É TEMPO DE PROIBIR A PUBLICIDADE BASEADA EM VIGILÂNCIA  
 **O caso contra a vigilância comercial online**  
Junho de 2021

Mudar puvlicidade baseada em vigilência para: ???

- Vigilância publicitária

- Publicidade baseada em Espionagem

- Espionagem com base na publicidade

-

Tabela de conteúdos  
1 Resumo2 Introdução3 O que é a "publicidade baseada na vigilância"?  
3.1 Formas alternativas de publicidade digital  
3.2 Dados de primeira e de terceiros  
4 Efeitos nocivos da publicidade baseada na vigilância

4.1 Falta de transparência  
4.2 Violações da privacidade e proteção de dados  
4.3 Manipulação  
4.4 Discriminação  
4.5 Desinformação  
4.6 Efeitos anti concorrência  
4.7 Fraude e perda de receitas   
4.8 Riscos de segurança  
4.9 Falta de confiança  
4.10 Tecnologia ineficiente   
5 Legislação atual  
5.1 Lei de privacidade e proteção de dados da UE  
5.2 A Diretiva relativa às práticas comerciais desleais  
5.3 Questões de execução  
6 Conclusão

1 Resumo

A vigilância comercial e a exploração dos consumidores são agora a norma a internet. À medida que utilizamos vários serviços digitais, estamos constantemente monitorizados por um grande número de atores comerciais sob o pretexto de mostrar-nos mais publicidade relevante. É hora de dar um passo atrás e considerar os problemas que este modelo criou e para imaginar um novo normal que capacita e protege os consumidores.

À medida que a vigilância comercial generalizada se infiltra em todos os aspetos do nosso dia-a-dia, torna-se claro que há uma necessidade de uma reforma sistémica da indústria de publicidade online. As discussões estão em curso na União Europeia sobre como lidar com a publicidade baseada em vigilância como parte da Lei Digital dos Serviços (Digital Services Act). Ao mesmo tempo, estão a decorrer discussões sobre a adoção federal legislação de privacidade e iniciativas legislativas para restringir a vigilância publicitária nos Estados Unidos, onde muitas das empresas envolvidas na publicidade baseada em monitorização está sediada. Estamos, portanto, diante de uma oportunidade legislativa única para resolver muitas questões prementes.

O resultado destas discussões pode ter consequências significativas para o  
modelo de negócio da maioria dos conteúdos online, e os consumidores poderiam vir a beneficiar de uma nova abordagem preventiva. Este documento fornece uma visão geral dos desafios da publicidade baseada na vigilância, e pode assim ser considerado uma parte das discussões políticas em curso.

Está a tornar-se claro que a maioria dos consumidores não quer ser rastreada e modelado para fins publicitários. Num inquérito populacional realizado pelo YouGov em nome do Conselho Norueguês do Consumidor, apenas um em cada dez inquiridos foram positivos para que os atores comerciais on-line recolham informações pessoais sobre eles, enquanto apenas um em cada cinco pensaram que receber anúncios com base em informações pessoais é aceitável. Isto assemelha-se a sondagens semelhantes de ambos os lados do Atlântico, e indica que os consumidores não consideram a vigilância comercial como uma troca aceitável para a possibilidade de ver anúncios personalizados.

Os desafios causados e profundidade da monitorização baseada em publicidade incluem, mas não se limitam a:

• infrações à privacidade e proteção de dados

• modelos de negócio pouco transparentes

• manipulação e discriminação em massa

• fraude e outras atividades criminosas

• riscos de segurança graves

Nos capítulos seguintes, descrevemos vários aspetos destes desafios e  
evidenciamos como é que modelo dominante da publicidade online de hoje é uma ameaça para consumidores, sociedades democráticas, meios de comunicação social, e até mesmo aos anunciantes si mesmos. Estas questões são significativas e sérias o suficiente para nós acreditarmos que é tempo de proibir estas práticas prejudiciais.

A proibição das práticas baseadas em vigilância deve ser complementada por uma mais forte aplicação da legislação em vigor, incluindo a Proteção Geral de Dados Regulação, regulação da concorrência e práticas comerciais desleais. No entanto, a aplicação da lei atualmente consome tempo significativo e recursos, e geralmente acontece depois dos danos já terem sido feitos. Proibir a publicidade baseada em vigilância em geral vai forçar mudanças estruturais para a indústria publicitária e aliviar uma série de danos significativos para consumidores e para a sociedade em geral.

A proibição da publicidade baseada na vigilância não significa que não se possa mais financiar conteúdos digitais usando publicidade. Para ilustrar isto, descrevemos algumas possíveis formas de avançar para conteúdos digitais financiados por publicidade, e apontar para tecnologias de publicidade alternativas que podem contribuir para uma mais segura e saudável economia digital tanto para consumidores como para empresas.

2 Introdução

"Publicidade baseada em vigilância", ou publicidade direcionada baseada em rastreamento e perfil profiling de consumidores, é o modelo dominante no negócio online de hoje. Esta forma de marketing usa informação sobre cada um de nós em tentativas de alterar o conteúdo das mensagens, utilizando fatores como a nossa escolha de canal e a que horas estamos on-line para determinar quando estamos mais suscetíveis a comportamental influência.

A publicidade baseada na vigilância tem sido um fator determinante no crescimento "economia de vigilância"1 online, onde os dados pessoais são recolhidos, agregados e vendido através de uma grande rede de atores comerciais.2 Isto está em desacordo com os direitos fundamentais à privacidade e proteção de dados pessoais, é prejudicial para a defesa do consumidor, e pode levar à manipulação e discriminação em massa. É também criador de problemas de segurança significativos devido à acumulação de dados pessoais, e deu origem a um crescente modelo de negócio que conduz uma grande quantidade de desinformação, conteúdo radicalizado, burlas e fraudes. A individualização obscura, a personalização e as técnicas de micro-segmentação da publicidade torna-a difícil de descoberta as atividades ilegais e aumenta a vulnerabilidade consumidor.

Como um todo, os benefícios potenciais da publicidade baseada na vigilância parecem insignificantes em comparação com os grandes danos que a economia de monitorização nos trouxe. Um sistema abrangente que implique uma monitorização contínua de todos os consumidores e que representa sérias ameaças a uma série de direitos fundamentais,  
com a promessa de mostrar anúncios potencialmente mais relevantes online, parece desproporcionado. Este seria o caso mesmo que a exatidão e o valor acrescentado da vigilância fosse tão bom quanto anunciado, o que não é o caso.

Várias instituições e organizações da sociedade civil apontado o dedo  
para os principais desafios da publicidade baseada na vigilância e para a vigilância economia que sustenta a tecnologia.3 Por exemplo, tanto o Parlamento Europeu4 como a Supervisão Europeia de Proteção de Dados5 têm argumentado que a publicidade baseada na vigilância deve ser eliminada progressivamente e, com o tempo, proibida. Estas discussões e desafios não se limitam ao contexto europeu.

1 A "economia de vigilância" é um termo abrangente para a economia digital com base na  
monitorização dos consumidores e comercialização de dados pessoais, e abrange processos  
como recolher, processar, partilhar, comprar e vender dados pessoais.  
2 ' Out of Control’. Forbrukerrådet. https://www.forbrukerradet.no/out-of-control/  
3 'Targeted Online: How Big Tech’s business model sells your deepest secrets for profit'.  
European Digital Rights. https://edri.org/our-work/targeted-online-big-tech-businessmodel-sells-your-deepest-secrets-for-profit/  
4 " Digital Services Act: Improving the functioning of the Single Market’. European   
Parliament resolution. https://www.europarl.europa.eu/doceo/document/TA-9-2020...  
0272\_EN.pdf  
  
  
  
Nos Estados Unidos, por exemplo, uma ampla coligação de ONG’s envolvidas em áreas como, direitos dos consumidores, controlo de armas, direitos civis, proteção à criança e o direito à palavra, free speech apelou recentemente à proibição da publicidade baseada na vigilância. A coligação cita preocupações sobre questões como a difusão de desinformação e extremismo, facilitando a discriminação, efeitos negativos na saúde pública, e desventrando a indústria do jornalismo.6

Como podemos examinar em profundidade nos seguintes capítulos, há outras formas de publicidade digital que não se baseiam na vigilância. Isto significa que é possível financiar conteúdos digitais através da publicidade, mesmo que a utilização de publicidade baseada em vigilância fosse levada a uma paragem.

Todos os consumidores estão vulneráveis quando confrontados com sistemas disfarçados que: recolhem secretamente informação sobre nós, exploram-nos, e tornam-nos alvo de uma forma que nos deixa vulneráveis por padrão7 e que comercializa todas as nossas atividades online. A dimensão massiva da tecnologia faz com que que os consumidores tenham pouca ou nenhuma margem individual para se protegerem contra a recolha massiva de dados, perfis e alvos abrangentes (profiling and pervasive targeting.).  
O desenvolvimento contínuo e a proliferação de novas tecnologias, incluindo inteligência artificial e aprendizagem computorizada, significa que estas questões estão a tornar-se mais urgentes à medida que o tempo passa.

A publicidade baseada na vigilância é prejudicial à sustentabilidade económica, aos indivíduos e a sociedade em geral. Podem ser traçados paralelismos de outras áreas onde as proibições de certas práticas têm impulsionado uma mudança positiva.

Por exemplo, as proibições e restrições à publicidade ao álcool e ao tabaco têm resultou em resultados positivos na saúde dos consumidores.8 A proibição dos gases CFC nos anos de 80 teve um efeito positivo na eliminação progressiva de materiais com graves riscos ambientais, e levou à inovação e produção de soluções amigas alternativas do ambiente. Da mesma forma, a proibição do amianto na construção levou a materiais menos poluentes serem utilizados substituindo este.  
  
5 ‘Opinion on the European Commission's proposal for a Digital Services Act’. European   
Data Protection Supervisor os. https://edps.europa.eu/data-protection/ourwork/publications/opinions/digital-services-act\_en  
6 " Ban Surveillance Advertising ". https://www.bansurveillanceadvertising.com/  
7 " EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets’. Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax, Joanna Strycharz. https://www.beuc.eu/publications/beuc-x-2021-018\_eu\_consumer\_protection.0\_0.pdf  
8 « The effects of tobacco control policies on global smoking prevalence’. Luisa S. Flor, Marissa B. Reitsma, Vinay Gupta, Marie Ng, Emmanuela Gakidou.  
https://www.nature.com/articles/s41591-020-01210-8  
  
Algumas das questões relacionadas com a publicidade baseada na vigilância já estão regulamentadas na UE através do Regulamento Geral de Proteção de Dados (RGPD) e a diretiva ePrivacy. No entanto, a aplicação fraca e despreocupada significa que os problemas estas leis procuram abordar ainda persistem, e particularmente, o RGPD apenas aborda desafios que estão relacionados com a proteção de dados. É claro que os desafios da publicidade baseada na vigilância vai muito além da área de dados proteção e privacidade.

Com isto em mente, é agora altura de proibir a publicidade baseada na vigilância. A proposta \*Digtal Services Act\* Lei de Serviços Digitais, que está atualmente a ser discutida pelos legisladores da EU, fornece uma oportunidade para fazê-lo. Além disso, alguns destes assuntoa poderiam e deveriam também ser abordadas noutros domínios, como os direitos dos consumidores, regras de privacidade digital (ePrivacy), lei de proteção de dados e regulação da Inteligência Artificial.

3 O que é a "publicidade baseada na vigilância"?

Toda a publicidade é, de certa forma, direcionada. O contexto de um anúncio, posicionamento e seu design significa que qualquer anúncio é personalizado para, e visto mais frequentemente por, alguns grupos de consumidores do que por outros. Isto também se aplica a Marketing offline 'tradicional', onde os anunciantes compram acesso a determinados atenção grupos de consumidores quando decidem onde querem colocar a sua anúncios.  
Neste contexto, usamos o termo "publicidade baseada na vigilância" como cobertor termo para publicidade digital que é dirigido a indivíduos ou consumidores segmentos, geralmente através de rastreio e perfis com base em dados pessoais.  
A publicidade baseada na vigilância inclui comportamental, personalizado e personalizado marketing. No marketing offline tradicional, os anúncios são colocados num pré-determinado contexto, por exemplo, comprando espaço de anúncios em uma revista de automóveis em a fim de chegar aos consumidores interessados em carros. A publicidade baseada em vigilância é diferente, porque o anúncio é direcionado para um indivíduo ou grupo baseado emcaracterísticas do indivíduo ou grupo. O contexto de onde o anúncio é colocado pode ser aleatório porque é alvo no consumidor e porque o anúncio pode seguir o consumidor em diferentes contextos. A tecnologia promete que, através de uma análise abrangente de dados, um anúncio pode ser mostrado ao "indivíduo certo" no "momento certo", por exemplo, mostrando um anúncio de fast food quando foi calculado que você pode estar se sentindo peckish, ou para cirurgia estética se não se sentir atraente. Variações desta tecnologia são também vulgarmente referidos como 'comportamental publicidade ' 'microtargeting' ou "publicidade programática".  
Na maioria dos casos, a publicidade baseada na vigilância é mostrada como parte de um totalmente autenticado processo, e cada anúncio individual é escolhido e colocado em uma questão de milissegundos. Isto significa que nem a editora (por exemplo. o proprietário de um site ou app) nem o anunciante (por exemplo, o proprietário da marca que é promovida) escolher quais anúncios mostrar e onde exibi-los. Isto é automaticamente decidida por sistemas tecnológicos que são muitas vezes controlados por terceiros intermediários (conhecidos como adtech empresas).   
Um grande número destas empresas terceiras estão simultaneamente a recolher grandes quantidades de dados pessoais dos consumidores, a fim de criar o consumidor perfis e segmentos que são usados em tentativas de direcionar os anúncios de forma mais eficiente.   
A automatização do processo permite monitorização e adaptação contínuas  
publicidade, que também permite que os anunciantes meçam e escalam direcionados campanhas de diferentes maneiras. No entanto, como será explicado abaixo, o uso de a publicidade baseada na vigilância também coloca desafios significativos aos editores e anunciantes sobre receitas, danos reputacionais e oferta opaca correntes.  
  
**3.1 Formas alternativas de publicidade digital**Um argumento comum em favor de publicidade baseada em vigilância é que uma proibição terá consequências negativas para os prestadores de serviços e conteúdos e levar a aumento dos custos para os consumidores, uma vez que a maioria dos serviços "gratuitos" online são financiados por anúncios.9  
Como será elaborado em baixo, este argumento é baseado na falácia que  
a publicidade baseada na vigilância é a única forma viável de financiar conteúdos digitais. Outro argumento em favor de permitir a publicidade baseada em vigilância é que os consumidores consideram que os anúncios direcionados são úteis e positivos. Este argumento assume que a única alternativa à publicidade baseada na vigilância é mostrar consumidores anúncios completamente aleatórios e irrelevantes, o que seria um incómodo e prevenir consumidores de receber ofertas interessantes. Esta é outra premissa defeituosa, como não é uma questão de anúncios baseados em vigilância por um lado e arbitrariedade por outro.

9 Para um exemplo deste argumento da indústria, veja 'O que seria uma internet sem alvo  
anúncios olhar Como'. Agência De Publicidade Interativa Europa. https://iabeurope.eu/knowledgehub/iab-research-what-would-an-internet-without-targeted-ads-look-like/  
  
Formas alternativas de publicidade digital já existem, e provaram ser  
fontes de rendimento eficazes para os fornecedores de conteúdos. Estes modelos alternativos são também com base em mensagens de segmentagem, mas não implicam mostrar anúncios não contextuais que não têm relevância para os consumidores.  
Por exemplo, há modelos em que os consumidores que querem juros  
a publicidade pode auto-relatar que tipo de anúncios gostariam de ver.10 Com tal um modelo, um consumidor poderia indicar o seu interesse em esportes, viagens, música ou mais interesses granulares e receber anúncios que são relevantes para estas questões. Isto poderia ser feito ao nível do navegador, e poderia garantir que os anúncios são relevantes para o consumidor interesses sem depender de vigilância ou rastreamento.  
Outro exemplo de formas alternativas de marketing digital é "contextual"  
publicidade'. A publicidade contextual funciona permitindo que os anunciantes comprem espaço de anúncios em tipos particulares de páginas web ou websites baseados no conteúdo em a página.11 Isto pode ser baseado em palavras-chave para que, por exemplo, anúncios para voos para a Inglaterra são colocados ao lado de artigos sobre futebol inglês. Por outras palavras, publicidade contextual permite aos anunciantes colocar anúncios para tipos particulares de produtos e serviços em contextos onde os anúncios serão exibidos para consumidores interessado em tipos particulares de conteúdo.  
De certa forma, a publicidade contextual pode ser comparada com a publicidade "tradicional".  
Semelhante à forma como o anunciante numa situação de marketing offline compra anúncio espaço numa revista para os entusiastas do motor chegarem a esse segmento de consumo, publicidade contextual permite que os anúncios de alvo do anunciante com base no conteúdo de um site ou serviço em vez de direcioná-los com base nas características do consumidor. Assim, os anunciantes podem chegar a públicos relevantes sem recolher ou agregação de dados pessoais. Isto afasta algumas das mais prementes privacidade questões do marketing, uma vez que diferentes atores na cadeia de fornecimento só precisam saber onde o anúncio é mostrado, não necessariamente quem está vendo isto.12  
Isto também aumenta a transparência e verificação do marketing, uma vez que o próprio anunciante escolhe que tipo de conteúdo ou palavras-chave desencadeiam um anúncio sendo mostrado. Isto significa que muitos visitantes de um determinado site ou app vão ver o mesmo anúncio.  
Experiências de certas editoras mostraram que remover vigilância publicidade em favor de publicidade contextual levou a um aumento  
receitas publicitárias.13

Por exemplo, a emissora holandesa NPO aumentou receitas publicitárias

10 'O que é a Gestão da Relação do Fornecedor?'. Doc Rio Searls.  
https://www.capgemini.com/2015/08/what-is-vendor-relationship-management/  
11 "Para rastrear ou não rastrear? Para publicidade online amiga da privacidade e sustentável".  
Karolina Iwanska. https://en.panoptykon.org/privacy-friendly-advertising  
12 Existem diferentes tipos de publicidade contextual. Alguns destes podem ser parcialmente  
com base no tratamento de dados pessoais e na criação de perfis de utilizador, e pode ser usado para  
contornar a proteção de privacidade percebida. Ao longo deste relatório, usamos o termo  
"publicidade contextual" para se referir a tipos de anúncios contextuais que não dependem do rastreio  
e perfis dos consumidores.  
  
  
até 79% após passar para publicidade contextual.14  
Além disso, quando o The New York Times deixou de servir com base na vigilância publicidade aos utilizadores europeus, as suas receitas publicitárias continuaram a crescer à medida que a sua parceiros de publicidade compraram espaço de anúncios independentemente do alvo capacidades.15 Embora não haja uma resposta definitiva para se estes casos podem ser replicado pela maioria dos editores, aponta para a possibilidade de alternativa modelos de receitas que não dependem da vigilância.  
Uma cadeia de abastecimento mais transparente também reduz os gastos em terceiros, tais como corretores de dados ou ferramentas de verificação, o que significa que anunciantes e editores será deixado com uma maior parte das receitas. Para ilustrar este ponto, um 2020 estudo da indústria descobriu que sob o atual regime de publicidade digital, apenas metade de gastos de publicidade realmente chegou a editores, enquanto 15% do dinheiro estava desaparecido.16

**3.2 Dados de primeira e de terceiros**Existem várias formas de publicidade baseada na vigilância, e o potencial os riscos e os danos que causam podem variar. Algumas formas de vigilância baseadas em vigilância publicidade envolvem a transferência de grandes quantidades de dados pessoais para vários terços partes sem o conhecimento dos consumidores, criando uma privacidade séria e riscos de segurança. Isto aplica-se ao que é tipicamente chamado de publicidade com base em terceiroparty dados.

13 'Pode matar cookies salvar Jornalismo?. Gilad Edelman.  
https://www.wired.com/story/can-killing-cookies-save-journalism/  
Depois do RGPD, o The New York Times cortou as bolsas de anúncios na Europa — e continuou a crescer  
anúncio receitas'. Jessica Davies. https://digiday.com/media/gumgumtest-new-york-timesgdpr-cut-off-ad-exchanges-europe-ad-revenue/  
14 'Atualização (Seis Meses de Dados): lições para aumentar as receitas dos editores através da remoção do 3º  
partido rastreio '. Johnny Ryan. https://brave.com/publisher-3rd-party-tracking/  
15 "Depois do RGPD, o The New York Times cortou as bolsas de anúncios na Europa — e manteve-se  
anúncio de crescimento receitas'. Jessica Davies. https://digiday.com/media/gumgumtest-new-yorktimes-gdpr-cut-off-ad-exchanges-europe-ad-revenue/  
16 ''A' é para o dinheiro anúncio estranhamente desaparecido: Sonda encontra intermediários sifonar metade de  
publicidade online gasta'. Tomás Rio Claburn.  
https://www.theregister.com/2020/05/07/ad\_tech\_fees\_sucked/

A escala de partilha de dados e de atores envolvidos no serviço à vigilância  
a publicidade baseada em dados de terceiros é enorme. Por exemplo, um único anúncio troca pode enviar centenas de biliões de "pedidos de oferta" potencialmente contendo quantidades significativas de dados pessoais para milhares de empresas num dia-a-dia base. Na prática, isto significa que centenas de triliões de pontos de dados são partilhados com um número desconhecido de empresas de terceiros todos os anos no que tem sido  
descrito como "a maior violação de dados alguma vez registada".17

Outras formas de publicidade baseada na vigilância tentam limitar os riscos limitando a partilha de dados com terceiros. Alguns atores, particularmente o grande digital plataformas, utilizem dados pessoais que tenham recolhido junto dos consumidores através da sua serviços próprios.18 Isto pode ser chamado de publicidade com base em dados de primeira parte. O ator que recolhe os dados pessoais muitas vezes terá uma relação direta com o consumidor, por exemplo, no caso em que o operador de uma rede social plataforma ou navegador web recolhe informações sobre os seus utilizadores. Embora alguns poderia argumentar que isso pode ser menos invasivo de uma perspetiva de privacidade, uma vez que menos as empresas podem aceder aos dados, a este tipo de publicidade baseada na vigilância podem implicar riscos graves relacionados, por exemplo, com a manipulação e a discriminação, além de levantar questões antitrust.19  
Embora grandes empresas como o Google e o Facebook muitas vezes dependam de primeira parte dados e partilhar menos dados sobre consumidores com terceiros, este acordo não cura o problema para os consumidores. Perfis intrusivos ainda levantam questões de privacidade, liberdade de escolha e incentivos à manipulação. Como 'digital gatekeepers', estas empresas recolhem dados sobre os consumidores em um grande número de serviços, tanto nas suas próprias plataformas como em toda a web. Para exemplo, um consumidor que usa um dispositivo móvel Android com um navegador Chrome como bem como o Google Maps e o Gmail são rastreados pela Google através destes serviços. Este oferece oportunidades para criar perfis de consumo altamente detalhados.20  
Além disso, em alguns casos, terceiros disfarçam-se como primeiras partes em ordem para contornar as medidas de proteção contra terceiros.21 Esforços de alguma indústria atores para conter o rastreio dos consumidores levou a uma corrida ao armamento por adtech empresas, a fim de evitar ser bloqueado.22

17 "Dois anos depois da denúncia à Comissão Irlandesa de Proteção de Dados, os dados do RTB  
violação é o maior já registado, e parece ter piorado.'. Johnny Ryan.  
https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-ProtectionCommissioner.pdf  
18 No entanto, isto é muitas vezes combinado com dados ou dados de terceiros recolhidos através de terceiro  
plataformas partidárias, por exemplo através de pixels de rastreio. Ver por exemplo 'Perdido por Filtro  
Listas: Deteção DesconhecidoThird-Rastreadores de festas com pixels invisíveis. Imane fouad,  
Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic.  
https://sciendo.com/article/10.2478/popets-2020-0038  
19 'Google's FLoC É um Terrível Ideia:. Bennett Cyphers.  
https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea  
20 'Plataformas online e mercado de publicidade digital estudar'. Concorrência e Mercados  
A autoridade. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-marketstudy  
21 'Facebook para lançar opção de cookie de primeira parte para anúncios, puxar a análise web de Safari'.  
Ginny Marvin. https://marketingland.com/facebook-to-release-first-party-pixel-for-adsweb-analytics-from-browsers-like-safari-249478

Portanto, é crucial olhar para a publicidade baseada na vigilância de um holístico ponto de vista – os riscos e efeitos nocivos da tecnologia não se limitam a publicidade com base em dados de terceiros. Não é tão simples como dados de terceiros sendo um problema e os dados de primeira parte sendo bons.

4 Efeitos nocivos da publicidade baseada na vigilância

Embora a publicidade baseada na vigilância seja por vezes apresentada como uma compensação, onde os consumidores são alegremente expostos à publicidade direcionada em troca de Serviços "gratuitos", esta é uma premissa instável. Enquanto muitos serviços online são apresentado como "livre" para o consumidor, a receita é impulsionada pela venda do consumidor atenção, ilustrado pelo Google gerando USD 40 bilhões em receitas publicitárias no primeiro trimestre de 2021.23  
No entanto, vários estudos indicam que a maioria dos consumidores são  
desconfortável com a recolha de dados pessoais.24 Um levantamento populacional realizada em nome do Conselho Norueguês do Consumidor mostrou que Consumidores noruegueses estão particularmente preocupados com o comércio vigilância.25 Apenas um em cada dez inquiridos foi positivo para o comercial atores que recolhem informações pessoais sobre eles on-line, enquanto apenas um fora cinco pensou que servir anúncios com base em informações pessoais é aceitável.  
Outras pesquisas também indicam que os consumidores muitas vezes não querem publicidade com base em dados pessoais, e um estudo descobriu que apenas 17% dos inquiridos rastreamento on-line visto para fins publicitários para ser ético.26 Mais longe apoiando este ponto, um inquérito de 2021 aos consumidores na Alemanha e em França concluiu que apenas 11% dos inquiridos estavam "bem com [os seus] dados pessoais sendo

22 'The CNAME of the Game: Large-scale Analysis of DNS-based Tracking Evasion'.  
Rio Yana Dimova, Armas AcarLukasz Olejnik, Wouter Rio Joosen, Tom Van Goethem.  
https://petsymposium.org/2021/files/papers/issue3/popets-2021-0053.pdf  
23 "O alfabeto reporta que os grandes ganhos batem à medida que a receita cresce 34%". Jennifer Elias.  
https://www.cnbc.com/2021/04/27/alphabet-goog-earnings-q1-2021.html  
24 Veja, por exemplo,Nordmenn og deling av dados pessoais‘. Norsk Regnesentral.  
https://www.nr.no/sites/default/files/files/NR-Rapport\_Nordmenn-og-deling-avpersondata\_ALerT2019.pdf  
25 «Publicidade baseada na vigilância: Atitudes dos consumidores em relação à vigilância baseadas na vigilância  
publicidade'. Conselho Norueguês do Consumidor. https://fil.forbrukerradet.no/wpcontent/uploads/2021/06/surveilance-marketing-survey.pdf  
26 'O Lado Negro do Cliente Dados:. A RSA. https://www.rsa.com/enus/company/news/the-dark-side-of-customer-data

usado para direcionar [eles] com anúncios'.27 Nos Estados Unidos, uma pesquisa mostrou que quatro em cada cinco consumidores apoiariam a proibição de vigilância baseada em publicidade.28 Em outro indicador de preferências dos consumidores, apenas entre 4% e 6% dos utilizadores optaram por aceitar o tracking depois da Apple ter introduzido um opt-in  
sistema de rastreio de anúncios em aplicativos.29  
Embora a perspetiva de anúncios que monitorizem as suas atividades pode ter um significativo "Fator assustador", muitas das questões problemáticas relacionadas com a vigilância a publicidade é "invisível". Por exemplo, é impossível para os consumidores saber que dados pessoais sobre eles são detidos, como é processado, transferido ou explorado, e por quem. É impossível para o indivíduo saber por que alguns os consumidores estão excluídos de ver certos anúncios ou mensagens. Manipulação é mais eficaz quando os consumidores não sabem se ou como estão sendo manipulado, e muitas vezes não sabem que estão numa situação vulnerável. Em o ambiente digital, cada consumidor é potencialmente vulnerável. Há poucas medidas que os consumidores podem tomar para limitar estes efeitos nocivos, além de abdicando de uma grande quantidade de serviços digitais úteis e importantes.  
Para efeitos deste documento, o Conselho Norueguês do Consumidor analisou um número de efeitos nocivos que são criados ou exacerbados por  
publicidade baseada em vigilância. A falta de transparência no sistema dominante é um problema abrangente e contribui para efeitos nocivos mais fortes relacionados a violações de privacidade, manipulação e discriminação. Estes são significativos questões que não podem ser resolvidas por maior transparência ou melhor informação para os consumidores. Pior ainda, a falta de transparência e controlo para as empresas intervenientes no sistema tem contribuiu para a criação de incentivos financeiros e modelos de negócio para desinformação e fraude em larga escala.  
O marketing baseado na vigilância também tem efeitos nocivos significativos nas empresas atores. Anticoncorrencial comportamento e os efeitos servem para entrincheirar dominante posições dos atores, enquanto cadeias de abastecimento complexas e tecnologias ineficazes lideram a perda de receitas para anunciantes e editores. Todos estes fatores criaram  
uma situação em que os consumidores geralmente têm pouca confiança nos serviços digitais. Falta de confiança significa que a absorção dos consumidores das novas tecnologias abranda. É também difícil para os consumidores para distinguir entre atores 'bons' e 'maus' no esfera digital, o que significa que os atores legítimos, entre eles muitos pequenos e as médias empresas, são diretamente afetadas pelas ações de empresas sem escrúpulos. Isto, por sua vez, prejudica tanto os consumidores como as empresas.

27 "As pessoas realmente querem personalizado anúncios on-line?. Testemunha Global.  
https://www.globalwitness.org/en/blog/do-people-really-want-personalised-ads-online/  
28 'Frequência tecnológica responsável Questionário:. Tecnologia responsável.  
https://accountabletech.org/wp-content/uploads/Accountable-Tech-FrequencyQuestionnaire.pdf  
29 'iOS 14.5 Taxa de opt-in - Atualizações diárias desde Lançamento'. Estelle Laziuk.  
https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparencyworldwide-us-daily-latest-update/

Todas estas questões são explicadas nas seguintes secções.  
**4.1 Falta de transparência**A individualização e personalização da publicidade baseada na vigilância  
significa que diferentes indivíduos vão ver diferentes anúncios com base em um número de fatores como o tempo, o contexto, a demografia, as características pessoais, etc.30 A novo anúncio é servido para cada visita de página, e muitas vezes apenas para alguns indivíduos em certos pontos no tempo. Os anúncios tornam-se 'fugazes', com um curto e limitado tempo de vida.  
A natureza fugaz destes anúncios significa que é muito difícil verificar ou controlar eles, em contraste com o marketing que não se baseia na vigilância. Noutras formas de publicidade, por exemplo, quando um anunciante compra espaço de anúncio diretamente a partir de um editor como um jornal ou emissor de TV, é simples voltar ao meio para controlar o que o anúncio foi impresso ou mostrado em um canal de TV em um tempo particular.  
Sistemas algorítmicos avançados podem tornar-se as chamadas "caixas negras", onde os dados é alimentado na caixa e os resultados são extraídos, enquanto o raciocínio por trás do resultados são opacos. Isto pode obscurecer a base de certas decisões, decisivas fatores e outros aspetos potencialmente problemáticos da tecnologia. Como será detalhado abaixo, isto levou a práticas discriminatórias ocultas. Opacidade também torna difícil para as autoridades de supervisão o levantamento e sanção infrações à lei, que pode ter consequências a jusante para várias violações de direitos que se tornam difíceis ou impossíveis de descobrir.  
A forma dominante de publicidade baseada na vigilância torna-a praticamente impossível para os consumidores entenderem por que lhes foi mostrado um anúncio particular, em que segmento foram colocados, e como os dados pessoais são partilhados e usado. Mesmo que esta informação fosse acessível de qualquer forma significativa, seria ser difícil ou mesmo impossível para os consumidores para fazer usá-lo devido ao complexidade técnica e o âmbito da prática, e porque raramente  
têm uma escolha real.31

30 As nuances e distinção entre individualização e personalização são exploradas  
em "Proteção do Consumidor da UE 2.0: Assimetrias estruturais nos mercados de consumo digitais".  
Natali HelbergerOrla Lynskey, Hans-W. MicklitzPedro Rott, Marijn Sax, Joanna  
StrycharzP. 94. https://www.beuc.eu/publications/beuc-x-2021...  
018\_eu\_consumer\_protection.0\_0.pdf  
31 '10 Razões por que a publicidade online é Quebrado'. Karolina Iwańska.  
https://medium.com/@ka.iwanska/10-reasons-why-online-advertising-is-brokend152308f50ec

Como é que a falta de transparência será resolvida através de uma proibição?  
Uma proibição contra a publicidade baseada na vigilância iria livrar-se de anúncios que são direcionadas e colocadas com base em dados sobre consumidores individuais. Se isto aconteceu, seria mais fácil pesquisar e controlar os anúncios, uma vez que não mais tempo ser individualizado e fugaz. Plataformas de anúncios ou plataformas de redes sociais poderia, por exemplo, estabelecer mais facilmente registos de todos os anúncios que exibem, tornando mais fácil controlar o conteúdo e garantir que a segmentagem contextual não é usado de forma inadequada para explorar vulnerabilidades dos consumidores.32 Isto contribuiria para aplicação mais eficaz contra práticas comerciais desleais, privacidade violações, e muito mais.  
**4.2 Violações da privacidade e proteção de dados**A fim de adaptar o marketing a indivíduos ou grupos, e exibir 'o anúncio certo para a pessoa certa', um grande número de empresas recolhem e processam vasta quantidades de informação sobre consumidores individuais. Dados sobre nós são processados cada vez que usamos uma app, visitamos um site, fazemos compras numa loja ou nos movemos em espaços públicos (por exemplo. através Wi-Fi rastreio).  
No início de 2020, o Conselho Norueguês do Consumidor publicou o relatório Fora de Controlo em que revelou como um grande número de empresas recolher, usar e partilhar dados pessoais sobre os consumidores sempre que visitam aplicativos e websites.33 Esta informação é agregada, muitas vezes por ambos os proprietários de o site/app e vários terceiros. Os dados são utilizados para fins relacionados para marketing e serviços personalizados, mas também pode ser usado (inadvertidamente ou  
não) para fins de discriminação, exclusão e manipulação.  
Os consumidores são constantemente manipulados para aceitar um rastreio abrangente através comportamental técnicas ou características de design obfuscados ('escuro padrões'),34 forçados a sistemas de vigilância comercial, a fim de aceder serviços necessários35, e são geralmente expostos à recolha de dados sem a sua conhecimento e consentimento (válido). A enorme quantidade de dados também significa que tentativas de pseudónimo ou anonimização da informação têm provado  
ineficaz.36

O âmbito da recolha e partilha de dados é tão vasto que se torna praticamente impossível saber como os dados pessoais podem ser usados. Como consequência, no contexto de publicidade baseada em vigilância, torna-se difícil de exercer direitos fundamentais previstos na Carta dos Direitos Fundamentais da EU (Carta) e elaborado no Regulamento Geral de Proteção de Dados (RGPD), incluindo os direitos a ser informado, ter acesso, retificar e eliminar dados ou para contestar decisões que afetam as nossas vidas.

32 Esses registos de anúncios teriam de evitar uma série de armadilhas para serem úteis. Ver  
por exemplo, 'Arquivos de anúncios de plataforma: promessas e armadilhas'. Paddy Rio Leerssen, Rio Jef Rio Ausloos,  
Rio Brahim ZaroualiNatali HelbergerClaes H. de Vreese.  
https://policyreview.info/articles/analysis/platform-ad-archives-promises-and-pitfalls  
33 'Fora de Controlo:. Forbrukerrådet. https://www.forbrukerradet.no/out-of-control/  
34 'Escuro Padrões'. Forbrukerrådet. https://www.forbrukerradet.no/dark-patterns/  
35 ‘Offentlige nettsteder esporer oss‘. Teknologirådet. https://teknologiradet.no/offentligenettsteder-sporer-oss/  
  
  
Como é que o risco de violações da privacidade e proteção de dados será resolvido por um proibição?  
Os riscos da publicidade baseada na vigilância para a privacidade e proteção de dados são já amplamente regulado na Europa através do ePrivacy Diretiva e RGPD. Após a entrada em aplicação do RGPD em 2018, execução da lei tem sido, infelizmente, lento e em alguns casos inexistente, com estrangulamentos significativos na aplicação transfronteiriça. Simultaneamente, lá é pouca indicação de que a proliferação da economia de vigilância tem abrandado para baixo, apesar da regulação mais forte. Isto resultou numa fronteira transfronteiriça lacuna de execução que precisa de ser urgentemente abordada.37  
Uma proibição geral da publicidade baseada na vigilância seria positiva para e complementar os direitos fundamentais à privacidade e proteção de dados pessoais que estão protegidos ao abrigo da Carta, do RGPD e do ePrivacy A diretiva. Apesar da introdução do RGPD, muitos intervenientes na economia de vigilância têm operado em grande parte sob o pretexto de negócios como de costume, embora tenhamos observou que alguns atores introduziram mudanças relativamente menores na forma como pedem consentimento para o tratamento de dados pessoais. Outros simplesmente tentaram passar para uma base legal diferente para o tratamento de dados.38  
O fosso de aplicação transfronteiriça do RGPD e o surgimento de novos desafios que vão além da proteção de dados pessoais têm demonstrado que há uma necessidade para uma abordagem mais sistémica e preventiva, e uma proibição geral pode forçar transformação estrutural abrangente de modelos de negócio de vigilância.

36 ‘Oráculo BlueKai rastreia-o através da web. Que os dados derramados online'. Zack Whittaker.  
https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/  
37 A lacuna de execução do RGPD é descrita em detalhe em "The Long and Winding Road:  
Dois anos do RGPD: Um processo transfronteiriço de aplicação da proteção de dados a partir de um  
consumidor perspectiva'. O BEUC. https://www.beuc.eu/publications/beuc-x-2020...  
074\_two\_years\_of\_the\_gdpr\_a\_crossborder\_data\_protection\_enforcement\_case\_from\_a\_consumer\_perspective.pdf  
38 'Desvio do RGPD do Facebook atinge Supremo austríaco Tribunal.. Noyb.  
https://noyb.eu/en/facebooks-gdpr-bypass-reaches-austrian-supreme-court  
  
Como complemento a uma proibição, é necessário reforçar a aplicação da lei autoridades e procedimentos, tanto no RGPD como ePrivacy Diretiva (ou uma nova ePrivacy Regulamento que substituirá a diretiva39), e no próximo Digital Lei dos Serviços.

**4.3 Manipulação**O aumento do marketing baseado na vigilância contribuiu para a tentativa  
manipulação de indivíduos e grupos numa escala sem precedentes. Empresas na posse de grandes quantidades de dados podem usar sistemas algorítmicos em tentativas para decidir quando os indivíduos são mais suscetíveis a comportar-se de determinadas maneiras ou a reagem a imagens, sons ou mensagens particulares.  
Isto pode implicar, por exemplo, que os consumidores estão expostos a anúncios de beleza ou produtos diet quando a sua auto-confiança é baixa40 ou que os anúncios de jogo são direcionados para os consumidores que lutam contra os vícios.41 Estas questões são exacerbada pela proliferação da comercialização de produtos e serviços nocivos para as crianças.42 A automatização torna o processo ainda mais opaco, e o otimização de mensagens pode ter efeitos negativos se não ético e prejudicial no entanto, métodos eficazes são automatizados.  
A publicidade pode explorar as vulnerabilidades dos consumidores mesmo sem observar diretamente as referidas vulnerabilidades. Por exemplo, através da utilização do chamado 'sósia públicos', os anunciantes podem duplicar grupos de consumidores com certos características, a fim de chegar a novos consumidores que partilham o mesmo características.43 Desta forma, a publicidade para os produtos farmacêuticos pode, por exemplo, ser mostrado a grupos de consumidores que têm características em comum com outros consumidores com doenças semelhantes, mesmo que o anunciante não tenha informação que indique diretamente o estado de saúde destes consumidores.44  
Do mesmo modo, esta forma de orientação tem sido associada à radicalização.45  
Através da publicidade baseada na vigilância, todos os consumidores ficam vulneráveis por defeito; em teoria podemos ser alvo nos nossos momentos mais vulneráveis em a fim de otimizar os efeitos do marketing.46

39 "Moldar o Futuro Digital da Europa. Proposta de proposta ePrivacy Regulamento:. Europeu  
A comissão. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation  
40 Facebook disse aos anunciantes que pode identificar adolescentes que se sentem "inseguros" e"inútil"..  
Sam Levin. https://www.theguardian.com/technology/2017/may/01/facebook-advertisingdata-insecure-teens  
41 'O que uma app de jogo sabe sobre Você.. Adam Satariano.  
https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking.html  
42 'Facebook permite que anunciantes direcionem crianças interessadas em fumar, álcool e  
peso perda'. Josh Taylor.  
https://www.theguardian.com/technology/2021/apr/28/facebook-allows-advertisers-totarget-children-interested-in-smoking-alcohol-and-weight-loss  
43 'Sobre Sósia Audiências. No Facebook.  
https://www.facebook.com/business/help/164749007013531?id=401668390442328

O bombardeamento constante de publicidade em espaços digitais também serve para quebrar enraizado defesas contra a persuasão e manipulação.47 Isto torna-se particularmente prejudicial quando crianças e outros grupos especialmente suscetíveis são submetidos a manipulação  
e comercialização extrema.48  
Como é que o risco de manipulação será resolvido através de uma proibição?  
A proibição geral da publicidade baseada na vigilância não resolverá todas as questões relacionadas para o marketing manipulador, uma vez que todo o marketing pode potencialmente ser usado para manipular os consumidores. Apesar disso, a proibição da publicidade baseada na vigilância contribuirá para acabar com os anúncios individualizados que são otimizados para chegar aos consumidores em situações vulneráveis, bem como mitigar os efeitos de "vulnerabilidade por padrão" em curso criada através da aplicação de constantemente perfis de persuasão melhorados.  
Manipulação que acontece através de outras formas de publicidade, como o conteúdo marketing49, deve ser resolvido através de meios que não a proibição de vigilância publicidade, como por exemplo através de disposições na Lei dos Serviços Digitais50 e um diretiva relativa às práticas comerciais desleais revistas.

44 'How Big Pharma Finds Sick Users in Facebook'. Colin Lecher.  
https://themarkup.org/citizen-browser/2021/05/06/how-big-pharma-finds-sick-users-onfacebook  
45 "Apesar da proibição, o Facebook continuou a rotular as pessoas como interessadas em milícias para  
Anunciantes. Ryan Mac. https://www.buzzfeednews.com/article/ryanmac/facebookmilitia-interest-category-advertisers-ban  
46 Para obter mais informações sobre a necessidade de novas e atualizadas conceções de vulnerabilidade do consumidor, consulte  
"Proteção do Consumidor da UE 2.0: Assimetrias estruturais no consumidor digital mercados'.  
Natali HelbergerOrla Lynskey, Hans-W. MicklitzPedro Rott, Marijn Sax, Joanna  
Strycharz. https://www.beuc.eu/publications/beuc-x-2021...  
018\_eu\_consumer\_protection.0\_0.pdf  
47 'WTF é padrão escuro design?. Natasha Lomas. https://techcrunch.com/2018/07/01/wtfis-dark-pattern-design/  
48 Para mais informações sobre os efeitos adversos do marketing digital nas crianças, consulte 'Big Food, Big  
Tecnologia e a Obesidade Infantil Global Pandemia. Jeff Chester, Kathryn C.  
Montgomery, Katharina Kopp. https://www.democraticmedia.org/article/big-food-bigtech-and-global-childhood-obesity-pandemic  
49 O marketing de conteúdos inclui conteúdo patrocinado em jornais online, influência  
marketing, e outros conteúdos promocionais pagos.  
50 'A Proposta de Lei dos Serviços Digitais - Posição BEUC Papel.. O BEUC.  
https://www.beuc.eu/publications/beuc-x-2021...  
032\_the\_digital\_services\_act\_proposal.pdf  
  
**4.4 Discriminação**  
Além de criar novas oportunidades para alcançar "a pessoa certa",  
a publicidade baseada na vigilância cria novas oportunidades para excluir e  
discriminar indivíduos e grupos.51 A automatização da publicidade permite isto numa escala crescente. Por exemplo, a Amnistia Internacional tem descreveu o modelo de negócio baseado na vigilância de empresas como o Google e Facebook como uma ameaça a uma série de direitos humanos fundamentais, incluindo liberdade de expressão e o direito à não discriminação, devido à forma como o modelo de negócio de vigilância cria efeitos arrepiantes e classifica indivíduos em grupos para fins de segmentagem.52  
Segmentação e segmentação podem ser usadas para não exibir certos anúncios a particular pessoas ou grupos de consumidores. Por exemplo, os anunciantes podem escolher mostrar anúncios de habitação apenas para pessoas que se encaixam no seu perfil ideal para indivíduos que querem  
ter vivido em um certo bairro e excluir indivíduos "indesejáveis" que, no entanto, pode ser capaz de se dar ao luxo de viver lá. Da mesma forma, potencial os empregadores podem escolher que tipo de pessoas são mostradas certas listas de emprego, que pode, por exemplo, excluir potenciais candidatos femininos, quer deliberadamente ou através da discriminação algorítmica.53 Na verdade, tais escolhas serão necessariamente excluir alguns indivíduos ou grupos.54 Isto é exacerbado pelo nível de opacidade e a impossibilidade de saber quem está a ver o anúncio.  
É impossível para os consumidores saber que anúncio de emprego ou habitação são não ver. Enquanto o marketing tradicional pode ser observado olhando para o conteúdo e análise em retrospetiva, isto é muitas vezes inviável se o anúncio era apenas mostrado a um determinado consumidor ou grupo num determinado momento. Se discriminação está acontecendo como parte de processos algorítmicos automatizados, torna-se muito difícil de descobrir e remediar a questão. Assim, vigilância a publicidade pode contribuir para obscurecer discriminação ou exclusividade práticas porque as questões problemáticas acontecem dentro da 'caixa preta'. Este mina o direito à não discriminação, que é um ser humano fundamental Certo.

51 Para uma análise detalhada da discriminação na publicidade baseada em vigilância, consulte 'Como  
anúncios online discriminam'. Frederike Rio Kaltheuner. https://edri.org/our-work/how-online-adsdiscriminate/  
52 "A vigilância generalizada do Facebook e do Google representa um perigo sem precedentes para  
humano direitos'. Amnistia Internacional.  
https://www.amnesty.org/en/latest/news/2019/11/google-facebook-surveillance-privacy/  
53 'Os algoritmos de anúncio do Facebook ainda estão excluindo as mulheres de ver empregos '. Karen Hao.  
https://www.technologyreview.com/2021/04/09/1022217/facebook-ad-algorithm-sexdiscrimination/  
54 'Anúncios de cartão de crédito foram alvo por idade, violando a anti-discriminação do Facebook  
Política'. Rio Corin Rio Faife e Alfred Ng. https://themarkup.org/citizenbrowser/2021/04/29/credit-card-ads-were-targeted-by-age-violating-facebooks-antidiscrimination-policy

Estas formas de discriminação e exclusão não se devem necessariamente a  
ato deliberado de malícia por parte do anunciante; algoritmos otimizando o  
os anúncios podem estar automaticamente a facilitar práticas problemáticas.55 Isto pode levar a discriminação automatizada, por exemplo, fazendo da geolocalização um proxy para atributos protegidos, tais como a etnia, a orientação sexual ou as crenças religiosas, porque os modelos estatísticos mostram que alguns grupos de pessoas têm sobreposição atributos.56  
Por outras palavras, mesmo que um sistema explicitamente proibido direcione os consumidores com base sobre crenças religiosas, o facto de que um indivíduo visita regularmente a geolocalização de uma mesquita ou usa uma certa aplicação de oração pode ser usado como um representante para o atributo "Muçulmano".57 Este tipo de automatização corre continuamente o risco de criar um novo proxy atributos à medida que o sistema evolui e decide quais os indivíduos que devem ver o que anúncios.  
A segmentação dos grupos de consumidores pode igualmente conduzir a preços individualizados de bens e serviços. Esta forma de discriminação de preços pode levar a injustiças diferenciação entre consumidores, dificultar a comparação de preços, e fazer os consumidores relutantes em comparar preços, porque pode afetar a final preço do produto ou serviço.58  
Como é que as práticas discriminatórias seriam resolvidas com uma proibição?  
Uma proibição geral da publicidade baseada na vigilância facilitaria o levantamento e sancionar práticas de marketing discriminatórias e de exclusão. Isto seria contribuir para um mercado publicitário onde as práticas discriminatórias são mais efetivamente sancionado, o que ajudaria a proteger o fundamental dos consumidores direitos.59

55 'Discriminação através da otimização: Como a entrega de anúncios do Facebook pode levar a distorções  
resultados '. Muhammad Ali Sapiezynski, Miranda Rio Bogen, Aleksandra Korolova,  
Rio Alan Mal-amado e Aaron Rieke. https://arxiv.org/abs/1904.02095  
56 'Facebook (Ainda) Deixar os Anunciantes de Habitação excluir utilizadores por Raça'. Julia Angwin,  
Ariana Tobin e Madeleine Varner. https://www.propublica.org/article/facebookadvertising-discrimination-housing-race-sex-national-origin  
57 'Dados de localização vazados mostra outro rastreio de aplicativo de oração muçulmano Utilizadores. José  
Cox, cox. https://www.vice.com/en/article/xgz4n3/muslim-app-location-data-salaat-first  
58 'Monstros de cookies: por que o seu histórico de navegação pode significar roubo preços'. Rio Arwa  
O Mahdavi. https://www.theguardian.com/commentisfree/2016/dec/06/cookie-monsterswhy-your-browsing-history-could-mean-rip-off-prices  
59 A fim de restringir práticas discriminatórias através de atributos de procuração, restrições  
quais categorias ou segmentos que possam ser utilizados no marketing devem ser considerados. Para  
exemplo, marketing a grupos baseados em fatores de saúde assumidos, ou com base em granular  
geolocalização pode ser banido.

**4.5 Desinformação**  
A falta de transparência em grande parte da publicidade baseada na vigilância indústria significa que muitos anunciantes não sabem onde os seus anúncios estão sendo exibido. Isto cria danos reputacionais para marcas e anunciantes, uma vez que eles perder o controlo sobre se os seus anúncios são exibidos em conjunto com desinformação ou conteúdo problemático.  
O risco de danos reputacionais levou a algumas categorias de websites ou  
palavras-chave sendo 'lista negra', que criou novas questões para conteúdo sério produtores e editores.60 Por exemplo, isto causou grandes problemas e vasto perdas de receitas para muitos editores quando um número de anunciantes não desejava para colocar os seus anúncios em sites que escrevem sobre COVID-19.61 Práticas semelhantes têm editores danificados criando conteúdo para minorias e potencialmente vulnerável grupos, por exemplo, através de palavras-chave relacionadas com a lista negra LGBTQ+.62  
Isto envolve dinheiro sendo desviado de editores respeitáveis em favor de menos fontes respeitáveis. Consequentemente, o conteúdo de baixa qualidade é incentivado, criando oportunidades de fraude e fraudes.  
Conteúdo controverso foi provado para criar um alto grau de envolvimento, levando muitas pessoas a clicar em links para artigos ou conteúdo que são enganosos ou manifestamente falso.63 Isto leva a receitas publicitárias para os atores que criam e espalhando tal desinformação, o que significa que a publicidade baseada na vigilância oferece incentivos financeiros para criar tal conteúdo.64 O uso de vigilância publicidade é um, não o único, modelo de negócio incentivando o criação e difusão de desinformação online.65 Além disso, a tecnologia por trás da publicidade baseada na vigilância pode ser usado para espalhar desinformação, com efeitos potencialmente devastadores sobre os indivíduos e a sociedade.66

60 "O futuro do marketing baseado em dados". Federação Mundial de Anunciantes.  
https://wfanet.org/knowledge/item/2021/03/10/WFA-report-The-future-of-data-drivenmarketing  
61 'Covid-19 aquece a corrida para combater o bloqueio da palavra-chave da publicidade problema '.  
Rebecca Stewart. https://www.thedrum.com/news/2020/04/30/covid-19-heats-up-therace-combat-advertising-s-keyword-blocking-problem  
62 'Vice bate listas negras de palavras-chave de segurança da marca após alarmar sonda'. Oliver McAteer.  
https://www.campaignlive.com/article/vice-slams-brand-safety-keyword-blacklistsalarming-probe/1495610  
63 O Índice de Desinformação. https://disinformationindex.org/  
64 Os anúncios direcionados são uma das tendências mais destrutivas do mundo. Aqui está. por que'. Rio Arwa  
O Mahdavi. https://www.theguardian.com/world/2019/nov/05/targeted-ads-fake-newsclickbait-surveillance-capitalism-data-mining-democracy  
65 "Como o Adtech Mercado incentiva o lucro Desinformação.. Joshua Braun.  
https://promarket.org/how-the-adtech-market-incentivizes-profit-driven-disinformation/  
66 O Facebook disse que deixaria de recomendar grupos anti-vacinas. Não é assim. Rio Corin  
Rio Faife e Dara Kerr. https://themarkup.org/citizen-browser/2021/05/20/facebook-said-it-ould-stop-recommending-anti-vacina-grupos-it-não

Como é que a prevalência da desinformação online será resolvida através de uma proibição?  
A proibição da publicidade baseada na vigilância não será um remédio perfeito para o prevalência de desinformação online. No entanto, uma proibição geral irá perturbar o modelos de negócio de um grande número de websites e outros atores que criam e espalhar desinformação.  
Uma cadeia de fornecimento mais transparente vai facilitar a conhecer os anunciantes onde os seus anúncios são exibidos. Isto significa que as marcas podem ter mais controlo sobre se os seus anúncios são usados para financiar a desinformação. Uma proibição deve no entanto, ser complementado por uma aplicação consistente e forte dos dados proteção, concorrência e direito do consumidor.67

**4.6 Efeitos anticoncorrenciais**No modelo de publicidade baseado na vigilância, alguns atores podem obter vantagens competitivas através da recolha de dados de todos os websites e serviços.68  
A crescente concentração do mercado da publicidade digital está a diminuir  
valor dos dados de primeira parte dos editores e criação de uma corrida até ao fundo. Em prática, adtech empresas podem recolher dados sobre consumidores em um site (por exemplo, um jornal online), combiná-lo com os dados que têm sobre esse utilizador dentro dos seus próprios serviços (por exemplo, redes sociais) e, em seguida, usar os dados para direcionar anúncios para os consumidores em outros sites que oferecem um preço mais baixo para anúncio colocações.69  
Mesmo que as receitas de anúncios da publicidade baseada em vigilância tenham crescido durante nos últimos anos, a maior parte das receitas foram para apenas algumas plataformas.70  
Plataformas como o Google e o Facebook são estimadas para cerca de dois terços do mercado de anúncios digitais nos Estados Unidos71 e cerca de   
67 'Qual é a ligação entre comportamental publicidade e fake news?'. O BEUC.  
https://www.beuc.eu/publications/beuc-x-2018...  
036\_what\_is\_the\_relation\_between\_behavioural\_advertising\_and\_fake\_news.pdf  
68 'Google stymies media companies from chiping away at his data domínio'. Rio Paresh  
O Dave. https://www.reuters.com/article/tech-antitrust-google-idINKBN2410ZD  
69 'Péssimos anúncios estão arruinando o online experiência'. Walt Mossberg.  
https://www.theverge.com/2017/1/18/14304276/walt-mossberg-online-ads-bad-business  
70 "O domínio digital do anúncio digital da Google está a prejudicar marketers e editores, diz novo estudar'.  
Ad Age. https://adage.com/article/digital/googles-digital-ad-dominance-harmingmarketers-and-publishers-says-new-study/2257576  
71 'Google, Facebook e Amazon serão responsáveis por quase dois terços do total de anúncios digitais dos EUA  
gastando este ano'. Mariel Soto Reyes. https://www.businessinsider.com/googlefacebook-amazon-were-biggest-ad-revenue-winners-this-year-2020-12  
  
 80% no Reino Unido.72 Isto significa que o dinheiro foi transferido para longe dos editores e potenciais concorrentes.  
Os atores dominantes podem abusar das suas posições no mercado da publicidade digital dando preferência aos seus próprios serviços.73 Por exemplo, o Google controla muitos aspetos da cadeia de valor, e funciona como um comprador, vendedor e mercado.74 Se o Google manipular as suas ferramentas para favor seu próprio anúncio on-line serviços e para sufocar a concorrência de tecnologias rivais, estes efeitos anticoncorrenciais não só prejudicariam potenciais concorrentes, mas também levariam a menos escolha e preços mais elevados para os consumidores.75  
Estes efeitos anticoncorrenciais podem ser ainda mais entrincheirados se o dominante as plataformas afastam-se da utilização e permitem a recolha de dados de terceiros.  
Mesmo que tais medidas limitassem o número de atores que podem aceder a pessoas dados, o que seria positivo do ponto de vista da privacidade, também pode contribuir para um pequeno número de atores dominantes mais entrincheirando a sua posição como porteiros.76  
Na situação de hoje, é difícil para modelos de negócio alternativos do digital  
publicidade para competir com os atores dominantes. Isto tem muitas causas, incluindo os efeitos da rede, anticoncorrencial comportamento de jogadores dominantes,77 e porque a maioria dos anunciantes já dependem de publicidade baseada em vigilância como o seu principal fluxo de receitas para conteúdos gratuitos.78 Além disso, muitos técnicos soluções ligadas a soluções publicitárias baseadas em vigilância podem ser incompatíveis  
com modelos que não dependem do tratamento de dados pessoais.  
Como é que os efeitos anticoncorrenciais serão resolvidos através de uma proibição?

72 "Plataformas online e estudo do mercado da publicidade digital". Concorrência e Mercados  
A autoridade. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-marketstudy#final-report  
73 'Algoritmos: Como podem reduzir a concorrência e prejudicar consumidores'. Competição e  
Autoridade dos Mercados. https://www.gov.uk/government/publications/algorithms-how-theycan-reduce-competition-and-harm-consumers  
74 "Falta de concorrência na tecnologia de publicidade que afeta editores, anunciantes e consumidores'.  
Comissão Australiana da Concorrência e do Consumidor. https://www.accc.gov.au/mediarelease/lack-of-competition-in...ad-tech-affecting-editores-anunciantes-e-consumidores  
75 Em 2021, a autoridade da concorrência francesa multou o Google em 220 euros por promover a sua própria  
serviços de publicidade sobre os seus rivais. .' Google multado em 220 milhões de euros em França por publicidade  
abuso'. Simon Read. https://www.bbc.com/news/business-57383867  
76 '4 Grandes Perguntas sobre a nova privacidade da Google posição'. Johnny Ryan.  
https://www.iccl.ie/digital-data/4-big-questions-about-googles-new-privacy-position/  
77 "As práticas publicitárias da Google visadas pela antitrust da UE sonda'. EURACTIV.  
https://www.euractiv.com/section/digital/news/googles-advertising-practices-targeted-byeu-antitrust-probe/  
78 'Receitas de Rastreio Online e Editores': Um Empírico Análise:. Veronica Marotta,  
Rio Vibhanshu Abhishek e Alessandro. Aquista. https://weis2019.econinfosec.org/wpcontent/uploads/sites/6/2019/05/WEIS\_2019\_paper\_38.pdf

Uma proibição geral da publicidade baseada na vigilância poderia contribuir para nivelar o campo de jogo entre editores e plataformas dominantes, o que seria estimular um mercado melhor competitivo para a publicidade. No entanto, o dominante as posições do Facebook e do Google também devem ser abordadas por outros meios, nomeadamente através da aplicação da regulamentação antitrust. Qualquer regulação intervenção deve ser complementada com a aplicação do direito da concorrência em  
o nível de acordos anticoncorrenciais (por exemplo, entre diferentes intervenientes no cadeia de fornecimento de publicidade) e para evitar o abuso de posições dominantes.  
A proibição da publicidade baseada na vigilância também poderia servir os consumidores contribuindo para uma maior liberdade de escolha e pluralidade dos meios de comunicação, e leigos o terreno para a nova inovação.

**4.7 Fraude e perda de receitas**Embora os defensores da publicidade baseada em vigilância, às vezes touts o capacidade de medir a eficiência dos anúncios, tais medições não são necessariamente preciso. Fraude de anúncios é um problema generalizado em toda a indústria, que tem sido mostrado para inflacionar fortemente o número de visualizações de anúncios e cliques. A automação e escala do marketing, eo número absoluto de intermediários, significa que há muito pouca transparência em torno de onde os anúncios são mostrados, quantos consumidores são realmente exposto aos anúncios, e onde o dinheiro gasto acaba.79  
Esta falta de controlo também significa que os consumidores podem facilmente ser expostos a fraudes e fraudes através de anúncios direcionados.80 Isto leva a que os consumidores sejam prejudicados,  
financeiramente e de outra forma, e para danos reputacionais para editores que terminam se hospedar anúncios criminais.81  
A complicada rede de atores na publicidade baseada na vigilância  
indústria tem levado a muitos anunciantes e editores tendo uma visão geral limitada de para onde vai o seu gasto de anúncios, o que, por sua vez, gerou uma grande indústria baseada sobre fraude de anúncios.82 Este tipo de fraude é comumente cometido por ter anúncios mostrados para bots em vez de seres humanos, o que por sua vez reduz o preço que os editores podem reivindicação para o espaço de anúncios e faz os anunciantes pagar por anúncios que nenhum consumidor é

79 'Ad Tech pode ser a próxima bolha da Internet'. Gilad Edelman.  
https://www.wired.com/story/ad-tech-could-be-the-next-internet-bubble/  
80 'Anúncios falsos; problemas reais: como é fácil publicar anúncios fraudulentos no Facebook e  
Google?. Andrew Laughlin. https://www.which.co.uk/news/2020/07/fake-ads-realproblems-how-easy-is-it-to-post-scam-adverts-on-google-and-facebook/  
81 'AI & Publicidade, um consumidor perspectiva'. Rio Harriet Kingaby.  
https://www.harrietkingaby.com/reports  
82 'Relatório: Fraude de anúncios para atingir 23 biliões de dólares, não vai para baixo '. George P. Slefo.  
https://adage.com/article/digital/report-ad-fraud-hit-23-bilhões-não vai descer/2174721

realmente ver.83 Por outras palavras, os atores legítimos acabam por pagar pela publicidade. que nunca atinge uma audiência em tudo.  
O uso de intermediários levou a grandes quantidades de receitas publicitárias indo para terceiros.84 Isto significa, por exemplo, que o dinheiro que de outra forma ter chegado a um jornal local está sendo engolido por atores de terceiros, e em alguns casos, não pode ser rastreado.85 Isto deu origem a perguntas sobre se a publicidade baseada na vigilância é financeiramente sustentável para editores.86  
O aumento da fraude de anúncios levou ao surgimento de um grande mercado de fraude ferramentas de deteção. Esta é a tecnologia que é usada para verificar que os anúncios têm sido mostrado aos seres humanos reais. Há diferentes maneiras de fazer isso, mas estes os métodos envolvem frequentemente a recolha de mais informação sobre os consumidores.87 O  
desenvolvimento de tais ferramentas é uma corrida de armas constante contra os burlões, que leva a custos acrescidos para anunciantes e a novas violações de privacidade contra consumidores.  
Ferramentas semelhantes também são usadas para rastrear o número de anúncios mostrados para determinar o que o anunciante tem que pagar pela colocação de anúncios. Estes números foram mostrados para ser impreciso ou totalmente falso, o que pode ter graves consequências para  
empresas.88 Outras ferramentas que se destinam a prevenir a fraude de anúncios e fornecer os anunciantes com segurança também foram encontrados com falhas significativas.89 O lutar contra a fraude de anúncios tornou-se uma espiral negativa onde os anunciantes, como bem como editores e consumidores, são todos perdedores.  
Como é que as questões relacionadas com a fraude serão resolvidas através de uma proibição?

83 "O paradoxo custo-desempenho do marketing digital moderno". Agostinho Fou.  
https://www.forbes.com/sites/augustinefou/2020/08/18/the-cost-performance-paradox-ofmodern-digital-marketing/  
84 No Digital, 'Wanamaker's 50%' é conhecido. Também é pior do que isso..'. Agostinho Fou.  
https://www.forbes.com/sites/augustinefou/2020/12/19/in-digital-wanamakers-50-isknown-its-also-worse-than-that/  
85 "Tempo para mudança e transparência em programática publicidade'. O ISBA.  
https://www.isba.org.uk/article/time-change-and-transparency-programmatic-advertising  
86 'Anúncio comportamental direcionado para não pagar para editores, estudo Sugere:. Rio Keach  
Rio Hagey. https://www.wsj.com/articles/behavioral-ad-targeting-not-paying-off-forpublishers-study-suggests-11559167195  
87 Por exemplo, o corretor de dados Tamoco alega usar dados de localização para detetar fraude de anúncios.  
O que é fraude de anúncios? Como os dados de localização podem detetar anúncios Fraude. Tamoco.  
https://www.tamoco.com/blog/location-digital-ad-fraud-detection/  
88 "O Facebook sabia há anos que as estimativas de alcance de anúncios eram baseadas em "dados errados", mas bloqueadas  
correções sobre o impacto da receita, por tribunal arquivamento'. Natasha Lomas.  
https://techcrunch.com/2021/02/18/facebook-knew-for-years-ad-reach-estimates-werebased-on-wrong-data-but-blocked-fixes-over-revenue-impact-per-court-filing/  
89 'Breitbart.com é parceria com RT.com & Outros Sites via Publicidade Mal-Rotulada  
Inventário'. Zach Edwards. https://medium.com/@thezedwards/breitbart-com-ispartnering-with-rt-com-other-sites-via-mislabeled-advertising-inventory-6e7e3b5c3318  
  
Uma proibição geral da publicidade baseada na vigilância levaria a mais  
transparência na cadeia de abastecimento e, provavelmente, reduzir a quantidade de fraude de anúncios. Este por sua vez diminuiria a necessidade de instrumentos de deteção de fraude dispendiosos e invasivos, que seria uma bênção para as linhas de fundo dos editores e anunciantes, bem como para privacidade e segurança do consumidor. A proibição deve ser complementada por outros medidas para reduzir a fraude, tais como obrigações para os mercados online para verificar legitimidade dos comerciantes, tal como proposto na Lei dos Serviços Digitais.

**4.8 Riscos de segurança**  
Como muitos sistemas usados na publicidade baseada em vigilância envolvem dados sendo compartilhado e espalhado entre potencialmente milhares de atores, há um risco significativo que pelo menos um destes atores aproveita a oportunidade de vender ou partilhar conjuntos de dados para outras empresas que têm modelos de negócio fora de publicidade.90  
Nestes sistemas, não há distinção real entre consumidores "regulares" e  
indivíduos em papéis críticos. Por exemplo, a emissora pública norueguesa NRK revelou como os dados pessoais recolhidos de aplicações populares poderiam ser usados para rastrear o movimento de militares.91 Num relatório de 2021, a NATO anunciou que esta forma de recolha e partilha de dados pessoais constitui uma séria ameaça à segurança nacional.92  
A recolha e armazenamento de informação também criam um risco de dados pessoais ser espalhado como resultado de hackeamento ou violação de dados. Isto significa que os criminosos pode ser capaz de aceder a informações que podem ser usadas para roubo de identidade, fraude, e  
fins de chantagem. Os dados que foram vazados também podem ser mal utilizados para identificar, rastrear e prejudicar indivíduos e grupos vulneráveis93 ou em tentativas de influenciar ou interferir nas eleições democráticas.

90 ‘Telefonen spionerte på Meg. Slik fant jeg overvåkerne‘. Martin Gundersen.  
https://nrkbeta.no/2020/12/03/telefonen-spionerte-pa-meg-slik-fant-jeg-overvakerne/  
91 ‘Når mobilen blir fienden‘. Martin Gundersen, Øyvind Adeus Habilidade, Henrik Lied, Mari  
GrafsrønningenHarald K.Jansson. https://www.nrk.no/norge/xl/norske-offiserer-ogsoldater-avslort-av-mobilen-1.14890424  
92 'Corretores de dados e Segurança:. NATO STRATCOM.  
https://stratcomcoe.org/publications/data-brokers-and-security/17  
93 A polícia egípcia está a usar o Grindr para encontrar e prender pessoas LGBT. Matt Payton.  
https://www.independent.co.uk/news/world/africa/egyptian-police-grindr-dating-apparrest-lgbt-gay-anti-gay-lesbian-homophobia-a7211881.html

Além de violações de dados que conduzem a riscos de segurança, a publicidade digital tem tornar-se um vetor para a propagação de código malicioso, como malware ou vírus.94 Isto significa que alguns banners de publicidade podem incluir scripts que infetam o dispositivo do consumidor, que pode levar a hackers a aceder ao dispositivo, danificando o dispositivo ou, de outra forma, interferir com as operações do dispositivo.  
Como é que os riscos de segurança serão resolvidos com uma proibição?  
Uma proibição geral da publicidade baseada na vigilância iria estrangular grandes partes de o fluxo de dados e a recolha de dados pessoais. Isto ajudaria a escalar para baixo o potencial para falhas de segurança e uso indevido destes dados. Simplificando, se os dados forem não recolhidos ou armazenados, não podem ser utilizados para prejudicar consumidores ou instituições.

**4.9 Falta de confiança**Embora as questões relativas a violações de privacidade e segurança online têm recebeu atenção pública significativa nos últimos anos, os consumidores são muitas vezes saiu com poucas alternativas, mas para continuar a usar os serviços problemáticos. Alguns plataformas não têm concorrentes, o que significa que os consumidores não podem mudar para  
um serviço diferente, mesmo que gostassem. Em outros casos, a complexidade e escala das práticas problemáticas são tão vasto que os consumidores não podem realisticamente compreender os danos, proteger-se ou tomar preventiva ação. Isto leva à desilusão, fadiga e falta de confiança no serviço digital fornecedores, impactando a economia digital para além da publicidade.95  
Embora a maioria dos consumidores tenha poucas ou mesmo nenhuma maneira de se proteger contra a vigilância comercial online, e não se pode esperar que tomem medidas, uma falta de confiança nos serviços digitais tem sido um fator importante no aumento de ferramentas de rastreio e bloqueio. Tais ferramentas são usadas por muitos consumidores, e são  
pré-instalado em vários navegadores populares da Web, como Safari, Firefox e Brave.  
Embora isto fortaleça a proteção do consumidor, também significa que os anúncios de os atores legítimos estão bloqueados, o que leva tanto a anunciantes como a editores perder receitas.  
Todas estas escolhas pressupõem que o consumidor tem um nível irrealista de poder, competência tecnológica e jurídica. Se o consumidor fosse fazer uma escolha verdadeiramente informada, ela teria que passar centenas de horas todos os anos ler documentação legal e combater padrões escuros projetados para influenciar sua autonomia, decisões e escolhas.

94 'Proteja-se De Ameaças de anúncios e 'Malvertising''. Michelle Drolet.  
https://www.forbes.com/sites/forbestechcouncil/2020/02/03/protect-yourself-from-adthreats-and-malvertising/  
95 'Deloitte Global Mobile Consumer Survey 2019: The Nordic cortar '. A Deloitte.  
https://www2.deloitte.com/no/no/pages/technology-media-andtelecommunications/topics/global-mobile-consumer-survey.html

O uso de padrões escuros para empurrar os consumidores para aceitar o rastreio muda o equilíbrio de informação e poder para a desvantagem do  
consumidor.96 A soma destas práticas significa que os consumidores estão constantemente pediu para fazer escolhas que não têm forma prática ou realista de controlar, compreender ou relacionar-se com. Esta situação absurda também contribui à falta de confiança nos serviços digitais.  
Devido às cadeias de fornecimento opacas de sistemas de publicidade baseados em vigilância, é também é difícil para os anunciantes ter o controlo de onde os seus anúncios são exibidos.  
Isto levou a um grande número de casos em que os anúncios são exibidos ao lado e usado para financiar conteúdo extremo ou odioso, levando a marca negativa associações.97  
Além disso, a falta geral de confiança pode reduzir a propagação e a absorção de serviços úteis, e têm um efeito negativo sobre as empresas que tomam privacidade e segurança a sério.98 Isto pode ter sérios efeitos arrepiantes no consumidor comportamento, que pode impedir os consumidores de utilizarem serviços importantes relacionados  
para a saúde mental99 ou procurando ajuda através de serviços públicos.100  
Os consumidores têm poucas formas de distinguir entre atores sérios e não sérios no espaço digital, que é suscetível de impactar negativamente os pequenos e médios tamanhodenterprises querendo competir em fatores como o desenvolvimento de privacidade tecnologias de preservação.  
Como é que a falta de confiança nos serviços digitais será resolvida através de uma proibição?  
Uma proibição geral da publicidade baseada na vigilância não será uma cura para restaurar confiança nos serviços digitais. Os escândalos são muito numerosos, e têm ocorrido repetidamente ao longo de um longo período. Vai levar tempo para restaurar a confiança. No entanto, uma proibição contribuiria para um campo de jogo nivelado onde as receitas de anúncios para um maior extensão chegar a atores sérios. Isto pode contribuir para que os consumidores já não se sintam como se os prestadores de serviços e marcas estão olhando sobre o seu ombro on-line e sendo tratados como mercadorias que são vendidas ao licitador mais alto. Também pode  
restaurar a confiança, tranquilizando os consumidores de que as marcas não estão patrocinando odioso conteúdo.

96 'Enganado pelo Design: como as empresas tecnológicas usam padrões escuros para nos desencorajar de  
exercendo os nossos direitos de privacidade'. Forbrukerrådet.  
https://www.forbrukerradet.no/undersokelse/no-undersokelsekategori/deceived-bydesign/  
97 'A semana má do Google: YouTube perde milhões à medida que a linha de publicidade chega EUA.. Olívia  
O Solon. https://www.theguardian.com/technology/2017/mar/25/google-youtubeadvertising-extremist-content-att-verizon  
98 Veja-se, por exemplo, o livro branco da Comissão Europeia "Sobre a Inteligência Artificial -  
Uma abordagem europeia da excelência e da confiança».  
https://ec.europa.eu/info/sites/default/files/commission-white-paper-artificial-intelligencefeb2020\_en.pdf  
99 "A sua saúde mental à venda". Privacidade Internacional.  
https://www.privacyinternational.org/campaigns/your-mental-health-sale  
100 "Vigilância no Conselho do Reino Unido sites '. Johnny Ryan.  
https://brave.com/ukcouncilsreport/  
  
  
**4.10 Tecnologia ineficiente**  
É contestado se, além de criar e exacerbar uma série de problemas sérios, a tecnologia por trás da publicidade baseada na vigilância é na verdade eficaz como uma ferramenta de marketing. Mesmo que a inovação em áreas como  
inteligência artificial é muitas vezes apresentado como revolucionário para a publicidade indústria, vale a pena questionar se os efeitos de marketing do a tecnologia está a ser vendida demais.101 Isto é exemplificado por estudos que mostram que publicidade baseada em vigilância têm, em muitos casos, não teve efeitos benéficos em taxas de conversão ou receitas editoriais.102  
Estudos têm demonstrado que as empresas que vendem tecnologia de publicidade são significativamente exagerando a eficácia da tecnologia e que o alvo real está longe de ser preciso.103 Embora perfis com base em dados cobrança pode ser preciso em certas circunstâncias, em outros casos o inferências desenhadas podem ser imprecisas ou planas erradas.104  
Há também desafios relacionados com os anunciantes que chegam aos consumidores que foram já planejando a compra ou que já comprou o produto sendo anunciado. Pode ser difícil ou mesmo impossível para um anunciante distinguir entre uma venda feita por causa de um anúncio ou se o anúncio foi exibido a um consumidor que teria feito a compra independentemente.105  
Além disso, a publicidade online é muitas vezes dependente dos consumidores, na verdade

101 'A nova bolha do ponto com está aqui: é chamada on-line publicidade'. Jesse Frederik,  
Maurits Martijn. https://thecorrespondent.com/100/the-new-dot-com-bubble-is-here-itscalled-online-advertising/13228924500-22d5fd24  
102 ‘Digiday Pesquisa: A maioria dos editores não beneficia de anúncios comportamentais visando'. Marca  
O Weiss. https://digiday.com/media/digiday-research-most-publishers-don-benefit-frombehavioral-ad-targeting/  
103 'Fronteiras: Quão eficaz é o perfil do consumidor de terceiros? Evidência de Field  
Estudos:. Nico Neumann, Catherine E. Tucker, Timothy Whitfield.  
https://pubsonline.informs.org/doi/pdf/10.1287/mksc.2019.1188  
104 "Pedi a uma empresa de rastreio online todos os meus dados e eis o que encontrei".  
Privacidade Internacional. https://privacyinternational.org/long-read/2433/i-asked-onlinetracking-company-all-my-data-and-heres-what-i-found  
105 ‘Overvurdering av digital reklameeffekt‘. CPM Analytics. https://www.cpm.no/wpcontent/uploads/2019/06/Overvurdering-av-digital-reklameeffekt-PDF-28062019.pdf

clicar nos anúncios, e o volume absoluto de publicidade pode levar à maioria material de marketing transformando-se em ruído de fundo.106  
Embora uma grande parte das tecnologias de publicidade digital possa ter limitado efeitos, isto não significa que as decisões baseadas em má tecnologia serão melhor para os consumidores do que decisões baseadas em tecnologia precisa. O imprecisão da tecnologia não é um fator atenuante se os consumidores estão sujeitos a discriminação, manipulação ou exclusão.  
Há também sérias ineficiências no poder de computação e no uso de energia de publicidade baseada em vigilância. Embora o consumo de energia de dados centros não é um problema exclusivo da publicidade, estudos têm demonstrado que o digital as tecnologias de publicidade têm pegadas de carbono significativas.107 O impacto ambiental da publicidade baseada na vigilância é exacerbado pela uso da inteligência artificial e a prevalência de bots usados para fraude de anúncios.108  
Como é que a tecnologia ineficiente será resolvida através de uma proibição?  
Uma proibição geral da publicidade baseada na vigilância limitará as oportunidades de vender tecnologias de "óleo de serpente" que prometem muito mais do que podem entregar a anunciantes e editores. Isto pode reduzir a perda de receitas para anunciantes e editor e ajudar a proteger os consumidores contra decisões baseadas em defeituosos tecnologias e suposições.  
O impacto ambiental da publicidade baseada na vigilância pode restringir alguns dos a pegada de carbono excessiva, mas outras medidas complementares são necessário para lidar com os níveis de emissão de dados centros e artificial inteligência.

5 Legislação em vigorComo descrito acima, a proibição da publicidade baseada na vigilância não é uma cura para todos solução. Os serviços digitais já estão sujeitos a uma série de regras e regulamentos na UE, e uma proibição seria complementar ao legal existente enquadramento. Na secção seguinte, a proteção de dados europeia existente e direito dos consumidores é avaliado em relação aos prejuízos decorrentes de vigilância publicidade.

106 'Banner Blindness Revisited: Users Dodge Ads on Mobile and Desktop'. Rio Kara  
Pernice. https://www.nngroup.com/articles/banner-blindness-old-and-new-findings/  
107 "Avaliação de impacto ambiental da publicidade online" M. Pärssinena, M.Kotilab,  
R.Cuevasc, A.Phansalkard, J.Mannere.  
https://www.sciencedirect.com/science/article/pii/S0195925517303505  
108 "AI & Publicidade, uma perspetiva do consumidor". Rio Harriet Kingaby.  
https://www.harrietkingaby.com/reports  
  
**5.1 Legislação da UE em termos de privacidade e proteção de dados**  
O Regulamento Geral de Proteção de Dados (RGPD) regula o processamento de dados pessoais. A proteção de dados pessoais é considerada fundamental direito humano, e o RGPD visa principalmente dar aos indivíduos o controlo sobre a sua dados pessoais e proibir o tratamento de dados pessoais sem um legal válido base. Regra geral, a utilização de dados pessoais para perfis e rastreios, especialmente quando isto envolve a partilha contínua de dados pessoais, requer um válido consentimento.109 Isto também foi afirmado pela proteção de dados europeia autoridades.110  
O trabalho feito pelo Conselho Norueguês do Consumidor no domínio do digital publicidade mostra que a indústria de publicidade baseada em vigilância opera em formas que envolvem recolha ilegal, partilha e uso de pessoal. Estas práticas são generalizadas e complicadas de entender, mesmo para especialistas. A soma de estas práticas é que todos os consumidores tornam-se vulneráveis por defeito no rosto de publicidade baseada em vigilância. Portanto, não é razoável afirmar que consumidores entendem o que estão a consentir se aceitarem o rastreio e perfis para fins publicitários. Se for esse o caso, o processamento de pessoal dados para fins de publicidade baseados em vigilância tem provado na maioria dos casos não para estar em conformidade com o RGPD. Isto foi ainda afirmado pelo norueguês Autoridade de Proteção de Dados (Datatilsynet), quando anunciou a sua intenção de multar a aplicação de encontros Grindr para o tratamento de dados pessoais para fins publicitários.111  
Mesmo que o RGPD seja adequado para abordar uma série de questões relacionadas com a privacidade no que diz respeito à publicidade baseada em vigilância, o regulamento limita-se aos casos onde os dados pessoais estão a ser tratados.  
Como mostrado acima, muitos dos potenciais danos da publicidade baseada na vigilância perduram mesmo que os dados pessoais não sejam transferidos do dispositivo do utilizador final. Em estes casos, tanto o RGPD como o ePrivacy A diretiva pode ser insuficiente para lidar com os problemas. Daí medidas complementares, como a proibição geral sobre a publicidade baseada na vigilância, pode ser necessário para combater estes mais amplos problemas.

109 ‘Adtech e licitação em tempo real no âmbito da Proteção de Dados Europeia Lei.. Miguel Veale  
e Frederik Zuiderveen Borgesius. https://osf.io/preprints/socarxiv/wg8fq/  
110 Ver, por exemplo, 'Atualizar relatório em adtech e em tempo real licitação'. Informação  
Gabinete do Comissário. https://ico.org.uk/media/about-theico/documents/2615156/adtech-real-time-bidding-report-201906-dl191220.pdf  
111 "Intenção de emitir multa de 10 milhões de euros à Grindr LLC'. Datatilsynet.  
https://www.datatilsynet.no/en/news/2021/intention-to-issue--10-million-fine-to-grindr-llc2/

**5.2 A Diretiva relativa às práticas comerciais desleais**  
A Diretiva relativa às práticas comerciais desleais (UCPD) estabelece um europeu quadro para que marketing, práticas comerciais e termos de utilização os atores comerciais podem participar em diferentes mercados. Consumidor autoridades de proteção são responsáveis pela aplicação desta lei e pela garantia que os consumidores estão protegidos.  
A UCPD é neutra em tecnologia, e pode, em teoria, ser usada em casos que  
dizem respeito à publicidade baseada na vigilância. Marketing dirigido a indivíduos no forma de publicidade baseada em vigilância pode dar origem a perguntas sobre se a tecnologia que é usada para influenciar o partido recetor cruza o limites para o que constituem influência ou pressão injusta e ilegal.  
Podem ser levantadas questões sobre se certas formas de vigilância baseadas publicidade satisfaz os critérios para práticas comerciais agressivas no âmbito do Lei de Controlo de Marketing.112 Esta disposição destina-se ao marketing que emprega medidas que são consideradas ofensivas para reconhecido e generalizado normas sociais.  
No entanto, a UCPD está predominantemente preocupada com o conteúdo e forma de atividades de marketing e materiais. As numerosas questões problemáticas que surgem da utilização da publicidade baseada na vigilância não estão necessariamente ligadas ao conteúdo do marketing, mas sim para os meios de entrega de anúncios, incluindo o processo de decidir que anúncio para mostrar a que pessoa em que tempo. Isto, em  
além da natureza fugaz da publicidade baseada em vigilância, pode significar que a UCPD não é adequada para o fim de regular esta área específica.  
Pelo que sabemos, nenhuma decisão sobre publicidade baseada em vigilância tem as autoridades de defesa do consumidor emitiram.

**5.3 Questões de execução**  
Embora o RGPD estabeleça requisitos rigorosos para o tratamento de dados pessoais, o regulamento não foi suficiente para parar os dados ilegais generalizados

112 Lei de Controlo de Marketing, secção 9, secção 6.

recolha e perfis de consumidores. As razões para esta deficiência são que  
empresas não cumpriram as regras e tem havido sério transfronteiriço estrangulamentos de execução e falta de aplicação.  
O RGPD introduziu novos mecanismos de execução que procuraram facilitar Aplicação transfronteiriça, mas até agora isso não funcionou como pretendido. Para exemplo, um grande número de queixas legais foram passadas para os Dados Irlandeses Comissão de Proteção, uma vez que muitas grandes empresas tecnológicas têm a sua europa sede na Irlanda. Isto levou a que as queixas não fossem tratadas e a atrasos graves nas decisões.113 Simultaneamente, as empresas continuam a operar mesmo depois de violações em larga escala do RGPD, uma vez que a probabilidade de um rápido decisão ou coima administrativa é relativamente pequena.  
Execução da UCPD contra infrações na área de vigilância a publicidade não teve, pelo que sabemos, ocorrido. Penalização isolado infrações é um processo demorado, e só acontece após o Ocorreu uma infração e os danos já foram causados. Na prática, isto significa que um grande número de empresas estão se safando com quebra a lei. O facto de o marketing em si ser personalizado e fugaz, uma vez que é apenas mostrado a pessoas particulares em determinados pontos no tempo, faz o controlo e execução difícil. Além disso, invasivo e problemático vigilância a publicidade não pode necessariamente violar a UCPD, uma vez que o conteúdo e forma de um certo anúncio pode estar fora do âmbito da lei ainda ser prejudicial  
na forma como o anúncio foi entregue ou como o destinatário foi escolhido.  
A falta de execução do RGPD também levou a uma situação em que uma grande número de atores têm sido capazes de continuar a operar ilegalmente sem enfrentar quaisquer consequências significativas. Modelos onde os perfis são criados e armazenados localmente em dispositivos de consumo pode ou não reduzir riscos de privacidade, mas a utilização de  
personalização e individualização ainda carrega problemas relacionados com discriminação, manipulação ou exclusão, e também é muito difícil de controlar ou verificar.  
Uma vez que investigar casos individuais de violações requer tempo considerável e recursos e vem depois do facto, é pertinente considerar se mais são necessários remédios abrangentes para travar a utilização de vigilância baseada em publicidade. Em vez de considerar casos individuais de marketing, um geral A proibição da publicidade baseada na vigilância deve ser considerada. Isto seria contribuir para uma aplicação mais eficiente e rápida, e enviaria um forte sinal para o marketing e adtech indústria.

113 Vigilância comercial pelo Google. Longo atraso no RGPD queixas'. O BEUC.  
https://www.beuc.eu/press-media/news-events/commercial-surveillance-google-longdelay-gdpr-complaints

6 ConclusãoA publicidade baseada na vigilância causa violações dos direitos fundamentais, fraude generalizada e perda de receitas, e tem contribuído para uma série de efeitos individuais e sociais negativos. Apesar dos repetidos avisos, multas, escândalos, e revelações, a indústria tem mostrado pouca vontade de alterar significativamente as suas práticas, e é questionável se significativo as alterações a partes do sector são mesmo possíveis sem uma reforma fundamental.  
A legislação nesta área é fragmentada e em grande parte baseada na aplicação da lei após os danos já foram feitos. É, portanto, oportuno perguntar se publicidade baseada em vigilância deve ser banido totalmente, de modo a evitar o problemas que estão a ser causados em primeiro lugar. Uma proibição também contribuiria para nivelamento do campo de jogo na publicidade digital e maximizar receitas para anunciantes e editores que atualmente estão nas mãos de alguns jogadores.114  
Uma proibição geral da publicidade baseada na vigilância forçará muitos atores da indústria para mudar os seus modelos de negócio. Estimularia o crescimento das tecnologias que respeitam os direitos dos consumidores e dos direitos fundamentais. Num cenário a longo prazo, ajudaria a restaurar a confiança dos consumidores nos serviços digitais. Esta seria uma rede positivo para os consumidores, para as empresas e para a sociedade em geral.

Exortamos os decisores políticos de ambos os lados do Atlântico a decretar regulamentos rigorosos para refrear os muitos danos da publicidade baseada na vigilância. Política eficaz, regulação e execução para abordar a vigilância comercial que penetra o nosso dia-a-dia há muito que devia. Como temos discutido ao longo de todo este relatório, quaisquer benefícios percebidos da publicidade baseada na vigilância estão longe  
superado pelos danos, e a proibição é, portanto, a solução certa.

114 Este ponto também está a ser feito por grandes atores da indústria, incluindo o CEO da Axel  
Springer: "Está na altura da Europa tirar dados privados das mãos de tecnologia poderosa  
monopólios e devolvê-lo ao pessoas'. Mathias Döpfner.  
https://www.businessinsider.com/big-tech-private-data-facebook-google-apple-europeeu-2021-1