

Privacidade digital e o novo cenário da publicidade: como as marcas se adaptam ao fim dos third-party cookies?

 **Ana Rita Oliveira e Silva**rita.silva14093@gmail.com<https://orcid.org/0009-0009-0704-6611>

ISCAP, Instituto Politécnico do Porto

Resumo

A crescente exigência de privacidade digital e o desaparecimento progressivo dos *third-party cookies* estão a provocar uma transformação estrutural no ecossistema de publicidade digital. Com base numa análise de literatura recente, este artigo identifica os principais desafios enfrentados pelas marcas, nomeadamente a perda da capacidade de rastreamento e o aumento da dependência de *first-party data*. Além disso, são exploradas alternativas a estes mecanismos, como a publicidade contextual (tradicional e semântica) e a colaboração bilateral com publishers. Apesar dos obstáculos, são destacadas oportunidades relevantes, nomeadamente o fortalecimento da confiança dos consumidores e a maior autonomia na gestão de dados próprios. Por fim, discute-se a intenção subjacente às soluções atualmente propostas, refletindo até que ponto estas representam uma verdadeira ruptura com lógicas de controlo digital, ou se correspondem apenas a uma reconfiguração de práticas já consolidadas.

Palavras-chave: Privacidade digital, *Third-party cookies*, Marketing digital, Segmentação de audiências, *First-party data*, Publicidade personalizada.

Abstract

The growing demand for digital privacy and the gradual disappearance of third-party cookies are driving a structural transformation in the digital advertising ecosystem. Based on a review of recent literature, this article identifies the main challenges faced by brands, namely the loss of tracking capabilities and the increased reliance on first-party data. Additionally, it explores alternatives to these mechanisms, such as contextual advertising (both traditional and semantic) and bilateral collaboration with publishers. Despite the obstacles, relevant opportunities are highlighted, namely the strengthening of consumer trust and greater autonomy in the management of first-party data. Finally, the article examines the underlying intention behind the currently proposed solutions, questioning whether they truly represent a break from traditional models of digital control or merely a technical reconfiguration of long-established practices.

Keywords: Digital privacy, Third-party cookies, Digital marketing, Audience targeting, First-party data, Personalized advertising.

Introdução

No contexto atual, é praticamente impossível navegar na internet sem deixar algum tipo de pegada digital. Cada pesquisa gera um rastro invisível de dados que, durante muito tempo, foram discretamente aproveitados pelas marcas para conhecer melhor os seus consumidores (Cooper et al., 2023; Latvala et al., 2022). Esse registo digital, alimentado maioritariamente através dos *third-party cookies*, tornou-se a base da personalização publicitária, permitindo anúncios relevantes e campanhas eficazes.

No entanto, à medida que os utilizadores se tornaram mais conscientes do volume de dados recolhidos e da forma como estes eram utilizados, a desconfiança em relação a estes ficheiros também aumentou (Sundqvist, 2024).

Este cenário de crescente apreensão, aliado à pressão legislativa - nomeadamente com a entrada em vigor do Regulamento Geral sobre a Proteção de Dados (RGPD) na União Europeia em 2018 - culminou no anúncio, feito pelo Google em janeiro de 2020, do fim progressivo dos *third-party cookies* no navegador Chrome no âmbito da iniciativa *Privacy Sandbox* (Google, 2020). Esta medida aplica-se a todos os utilizadores do Chrome e prevê-se que esteja totalmente implementada em 2025, após sucessivos adiamentos (McGuigan et al., 2023). Mais do que uma mudança técnica, trata-se de uma transição simbólica, que obriga as marcas a repensar profundamente a forma como se relacionam e comunicam com os consumidores.

Neste artigo, analisa-se o impacto desta mudança no ecossistema da publicidade digital e explora-se de que modo as marcas estão a ajustar as suas práticas. Para isso, serão aprofundadas estratégias alternativas como a utilização de *first-party data* (dados primários), a publicidade contextual (incluindo a sua vertente semântica), colaborações com *publishers* e as parcerias com redes sociais.

O estudo estrutura-se em torno de cinco secções principais. Começa-se por abordar o papel dos *cookies* na navegação *online* e os seus efeitos sobre a privacidade digital, distinguindo-se os *first-party cookies* e os *third-party cookies*, bem como as suas vantagens e riscos. Em seguida, explora-se a evolução da percepção pública sobre a privacidade, o impacto do RGPD e de outras regulamentações, e as medidas individuais adotadas pelos utilizadores. Posteriormente, analisa-se a nova realidade da publicidade digital, destacando as implicações para o marketing e a adoção de estratégias alternativas como o uso de *first-party data*, publicidade contextual e colaborações com *publishers*. Por fim, discute-se a eficácia destas abordagens à luz das transformações em curso, refletindo sobre os desafios éticos, técnicos e estratégicos que moldarão o futuro da publicidade digital.

O papel dos *cookies* e a privacidade digital

Os *cookies* são pequenos ficheiros de texto armazenados no dispositivo do utilizador pelo navegador, com a finalidade de guardar informações sobre a sua atividade *online*. Posteriormente, o próprio website ou terceiros com *scripts* incorporados podem recuperar essas informações para personalizar a experiência de navegação ou segmentar publicidade (Ha et al., 2006).

Ao longo do tempo, estes mecanismos consolidaram-se como uma peça fundamental para a navegação na internet, permitindo aprimorar a usabilidade dos *websites*, através do reconhecimento automático de preferências, credenciais de acesso e histórico de navegação. Apesar das suas vantagens na personalização da experiência do utilizador, os *third-party cookies* levantam preocupações não apenas ao nível da privacidade, mas também da segurança. Para além da recolha extensiva de dados por entidades terceiras, estes

ficheiros podem ser explorados em diversas práticas maliciosas, expondo os utilizadores a riscos de acesso não autorizado (Barth, 2011).

First-party cookies vs. Third-party cookies

No âmbito dos *cookies*, é fundamental distinguir dois tipos principais: *first-party cookies* e *third-party cookies*. Os *first-party cookies* são criados pelo próprio *website* que o utilizador visita com o objetivo de personalizar a sua experiência de navegação, armazenando preferências, facilitando o preenchimento de formulários e evitando que os utilizadores necessitem de inserir repetidamente as suas credenciais.

Por outro lado, os *third-party cookies* são maioritariamente utilizados por empresas do setor publicitário para rastrear o comportamento dos utilizadores em diferentes *websites*. Isto ocorre através de um mecanismo que permite a terceiros recolher informações sobre as interações do utilizador no *website*. Como explicam Cooper et al. (2023, p.11):

(...) terceiros podem colocar um cookie no computador de um utilizador se receberem uma chamada de um site, e isso permite que o terceiro saiba que o utilizador visitou o site e quando a visita aconteceu. A fim de facilitar esta chamada, as entidades responsáveis pela recolha de dados fazem acordos com sites e colocam um pixel de rastreamento (às vezes chamado de cookie de rastreamento ou tag) no site.

Vantagens e riscos

Apesar dos benefícios significativos destes ficheiros, o seu uso abusivo tem vindo a gerar sérias preocupações no que diz respeito à privacidade e à segurança dos utilizadores, sendo frequentemente utilizados para monitorizar a atividade *online* sem o respetivo consentimento.

Determinadas vulnerabilidades associadas à utilização destes mecanismos são frequentemente exploradas através de ataques cibernéticos, tais como *Pass the Cookie*, *Session Hijacking*, *Session Fixation* e *Cross-Site Request Forgery*. Estes ataques comprometem informações privadas e sensíveis, tais como informações financeiras e dados pessoais, o que enfatiza a necessidade de regulamentações mais rigorosas e da eliminação definitiva dos *third-party cookies* (Hormozi, 2005).

A evolução da percepção pública sobre a privacidade digital

Na era digital contemporânea, a privacidade tornou-se um assunto de destaque no debate público e mediático. A rápida evolução das tecnologias digitais, associada à recolha massiva de dados, contribuiu para uma maior consciencialização dos consumidores sobre a forma como os seus dados pessoais são partilhados e utilizados. Como resultado, a confiança dos utilizadores na internet tem sido amplamente afetada, o que tornou a proteção da privacidade digital uma questão prioritária e global.

De acordo com o estudo de Sundqvist (2024), existe uma nítida divisão entre os consumidores no que diz respeito à privacidade dos dados. Por um lado, existem os utilizadores que encaram a perda de privacidade como algo inevitável, adotando uma postura passiva perante a utilização dos seus dados pessoais. Por outro lado, existem aqueles

que demonstram um profundo desconforto e desagrado ao constatar que as suas pesquisas e até as suas conversas privadas influenciam os anúncios que veem.

Consequentemente, os consumidores têm-se mostrado cada vez mais exigentes quanto ao investimento das marcas em infraestruturas tecnológicas e organizacionais resilientes, incluindo *hardware*, *software* e sistemas de comunicação adequados, capazes de garantir a segurança dos seus dados pessoais (Obiki-Osafiele et al., 2024).

O impacto do RGPD e outras regulamentações

Devido a esta crescente preocupação, regulamentações mais rígidas têm sido entendidas como fundamentais para proteger os dados pessoais dos utilizadores, como é o caso do RGPD, um regulamento da União Europeia que entrou em vigor a partir de 25 de maio de 2018.

Em Portugal, a aplicação do RGPD é assegurada pela Lei n.º 58/2019, de 8 de agosto, que adapta as disposições europeias à realidade nacional, nomeadamente para:

(...) harmonizar a legislação nacional com as disposições já vigentes do RGPD e detalhar a regulação da proteção de dados em diferentes matérias que, por um lado, não estão expressamente previstas no RGPD ou que, por outro lado, apesar de se encontrarem reguladas no RGPD são ali tratadas com mais detalhe (Mota, J., & Sampaio, A. P., 2019, p. 143).

Estas regulamentações foram criadas para assegurar que as empresas e organizações que armazenam e processam detalhes privados dos utilizadores o façam de forma ética e responsável (Wolford, 2025). Para isto, este regulamento estabelece requisitos rigorosos, incluindo a necessidade de medidas técnicas e organizacionais que garantam a segurança das informações.

A autoridade responsável pela fiscalização do cumprimento destas normas em Portugal é a Comissão Nacional de Proteção de Dados (CNPD), que, em 2022, intensificou significativamente a sua atividade regulatória. De acordo com o Relatório de Atividades de 2023, a CNPD aplicou 90 coimas no valor de 559.950,00 euros, emitiu 7 medidas corretivas e realizou 253 advertências por infrações à Lei n.º 58/2019, de 8 de agosto. Estes dados refletem uma continuidade da postura proativa da CNPD na aplicação da legislação nacional e europeia em matéria de proteção de dados, com especial incidência na fiscalização de práticas de marketing digital e tratamento indevido de dados pessoais (Comissão Nacional de Proteção de Dados, 2024).

Deste modo, ao serem implementadas práticas de segurança mais complexas, as marcas tornam-se capazes de assegurar o cumprimento das obrigações legais enquanto contribuem para o fortalecimento da confiança dos utilizadores. Contudo, a regulamentação apenas não é suficiente, pois a proteção da privacidade digital depende sobretudo do comportamento consciente dos próprios utilizadores.

Medidas individuais de proteção

Apesar de regulamentações como o RGPD representarem um avanço notável na proteção da privacidade digital, a responsabilidade pela proteção dos dados pessoais depende em grande parte dos próprios utilizadores, pois são eles que aceitam as *cookies* e partilham as suas informações privadas *online*. Por conseguinte, a privacidade digital não é apenas um direito, mas sim uma escolha e decisão individual.

Esta crescente consciencialização sobre os riscos digitais tem estimulado a adoção de medidas individuais de proteção, tais como evitar redes Wi-Fi públicas, manter os softwares de segurança atualizados, aceder a websites com rastreamento reduzido e limitar a partilha de dados pessoais (Fang, 2023). Como explica Fang (2023, p. 391), “se quisermos ter uma vida normal, devemos tomar medidas proativas e conscientes”.

A adoção de ferramentas tecnológicas também é uma das formas mais utilizadas para garantir a proteção *online*. Navegadores alternativos, como *DuckDuckGo*, *Brave*, *Tor Browser*, bem como *ad blockers*, VPNs e extensões de privacidade são as escolhas mais frequentes dos utilizadores. Estudos recentes revelam que esses recursos são escolhidos como forma de autoproteção e de contestação à vigilância algorítmica associada à publicidade digital (Houda Elmimouni et al., 2023; Lund & Beckstrom, 2022; Kulkarni & Bedekar, 2022).

Consequentemente, a adoção de medidas individuais por parte dos utilizadores torna-se um exercício contínuo de literacia digital e de responsabilidade pessoal.

O fim dos *third-party cookies* e a nova realidade da publicidade

De forma cada vez mais evidente, a indústria da publicidade digital tem sido pressionada a enfrentar as verdadeiras consequências do abandono dos *third-party cookies*. Esta transição assinala o fim de um modelo assente no rastreamento intensivo e o início de uma nova fase marcada por soluções tecnológicas alternativas.

Contudo, esta transição não representa um verdadeiro abandono das práticas anteriores. Segundo McGuigan et al. (2023, p. 10), “as maiores destas empresas estão a explorar a privacidade através de medidas técnicas autorregulatórias que consolidam o seu poder e tornam as empresas mais pequenas ainda mais dependentes delas”. Assim, apesar da intenção declarada de eliminar definitivamente os *third-party cookies* e da tentativa de alinhamento com os princípios da privacidade, o controlo sobre o ecossistema publicitário e o consequente favorecimento destas empresas mantém-se praticamente inalterado.

Estas alterações abriram espaço para diferentes respostas e estratégias, que refletem abordagens distintas relativamente ao equilíbrio entre personalização e privacidade.

Emerge, assim, uma nova abordagem à publicidade personalizada, uma abordagem baseada em tecnologias de privacidade local nas quais os dados são processados diretamente no dispositivo do utilizador, em vez de serem enviados para servidores externos.

Assim sendo, o setor da publicidade digital encontra-se num momento de transição no qual as marcas são obrigadas a reinventar urgentemente as suas estratégias e a adaptar-se a um novo cenário, onde a privacidade e as limitações legais ganham destaque.

O impacto para o marketing e publicidade digital

Nas últimas décadas, os *third-party cookies* constituíram uma das principais ferramentas utilizadas pelas marcas para monitorizar o comportamento dos utilizadores, segmentar audiências e avaliar o desempenho de campanhas publicitárias (Latvala et al., 2022). Esta capacidade de recolher dados permitia otimizar os investimentos, personalizar comunicações e melhorar significativamente o retorno sobre o investimento (ROI).

Com o fim progressivo destes arquivos, as marcas veem-se privadas do acesso aos dados que durante anos alimentaram as suas práticas, sendo agora obrigadas a reformular as suas estratégias de segmentação e personalização. Neste contexto, Venter et al., (2015, citado

por Lönberg et al., 2022, p.10) alertam que “*a segmentação de mercado será um problema centralizado, uma vez que a segmentação é central e parte fundamental da estratégia de marketing*”. Esta limitação compromete seriamente a eficácia das campanhas publicitárias, exigindo a exploração de novas abordagens, baseadas em *first-party data*, processamento local e novas APIs centradas na privacidade.

A nível financeiro, o impacto é igualmente relevante. A eliminação destas ferramentas afeta diretamente a performance das campanhas, refletindo-se numa menor taxa de conversão, no aumento do custo por aquisição e numa maior dificuldade em medir e justificar o ROI (Aridor et al., 2024). Como explica Jonathan Burns, gestor de desenvolvimento de negócios na Nodehill, “*o marketing vai custar mais e gerar um menor retorno sobre o investimento*” (citado por Lönberg et al., 2022, p. 25).

Este cenário revela-se particularmente desafiante para pequenas e médias empresas (PME), cuja dependência de soluções baseadas em *third-party cookies* é maior e cujos recursos para investir em alternativas são, muitas vezes, limitados (Aridor et al., 2024).

Outro desafio está relacionado com a atribuição de conversões, ou seja, com a capacidade de determinar qual canal, anúncio ou estratégia contribuiu para uma conversão (compra, inscrição, *lead*, etc.). Com os *third-party cookies*, acompanhar a jornada do utilizador em diferentes *websites* e plataformas era algo simples, porém, sem este contínuo rastreamento, os dados tornam-se menos precisos e “*perdem-se muito mais atribuições porque a vida útil do cookie não é tão longa quanto antes*” (Michael Wahlgren, fundador da Pineberry, citado Lönberg et al., 2022, p.29), sendo muito mais difícil saber qual campanha realmente influenciou a conversão.

Neste contexto, é necessário que as marcas adotem processos estratégicos mais flexíveis e responsivos, de modo que consigam adaptar-se às novas exigências legais e tecnológicas. Como explica Matzler et al. (2018, citado por Lönberg et al., 2022, p.8), é necessário “*abrir o processo estratégico até certo ponto, a fim de serem ajustáveis e adaptáveis quando confrontadas com novas condições e leis na sua área de atuação*”.

Estratégias alternativas para as marcas

Com a eliminação iminente dos *third-party cookies*, as marcas enfrentam o desafio de uma adaptação contínua das suas estratégias de *marketing* digital. Neste novo cenário, surgem diversas estratégias alternativas, com o objetivo de manter a eficácia e a personalização das campanhas publicitárias.

Entre estas estratégias, destacam-se: a utilização de *first-party data*, a publicidade contextual tradicional e a publicidade contextual semântica, a colaboração bilateral com *publishers*, a parceria com plataformas de redes sociais, a adoção de tecnologias de identificação alternativas, entre várias outras.

Para este artigo, serão aprofundadas as estratégias consideradas mais promissoras no contexto atual, nomeadamente a estratégia de *first-party data*, a publicidade contextual tradicional e a semântica e a colaboração bilateral com *publishers*.

First-party data

Uma das abordagens mais promissoras consiste na utilização intensiva de *first-party data*, isto é, na utilização de informações recolhidas diretamente dos próprios utilizadores, através dos registo em *websites*, *newsletters* e programas de fidelização (Latvala et al, 2022). Esta estratégia permite às marcas contornar as limitações impostas pelos navegadores e

fortalecer a autonomia sobre os seus próprios dados. Porém, apresenta limitações no alcance de novos públicos, já que estes dados refletem as interações diretas e prévias com a marca.

Oksanen (2022) destaca que as marcas mais bem preparadas são aquelas que já investem em sistemas de recolha e gestão de dados próprios, permitindo manter a relevância e personalização sem ficar dependente de rastreamento de terceiros.

Publicidade contextual tradicional e publicidade contextual semântica

Outra alternativa viável aos *third-party cookies* é a publicidade contextual que consiste na exibição de anúncios com base no conteúdo da página visitada e não no histórico do utilizador. Esta estratégia é baseada numa segmentação por *coortes*¹ e evita os desafios legais e éticos associados ao rastreamento individualizado (El Hana et al., 2023).

Contudo, esta abordagem não possui o mesmo nível de personalização hipersegmentada oferecido anteriormente pelos *third-party cookies*. De forma a ultrapassar esta limitação, surgiu a publicidade contextual semântica, uma abordagem que recorre à inteligência artificial (IA) para garantir a relevância do conteúdo. Como destacam El Hana et al. (2023, p.8), ao citarem o Entrevistado 9, esta técnica é cada vez mais essencial para as marcas, uma vez que permite “*analisar o conteúdo da página e prever comportamentos e interesses com base no conteúdo ao qual os utilizadores estão expostos*”.

Colaboração bilateral com publishers

A colaboração bilateral com *publishers*, também designada como estratégia de *second-party data*, baseia-se na partilha direta de *first-party cookies* entre anunciantes e meios de comunicação. Esta colaboração permite enriquecer as bases de dados do anunciante e aumentar a relevância das campanhas publicitárias (El Hana et al., 2023).

Por exemplo, “*(...) um anunciente que vende ração para animais faria bem em estabelecer uma parceria direta com um publisher que tenha uma audiência forte de donos de animais de estimação... Isso pode alimentar o CRM*” (Entrevistado 9, citado em El Hana et al., 2023, p.8). Ou seja, esta colaboração bilateral permite ao anunciente integrar diretamente informações importantes, como comportamentos e interesses deste grupo específico de consumidores nos sistemas internos de gestão de relacionamento com o cliente (CRM). Desta forma, as marcas conseguem alcançar audiências altamente segmentadas sem ter de recorrer ao uso de *third-party cookies*.

Discussão de resultados

O fim dos *third-party cookies* representa, como discutido ao longo deste artigo, uma disruptão estrutural no ecossistema da publicidade digital. Vários autores apontam para o impacto direto que esta mudança tem na capacidade de segmentação e, consequentemente, na eficácia das campanhas (Latvala et al., 2022; Lönberg et al., 2022). Tal como sublinhado por Venter et al. (2015, citado por Lönberg et al., 2022), a segmentação

¹ Grupos de pessoas anónimas que possuem interesses e comportamentos semelhantes.

constitui um pilar fundamental das estratégias de marketing, sendo a sua limitação um dos principais desafios desta transição.

Apesar da relevância atribuída a esta perda, alguns estudos poderão sobrevalorizar o seu caráter disruptivo, ignorando os esforços de reinvenção estratégica de diversas marcas. Embora o aumento do custo por aquisição e a redução da taxa de conversão sejam realidades confirmadas por Aridor et al. (2024), é importante destacar que esses impactos não são uniformes, pois afetam de forma mais significativa as PME que dependem exclusivamente de ferramentas de *targeting* baseadas em terceiros.

Paralelamente, a aposta em *first-party data*, como sugerido por Latvala (2022), tem-se revelado uma alternativa promissora aos *third-party cookies*. Embora Oksanen (2022) destaque as vantagens competitivas associadas à adoção precoce de *first-party cookies*, esta perspetiva tende a ignorar o fosso tecnológico entre grandes marcas e PME, que continuam excluídas deste modelo por falta de recursos. Neste sentido, este argumento não deve ser tomado como verdade absoluta, já que não se aplica de forma igual a todas as realidades.

No domínio da segmentação, a publicidade contextual tradicional e, mais recentemente, a publicidade contextual semântica, surgem como estratégias relevantes. Os dados apresentados por El Hana et al. (2023) evidenciam a eficácia crescente destas abordagens, em particular quando aliadas à IA. Porém, apesar de promissoras, estas soluções enfrentam limitações evidentes, como a incapacidade de replicar com precisão os resultados das campanhas anteriores que utilizavam o rastreamento comportamental. Consequentemente, isto levanta sérias dúvidas sobre a eficácia dessas estratégias num mercado que exige cada vez mais resultados concretos.

A colaboração bilateral com *publishers* revela-se especialmente eficaz quando existe uma clara afinidade entre o público do *publisher* e o público-alvo da marca. Como referem El Hana et al. (2023), parcerias estratégicas podem alimentar eficazmente os sistemas de CRM. Esta análise sustenta a ideia de que estas colaborações oferecem um equilíbrio entre personalização e conformidade legal, sem a opacidade associada aos *third-party cookies*.

Importa ainda referir que muitas das soluções propostas como alternativas a estes mecanismos não representam uma verdadeira ruptura dos modelos tradicionais de controlo de dados. Embora prescindam da monitorização através dos *third-party cookies*, continuam a basear-se na recolha massiva de dados através de meios poucos transparentes. A recolha de *first-party data*, por exemplo, pode parecer mais ética por estar diretamente associada ao consentimento, porém mantém a lógica de capitalização sobre o utilizador e coloca empresas com menos recursos em desvantagem competitiva. Já a publicidade contextual semântica recorre a tecnologias de IA que inferem padrões e interesses a partir da navegação, reproduzindo, de forma mais visível, práticas de vigilância algorítmica.

Tal como argumentam McGuigan et al. (2023), estas abordagens configuram, sobretudo, uma reformulação técnica de práticas anteriores, perpetuando os mesmos centros de poder. Deste modo, é possível reconhecer, à semelhança da visão crítica de alguns autores, que a promessa de privacidade parece mais um discurso para mostrar boas intenções do que uma mudança efetiva nos princípios da publicidade digital.

Para além das soluções tecnológicas, é essencial refletir sobre a dimensão ética desta mudança. Os consumidores estão cada vez mais atentos e exigem transparência e controlo sobre os seus próprios dados. Embora regulamentações como o RGPD tenham representado um marco importante, o verdadeiro desafio está na capacidade das marcas passarem da teoria à prática, ou seja, transformarem estas obrigações legais em comportamentos reais.

Conclusão

Ao longo deste artigo, observou-se que o fim progressivo dos *third-party cookies* está a desafiar os pilares sobre os quais a publicidade digital se construiu nas últimas décadas. Esta transição tem vindo a exigir uma adaptação, especialmente por parte das PME, que enfrentam maiores dificuldades em acompanhar esta mudança significativa.

As estratégias alternativas analisadas revelam-se opções possíveis, mas ainda assim imperfeitas, uma vez que persistem limitações técnicas e desigualdades de acesso.

Num cenário marcado por uma crescente literacia digital e por uma sociedade cada vez mais consciente dos seus direitos, a confiança passou a assumir um papel central. E é aqui que reside talvez o maior desafio e a maior oportunidade para as marcas: criar relações mais transparentes e respeitadoras com os utilizadores.

Deste modo, a eventual eliminação destes arquivos convida a um novo posicionamento. Um posicionamento que reconhece que, no futuro da publicidade, o respeito pela privacidade não será apenas uma obrigação legal, mas uma verdadeira vantagem competitiva. As marcas que souberem ler este momento com sensibilidade, visão estratégica e autenticidade, estarão um passo à frente num ecossistema que já não aceita “seguir o utilizador”, mas exige acompanhá-lo com ética e responsabilidade.

Neste sentido, torna-se pertinente que futuras investigações explorem até que ponto estas estratégias alternativas são capazes de manter a eficácia das campanhas. Importa também compreender como é que os consumidores percebem estas mudanças e se, de facto, se sentem mais protegidos e confiantes. Além disso, seria fundamental aprofundar o impacto desta transformação nas PME, cuja capacidade de adaptação é muitas vezes limitada. Através destas linhas de investigação, será possível construir uma publicidade digital mais justa, transparente e verdadeiramente alinhada com as expectativas da sociedade atual.

Declaração de uso de IA

Durante a elaboração deste artigo, a autora utilizou a ferramenta ChatGPT para reestruturação do texto e aperfeiçoamento gramatical. Todo o conteúdo gerado foi submetido a uma análise crítica, sendo revisto, validado e complementado pela autora garantindo o seu rigor conceptual e a sua conformidade com princípios éticos e científicos.

Referências

- Aridor, G., Che, Y. K., Hollenbeck, B., McCarthy, D., & Kaiser, M. (2024). Evaluating the impact of privacy regulation on e-commerce firms: *Evidence from Apple's app tracking transparency*. *Social Science Research Network*.
<https://doi.org/10.2139/ssrn.4717752>
- Barth, A. (2011). HTTP State Management Mechanism (RFC 6265). Internet Engineering Task Force (IETF). Disponível em: <https://datatracker.ietf.org/doc/html/rfc6265>
- Comissão Nacional de Proteção de Dados. (2024). *Relatório de atividades 2023*.
https://www.cnpd.pt/media/rxvfiafs/cndp_relatorioatividades_2023.pdf
- Cooper, D. A., Yalcin, T., Nistor, C., Macrini, M., & Pehlivan, E. (2022). Privacy considerations for online advertising: a stakeholder's perspective to programmatic advertising. *Journal of Consumer Marketing*, 40(2). <https://doi.org/10.1108/jcm-04-2021-4577>

El Hana, N., Mercanti-Guérin, M., & Sabri, O. (2023). Cookiepocalypse: What are the most effective strategies for advertisers to reshape the future of display advertising? *Technological Forecasting and Social Change*, 188, 122297. <https://doi.org/10.1016/j.techfore.2022.122297>

Elmimouni, H., Shusas, E., Skeba, P., Baumer, E. P., & Forte, A. (2023, March). What Makes a Technology Privacy Enhancing? Laypersons' and Experts' Descriptions, Uses, and Perceptions of Privacy Enhancing Technologies. In *International Conference on Information* (pp. 229-250). Cham: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-28032-0_20

Fang, W. (2023). Social Media Changed the Notion of Privacy. *Journal of Education, Humanities and Social Sciences*, 14, 388–392. <https://doi.org/10.54097/ehss.v14i.8894>

Google. (2020, 14 de janeiro). *Building a more private web: A path towards making third party cookies obsolete*. Chromium Blog. <https://blog.chromium.org/2020/01/building-more-private-web-path-towards.html>

Ha, V., Inkpen, K., Al Shaar, F., & Hdeib, L. (2006). An examination of user perception and misconception of internet cookies. *CHI '06 Extended Abstracts on Human Factors in Computing Systems - CHI EA '06*. <https://doi.org/10.1145/1125451.1125615>

Hormozi, A. M. (2005). Cookies and Privacy. *Information Systems Security*, 13(6), 51-59. <https://www.proquest.com/scholarly-journals/cookies-privacy/docview/229516983/se-2>

Kulkarni, S., & Bedekar, M. (2022). Perception of privacy in a data driven world. *International Journal of Modern Education and Computer Science*, 8(4), 380–388. https://www.researchgate.net/publication/360081637_Perception_of_privacy_in_a_data_driven_world

Latvala, L., Horn, J., & Bruno, B. (2022). Thriving in the age of privacy regulation: A first-party data strategy. *Applied Marketing Analytics*, 7(3), 211–211. <https://doi.org/10.69554/kmbl6487>

Lönberg, N., Mantovaara, L. A., & Johansson, P. (2022). *The death of the third-party cookie: A qualitative study regarding new strategies and methods for collecting consumer data to obtain effective digital marketing* [Master's thesis, Umeå University]. DiVA portal. <https://www.diva-portal.org/smash/get/diva2:1743208/FULLTEXT01.pdf>

Lund, B. D., & Beckstrom, M. A. (2022). What Is the Anonymous Web? Routledge EBooks, 21–37. <https://doi.org/10.4324/9781003093732-3>

McGuigan, L., Sarah Myers West, Ido Sivan-Sevilla, & Parham, P. (2023). The after party: Cynical resignation in Adtech's pivot to privacy. *Big Data & Society*, 10(2). <https://doi.org/10.1177/20539517231203665>

Mota, J., & Sampaio, A. P. (2019). Regulamento Geral de Proteção de Dados em Portugal – alguns apontamentos à sua lei de execução. *Actualidad Jurídica Uría Menéndez*, (53), 142–148. <https://www.uria.com/documentos/publicaciones/6855/documento/port01.pdf?id=9341>

Obiki-Osafiele, A. N., Efunniyi, C. P., Abhulimen, A. O., Osundare, O. S., Agu, E. E., Adeniran, I. A., & OneAdvanced, U. K. (2024). Theoretical models for enhancing operational efficiency through technology in Nigerian businesses. *International Journal of*

Applied Research in Social Sciences, 6(8), 1969-1989.

<https://doi.org/10.51594/ijarss.v6i8.1478>

Oksanen, T. (2022). *Companies' maturity for the depreciation of third-party cookies* (Master's thesis, LUT University). LUTPub.

https://lutpub.lut.fi/bitstream/handle/10024/164359/Pro_Gradu_Oksanen_Timo_2022.pdf

Sundqvist, H. (2023). *Behind the Screen: Unpacking Consumer Resistance to Digital Advertising Thesis*.

https://www.theseus.fi/bitstream/handle/10024/870969/Sundqvist_Henrik.pdf?sequence=2&isAllowed=y

Wolford, B. (2025). *What is GDPR, the EU's new data protection law?* GDPR.eu.

<https://gdpr.eu/what-is-gdpr/>