DOI: 10.5433/1981-8920.2023v28n4p289

COOKIES COMO FORMA DE COLETA DE DADOS EM SITES E A INSCIÊNCIA DO USUÁRIO

COOKIES AS A WAY OF COLLECTING DATA ON WEBSITES AND USER UNCONSCIOUSNESS

Daiane Marcela Piccolo[a]
Elaine Parra Affonso[b]
Ricardo César Gonçalves Sant'Ana[c]

RESUMO
Objetivo: A opacidade na coleta de dados em *sites* pode afetar a privacidade dos usuários, pois, muitas vezes, as empresas coletam dados sem informar claramente quais informações estão sendo coletadas, como serão usadas e com quem serão compartilhadas. Isso pode levar à coleta excessiva de dados, o que pode ser usado para fins não autorizados. Nesse cenário, este artigo tem como objetivo identificar os possíveis *cookies* coletados pelos *sites*, a fim de demonstrar a opacidade presente na coleta desses dados, principalmente em relação a quantidade e diversidade de *cookies*, incluindo os terceiros envolvidos nesse processo. **Método:** A metodologia constitui de uma pesquisa descritiva e de abordagem qualitativa e quantitativa. Utilizou-se como métodos a pesquisa bibliográfica, a fim de explanar sobre os aspectos técnicos da coleta de dados por *cookies*; coleta de dados em sites, para demonstrar os possíveis *cookies* coletados pelos *sites* durante a interação com o usuário. Para a identificação dos *cookies*, foi utilizado como recurso tecnológico, a Plataforma de Gerenciamento de Consentimento *Cookiebot*. **Resultado:** Identificou-se um total de 776 *cookies* nos *sites* analisados, sendo os cookies da categoria de *marketing* e *cookies* do tipo persistente com maior representatividade, além de 208 empresas terceiras presentes nesses cookies. **Conclusões:** Observou-se uma diversidade de *cookies* que são utilizados pelos *sites* para coleta de dados e, essa quantidade de *cookies* pode revelar muita informação sobre atividades do usuário, consequentemente, ameaçar a privacidade dos indivíduos referenciados nesses dados, sem que esses tenham consciência sobre a coleta de dados.

Descritores: Coleta de dados. *Cookies*. Privacidade. Proteção de dados pessoais.

[a] Doutora em Ciência da Informação pela Universidade Estadual Paulista (UNESP). Docente na Faculdade de Tecnologia de Presidente Prudente (FATEC) e da Escola Tecnica Amim Jundi (ETEC), Osvaldo Cruz, Brasil. E-mail: daiane.piccolo@unesp.br

[b] Doutora em Ciência da Informação pela Universidade Estadual Paulista (UNESP). Docente na Faculdade de Tecnologia de Presidente Prudente (FATEC), Presidente Prudente, Brasil. E-mail: elainepff@gmail.com

[c] Doutor em Ciência da Informação pela Universidade Estadual Paulista (UNESP). Docente na Universidade Estadual Paulista (UNESP), Marília, Brasil. E-mail: ricardo.santana@unesp.br

1 INTRODUÇÃO

O consentimento na coleta de dados é um princípio fundamental da proteção de dados pessoais, ou seja, as empresas só podem coletar, armazenar ou usar dados pessoais com o consentimento explícito e informado do titular desses dados.

Para fins da Lei Geral de Proteção de Dados (LGPD) o consentimento deve ser livre, isto é, o titular dos dados deve ter a escolha de consentir ou não com a coleta e tratamento dos seus dados. Além disso, o consentimento deve ser específico, ou seja, as empresas devem informar claramente quais dados estão sendo coletados, para que finalidade e por quanto tempo esses dados serão armazenados e utilizados. O consentimento também deve ser informado, o que significa que o titular dos dados deve ter acesso a informações claras e compreensíveis sobre o tratamento de seus dados pessoais, incluindo informações sobre os responsáveis pelo tratamento, as finalidades do tratamento, a base legal para o tratamento, os direitos do titular dos dados e como exercê-los (Brasil, 2018).

É importante ressaltar que o consentimento não pode ser uma condição obrigatória para a prestação de um serviço, a menos que a coleta dos dados seja essencial para a execução desse serviço. Além disso, o consentimento pode ser revogado a qualquer momento pelo titular dos dados, e as empresas devem garantir que esse processo seja fácil e acessível.

Dessa forma, as empresas devem adotar práticas transparentes e responsáveis em relação ao tratamento de dados, garantindo que os titulares dos dados possam tomar decisões informadas sobre a coleta e uso de seus dados pessoais.

Nos sites, os avisos de consentimento para o uso de cookies é uma maneira de garantir o consentimento informado do usuário em relação a possível coleta de dados pessoais. Os cookies são pequenos arquivos de texto armazenados no computador do usuário quando ele acessa um site. Esses cookies podem coletar informações sobre a atividade do usuário na internet, como suas preferências de navegação e histórico de compras (Lin; Loui, 1998).

Segundo o Regulamento Geral de Proteção de Dados (GDPR) o consentimento na coleta de dados pessoais por meio de cookies deve apresentar um aviso de consentimento claro e compreensível aos usuários. Esse aviso deve informar sobre a coleta de dados pessoais por meio de cookies e dar ao usuário a escolha de aceitar ou recusar essa coleta.

Além disso, o aviso de consentimento de cookies deve informar claramente quais dados estão sendo coletados, para que finalidade e por quanto tempo esses dados serão armazenados e utilizados. Os usuários também devem ter a opção de gerenciar seus cookies e revogar seu consentimento a qualquer momento (European Data Protection Board, 2020).

Neste contexto, *sites* vêm adotando medidas para garantir a conformidade com os requisitos legais para obter consentimento do usuário na coleta de dados, que pode vir por meio de avisos de consentimento de *cookies* e políticas de privacidade dos *sites*, nos quais são recorrentes em serviços *online*, pois regulam o uso dos dados pessoais coletados, instituindo um compromisso com os usuários. No entanto, a forma como as políticas de privacidade vem disponibilizando informações em relação ao tratamento dos dados, pode ser complexo para o entendimento do usuário. Pois, percebe-se políticas de privacidade longas e complexas, e muitas vezes escritas em linguagem jurídica difícil de entender. Isso pode fazer com que os usuários não entendam completamente como suas informações pessoais serão usadas ou compartilhadas (Steinfeld, 2016).

Para Daoudagh *et al.* (2021), os avisos de consentimento de *cookies*, apesar de serem uma forma de fornecer aos usuários mais controle sobre a coleta de dados, muitos são vistos como inadequados e insuficientes para proteger a privacidade dos usuários. Muitos avisos são confusos e complexos, e muitos usuários acabam aceitando *cookies* sem saber realmente o que estão permitindo.

Neste contexto, este artigo tem como objetivo identificar os possíveis *cookies* coletados pelos *sites*, a fim de demonstrar a opacidade presente na coleta desses dados, principalmente em relação a quantidade e diversidade de *cookies*, incluindo os terceiros envolvidos nesse processo.

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

2 *COOKIES* E SUAS ESPECIFICIDADES

Existem diversas tecnologias para coletar e armazenar dados, dentre essas tecnologias, encontram-se os *cookies*. *Cookies* é um bloco de texto que é enviado por um navegador, armazenando dados e salvando preferências, com isso, em cada visita o *site* pode fornecer um serviço personalizado, pois a cada acesso o navegador se lembra do bloco de texto que é armazenado no disco rígido do usuário (Lin; Loui, 1998). Para Brain (2000), esse bloco de texto pode proporcionar uma melhor experiência ao usuário, por meio das informações que foram coletadas.

O termo *cookie* deriva de uma antiga gíria dos programadores, onde um programa solicita algo a um servidor e recebe de volta algo que provavelmente precise apresentar mais tarde para conseguir realizar alguma tarefa (Tanenbaum, 2003). Nesse contexto, o W3C define *cookie* como dados enviados por um servidor da *Web* para um cliente da *Web*, para serem armazenados localmente pelo cliente e enviados de volta ao servidor em solicitações subsequentes.

Os *cookies* foram inventados pelo Engenheiro de Software da Netscape, Lou Montulli, em junho de 1994, com o propósito específico de lembrar interesses do usuário, como o conteúdo do carrinho de compras da *Web* (Pierson; Heyman, 2011). Eles foram criados para estender uma limitação da tecnologia *Web*, pois as páginas da *Web* são apátridas, o que significa que elas não têm memória e não podem passar informações entre si, pois cada transição é distinta de outra, não apresentando uma memória para identificar alguém que está retornando no *site*.

Assim, os *cookies* acrescentaram memória ao protocolo *Hypertext Transfer Protocol* (HTTP), que é um protocolo de comunicação responsável pela

comunicação dos dados da *Web*. Dessa forma, o uso de *cookies* permitiu acrescentar estados ao protocolo HTTP durante a navegação do usuário, facilitando a navegação para os usuários nos acessos a *sites*, sem ter que realizar a identificação em toda visita, o que poupa tempo e pode usufruir de visitas mais personalizadas ao mesmo *site* futuramente (Hormozi, 2005).

A utilização das técnicas de *cookies* na Internet, para coleta e manipulação de perfis do usuário, procura atender as estratégias de *marketing* das corporações que financiam os provedores de serviços de tecnologias (Lin; Loui, 1998). Neste sentido, o uso dos *cookies* permitiu uma interação *online* mais rápida e fácil, ou seja, uma experiência mais personalizada de navegação nas redes (Salesforce, 2022), garantindo o armazenamento de dados, sem que se tenha de repetir ações de *login* ou refazer operações já realizadas.

Para Siebecker (2003), uma preocupação em relação aos *cookies* é a implantação e a coleta de informações pessoais, muitas vezes sem o consentimento do usuário. Essas informações pessoais permitem a construção de perfis detalhados do usuário, revelando padrões de acesso, preferências e características. E a maneira como o conhecimento das preferências pessoais e atividades privadas de um usuário podem ser usadas é outra preocupação.

Eichelberger (2011) ressalta que, a questão mais premente sobre *cookies*, é a preocupação com a privacidade do usuário, pois empresas *online* usam *cookies* para desenvolver perfis detalhados de usuários e seus hábitos de navegação por meio de dados coletados, podendo gerar um potencial abuso no uso desses dados.

Castells (2003, p. 139) enfatiza que “[...] a privacidade era protegida pelo anonimato da comunicação na Internet e pela dificuldade de investigar as origens e identificar o conteúdo de mensagens transmitidas com o uso de protocolos da Internet”. Entretanto, Magrani (2019) acredita que com o avanço das novas interfaces tecnológicas no mundo digital, maior o número de dispositivos conectados, e assim mais dados são produzidos e disponibilizados, apresentando um risco à privacidade, pois tudo o que fazemos na Internet deixa vestígios digitais, podendo afetar nossa privacidade (Grassegger; Krogerus, 2017).

Os defensores da privacidade na Internet se opõem aos *cookies* por vários motivos. No artigo *Taking the Byte Out of Cookies: Privacy, Consent, and the Web* de Lin e Loui (1998), os autores relatam sobre o uso moral e da imoralidade dos *cookies*. Por um lado, defendem o uso de *cookie* pelas organizações quando os *cookies* são usados para personalização de *sites* e sistemas de pedidos *online*, pois nesse caso, a finalidade é para "fazer bons negócios" na *Web*, no qual há benefícios tanto para o *site* quanto para o usuário. Reforçam ainda que, os *cookies* são apenas uma ferramenta que é usada para coletar informações pessoais, não resultando necessariamente em uma violação de privacidade.

> Quando o cliente vai com frequência a uma loja o vendedor passa a conhecer suas preferências e logo começa a ter um serviço personalizado, o cliente sai da loja com um nível de satisfação alto pensando em voltar devido ao atendimento que é oferecido naquela loja. Nesse caso, a coleta de informações realizadas por *cookies* nada mais faz do que imitar a memória do vendedor, um cliente repetido para a loja, implicitamente consentiu em fazer o vendedor lembrar de suas preferências (Li; Loui, 1998, p. 7, tradução e grifo nossos).

Por outro lado, os autores argumentam sobre a imoralidade dos *cookies* em relação a centralização de informações por parte da indústria de *marketing*:

> O uso de *cookies* pela indústria de *marketing*-alvo para rastrear nosso comportamento na Internet é uma tentativa de centralizar informações pessoais. Seu objetivo inicial na coleta de informações é a centralização das informações. Os profissionais de *marketing*-alvo desenvolveram uma técnica para nos rastrear por toda a Internet, adicionando *cookies* aos avisos de anúncios em páginas da *Web*. Tais usos de *cookies* não parecem se encaixar dentro de uma proposta razoável de privacidade na *Web* (Lin; Loui, 1998, p. 11, tradução e grifo nossos).

Os autores finalizam reforçando que “[...] o uso de *cookies* para rastrear usuários à medida que se movem de *site* para site é uma invasão antiética de privacidade. Tal uso viola nossa privacidade porque cria uma perda indesejável de anonimato e sigilo” (Lin; Loui, 1998, p. 18, tradução e grifo nossos).

Mayer-Schönberger (1998) no seu artigo *The Internet and Privacy Legislation: Cookies for a Treat?* expõe motivos pelos quais os *cookies* são uma invasão de nossa privacidade e suas amplas implicações legais internacionais. O *cookie* é armazenado no computador do usuário sem seu consentimento ou conhecimento, “[...] podendo divulgar informações pessoais de usuários da *Web* desavisados a uma taxa inimaginável, violando uma série de normas nacionais

e internacionais que foram projetadas para proteger dados pessoais" (Mayer-Schönberger, 1998, p. 167, tradução e grifo nossos).

Ainda, o autor reforça que mesmo que exista um regime de proteção de dados com foco na restrição de acesso e transparência do usuário, quase todos os recursos e aspectos do conceito de *cookies* podem ser usados para violar os princípios da Diretiva da EDPB, pois os *cookies* tornam possível o acesso involuntário e automático aos dados pessoais do usuário, como exemplo, "[...] um servidor da *Web* pode definir um cookie para que um número quase ilimitado de outros servidores tenha acesso às informações de *cookies* também" (Mayer-Schönberger, 1998, p. 168, tradução e grifo nossos).

No entanto, Cavalcanti (2021) vê que o risco na utilização de *cookies* se dá nos aspectos do nível de personalização que é gerada e com quais finalidades, além do rastreamento e aspecto que rompe todos os limites da privacidade. Para Odlyzko (2003) um fator que influencia a privacidade na Internet, está relacionado com falta de conhecimento, na maioria das vezes, sobre as práticas adotadas pelos *sites* sobre coleta dos *cookies*.

Freudiger, Vratonjic e Hubaux (2009) afirmam que por meio dos dados existentes nos *cookies* do computador do usuário, é possível extrair diversas informações, e assim as empresas conseguem ter um perfil mais personalizado do usuário, procurando oferecer produtos e ou promoções por meio dos dados coletados, no qual isso muitas vezes pode afetar a privacidade do usuário.

Neste contexto, para reorganizar as formas como os *sites* devem solicitar, coletar e armazenar consentimento de *cookies* para os titulares de dados, a LGPD e o GPDR juntamente com a Diretiva de Privacidade Eletrônica, desencadearam uma nova abordagem no âmbito da privacidade dos dados, o que determina uma mudança da política de *cookies.*

O processo de obter e armazenar dados é representado pelo Ciclo de Vida dos Dados (CVD). Sant´Ana (2016) ao abordar sobre o CVD ressalta que a fase de Coleta envolve ações de planejamento relacionado aos meios de como serão obtidos, filtrados e organizados os dados que estarão no fluxo, definindo-se a estrutura, formato e meios de descrição a ser utilizada. Na fase de armazenamento considera atividades relacionadas ao processamento,

transformação, inserção, migração, transmissão e toda e qualquer ação que vise à persistência dos dados em suporte digital. Todas as fases do CVD são permeadas por objetivos específicos, como: Privacidade, Integração, Direitos Autorais, Disseminação, Preservação e Qualidade (Sant'ana, 2016).

No ambiente *Web*, o processo de coleta de dados se inicia quando o usuário (Ciclo de Vida dos Dados do Usuário – CVD Usuário) solicita uma página ao servidor *Web* (Ciclo de Vida dos Dados do Detentor – CVD Detentor de Dados). A interação do usuário com esse *site* se efetua a partir dos dados que ele fornece de forma explícita e implicitamente. A partir dessa coleta, os dados são armazenados e coletados novamente no momento de um novo acesso. Essa dinâmica é comum nas solicitações de acesso a sites que registram o consentimento da coleta por meio de *cookies*. Esses *cookies* quando aceitos, podem ficar armazenados no computador do usuário por um longo período, assim, enquanto eles permanecerem esses continuam coletando dados

Para Affonso e Sant'Ana (2018) nesse cenário, onde o usuário é alvo de fases de coleta pelos detentores de dados, o usuário é insciente em relação a muitos dados coletados por essa atividade.

De acordo com as regulamentações, essas solicitações realizadas pelas empresas detentoras de dados, sob consentimento, devem ser transparentes e ser apresentadas de forma clara e concisa, utilizando uma linguagem de fácil compreensão, e que não induza o usuário a dar um consentimento ilegítimo.

Uma das mudanças mais notáveis determinadas na LGPD e no Regulamento Europeu para sites foi o aumento do número de avisos que solicita o consentimento do usuário para a coleta de dados. Geralmente essas notificações são apresentadas na forma de avisos de *cookies*, que informa o usuário sobre utilização de *cookies* como instrumento de coleta de dados.

Nesta pesquisa foi possível observar o comportamento de alguns *sites* a esse respeito. Empresas como Microsoft, Mercado Livre, Casas Bahia dentre outras, informam ao usuário sobre coleta de dados, por meio dos avisos de *cookies*.

Para Araújo e Araújo (2020), "o informar" é uma das etapas mais importantes do processo de conformidade, uma vez que é por meio da

informação que o usuário poderá ter insumos para eliminar toda e qualquer condicionante do seu consentimento e fornecê-lo de modo claro e livre.

É perceptível que o consentimento implícito é uma prática que infringe o princípio da transparência, sendo que o usuário deixa de participar ativamente da decisão de aceitar ou não *cookies* em seu dispositivo (Zanfir-Fortuna, 2013), por exemplo, os *cookies walls.*

Os *cookies walls*, ou parede de cookie, é uma forma dos *sites* negarem o acesso dos usuários se eles não consentirem com todos os *cookies* e rastreadores presentes neste *site.* Para Magrani (2019), os *cookies walls* é uma espécie de barreira que coloca o usuário em uma situação de "pegar ou largar", em que ele deve optar por *cookies* de *marketing* e tecnologia de rastreamento semelhante ou ter o acesso totalmente negado ao *site* e seus serviços.

No entanto, as diretrizes do Conselho Europeu de Proteção de Dados, sobre o consentimento válido de maio de 2020, excluem os *cookies walls* como uma forma válida dos *sites* obterem o consentimento do usuário para o processamento de dados pessoais e o uso de *cookies.*

2.1 CLASSIFICAÇÃO DOS *COOKIES*

Os *sites* podem utilizar diversos tipos de *cookies*, sendo comum encontrar nas respectivas políticas vários tipos de *cookies* elencados e as mais diferentes classificações. Para se classificar os *cookies* deve-se considerar o seu objetivo, a sua proveniência e o seu tempo de duração (*The Cookie Collective*, 2019).

Segundo Cahn *et al*. (2016), existem dois tipos de *cookies*, os *First Party* e os *Third Party*. Os *First Party Cookies* são *cookies* colocados pelo domínio mostrado na barra de endereço no navegador, e são normalmente utilizados em aplicações de comércio eletrônico, permitindo, por exemplo, a persistência do carrinho de compras. Os *Third Party Cookies* são *cookies* colocados por um domínio que é diferente do que é mostrado na barra de endereço do navegador, são rotineiramente implantados por anunciantes *online* e aplicações de rastreamento, por exemplo, a Google Analytics e usa para monitorar e rastrear o comportamento *online*, pesquisas e *sites* visitados. São colocados em milhares de *sites* que pertencem à rede de publicidade com a finalidade de exibir

publicidade "relevante" (Laudon; Traver, 2019). Estes dois tipos de *cookies* dividem-se em duas subcategorias: *cookies* de sessão e *cookies* de persistência (Wojtowicz, 2013).

Wojtowicz (2013) classifica os *cookies*, de acordo com sua finalidade, como família de *cookies* de navegador, no qual a primeira família listada pelo autor é a dos *cookies* técnicos, sendo subdivididos entre *cookie* de sessão e *cookie* persistente, nos quais destinam-se ao correto funcionamento de uma página na Internet. Segundo o autor, o cookie de sessão se desfaz cada vez que o navegador é fechado, ou seja, permanecem no computador do cliente somente enquanto ele está visitando o site da *Web*, um exemplo são os cookies em sistemas de *login* nos quais você não clicou em “lembrar de mim” (Rohr, 2010). Já o *cookie* persistente é utilizado para autenticar, rastrear e memorizar as informações sobre a sessão do navegador do usuário, permanecendo até a data programada para expirar, podendo durar meses ou até mesmo anos, pois são armazenados em um arquivo de texto no computador do cliente (Gonçalves, 2007).

Os *cookies* de sessão são *cookies* temporários que só são armazenados no dispositivo de um usuário durante sua permanência em um determinado *site*, sua sessão. Normalmente, eles são usados para funções como manter os itens em seu carrinho de compras (*Cookiebot*, 2022).

Para Grande (2006), na *Web*, uma sessão pode ser considerada como o período em que ocorre uma transação entre o usuário e um *site*, e os *cookies* são utilizados para identificá-la e determinar sua existência, e esses *cookies* delimitam sessões de navegação, as quais são essenciais para existência de certos serviços *Web*. Por outro lado, os *cookies* persistentes, de acordo com os autores, um *cookie* persistente é um tipo de *cookie* que é armazenado no dispositivo do usuário por um período mais longo do que os *cookies* de sessão. Ao contrário dos cookies de sessão, os cookies persistentes não são excluídos automaticamente quando a sessão do usuário termina ou quando o navegador é fechado.

Os *cookies* persistentes são usados para lembrar as preferências do usuário e fornecer uma experiência personalizada em um *site*, como lembrar o

nome de usuário e senha de *login*, lembrar o idioma preferido do usuário ou lembrar o histórico de compras do usuário. Eles também são usados para rastrear a atividade do usuário em diferentes sessões e em diferentes *sites*, permitindo que os anunciantes e os proprietários de sites analisem e melhorem a experiência do usuário.

Os *cookies* persistentes têm um prazo de validade definido pelo *site* que os cria, podendo durar dias, semanas, meses ou até anos. Os usuários podem excluir os *cookies* persistentes manualmente a qualquer momento nas configurações do navegador.

Muitas vezes, os *cookies* persistentes, são "*cookies* necessários" e "*cookies* de preferência" que lidam com itens como *login* do usuário ou configurações de idioma em um *site*, mas também podem ser "*cookies* analíticos", "*cookies* de publicidade" e "cookies de mídia social" que permitem ações como perfis pessoais e *marketing online* direcionado (*Cookiebot*, 2022).

Para Araújo (2003), os *cookies* persistentes é um tipo de *cookie* que armazena conjunto de dados para uso posterior ou como forma de personalizar serviços, direcionando-os conforme o perfil de cada usuário. Esses *cookies* só deveriam armazenar informações básicas dos usuários, no entanto, em consequência dos diversos serviços oferecidos pelos provedores, eles acabam armazenando informações de grande importância, tanto para usuário como para as empresas (Palmer, 2008).

Segundo Cavalcanti (2021), os *cookies* permanentes estabelecem ações como “*Expire*” e “*Max-Age*”, ou seja, possuem datas de validade e duração, permitindo acesso contínuo do navegador ou mesmo de terceiros, além de alguns *sites* utilizarem os *cookies* de persistência de forma bastante avançada, armazenando informações muitas vezes não fornecidas diretamente pelo usuário, mas após análise do seu comportamento durante a navegação, independente da atividade do usuário no momento da captação dos dados (Toubiana; Narayanan; Boneh, 2010).

Hoofnagle *et al*. (2012, p. 276, tradução nossa) destacam que os *cookies* de terceiros “[...] podem ser próprios, ou seja, gerenciados pelo respectivo *site* que o usuário acessa. Podem ainda ser de terceiros, quando gerenciados por

um *site* diferente do acessado". Nesse contexto, os autores explicam que ao acessar o "*site* A", o sujeito pode interagir com *cookies* de navegador do mesmo *site*, mas também do "*site* B", do "*site* C" e por aí em diante, pois os *cookies* de terceiro fornecem os padrões de navegação dos usuários a empresas ou sujeitos que não guardam relação com seu acesso.

Para Queiroz (2011), os *cookies* de terceiros se originam de relacionamentos entre diversos domínios e serviços oferecidos entre eles, ou seja, são *sites* que mantêm relação comercial com o *site* utilizado pelo usuário. A maior parte destes *cookies* são gerenciados por corporações especializadas em *marketing* digital, publicidade ou grandes bancos de dados privados de usuários. São utilizados pelos *sites* acessados como fonte para propagandas ou buscas direcionadas (Avelino, 2019).

Os *cookies* de terceiros podem ser pertencentes a uma plataforma de mídia social, que rastreiam e monitoram o comportamento dos usuários em um *site*, seu acesso habilitado, por exemplo, pela implementação de um "botão de compartilhamento" ou um "comentário" no *site* principal local na rede Internet (*Cookiebot*, 2022).

A lei sobre *cookies* exige que os usuários devem receber informações sobre o uso de *cookies* para poderem consentir ou reter o consentimento. Mesmo que não haja requisitos específicos de como esta informação deve ser dada, existe um acordo de que diferentes tipos de *cookies* podem ser classificados em grupos, de acordo com sua finalidade. Assim, para estar em conformidade com o GDPR, plataformas de gerenciamentos categorizam os *cookies* conforme seu objetivo. A *Cookiebot* (2022) categoriza os *cookies* de acordo com quatro objetivos: necessário, preferência, estatístico e *marketing*.

Os *cookies* necessários são, na maioria das vezes, do próprio *site* (originais) e importantes para serem ativados o tempo todo para que seu domínio funcione corretamente. Na maioria das vezes, são *cookies* de sessão que duram apenas o tempo da visita do usuário ao seu *site*. Apenas os *cookies* estritamente necessários podem ser incluídos na lista para serem isentos do consentimento de *cookies* do GDPR (*Cookiebot*, 2022), no entanto, é importante dar aos usuários a oportunidade de entender esses *cookies* e as razões pelas quais eles

são usados.

Esse tipo de *cookie* é fundamental para o funcionamento do *site*, pois permitem que o usuário navegue por meio do *site*, deixando o *site* acessível às várias funcionalidades sem intercorrências, proporcionando a operacionalização de funções básicas como a navegação na página e o acesso a suas áreas seguras (*International Chamber Of Commerce*, 2012). Portanto, sem eles é praticamente impossível efetuar tarefas básicas, por exemplo, ter uma cesta de compras num *site* de comércio eletrônico, ou manter os requisitos mínimos de segurança do *site* (*The Cookie Collective*, 2019).

Os *cookies* estritamente necessários geralmente são usados para armazenar um identificador exclusivo para gerenciar e identificar o usuário como exclusivo para outros usuários que atualmente visualizaram o *site*, a fim de fornecer um serviço consistente e preciso ao usuário.

O *International Chamber of Commerce* (2012) reforça ainda que esses *cookies* não serão usados para coletar informações que possam ser usadas para comercialização ao usuário e nem para lembrar as preferências do cliente.

Os *cookies* de preferência, também conhecidos como "*cookies* de funcionalidade", é um tipo de *cookie* que registra as preferências do usuário, ou seja, lembram as escolhas do usuário, como configurações de idioma ou moeda. Com esses *cookies* é possível que um *site* "lembre" ao usuário, ao retornar no *site*, as preferências em um próximo acesso, tornando-o mais funcional e prático de usar (*Cookiebot*, 2022), pois com base nas informações coletadas é possível fornecer recursos mais personalizados e permitir ao usuário não repetir as suas preferências a cada acesso (*International Chamber Of Commerce*, 2012).

Os *cookies* estatísticos geralmente vêm de serviços de terceiros, por exemplo, *software* de análise que é implementado no *site*. Esses *cookies* coletam informações sobre como os visitantes usam um *site*, por exemplo, para quais páginas os visitantes vão com mais frequência e se recebem mensagens de erro de páginas da *Web*. Esses *cookies* não coletam informações que identificam um visitante, pois todas as informações coletadas por esses *cookies* são agregadas e, portanto, anônimas. Assim, o único objetivo do *cookie* é captar os dados estritamente necessários para a análise e a partir daí utilizar para

otimizar as funções do *site*.

Análises da *Web* que usam *cookies* para coletar dados para melhorar o desempenho de um *site* se enquadram nessa categoria.

Os *cookies* de *marketing* quase sempre vêm de empresas terceirizadas de tecnologia ou publicidade com a finalidade de servir anúncios aos seus usuários ou coletar dados pessoais para fins de *marketing* futuros (*Cookiebot*, 2022). Esses *cookies* são usados para fornecer anúncios mais relevantes para usuários e seus interesses. Eles também são usados para limitar o número de vezes que o usuário vê um anúncio, bem como ajudar a medir a eficácia das campanhas publicitárias. Geralmente os *cookies* de *marketing* são colocados por redes de publicidade com a permissão do operador do *site* (*International Chamber Of Commerce*, 2022).

3 METODOLOGIA

Esta pesquisa é de caráter descritivo, com abordagem qualitativa e quantitativa. Os procedimentos metodológicos, e técnicas de coleta e análise de dados foram definidos conforme o atendimento do objetivo. Assim, este trabalho utiliza os métodos descritos a seguir.

a) **Pesquisa bibliográfica**: Utilizou-se da pesquisa bibliográfica, para explanar sobre os “Aspectos envolvidos no consentimento na coleta de dados em *sites”* e a “Caracterização da coleta de dados por meio de *cookies*”.

b) **Coleta de dados em *sites*:** Para demonstrar os possíveis *cookies* coletados pelos *sites* durante a interação com o usuário, principalmente no consentimento na coleta de dados, foi realizada uma pesquisa nos *sites* estudados neste trabalho.

Para a identificação dos *cookies*, foi utilizado como recurso tecnológico, a Plataforma de Gerenciamento de Consentimento *Cookiebot*[1]. Essa plataforma é líder mundial em conformidade com as principais leis e regulamentos de privacidade de dados como a LGPD do Brasil e o GDPR da União Europeia,

[1] Cf. https://www.cookiebot.com

mantido pela *Usercentrics*[2], no qual detecta e controla *cookies* de *sites*. O *Cookiebot* oferece a versão paga por prazo indeterminado e a versão livre por 30 dias. Para esta pesquisa utilizou-se a versão gratuita e foi realizada no mês de abril de 2022.

Inicialmente foram inseridos na ferramenta de pesquisa do *Cookiebot* os endereços dos *sites* de *e-commerce* presentes na lista dos *sites* mais acessados em março de 2022, segundo o relatório de ranqueamento disponibilizado pelo *site E-commerce* Brasil[3]. O relatório com o resultado da coleta foi disponibilizado em formato PDF por *site*, direto no e-mail cadastrado. Como o relatório não estava estruturado, o resultado foi tabulado em planilha de *Excel* e foi representado por meio de quadros para análise dos atributos de *cookies* identificados na coleta.

Em um primeiro momento foi realizada a análise geral da identificação dos *cookies* presentes nos *sites*, e na sequência, a correlação dos dados que foram identificados pela ferramenta Cookiebot e a informação disponibilizada pelos *sites* a respeito da coleta de dados por meio de suas políticas de privacidade e das práticas adotadas pelos *sites*.

4 RESULTADOS

Na interação entre usuário e *site*, ocorre a coleta de dados que na maioria das vezes, as entrelinhas desse processo se tornam opacas para o usuário. Neste contexto, essa seção apresenta a coleta dos *cookies* utilizados pelos *sites* durante essa interação com o usuário, evidenciando a opacidade presente na coleta desses dados, principalmente em relação a quantidade e diversidade de *cookies*, incluindo os terceiros envolvidos nesse processo. Para identificação dos *cookies*, foi utilizada a Plataforma de Gerenciamento de Consentimento *Cookiebot*.

A interação com a ferramenta consistiu na digitação do nome do *site* no campo de busca da ferramenta. Esse processo resultou em relatórios não

[2] Cf. https://usercentrics.com/br/

[3] Cf. https://www.ecommercebrasil.com.br/.

estruturados, dessa forma, o resultado foi tabulado e organizados em três grupos:

a) “Empresa”, que indica o *site* pesquisado;
b) “Resultado da busca”, que apresenta os campos: “Localização do servidor”, que é o local do processamento dos dados; “Total de *cookies*”, informa a quantidade de *cookies* encontrados pela ferramenta e a coluna “*Cookies* não classificados”, que são os *cookies* não reconhecidos pela ferramenta. Por norma, quando a ferramenta do *Cookiebot* não reconhece um *cookie*, classifica-o como desconhecido, que quer dizer que este é unicamente utilizado pela empresa proprietária do *site*, tendo sido criado pela mesma empresa, ou criado por uma empresa terceira, para fins específicos.
c) “Categorias dos *cookies*”, no qual classifica os tipos de cookies encontrados nos *sites*.

O Quadro 1 apresenta a categorização do resultado da coleta.

Quadro 1 - Categorização dos *cookies* identificados nos *sites*[*]

Empresa	Resultado da busca			Categoria do *cookie*			
	Localização do servidor	**Total de *cookies***	***Cookies* não classificados**	**Necessários**	**Estatísticos**	***Marketing***	**Preferência**
Mercado Livre	Reino Unido	37	16	4	7	10	N/A
Americanas	Irlanda	12	12	N/I	N/I	N/I	N/I
Amazon Brasil	Reino Unido	70	13	4	3	50	N/A
Shopee	Singapura	50	28	6	7	9	N/A
Magazine Luiza	Reino Unido	129	29	5	19	76	N/A
Aliexpress	Reino Unido	158	49	11	12	85	1
Microsoft	Irlanda	77	10	14	15	35	3
Casas Bahia	Irlanda	2	1	1	N/A	N/A	N/A
Netshoes	Reino Unido	167	55	10	22	78	2
Amazon	Irlanda	74	2	4	3	65	N/A

Fonte: Elaborado pelos autores.

[*] N/I: não identificado; N/A: não apresenta

Os dados apresentados no Quadro 1 foram extraídos dos relatórios referentes à coleta de *cookies* nos *sites*. O *site* Americanas, houve um total de 12 cookies identificados, porém, não foram classificados pela ferramenta. Dessa forma, nas colunas de categorias usou-se o termo “não identificado (N/I)”. O termo “não apresenta (N/A)”, foi utilizado para as categorias, nas quais não teve *cookies* presentes.

No resultado da busca foram identificados três países, Reino Unido, Irlanda e Singapura, no qual o Reino Unido se sobressai, sendo responsável por cinco países para processamento dos dados. Esse país possui uma lei específica de proteção de dados pessoais, *Data Protection Act* 2018, contendo disposições que complementam o GDPR e implementa a Diretiva de Aplicação da Lei na EU, definindo regras sobre processamento de dados pessoais.

O país também possui o Regulamento de Privacidade e Comunicações Eletrônicas do Reino Unido, *The Privacy and Electronic Communications (EC Directive) Regulations 2003*, que apresenta notificação sobre coleta e consentimento para coleta de dados. É importante ressaltar que não é explícito o termo *cookies* no regulamento (United Kingdom, 2003).

Outro país que foi identificado pela ferramenta foi a Irlanda, que possui a *Data Protection Act* 2018, no qual aborda a proteção de dados por *design* e por *default* e consentimento do titular para processamento de dados pessoais. Não é evidente o termo *cookie* (Ireland, 2018).

O terceiro país identificado foi Singapura, que é regulamentado pela Lei de Proteção de Dados Pessoais de 2012, essa lei abarca além da proteção de dados pessoais, a transferência de dados pessoais internacionalmente para processamento. O uso de consentimento é mencionado na legislação, no entanto, não é explícito regras para o uso de *cookies* (Singapore, 2022).

Esses países foram identificados como principais países para processamento dos dados, porém, em uma análise mais específica dos *cookies* coletados, outros países aparecem recebendo determinados *cookies*. Por exemplo, o *site* do *Aliexpress*, além do Reino Unido, outros servidores foram encontrados, tais como: Rússia, China, Singapura, Irlanda, França. Esses servidores nesses países recebem *cookies* específicos, como é o caso do *cookie*

"uid", esse *cookie* foi classificado como *cookie* de *marketing*, e pertence ao domínio criteo.com, que é uma empresa global de tecnologia voltada para atividades de *marketing* localizada em diversos países, inclusive na França.

Essa é uma informação desconhecida para os usuários, ou seja, o usuário não tem ciência do tamanho da transição que é realizada a partir da coleta de dados, pois é uma informação que não é disponibilizada nas políticas de privacidade.

Foram identificados um total de 776 *cookies* nos *sites* analisados, essa quantidade de *cookies* pode revelar muita informação sobre atividades do usuário e, consequentemente, ameaçar a privacidade dos indivíduos referenciados nesses dados, sem que esses tenham consciência sobre a coleta de dados.

Observa-se no Quadro 1, que o Netshoes foi o *site* com maior número de *cookies* identificados, representando 21%. Desses *cookies* identificados, 55 não foram classificados pela ferramenta, ou seja, não foi possível definir a finalidade ou o objetivo desses *cookies*.

Na sequência destaca-se o *site* Aliexpress representando 20% dos *cookies* coletados e em seguida vem o *site* Microsoft com 17%. A quantidade expressiva de *cookies* presentes nos *sites* da Netshoes e do Aliexpress, pode estar relacionado com a quantidade elevada de empresas terceiras existentes nos *sites*.

Foram identificados 208 domínios únicos de empresas terceiras presentes nos *sites*. Dentre esses domínios aparecem empresas como *Facebook*, *Google*, 360yield e *Doubleclick*, esta última com maior representatividade nos *sites*.

O domínio doubleclick.net está presente em oito *sites* analisados, se sobressaindo, até mesmo, em número de vezes presentes em cada *site* com *cookies* diferentes. A *Doubleclick* é uma empresa de publicidade usada pela maioria dos portais da Internet. O objetivo dos *cookies* no contexto da Doubleclick é "[...] direcionar publicidade de acordo com as preferências do usuário" (Google, 2013, local. 1), e para isso, é inserido um *cookie* no computador do usuário no momento do acesso a um *site* que tem a empresa Doubleclick como parceira. Esse *cookie* vincula o computador do usuário ao

servidor Doubleclick no qual envia a publicidade.

Para os defensores da privacidade na Internet essa ação é uma invasão do direito à privacidade, "[...] é um tipo de monitoramento eletrônico independentemente de como o direito à privacidade é concebido." (Charters, 2002, p. 3, tradução nossa).

Essa prática adotada pela Doubleclick e por outras empresas não é recente, gerando preocupações relacionadas à privacidade desde 1999, quando o Electronic Privacy Information Center (EPIC) demonstrou preocupações sobre as práticas adotadas pela empresa em relação à violação de privacidade em ambiente *online*.

Mesmo a EPIC apresentando queixa à Federal Trade Commission (FTC), alegando violações de privacidade, os autores Dhillon, Oliveira e Syed (2018) relatam que desde 1999 não mudou muito as questões de privacidade no cenário das empresas de comércio eletrônico, pois essas empresas não tomaram nenhuma medida concreta para entender as preocupações sobre privacidade ou para garantir a proteção adequada dos dados de usuários.

Essa ação de coleta de dados não é exclusiva da Doubleckick, percebe-se nos resultados desta pesquisa, representados no Quadro 1, a quantidade *cookies* e empresas terceiras presentes nos *sites*, onde a ação de coleta de dados pode ocorrer a cada acesso no ambiente, armazenado dados de sessão, dados de *login*, fornecendo recursos de personalização, no entanto, eles também podem ser usados para rastrear a atividade de um usuário (McKinkey, 2008), sem mesmo ele ter conhecimento desse processo, pois "[...] os usuários podem ter uma compreensão limitada do que precisam proteger e como essa proteção pode ser obtida" (Dhillon; Oliveira; Syed, 2018, p. 9, tradução nossa).

Mediante o uso de *cookies* pelos *sites*, é possível armazenar dados para serem usados em diferentes finalidades, como para análises estatísticas, para personalização de perfil, sendo que cada *cookie* armazenado pode pertencer a um tipo de categoria. No Quadro 1 é possível verificar essas categorias e a distribuição dos *cookies*.

Observa-se, no Quadro 1, a grande presença dos *cookies* de *marketing*, representando 73% dos *cookies* identificados. No total foram 408 de *marketing*,

contra 88 *cookies* estatísticos, 50 necessários e 6 de preferência.

Os *cookies* de *marketing* podem ser estabelecidos pelo próprio *site* como também por empresas terceiras para construir um perfil sobre os interesses do usuário para serem enviadas propagandas até mesmo de outro site. Alguns *sites* explicam que caso o usuário não permita estes *cookies*, terá menos propaganda direcionada, porém, observou-se que a maioria dos *sites* não disponibilizam esse recurso de personalização de *cookies*, o que força o usuário permanecer com as configurações do *site*.

Percebe-se que o Aliexpress é o *site* que mais possui *cookies* de *marketing*, esses *cookies* foram inseridos no *site* do Aliexpress por 26 empresas diferentes com servidores em diversos países.

O *cookie* tradicional é um *cookie* HTTP, mas outros tipos de *cookies* foram surgindo e adotados pelos *sites*, possuindo as mesmas características de coleta de dados de usuários. Nessa pesquisa foi possível identificar que dos 776 *cookies*, 74% são *cookies* HTTP, enquanto 17% foram identificados com *cookies* HTML e 9% *cookies* do tipo Pixel.

Os *cookies* HTML são os que vão no corpo do documento principal do código, ao invés de ser carregados dentro de uma linha de código específico, ele normalmente é usado para disparar avisos de *cookies* nas páginas e mostrar propagandas em tempo real, dessa forma, captando dados sobre preferências e comportamento do usuário em diferentes *sites*, por meio das propagandas enviadas aos usuários. Ao clicar nesses anúncios o usuário é levado a outro *site* que também pode ter ações de captura de dados por meio dos *cookies*. Esse tipo de *cookie* foi encontrado nos *sites* Mercado Livre, Amazon, Shoppe, Magazine Luiza, Microsoft e Netshoes, podendo ser vistos em categorias diferentes e fornecidos por domínios distintos.

Os *cookies* do tipo *Pixel* normalmente vêm no formato de uma imagem invisível, e é colocado, por exemplo, no cabeçalho de um e-mail ou no início da mensagem. Os *cookies* Pixel são capazes de captar diversas informações tais como: quantidade de acesso a determinada página, data e hora dessa ação, dispositivo usado e localização geográfica. O *site* Aliexpress foi o que mais apresentou esse tipo de *cookie*. Da mesma forma dos *cookies* HTML, esses

cookies podem vir de domínios e categorias diferentes, porém apresentam a mesma finalidade.

Os *cookies,* uma vez inseridos no computador do usuário, podem permanecer por longa data ou até o usuário excluí-lo do computador. Essa característica refere-se aos *cookies* persistentes. Verificou-se nesta pesquisa, que a quantidade de *cookies* persistentes sobressaiu em relação aos *cookies* de sessão.

Dos 776 *cookies* identificados, 538 foram *cookies* persistentes, ou seja 69,32%. Esse tipo de *cookie* pode permanecer no disco rígido do usuário por anos, pois para ser apagado vai depender da data de expiração do *cookie*.

Para Gonzalez (2018), esse tipo de *cookie* aumenta os riscos à privacidade em relação aos *cookies* de sessão, pois podem ser usados pelos anunciantes para registrar informações sobre os hábitos de navegação de um usuário por um longo período.

Os *cookies* persistentes apresentam uma quantidade elevada em relação aos *cookies* de sessão. Os *sites* com maior índice desse tipo de *cookie* é o Netshoes e Aliexpress. Ressalta-se que os *cookies* persistentes podem ser do próprio *site*, ou muitas vezes, de empresas terceiras, por exemplo o *site* da Netshoes, dos 147 *cookies* persistentes, 55 são de domínios de terceiros, ou seja, 37,41%. Em relação aos cookies de terceiros, uma opção para minimizar ameaças a privacidade é o usuário configurar as opções do navegador referentes a privacidade/segurança, bloqueando cookies de terceiros, ou ainda, quando no aviso de consentimento do site existe a opção de configuração de cookies, o usuário deverá configurar para não permitir o uso de cookies de terceiros.

5 CONSIDERAÇÕES FINAIS

Por meio da identificação de *cookies*, realizada pela ferramenta Cookiebot, foi possível identificar as especificidades dos *cookies* quando há a interação com o usuário. Percebe-se uma diversidade de *cookies* que são utilizados pelos *sites* para coleta de dados. Esses *cookies* possuem características que muitas vezes são opacas para o usuário. Por exemplo, a

quantidade de *cookies* presentes no *site* com finalidades distintas, nos quais coletam dados no intuito de personalizar o perfil do usuário. Além, da existência do compartilhamento dos dados com terceiros, pois notou-se uma expressiva presença desses tipos de *cookies* sendo enviados para diversos países.

Outro ponto importante identificado, nesse resultado, foi a classificação dos *cookies* pertencendo a categorias distintas. Categorias essas, que as leis e regulamentos de proteção de dados, impõe clareza, pois o usuário tem direito de escolha sobre a coleta de dados ao fornecer o consentimento. Percebe-se situações como caixas de seleção pré-marcadas, falta de opções de gerenciamento de *cookies* para que o usuário tenha o direito do controle de seus dados.

Outra característica que pode refletir no controle dos dados, por parte do usuário, é o armazenamento dos *cookies* com tempo de expiração considerado eterno. Esses *cookies* foram encontrados em diversos *sites*, com tempo de expiração em torno de 60 anos, ou seja, mesmo que o usuário finalize a sessão, estes *cookies* continuam alojados no computador do usuário coletando dados toda vez que o usuário acessar o *site* novamente.

Por meio dessa coleta, foi possível verificar que muitas dessas informações não estão acessíveis aos usuários. Pois, o que se tem são políticas de privacidade rasas ao disponibilizar informação sobre a coleta de dados ao indicar os possíveis dados que o *site* terá acesso, quais tipos e usos desses dados. Além de não deixar explícita a indicação do potencial destinatário e os dados coletados por cada serviço oferecido ao usuário.

Assim, a opacidade no processo de coleta de dados por cookies pode resultar na falta de conscientização por parte do usuário sobre o que está sendo coletado e como está sendo usado, pois muitos usuários podem não estar cientes de que suas informações estão sendo coletadas, como elas estão sendo usadas e com quem estão sendo compartilhadas. Isso pode levar a uma sensação de falta de controle sobre seus dados pessoais.

REFERÊNCIAS

AFFONSO, E. P.; SANT'ANA, R. C. G.. Privacy awareness issues in user data collection by digital libraries. **IFLA journal**, v. 44, n. 3, p. 170-182, 2018.

ARAÚJO, I.; ARAÚJO, I. Developing trust in internet commerce. *In:* CASCON '03: 2003 CONFERENCE OF THE CENTRE FOR ADVANCED STUDIES ON COLLABORATIVE RESEARCH, 2003, Toronto. **Proceedings** […] ACM, Oct. 2003. p. 1-15.

ARAÚJO, X. W. A. **O uso dos cookies à luz do regulamento geral de proteção de dados: uma análise da conformidade**. 2020. Dissertação (Mestrado em Direito e Gestão) – Universidade Nova de Lisboa, Lisboa, 2020. Disponível em: https://run.unl.pt/bitstream/10362/132676/1/Ara%C3%BAjo_2020.pdf. Acesso em: 10 mar. 2023.

AVELINO, S. R. A evolução dos mecanismos de rastreamento e vigilância instrusivos em clientes web. *In:* SIMPÓSIO INTERNACIONAL LAVITS, 6., 2019, Salvador. **Anais** [...], Salvador: [*s. n*.], 2019. Disponível em: https://lavits.org/wp-content/uploads/2019/12/SilvaAvelino-LAVITISS-2019.pdf. Acesso em: 10 jul. 2021.

BRAIN, M. **How internet cookies work**. [*S. l.*], 2000. Disponível em: http://computer.howstuffworks.com/cookie.htm. Acesso em: 31 jan. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art1. Acesso em: 10 jul. 2022.

CAHN, A.; ALFELD, S.; BARFORD, P.; MUTHUKRISHNAN, S. An empirical study of web cookies. *In*: INTERNATIONAL WORLD WIDE WEB CONFERENCE, 25., 2016, Montreal. **Proceedings** [...]. New York: ACM, 2016. p. 891-901. DOI https://doi.org/10.1145/2872427.2882991

CASTELLS, M. **A galáxia da internet**: reflexões sobre internet, os negócios e a sociedade. Rio de Janeiro. Editora: Zahar, 2003.

CAVALCANTI, M. F. Cookies para quem? Entre o escambo digital e os direitos à privacidade e proteção de dados. **Revista Acadêmica da Faculdade de Direito do Recife**, Recife, v. 93, n. 2, p. 96-115, out. 2021. Disponível em: https://periodicos.ufpe.br/revistas/ACADEMICA/article/view/249887. Acesso em: 10 mar. 2023.

COOKIEBOT. [*S. l.*], 2022. Disponível em: https://www.cookiebot.com/. Acesso em: 10 jul. 2022.

DAOUDAGH, S.; MARCHETTI, E.; SAVARINO, V.; BERNABE, J. B.; MARTINEZ, J.A.; GARCÍA-RODRÍGUEZ, J.; MORENO, R. T.; MARTINEZS, J. A.; SKARMETA, A. F. Data Protection by Design in the Context of Smart Cities: A Consent and Access Control Proposal. **Sensors**, [*S. l.*], v. 21, n. 21, 7154, 2021.

DHILLON, G.; OLIVEIRA, T.; SYED, R. Value-based information privacy objectives for Internet Commerce. **Computers in Human Behavior**, [*s. l.*], v. 87, p. 292-307, 2018. DOI 10.1016/j.chb.2018.05.043

EICHELBERGER, L. **The cookie controversy**. Introduction. [*S. l.*], 2011. Disponível em: http://www.cookiecentral.com/ccstory/. Acesso em: 17 jul. 2021.

EUROPEAN DATA PROTECTION BOARD. **Guidelines 05/2020 on consent under Regulation 2016/679**. Version 1.1. [*S. l.*]: EDPB, 2020. Disponível em: https://edpb.europa.eu/sites/default/files/files/file1/edpb_guidelines_202005_consent_en.pdf. Acesso em: 17 mar. 2023.

FREUDIGER, J.; VRATONJIC, N.; HUBAUX, J. Towards Privacy-Friendly Online Advertising. *In:* IEEE WEB 2.0 SECURITY AND PRIVACY (W2SP), 2009, Oakland. **Proceedings** [...]. Oakland: IEEE, 2009. Disponível em: https://citeseerx.ist.psu.edu/viewdoc/download?doi=10.1.1.296.9525&rep=rep1&type=pdf. Acesso em: 10 jul. 2021.

GONÇALVES, E. **Desenvolvendo aplicações Web com JSP Servelets, Java Server Faces, Hibernate, EJB3 Persistence e Ajax**. Rio de Janeiro: Ciência Moderna, 2007.

GONZÁLEZ, V. Las Cookies y el cumplimiento de la Ley Orgánica de Protección de Datos: Opinión. **Advertising and Marketing Weekly**, n. 1568, 2018.

GOOGLE. **DoubleClick Digital Marketing platform**. [*S. l.*], Jan. 2013. Disponível em: https://www.thinkwithgoogle.com/intl/en-apac/marketing-strategies/automation/doubleclick-digital-marketing-platform/. Acesso em: 10 mar. 2022.

GRANDE, R. E. de. **Sistema de Integração de técnicas de proteção de privacidade que permitem personalização**. 2006. Dissertação (Mestrado em Ciência da Computação) – Universidade Federal de São Carlos, São Carlos, 2006. Disponível em: https://repositorio.ufscar.br/bitstream/handle/ufscar/343/DissREG.pdf?sequence=1&isAllowed=y. Acesso em: 10 mar. 2023.

GRASSEGGER, H.; KROGERUS, M. **The Data That Turned the World Upside Down**. New York: Vice, 2017. Disponível em: https://www.vice.com/en_us/article/4x4x8n/the-data-that-turned-the-world-upside-down. Acesso em: 10 jun. 2021.

HOOFNAGLE, C. J.; SOLTANI, A.; GOOD, N.; WAMBACH, D. J. Behavioral Advertising: The Offer You Can't Refuse. **Harvard Law & Policy Review**, [*S. l.*], v. 6, p. 273-296, 2012.

HORMOZI, A. M. Cookies and Privacy. **Information Systems Security**, [*S. l.*], v. 13, n. 6, p. 51-59, 2005. DOI 10.1201/1086/44954.13.6.20050

INTERNATIONAL CHAMBER OF COMMERCE. **ICC UK Cookie Guide**. 2nd. ed. [*S. l.*]: ICC, 2012. Disponível em: https://www.cookielaw.org/wp-content/uploads/2019/12/icc_uk_cookiesguide_revnov.pdf. Acesso em: 10 jul. 2022.

IRELAND. **Data Protection Act 2018**. [Ireland]: ISB, 2018. Disponível em: https://www.irishstatutebook.ie/eli/2018/act/7/enacted/en/html. Acesso em: 10 mar. 2023.

LIN, D.; LOUI, M.C. Taking the Byte Out of Cookies: Privacy, Consent and the web. **ACM SIGCAS Computers and Society**, [*S. l.*], v. 28, n. 2, p. 39-51, June 1998. DOI https://doi.org/10.1145/276758.276775

MAGRANI, E. **Entre dados e robôs**. Ética e privacidade na era da hiperconectividade. 2. ed. Porto Alegre: Arquipélago Editorial, 2019.

MAYER-SCHÖNBERGER, V. The internet and privacy legislation: Cookies for a treat? **Computer Law & Security Review**, [*S. l.*], v. 14, n. 3, p. 166-174, 1998. DOI 10.1016/s0267-3649(98)80024-1

ODLYZKO, A. Privacy, Economics, and Price Discrimination on the Internet. *In:* ICEC2003: INTERNATIONAL CONFERENCE ON ELECTRONIC COMMERCE, 5., 2003, Pittsburgh. **Proceedings** [...] New York: ACM, 2003. p. 1-16. DOI: http://dx.doi.org/10.2139/ssrn.429762

PALMER, C. **Secure Session Management with Cookies for Web Applications**. San Francisco: iSEC Partners, 2008.

PIERSON, J.; HEYMAN, R. Social media and cookies: challenges for online privacy. **Info**, [S*. l.*], v. 13, n. 6, p. 30-42, 2011.

QUEIROZ, A. A. L. **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 em Ciência da Computação) – Universidade Federal de Pernambuco, Recife, 2011. Disponível em: https://repositorio.ufpe.br/bitstream/123456789/1298/1/arquivo1177_1.pdf. Acesso em: 21 jul. 2021.

ROHR, A. 'Cookie eterno' pode rastrear internauta e é impossível de apagar. **G1**, [*s. l.*], 2010. Tecnologia e Games. Disponível em: https://g1.globo.com/tecnologia/noticia/2010/10/cookie-eterno-pode-rastrear-internauta-e-e-impossivel-de-apagar.html#:~:text='Cookie%20eterno'%20pode%20rastrear%20internauta,ap

agar%20%7C%20Tecnologia%20e%20Games%20%7C%20G1&text='Evercookie'%20tamb%C3%A9m%20%C3%A9%20compartilhado%20entre,pol%C3%AAmica%20sobre%20privacidade%20na%20web. Acesso em: 17 jul. 2022.

SALESFORCE. [*S. l.*], 2022. Disponível em: https://www.salesforce.com/br. Acesso em: 17 jul. 2022.

SANT'ANA, 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. p. 1-21.

SIEBECKER, R. M. Cookies and the common law: are internet advertisers trespassing on our computers? **Computer & Internet Law**, [*S. l.*], v. 94, n. 3, p. 893-952, 2003.

SINGAPORE. **PDPA Overview**. Singapore: Personal Data Protection Comission, 2022. Disponível em: https://www.pdpc.gov.sg/Overview-of-PDPA/The-Legislation/Personal-Data-Protection-Act. Acesso em: 10 mar. 2023.

STEINFELD, N. "I agreetothetermsandconditions": (how) do usersreadprivacy policies online? aneye-tracking experiment. **Computers in Human Behavior**, [*S. l.*], v. 55, p. 992-1000, 2016.

TANENBAUM, A. S. **Redes de computadores**. 4. ed. Rio de Janeiro: Campus, 2003.

THE COOKIE COLLECTIVE. **Five Models for Cookie Law Consent**. London: CookiePro LLC, 2019. Disponível em: https://www.cookielaw.org/wp-content/uploads/2019/12/five-models-for-cookie-law-consent.pdf. Acesso em: 10 jul. 2022.

TOUBIANA, V.; NARAYANAN, A.; BONEH, D. Privacy Preserving Targeted Advertising *In:* NETWORK AND DISTRIBUTED SYSTEM SYMPOSIUM, 2010, San Diego. **Proceedings** [...]. [*S. l.: s. n.*], 2010. Disponível em: https://crypto.stanford.edu/adnostic/adnostic-ndss.pdf. Acesso em: 10 jul. 2021.

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 jul. 2021.

WOJTOWICZ, P. **Darknet e Deep Web**: il Lato Oscuro del Web per la Privacy e la Protezione dei Dati. 2013. Tesi di Laurea (Coso di Laurea in Ingegneria Elettronica, Informatica e Telecomunicazioni) – Università di Bologna, Italia, 2013.

COOKIES AS A WAY OF COLLECTING DATA ON WEBSITES AND USER UNCONSCIOUSNESS

ABSTRACT
Objective: The opacity in data collection on websites can affect the privacy of users, as companies often collect data without clearly informing what information is being collected, how it will be used and with whom it will be shared. This can lead to excessive data collection, which can be used for unauthorized purposes. In this scenario, this article aims to identify the possible cookies collected by the websites, in order to demonstrate the opacity present in the collection of this data, mainly in relation to the number and diversity of cookies, including the third parties involved in this process. **Method**: The methodology consists of a descriptive research with a qualitative and quantitative approach. Bibliographical research was used as methods in order to explain the technical aspects of data collection by cookies; collection of data on websites, to demonstrate the possible cookies collected by websites during interaction with the user. For the identification of cookies, the Cookiebot Consent Management Platform was used as a technological resource. **Result:** A total of 776 cookies were identified on the analyzed websites, with the marketing category cookies and persistent cookies being the most representative, in addition to 208 third-party companies present in these cookies. **Conclusions:** A variety of cookies were observed that are used by websites for data collection, this amount of cookies can reveal a lot of information about user activities and, consequently, threaten the privacy of individuals referenced in this data, without them being aware of the data collect.

Descriptors: Data collection. Cookies. Privacy. Personal data protection.

COOKIES COMO FORMA DE RECOGIDA DE DATOS EN SITIOS WEB E INCONSCIENCIA DEL USUARIO

RESUMEN
Objetivo: La opacidad en la recopilación de datos en los sitios web puede afectar la privacidad de los usuarios, ya que las empresas suelen recopilar datos sin informar claramente qué información se recopila, cómo se utilizará y con quién se compartirá. Esto puede dar lugar a una recopilación excesiva de datos, que pueden utilizarse para fines no autorizados. En este escenario, este artículo tiene como objetivo identificar las posibles cookies recopiladas por los sitios web, con el fin de demostrar la opacidad presente en la recopilación de estos datos, principalmente en relación con la cantidad y diversidad de cookies, incluidos los terceros involucrados en este proceso. **Metodología:** La metodología consiste en una investigación descriptiva con enfoque cualitativo y cuantitativo. Se utilizó la investigación bibliográfica como método para explicar los aspectos técnicos de la recolección de datos por parte de las cookies; recopilación de datos en sitios web, para demostrar las posibles cookies recopiladas por los sitios web durante la interacción con el usuario. Para la identificación de las cookies se utilizó como recurso tecnológico la Plataforma de Gestión de Consentimiento Cookiebot. **Resultados:** Se identificaron un total de 776 cookies en los sitios web analizados, siendo las cookies de categoría marketing y persistentes las más representativas, además de 208 empresas de terceros presentes en estas cookies. **Conclusiones:** Observou-se uma diversidade de cookies que são utilizados pelos sites

para coleta de dados essa quantidade de cookies pode revelar muita informação sobre atividades do usuário e, consequentemente, ameaçar a privacidade dos indivíduos referenciados nesses dados, sem que esses tenham consciência sobre a recolección de datos.

Descriptores: Recopilación de datos. Galletas. Privacidad. Protección de datos personales.

Recebido em: 26.06.2023
Aceito em: 14.07.2024