse ambiente deve apresentar novas possibilidades de interação além do paradigma *opt-in/opt-out*, pois os titulares dos dados podem especificar suas preferências quanto ao uso de suas informações antes de fazer uso ou entrar no site (Federal Trade Commission, 1998).

Em relação às caixas de diálogo, Bione (2020) ressalta que essa estratégia é uma forma do usuário externar o seu consentimento e exercer de forma amistosa o controle sobre seus dados pessoais. Normalmente essas caixas de diálogos são vinculadas ao uso de *cookies*, que retrata um meio de coleta e compartilhamento de dados mais comuns em sites e, que, de acordo com Mendes (2017) é a ferramenta de coleta de informação de identificação pessoal que demonstra o maior risco em relação ao nível de consciência sobre privacidade.

Nesse cenário de coleta de dados mediante caixas de diálogos vinculadas ao uso de *cookies*, o usuário pode se tornar insciente e, implicar em ameaças à privacidade. Para Afonso (2018, p. 29), “a insciência do usuário, enquanto alvo de fases de coleta de dados, sobre a ação dos detentores desses dados coletados, pode ser fator importante na precarização de seu direito à privacidade”.

Um dos meios de coletar dados em sites é mediante o uso de *cookies*, estes podem ser definidos como pequenos arquivos de texto que os sites colocam em seu navegador para armazenar informações sobre sua atividade na web. Eles permitem que os sites personalizem sua experiência de navegação e forneçam conteúdo relevante com base em suas preferências. No entanto, eles também podem ser usados para rastrear sua atividade online e coletar informações pessoais, o que pode apresentar riscos à privacidade e segurança do usuário (Da Silveira, 2017).

Para Mckinley (2010) os *cookies* fornecem quatro principais vantagens para o desenvolvedor do site: armazenam dados de sessão, registram localmente credenciais de login, dados de personalização relacionados a interação usuário-interface e, permitem, ainda, rastrear as atividades de usuários. Nesse sentido, os *cookies*

³ Em 1973, o comitê consultivo do governo dos Estados Unidos propôs um conjunto de princípios para proteção de dados pessoais, a denominada *Fair Information Practice Principles* (FIPPs). Esse foi o primeiro documento dos Estados Unidos que deu suporte às leis e à criação de frameworks de diversos países. As FIPPs são fruto do estudo ao longo dos anos de várias agências governamentais dos Estados Unidos, Canadá e Europa para investigar como entidades coletam e usam informações pessoais, denominadas de “Práticas de informação” (Federal Trade Commission, 1998).

podem desempenhar um papel multifuncional na otimização da experiência do usuário, desde a preservação de dados de sessão até o aprimoramento da personalização e análise do comportamento do usuário.

Mendes (2017) justifica que um cookie ao ser capaz de armazenar a interação entre o usuário e o site melhora a experiência de navegação e a torna personalizada, no entanto, essa atividade além de gerar ameaças de privacidade incorpora a perda de poder do usuário. Portanto, enquanto os cookies oferecem benefícios substanciais, é importante que os sites implementem práticas éticas para mitigar essas ameaças, garantindo a privacidade e segurança dos usuários online. Isso inclui transparência no uso de cookies e consentimento claro do usuário.

Devido ao fato de os *cookies* serem coletados e transmitidos automaticamente, essa atividade se torna opaca para o usuário, assim, os *cookies* se configuram como um recurso que reforça a opacidade para os titulares que não têm maiores informações dos pormenores dessa atividade de coleta, detalhes dessa operação não são facilmente perceptíveis o que enfraquece todas as outras ações para capacitar os usuários em relação ao controle de sua privacidade (Mendes, 2017). “O usuário pode ter a ciência de que há a coleta de *cookies*, pois está explícito nas políticas de privacidade; no entanto, não está perceptível o que representa, semanticamente, o conteúdo dos *cookies*, o que torna o usuário insciente sobre a coleta” (AFFONSO, 2018, p.232). Assim, a transparência no uso de cookies é fundamental para construir a confiança dos usuários e garantir que eles tenham controle sobre suas informações pessoais

Diante do exposto, observa-se que o uso de *cookies* se torna elemento facilitador para a coleta de dados de interação do usuário nos websites e que, para minimizar quebras de privacidade e atender às regulamentações de proteção de dados pessoais, faz-se necessária maior atenção e cuidado à obtenção do consentimento do usuário, fator determinante para que esses tenham consciência sobre a coleta, uso e compartilhamento de seus dados.

Em maio de 2020, o *European Data Protection Board* (EDPB) adotou diretrizes para conformidade com o GDPR, nas quais, constitui o que é válido para processamento de dados pessoais na União Europeia. De acordo com as diretrizes da EDPB, o aviso de *cookies* do site deve ser interativo e o site não deve ativar quaisquer *cookies* que coletam dados pessoais até que o titular tenha selecionado as categorias de *cookies* que eles permitirão operar, conhecido como consentimento prévio. Também fica determinado que a utilização de caixas *opt-in* pré-assinaladas em avisos de *cookies* não está em conformidade com o GDPR, uma vez que, não cumpre o requisito de “ação clara e afirmativa”. Assim, o site não tem permissão para ativar *cookies* que processam dados pessoais, a menos que o titular tenha dado seu consentimento claro e afirmativo para essa atividade (European Data Protection Board, 2020). Para estar em conformidade com os regulamentos de proteção de dados pessoais no âmbito de uso de *cookies*, os sites devem seguir determinações, conforme apresentadas no Quadro 1:

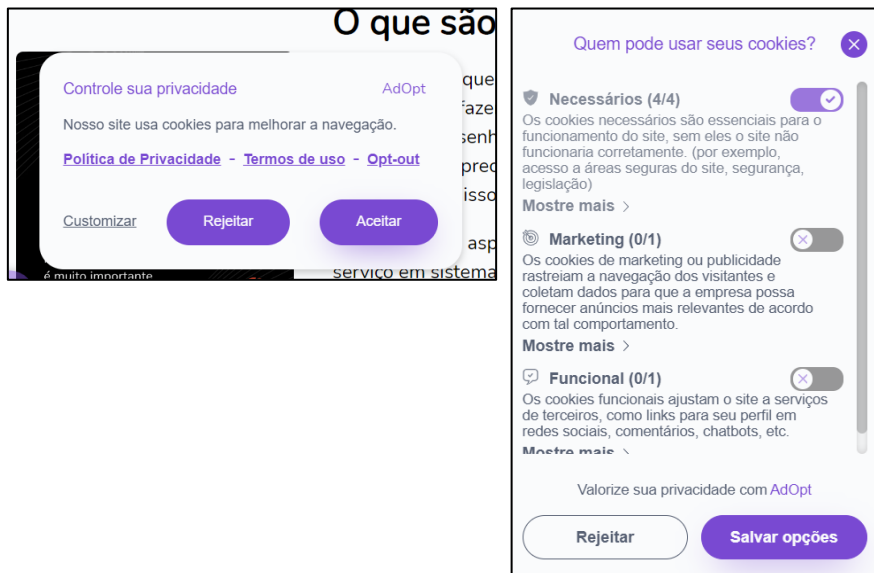
Quadro 1 - Recomendações de conformidade com os regulamentos de proteção de dados

Item	Recomendação	Legislação
1	Não utilizar caixas de seleção pré-marcadas em seus avisos de cookies	GDPR e LGPD
2	A interação de rolar e navegar continuamente na página web não é um consentimento válido	GDPR
3	Os <i>cookies walls</i> não são compatíveis para obtenção de consentimento do usuário	GDPR e LGPD
4	O bloqueio automático de todos os cookies e rastreadores para consentimento prévio ⁵	GDPR
5	A escolha granular e afirmativa de consentimento de tipos de cookies	GDPR
6	A descrição completa de cookie, finalidade, duração e tipo de cada <i>cookie</i>	GDPR e LGPD
7	Permitir uma maneira simples para que os titulares alterem ou retirem o consentimento, de acordo com sua vontade	GDPR e LGPD
8	Consentimento do Usuário documentado de forma segura	GDPR e LGPD
9	Renovação automática do Consentimento do Usuário	GDPR e LGPD

Fonte: Elaborado pelos autores (2023) com base na GDPR e na LGPD

A Figura 1 apresenta um tipo de aviso de *cookie* com características de compatibilidade com a GDPR e com LGPD, pois permite opções de escolha para o titular dos dados. O usuário ao clicar em customizar, ele pode escolher entre as opções “necessários”, “marketing”, “funcional” e, ainda, pode ter conhecimento dos detalhes sobre o uso dos *cookies* de cada item, a opção “Necessários” já vem pré-selecionada pelo *site*. Ao clicar em política de privacidade o titular é direcionado para as informações dessa política.

Figura 1: Exemplo de aviso de cookies



Fonte: AdOpt (2024).

4 Cookies walls é quando o site utiliza de uma pop-up para informar sobre o uso de cookies no site, no entanto o usuário não tem a opção de rejeitar. A única maneira de visualizar o conteúdo é aceitar e prosseguir (Hulsebos, 2011).

5 A função do bloqueio automático é verificar, encontrar e bloquear todos os cookies que rastreiam o comportamento do usuário, sendo que o desbloqueio acontece mediante o aviso de cookies com o consentimento do usuário (Privacytools, 2024).

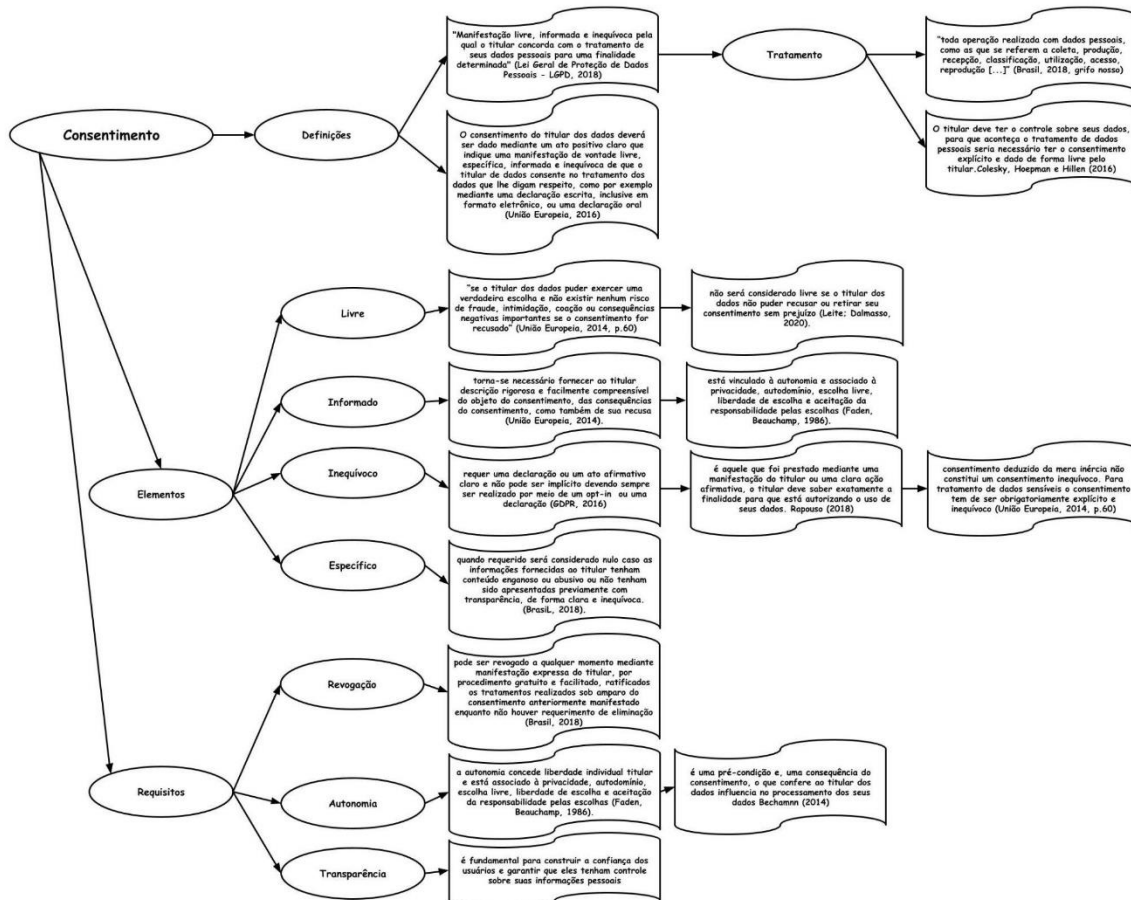
O uso das políticas de privacidade torna-se um recurso para que os provedores de serviços *online* disponibilizem informações a respeito das diretrizes da empresa em relação ao uso de dados e, podem ser utilizadas pelos titulares para supervisionar a maneira como seus dados pessoais são tratados pelas empresas (Steinfeld, 2016).

Reforça-se que, as políticas de privacidade contêm informações que podem auxiliar os usuários na compreensão sobre os seus direitos e quais opções são oferecidas para controlar melhor o uso de seus dados, porém, é perceptível que as políticas de privacidade são ignoradas pelos titulares, pois raramente leem seu conteúdo. Essa situação é devido à complexidade das frases utilizadas, que, muitas vezes são elaboradas com linguagem técnica de ordenamento jurídico, textos longos ou uso de linguagem vaga (Steinfeld, 2016), dificultando assim, a compreensão do usuário em relação à política, fator que pode acarretar a desmotivação pela leitura.

Nesse contexto, para que os usuários estejam cientes sobre o uso de seus dados, a informação disponibilizada, precisa ser clara, objetiva, completa e de fácil leitura e acessível, de forma que os usuários entendam quais dados são coletados, em que situações a coleta ocorre, se há compartilhamento de seus dados, onde são armazenados seus dados, quais terceiros fornecem dados à empresa, a finalidade da coleta de dados pela empresa, o tempo de armazenamento dos dados e se ocorre a exclusão de seus dados (Donda, 2020), fazendo com que o consentimento do usuário em relação a coleta de dados ocorra de modo livre, informado e inequívoco, minimizando a insciência do usuário nesse processo.

A figura 2 apresenta uma sistematização dos elementos envolvidos no consentimento informado mediante aviso de cookies em sites.

Figura 2: Sistematização de elementos do consentimento em aviso de cookies



Fonte: Elaborado pelos autores (2023)

4. Resultados

Ao analisar os avisos de cookies nos sites selecionados a partir da categorização do site E-commerce Brasil obteve-se as informações disponibilizadas no Quadro 2. Na primeira coluna do Quadro 2 é indicado o nome do site no qual o aviso de cookies foi analisado. A coluna “Informação disponibilizada” indica a mensagem exibida no aviso de cookies. A coluna “Opções de Confirmação” representa as alternativas em relação ao uso de cookies, permitindo que o usuário escolha, por exemplo, as seguintes opções: entendi, configurar cookies, gerenciar cookies, aceitar, rejeitar, preferências de cookies, N/A, concordar e fechar. A coluna “Opções de gerenciamento de cookies” vem dividida em duas colunas, sendo, respectivamente, “Categoria de cookie” (podendo ser funcionais, de publicidade, obrigatórios, mídias sociais, essencial, análise e personalização, desempenho e funcionalidade) e a coluna “Opções pré-marcadas” (sim ou não).

De acordo com a verificação nos sites selecionados, observou-se que para solicitar o consentimento da coleta de dados do usuário a prática adotada por 6 (seis) sites foi por meio de avisos de consentimento de cookies, o que pode ser observado na coluna “disponibilização da informação”. Nota-se que, a forma de solicitar o consentimento nos sites foi semelhante, uma justificativa para esse resultado pode ser o uso do mesmo Content Management System (CMS - Sistema de Gerenciamento de Conteúdo). Um CMS possibilita a criação, o gerenciamento, a edição, e a publicação de conteúdos em plataformas digitais para melhorar a gestão do conteúdo dos sites das organizações (Moreira e Hippert, 2020). Segundo o E-commerce Brasil, até 2020, 30% dos e-commerce utilizam essa plataforma, como Casas Bahia, Americanas, Microsoft, Amazon, Magazine Luiza e Netshoes. Já a Shoppe e o Mercado Livre têm o seu próprio CMS.

Observa-se na coluna “Informação disponibilizada” do Quadro 2 que as mensagens mostradas nos avisos de cookies pelos sites são curtas, somente informando o uso de cookies para “melhorar a experiência do usuário no site”, seguida por um link direcionando para a sua política de privacidade, caso o usuário queira obter mais informações.

Embora seja disponibilizado um link para a política de privacidade do site, tal link não deixa claro ao usuário que o acesso à política de privacidade é realizado por meio dele, pois ele faz parte da mensagem, sendo que parte dos links vêm com a palavra Política de Privacidade grifado e outra parte somente com a palavra em destaque. Dessa forma, cabe ao usuário entender que o acesso às políticas de privacidade, pode ser por meio desses termos.

Com exceção dos sites Mercado Livre, Microsoft e Casas Bahia, os 6 (seis) sites restantes apresentam apenas os avisos de consentimento de cookies, com botão de “Concordar”, “Entendi” e “Fechar”, conforme apresentado na coluna “Opções de Confirmação” do Quadro 2, sem a opção de personalização de tipos de cookies. Assim, ao continuar navegando, o titular concorda livremente com os termos de uso dos sites. Desta forma, o consentimento do usuário ocorreu de forma livre, porém, muitas vezes sem o conhecimento do tipo de coleta de dados que está sendo realizada. Dessa forma, para auxiliar os usuários na interpretação desses avisos de cookies, os sites apresentam em suas políticas de privacidade menções sobre essa forma de coleta de dados.

Verificou-se que, o contexto principal das informações sobre cookies nas políticas de privacidade dos sites está na Definição e explicação sobre o termo de cookies; na Justificativa e benefícios do uso cookies para coleta de dados; na participação de empresas terceiras na interação com os serviços do site e a classificação dos cookies por meio das Categorias.

Percebe-se que é recorrente, pelos avisos de consentimento dos sites, o direcionamento para as políticas de privacidade, pois os avisos vêm com informações curtas, somente informando que utiliza cookies, o que pode deixar muitas vezes os usuários em dúvida do significado dessa informação. Assim, para o titular obter mais informações, é necessário a leitura das extensas políticas de privacidade dos sites.

Quadro 2 - Descrição da informação adotada pelos avisos de cookies dos sites

Site	Prática			
	Informação disponibilizada	Opções de Confirmação	Opções de gerenciamento de cookies	
			Categoria de cookie	Opções pré-marcadas?
Mercado Livre	“Este site usa cookies: Ao navegar no nosso site você aceita o uso de cookies para personalizar sua experiência de acordo com a <u>Declaração de Privacidade</u> ”.	Entendi		
		Configurar cookies	Cookies funcionais	Sim
			Cookies de publicidade	Sim
Americanas	“Americanas e os cookies: a gente usa cookies para personalizar anúncios e melhorar a sua experiência no site. Ao continuar navegando, você concorda com a nossa <u>Política de Privacidade</u> ”.	Continuar e Fechar	N/A	N/A
Amazon.Brasil	N/A	N/A	N/A	N/A
Shopee	N/A	N/A	N/A	N/A
Magazine Luiza	“Cookies: a gente guarda estatísticas de visitas para melhorar sua experiência de navegação, saiba mais em nossa <u>política de privacidade</u> ”.	Entendi	N/A	N/A
		Fechar		
Aliexpress	N/A	N/A	N/A	N/A
Microsoft	“Usamos cookies opcionais para melhorar sua experiência em nossos sites, como por meio de conexões de mídia social e para exibir publicidade personalizada com base em sua atividade online. Se você rejeitar os cookies opcionais, serão usados somente os cookies necessários para fornecer os serviços. Você pode alterar sua escolha clicando em 'Gerenciar cookies' na parte inferior da página”. <u>Política de privacidade</u> <u>Cookies de terceiros</u>	Aceitar		
		Rejeitar		
		Gerenciar Cookies	Obrigatórios	Sim
			Análise	Não
	Mídia sociais	Não		
	Publicidade	Não		
Casas Bahia	“Utilizamos cookies para otimizar e aprimorar sua navegação no site. Todos os cookies, exceto os essenciais, necessitam de seu consentimento para serem executados. Saiba mais em nossa <u>Política de privacidade</u> ”.	Aceitar Cookies		
		Preferência de Cookies	Essencial	Sim
			Publicidade	Sim
			Análise e personalização	Sim
	Desempenho e funcionalidade	Sim		
Netshoes	“Cookies: a gente guarda estatísticas de visitas para melhorar sua experiência de navegação. Ao continuar, você concorda com nossa <u>Política de privacidade</u> ”.	Concordar	N/A	N/A
		Fechar		
Amazon.com	N/A	N/A	N/A	N/A

Fonte: Elaborado pelos autores (2023)

Observa-se que mesmo que o termo cookies seja recorrente nas políticas, há pontos falhos, ou seja, há poucas definições e explicações sobre de fato qual é a função dos cookies. Notou-se que o foco das políticas está em justificar o motivo de usar cookies na coleta de dados, sempre com o argumento de proporcionar melhores resultados e serviços para o usuário. Percebe-se que a interação de dados, entre site e usuário, ocorre pela política de troca e benefício.

A exposição sobre as categorias de cookies que os sites utilizam para coleta de dados mostrou-se insuficiente. Somente a política do Mercado Livre, Aliexpress e Microsoft disponibilizaram essa informação, porém, com detalhes insuficientes. Deixar claro a funcionalidade dessas categorias pode ser requisito fundamental para o usuário manter o controle sobre seus dados e minimizar a insciência que pode ocorrer sobre essa questão.

Nas políticas do Aliexpress e da Microsoft, caso o usuário queira obter mais informações, é disponibilizado links extras dentro da política para leitura com mais detalhes. Estes links apresentam uma relação de cookies que podem ser utilizados no site para coleta de dados, além de apresentar empresas terceiras autorizadas na implantação de cookies nos sites. No entanto, percebeu-se textos longos com linguagem técnica, o que pode dificultar o entendimento do usuário, e mesmo assim, os sites não especificam todos os cookies utilizados e não é possível identificar quais dados serão realmente coletados da máquina do usuário.

A informação sobre a presença de empresas terceiras nos sites foi mencionada por cinco políticas, sendo a Amazon Brasil, Shopee, Microsoft, Aliexpress e Amazon.com. Porém, não é disponibilizada a relação dessas empresas, com exceção da Microsoft e do Aliexpress, que lista empresas que participam do compartilhamento de cookies.

5. Discussão

Inserir uma menção sobre o uso de cookies nas políticas de privacidade do site está distante da percepção do usuário e das potenciais ramificações dessa coleta. Mesmo com essa notificação, a coleta de dados persiste, contribuindo para a crescente falta de consciência do usuário e dificultando qualquer tentativa de controle sobre seus dados, devido à ausência de informações claras.

O usuário pode ter conhecimento da coleta de cookies, uma vez que isso é explicitamente indicado nas políticas de privacidade. Contudo, a natureza exata do conteúdo desses cookies, as identidades das empresas terceiras envolvidas e as finalidades específicas para as quais esses dados são coletados não são claramente discerníveis, pois as políticas não discriminam esses detalhes de maneira abrangente. A falta de transparência na descrição do processo de coleta de dados pode, portanto, levantar preocupações éticas, uma vez que os usuários podem não ter ciência dos dados coletados e de como serão utilizados.

Nesse contexto, torna-se essencial a implementação de políticas de privacidade claras e a obtenção de consentimento informado para mitigar a falta de consciência dos usuários ao concordarem com o uso de seus dados. Os sites, ao assumirem essa responsabilidade, devem fornecer informações detalhadas sobre a coleta de dados, incluindo quais dados são coletados, com que finalidade e o período de retenção. Essa abordagem não apenas cumpre padrões éticos, mas também estabelece uma base sólida para a confiança entre usuários e sites.

Um aspecto adicional a ser considerado é a complexidade das tecnologias de rastreamento e coleta de dados, como os cookies. Essa complexidade pode dificultar a compreensão dos usuários sobre esses processos. Assim, simplificar as explicações ou fornecer informações mais acessíveis pode elevar o nível de consciência dos usuários em relação ao processo de coleta de dados, capacitando-os a exercer maior controle sobre suas informações pessoais. Essa abordagem não apenas promove a transparência, mas também respeita o direito dos usuários de entender e gerenciar o uso de seus dados online.

Neste estudo sobre os avisos de cookies em sites de e-commerce, foi possível identificar elementos com base nas informações disponibilizadas nos avisos de cookies, relacionadas à coleta de dados por meio do consentimento do usuário. Primeiramente, a importância do consentimento livre, informado e inequívoco foi destacada, em conformidade com a legislação brasileira e europeia, como a LGPD e o GDPR. Os avisos de cookies devem garantir que os usuários concedam seu consentimento de forma voluntária, com informações suficientes para tomar uma decisão consciente, e de maneira clara e específica para cada finalidade determinada.

Além disso, o estudo destacou a importância da transparência e da facilidade de revogação do consentimento. Os usuários devem ser informados sobre seu direito de retirar o consentimento a qualquer momento, de forma gratuita e facilitada. A transparência no uso de cookies também foi enfatizada como fundamental para construir a confiança dos usuários e garantir que eles tenham controle sobre suas informações pessoais. Por fim, o estudo ressaltou a necessidade de evitar práticas que possam comprometer a validade do consentimento, como o uso de pré-validação ou caixas *opt-in* pré-assinaladas, que não cumprem os requisitos de ação clara e afirmativa exigidos pelo GDPR.

Em suma, os elementos encontrados nos avisos de consentimento de coleta de cookies à luz das regulamentações de proteção de dados, contribuindo para uma maior conscientização sobre a importância do consentimento informado, livre, específico e inequívoco na preservação da privacidade dos usuários online.

6. Conclusão

O consentimento informado ganha notoriedade nos sites devido ao surgimento de regulamentações para proteção de dados pessoais, destaque para o GDPR na Europa e para a LGPD no Brasil. Essas regulamentações têm exigido que sites proporcionem meios para que o titular dê o consentimento para a coleta de dados ou recuse essa atividade. O consentimento deve ser uma manifestação livre, informada e inequívoca, para tanto, sites têm utilizado de avisos de cookies apresentando somente um botão de "OK" ou "concordo" como forma do usuário dar o consentimento, sem detalhes sobre os tipos de *cookies*, o que é considerado ilegal nas regulamentações de proteção de dados pessoais.

Este trabalho teve como objetivo identificar e descrever como os sites têm abordado questões relacionadas ao consentimento informado por meio de avisos de cookies. Observou-se que o uso de avisos de *cookies*, como fonte de informação sobre a coleta de dados é recorrente nos sites. No entanto, a explicitação sobre a coleta, ou seja, o tipo de *cookie*, sua finalidade e opções de configuração do uso de *cookie*, apresentam deficiências nos sites estudados. Estas deficiências podem fazer com que usuários ignorem avisos e concordem por meio de um simples toque no botão "Aceitar". Esta situação pode levar a uma falsa sensação de controle sobre a coleta de seus dados, já que os usuários tendem a não estar cientes do que estão consentindo. Além disso, avisos de consentimento são projetados com características que dificultam o entendimento.

Dessa forma, tornar o titular ciente sobre questões envolvidas com a coleta de dados é fundamental para iniciar a proteção da privacidade, assim, o uso de aviso de consentimento informado quando em consonância com as leis de proteção de dados podem ser uma estratégia para que o titular se torne mais consciente e tenha a percepção que pode dispor de mecanismos de controle sobre as atividades relacionadas com seus dados.

REFERÊNCIAS

AdOpt. LGPD e Cookies: O que você precisa saber. Disponível em: <https://goadopt.io/blog/cookies-e-lgpd/>. Acesso em: 24 de janeiro de 2024.

AFFONSO, Elaine P. A insciência do usuário na fase de coleta de dados: privacidade em foco. Tese (Doutorado em Ciência da Informação) - Universidade Estadual Paulista (Unesp), Faculdade de Filosofia e Ciências, 2018.

AFFONSO, ELAINE P.; SANTANA, R. C. G. Privacy awareness issues in user data collection by digital libraries. *IFLA Journal*, v. 44, p. 170-182, 2018.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/13709.htm

CHOI, Jay Pil; JEON, Doh-Shin; KIM, Byung-Cheol. Privacy and personal data collection with information externalities. *Journal of Public Economics*, v. 173, p. 113-124, 2019.

COLESKY, Michael; HOEPMAN, Jaap-Henk; HILLEN, Christiaan. A critical analysis of privacy design strategies. In: 2016 IEEE security and privacy workshops (SPW). IEEE, 2016. p. 33-40

CRESWELL, Jon W. *Investigação qualitativa e projeto de pesquisa: escolhendo entre cinco abordagens*. 3ª ed. Porto Alegre: Penso, 2014.

CUNNINGHAM, Patrick J. Are cookies hazardous to your privacy? Cookies allow businesses to collect information about Internet users, but some question whether they are valuable records or unethical tracking mechanisms. (NetWise). *Information management journal*, v. 36, n. 3, p. 52-55, 2002.

DA SILVEIRA, Sergio Amadeu. *Tudo sobre todos: Redes digitais, privacidade e venda de dados pessoais*. Edições Sesc, 2017.

DENSMORE, Russell. *Gestão do programa de privacidade: Ferramentas para gerenciar a privacidade na sua organização*. 2 ed. IAPP, 2019.

DONDA, Daniel. *Guia prático de implementação da LGPD*. Editora Labrador, 2020.

FADEN, Ruth R.; BEAUCHAMP, Tom L. *A history and theory of informed consent*. Oxford University Press, 1986.

FEDERAL TRADE COMMISSION. *Privacy online: a report to congress*. 1998. Disponível em: <https://www.ftc.gov/sites/default/files/documents/reports/privacy-online-report-congress/priv-23a.pdf>. Acesso em: 18 de março de 2023.

GIL, A. C. *Como elaborar projetos de pesquisa*. 5. ed. São Paulo: Atlas, 2010.

GUIDELINES 05/2020 on consent under Regulation 2016/679. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 17 de março de 2023.

HULSEBOS, A. What is cookie wall? *Complianz*. Disponível em: <https://complianz.io/definition/what-is-a-cookie-wall/>. Acesso em: 17 de março de 2023.

LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: Editora 34, 2008, p 17

MACHADO, Daniel Carlos. *Contratos Eletrônicos de Consumo: Formação Válida e Proteção de Dados Pessoais*. Editora Thoth, 2023.

MARCONI, M. A.; LAKATOS, E. M. *Metodologia científica*. São Paulo: Atlas, 2011.

MCKINLEY, Katherine. *Cleaning Up After Cookies Version 1.0*. Technical report, ISEC Partners, 2010.

MENDES, Laura Schertel. *Privacidade, proteção de dados e defesa do consumidor - Linhas gerais de um novo direito fundamental*. Saraiva Educação SA, 2017.

MOREIRA, Adriano Castro; HIPPERT, Maria Aparecida S. *Gestão de sistemas construtivos e de manutenção com ambientes cms em pequenas e médias empresas construtoras*. *Brazilian Journal of Development*, v. 6, n. 10, p. 79475-79486, 2020.

PITHAN. *O consentimento informado no Poder Judiciário brasileiro*. http://repositorio.pucrs.br/dspace/bitstream/10923/13017/2/O_consentimento_informado_no_Poder_Judiciario_brasileiro.pdf

PRIVACYTOOLS. *Como funciona o bloqueio automático de cookies*. Disponível em: <https://privacytools.com.br/como-funciona-o-bloqueio-automatico-de-cookies/>. Acesso em: 24 de janeiro de 2024.

RAPOSO, Jorge Nunes. *Guia Prático do Regulamento Geral sobre a Proteção de Dados*. Leya, 2018.

SANTANA, R. C. G. *Ciclo de vida dos dados e o papel da Ciência da Informação*. In: ENCONTRO NACIONAL DE PESQUISA EM CIÊNCIA DA INFORMAÇÃO, 14., 2013, Florianópolis. Anais... Florianópolis: ANCIB, 2013.

SANTANA, R. C. G. *Ciclo de vida dos dados: uma perspectiva a partir da ciência da informação*. *Informação & Informação*, v. 21, n. 2, p. 116-142, 2016.

SARLET, Gabrielle Bezerra Sales; CALDEIRA, Cristina. *O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana*. *Civilistica.com*. Rio de Janeiro, a. 8, n. 1, 2019. Disponível em: Acesso em: 15 de março 2023.

SPENCER, Patricia; VANHANEGHAN, James; BAXTER, Abigail. *Exploring social networks, employment and self-determination outcomes of graduates from a postsecondary program for young adults with an intellectual disability*. *Journal of Vocational Rehabilitation*, v. 55, n. 3, p. 251-270, 2021.

STEINFELD, Nili. "I agree to the terms and conditions": (How) do users read privacy policies online? An eye-tracking experiment. *Computers in human behavior*, v. 55, p. 992-1000, 2016.

STRYCHARZ, J.; SMIT, E.; HELBERGER, N.; VANNOORT, G. No to cookies: Empowering impact of technical and legal knowledge on rejecting tracking cookies. *Computers in Human Behavior*, [s. l.], v. 120, 106750, July 2021. DOI 10.1016/j.chb.2021.106750

UNIÃO EUROPEIA, Agência dos Direitos Fundamentais. Manual da Legislação Europeia sobre Proteção de Dados. Luxemburgo: Serviço das Publicações da União Europeia, 2014. Disponível em: https://www.echr.coe.int/Documents/Handbook_data_protection_Por.pdf. Acesso em: 17 de março de 2023.

UNIÃO EUROPEIA. European Parliament. Council of Europe. Regulation (EU) 2016/679 of the European Parliament and of the Council. EUR-Lex, 27 abr. 2016.

UNIÃO EUROPEIA. Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, 2020. Disponível em: https://www.edpb.europa.eu/our-work-tools/documents/public-consultations/2020/recommendations-012020-measures-supplement_en. Acesso em: 10 de março de 2023.

Dados dos autores

Daiane Marcela Piccolo

Doutorado em Ciência da Informação - Faculdade de Filosofia e Ciências (UNESP/Marília). Mestrado em Ciência da Computação pela Universidade Estadual de Maringá - UEM (2013), Pós-Graduação em Redes de Computadores e Internet Avançada pela Fundação Eurípedes - UNIVEM (2005), Graduação em Tecnologia em Processamento de Dados - Faculdades Adamantinenses Integradas (2002) e Técnico em Processamento de Dados pela Escola Técnica Amim Jundi (1998). Professora da Faculdade de Tecnologia (FATEC) de Presidente Prudente, professora da Escola Técnica Amim Jundi de Osvaldo Cruz. Coordenadora de curso da Escola Técnica Amim Jundi do eixo tecnológico informação e comunicação nos cursos de Desenvolvimento de Sistemas, Informática para Internet e Redes de Computadores. Exerceu o cargo de professora na Universidade Paranaense (UNIPAR) - campus Cianorte. Membro do Grupo de Pesquisa Tecnologia de Acesso a Dados - GPTAD (UNESP/ Tupã). Atua nas áreas da Ciência da Informação e da Ciência da Computação, com ênfase em Engenharia de Software, Bancos de Dados, Gestão de Projetos.

<https://orcid.org/0000-0003-3854-0654>

daiane.piccolo@unesp.br

Elaine Parra Affonso

Doutora em Ciência da Informação pela Universidade Estadual Paulista (UNESP/Marília) pelo Programa de Pós-Graduação em Ciência da Informação (PPGCI); Mestre em Ciência da Computação pela Fundação Eurípedes Soares da Rocha (UNIVEM/Marília). Possui Graduação em Tecnologia em Processamento de Dados pela Faculdade de Tecnologia de Ourinhos; Licenciatura em Informática pela Universidade Católica de Brasília (UCB/Brasília) e Especialista em Métodos Quantitativos Aplicados pela Faculdades Adamantinenses Integradas (FAI/Adamantina). É docente desde 2008 na Fatec Presidente Prudente nos cursos de Análise e Desenvolvimento de Sistemas e Gestão Empresarial. No período de 2018 a 2023 foi coordenadora do CST em Análise e Desenvolvimento de Sistemas e, atualmente é coordenadora do curso AMS em Análise e Desenvolvimento de Sistemas. Atua na área da Ciência da Informação e da Ciência da Computação, com ênfase em Sistemas de Informação, Gestão e Governança de Tecnologia da Informação, focada principalmente nos seguintes temas: Privacidade e Anonimização de dados.

<https://orcid.org/0000-0002-3953-462X>

melaine.affonso@fatec.sp.gov.br

Ricardo César Gonçalves Sant'Ana

Professor Associado da Universidade Estadual Paulista - UNESP, Faculdade de Ciências e Engenharias - FCE, Campus de Tupã, em regime de dedicação exclusiva. Professor do Programa de Pós-Graduação em Ciência da Informação da Universidade Estadual Paulista, Campus de Marília. Graduado em Matemática e Pedagogia, Mestrado em Ciência da Informação (2002), Doutorado em Ciência da Informação (2008) e Livre-Docente em Sistemas de Informações Gerenciais pela UNESP (2017). Possui especializações em Orientação à Objetos (1996) e Gestão de Sistemas de Informação (1998). Parecerista ad hoc de periódicos e de agências de fomento. Líder do Grupo de Pesquisa - Tecnologias de Acesso a Dados (GPTAD) e membro do Grupo de Pesquisa -

Novas Tecnologias em Informação GPNTI. Membro da Associação Nacional de Pesquisa e Pós-Graduação em Ciência da Informação - ANCIB. Tem experiência na área de Ciência da Computação, atualmente realiza pesquisas com foco em: ciência da informação e tecnologia da informação, investigando temas ligados ao Ciclo de Vida dos Dados, Transparência e ao Fluxo Informacional em Cadeias Produtivas. Foi Presidente da primeira composição da Comissão de Acompanhamento e Avaliação dos Cursos de Graduação - CAACG da UNESP, entre 2018 e 2020. Atuou como professor na Faccat Faculdade de Ciências Contábeis e Administração de Tupã, onde coordenou curso de Administração com Habilitação em Análise de Sistemas por dez anos e o curso de Licenciatura em Computação. Atuou no setor privado como consultor, integrador e pesquisador de novas tecnologias informacionais de 1988 a 2011.

<https://orcid.org/0000-0003-1387-4519>
ricardo.santana@unesp.br

Received: 2023-06-26

Accepted: 2024-01-24