É TEMPO DE BANIR A PUBLICIDADE BASEADA EM VIGILÂNCIA.

Tradução autorizada do relatório: Time to Ban Surveillance Based Advertising do Conselho Norueguês do Consumidor (Forbrukerradet) para língua Portuguesa.

O caso contra a vigilância comercial online, Junho de 2021

Nota do tradutor:
- O documento original, Time to Ban Surveillance Based Advertising, foi um dos documentos usados na discussão e elaboração de leis da União Europeia referentes à Proteção de Dados e Serviços Digitais nos anos 2021 e 2022. Esta tradução não oficial e voluntária serve como forma de disponibilizar o seu conteúdo em Língua Portuguesa.

- Há muito que é dito que os dados são o novo petróleo. Os dados associados a individuos são valiosos, contúdo, a invasão de privacidade acarreta potenciais perigos de segurança. Não são apenas riscos minoritários criados pela publicidade digital.

- Como muitos, também tenho uma certa alergia à palavra proibir, os seus sinónimos e significados mas, todos reconhecemos que determinados químicos/pesticidas não podem ser usados na água potável ou agricultura, por exemplo.

Tabela de conteúdos

1. Resumo

A vigilância comercial e a exploração dos consumidores são agora a norma na internet. À medida que utilizamos os mais variados serviços digitais, estamos constantemente a ser 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 imaginar um novo normal que capacite e proteja os consumidores.

À medida que a vigilância comercial se generaliza e se infiltra em inúmeros 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 dos Serviços Digitais (*Digital Services Act*). Ao mesmo tempo, estão a decorrer discussões sobre a adoção federal de legislação de privacidade e iniciativas legislativas para restringir a vigilância publicitária nos Estados Unidos, onde muitas das empresas envolvidas na publicidade baseada em monitorização estão sediadas. 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 podem 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 como uma parte das discussões políticas em curso.

Tem-se verificado com clareza que a maioria dos consumidores não quer ser rastreado 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 online recolham informações pessoais sobre eles, enquanto que 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 a profundidade da publicidade baseada em vigilância 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 o modelo atual dominante da publicidade online é uma ameaça para consumidores, sociedades democráticas, meios de comunicação social, e até mesmo para os próprios anunciantes. Estas questões são importantes e sérias o suficiente para nós acreditarmos que é tempo de banir estas práticas prejudiciais.

O veto das práticas baseadas em vigilância deve ser complementada por uma mais forte aplicação da legislação em vigor, incluindo o Regulamento Geral de Proteção de Dados (RGPD) e da 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 vai forçar a mudanças estruturais para a indústria publicitária e aliviar uma série de danos significativos para consumidores e consequentemente para sociedade em geral.

A proibição da publicidade com base na vigilância não significa que esta não se possa mais financiar através de 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 alicerçada em monitorização massiva e na criação de perfis *profiling* de consumidores, é o modelo dominante no negócio online hoje em dia. Esta forma de marketing usa informação sobre cada um de nós por forma a alterar o conteúdo das mensagens, utilizando fatores como a nossa escolha de canal e a que horas estamos online para determinar quando estamos mais suscetíveis a influências comportamentais, por exemplo.

A publicidade baseada na vigilância tem sido um fator determinante no crescimento "economia de vigilância" online[1], onde os dados pessoais são recolhidos, agregados e vendidos 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 crescentes modelos de negócio que conduzem uma grande quantidade de desinformação, conteúdo radicalizado, burlas e fraudes. A individualização ofuscada, a personalização e as técnicas de micro-segmentação da publicidade tornam-a difícil de descobrir/revelar as atividades ilegais aumentando a vulnerabilidade consumidor.

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

Há várias instituições e organizações da sociedade civil que estão desenvolver esforços para enfrentar os principais desafios desta invasão publicitária e da economia que sustenta a tecnologia.[3] Por exemplo, tanto o Parlamento Europeu[4] como a Supervisão Europeia de Proteção de Dados[5] 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.

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 movimento, f*ree speech* apelaram recentemente à proibição da publicidade baseada na vigilância. A coligação cita preocupações sobre questões como a difusão de desinformação, extremismo, facilitar a discriminação, efeitos negativos na saúde pública, e degradação da 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 o uso de publicidade baseada em vigilância fosse levada a uma fim.

Todos os consumidores estão vulneráveis quando confrontados com sistemas disfarçados que: recolhem secretamente informação sobre nós, exploram-nos, tornam-nos alvo de uma forma que nos deixa vulneráveis por padrão[7] e que comercializam 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, criação de perfis e direcionamentos forçados. 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 resultados positivos na saúde dos consumidores.[8] A proibição dos gases CFC nos anos 80 teve um efeito positivo na eliminação progressiva de materiais com graves riscos ambientais, e levou à inovação e produção de soluções alternativas amigas do ambiente. Da mesma forma, a proibição do amianto na construção levou a materiais menos poluentes serem utilizados substituindo-o.

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 que estas leis procuram abordar ainda persistem, e particularmente, o RGPD apenas aborda desafios que estão relacionados com a proteção de dados. Torna-se claro que os desafios da publicidade baseada na vigilância vão muito além da área de proteção dados e privacidade.

Com isto em mente, é agora altura de banir a publicidade baseada no "rastreamento" e monitorização dos indivíduos. 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 assuntos 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, o seu enquadramento e o seu design significam que qualquer anúncio é direcionado, e é visto mais frequentemente, em alguns grupos de consumidores do que outros. Isto também se aplica à publicidade "tradicional" ou ao marketing offline, onde estes agentes compram acessos a determinados grupos de consumidores quando decidem onde querem colocar os seus anúncios.

Perante este contexto, usamos o termo "publicidade baseada na vigilância" como um termo abrangente para a publicidade digital que é direcionada a indivíduos ou segmentos de consumidores, geralmente através de rastreamento e criação de perfis *profiling* com base em dados pessoais. A publicidade baseada na vigilância pressupõe um marketing comportamental, personalizado e direcionado. No marketing tradicional offline, os anúncios são colocados num pré-determinado contexto, por exemplo, ao comprar um espaço de anúncio numa revista de automóveis com o objetivo de chegar aos consumidores interessados em carros. A publicidade baseada em vigilância é diferente, porque o anúncio é pré-direcionado para um indivíduo ou grupo baseado em características do indivíduo ou do grupo. O contexto ou sítio onde o anúncio é colocado pode ser aleatório porque já tem como alvo o consumidor e porque "o anúncio" pode seguir o consumidor em diferentes contextos.

A tecnologia possibilita que, através de uma análise complexa de dados, um anúncio pode ser mostrado ao "indivíduo certo" no "momento certo", por exemplo, mostrando um anúncio de *fast food* quando foi calculado previamente quando a pessoa pode estar a começar a ter fome, ou um anúncio para uma cirurgia estética quando não se sente atraente. Há diversas variações destas técnicas que são vulgarmente referidas como “marketing comportamental”, “microtargeting” ou "publicidade programática".

Na maioria dos casos, a publicidade baseada na vigilância é mostrada como parte de um processo totalmente automatizado, em que cada anúncio particular é escolhido e colocado numa questão de milissegundos. Isto significa que nem o promotor (por exemplo, o proprietário de um site ou *app*) nem o anunciante (por exemplo, o proprietário da marca que é promovida) escolhem quais anúncios a mostrar e onde exibi-los. Isto é automaticamente decidido por sistemas tecnológicos que são muitas vezes controlados por terceiros e/ou intermediários (conhecidos como empresas *Adtech*).

Um grande número destas empresas terceiras estão sistemáticamente a recolher gigantescas quantidades de dados pessoais dos consumidores, com o objetivo de criar perfis de consumidores e diretrizes que são usadas em tentativas de direcionar os anúncios de forma mais eficiente. A automatização do processo, permite monitorização e adaptação contínua de formas publicitárias, que também permite aos anunciantes que determinem e escalem campanhas direcionados de diferentes maneiras. No entanto, como será explicado abaixo, o uso de a publicidade baseada em vigilância também coloca desafios significativos aos editores e anunciantes no que respeita a receitas, danos reputacionais e promoções de cadeias obscuras.

3.1 Formas alternativas de publicidade digital

Um argumento comum a favor da publicidade que temos hoje, é que uma proibição terá consequências negativas para os prestadores destes serviços e conteúdos e que levará a um aumento

dos custos para os consumidores, uma vez que a maioria dos serviços "gratuitos" online são financiados por anúncios.[9] Como será detalhado mais 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 a favor desta forma de publicidade é que os consumidores consideram que os anúncios direcionados são úteis e positivos. Este argumento assume que a única alternativa seria mostrar aos consumidores anúncios completamente aleatórios e irrelevantes, o que seria um incómodo e impediria os consumidores de receber ofertas interessantes. Esta é outra premissa enganadora, pois não é uma questão de anúncios baseados em invasão de privacidade por um lado e arbitrariedade pelo outro.

Já existem formas alternativas de publicidade digital e que provaram ser fontes de rendimentos eficazes para os fornecedores de conteúdos. Estes modelos alternativos também têm como base as premissas já pré-determinadas, mas não implicam mostrar anúncios fora do contexto (não contextualizados), que não têm relevância para os consumidores.

Por exemplo, há modelos em que os consumidores com determinado interesse num tipo de publicidade podem auto-permitir anúncios do tipo que gostariam de ver.[10] Com um modelo destes, um consumidor poderia indicar o seu interesse em desporto, viagens, música ou mais interesses específicos e receber anúncios que são relevantes para estas questões. Isto poderia ser feito ao nível do *browser*, e poderia garantir que os anúncios são relevantes para os interesses do consumidor sem depender da constante monitorização ou localização.

Outro exemplo de formas alternativas de marketing digital é a publicidade contextualizada. A publicidade contextualizada permite que os anunciantes comprem espaços de anúncios para tipos específicos de páginas web ou web sites baseados no conteúdo da página, site ou *app*.[11] Este modelo 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, a publicidade contextualizada permite aos anunciantes colocar anúncios para certos tipos de produtos e serviços em contextos onde os anúncios serão exibidos para os consumidores que têm interesse naqueles tipos de conteúdos.

De certa forma, a publicidade contextualizada pode ser comparada com a publicidade "tradicional". Tal como um anunciante numa situação de marketing offline, compra um espaço para um anúncio numa revista para entusiastas de carros para chegar a esse segmento de consumo, a publicidade contextual permite que os anúncios selecionados de um anunciante sejam direcionados, 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 agregar dados pessoais. Isto responde a algumas das mais prementes questões entre privacidade e publicidade, uma vez que os diferentes atores na cadeia de fornecimento só precisam saber onde o anúncio é mostrado, não necessariamente quem o está a ver.[12]

Isto aumenta também a transparência e verificação do marketing, uma vez que o próprio anunciante escolhe que tipo de conteúdos ou palavras-chaves desencadeiam um anúncio a ser mostrado. Significa portanto que muitos visitantes de um determinado site ou *app* vão ver o mesmo anúncio.

Diversas experiências de algumas editoras mostraram que remover as práticas desta publicidade baseada em nos vigiar em favor de publicidade contextual levou a um aumento receitas publicitárias.[13] Por exemplo, a emissora holandesa NPO aumentou as receitas publicitárias até

79% após passar para publicidade contextual.[14] Outro exemplo, foi quando o The New York Times deixou de servir *ads* com base em *tracking* e recolha de informações dos utilizadores europeus devido ao RGPD, as suas receitas publicitárias continuaram a crescer à medida que os seus parceiros de publicidade continuaram a comprar espaços de anúncios independentemente da capacidade de rastreio *targeting*.[15] Embora não haja uma resposta definitiva, se estes casos podem ser replicados pela maioria dos editores/atores, aponta para a possibilidade alternativa de modelos de receitas que não dependem da vigilância *quasi* espionagem.

Uma cadeia de atores mais transparente reduz também os gastos em terceiros, tais como corretores de dados ou serviços de verificação, o que significa que anunciantes e editores ficarão com uma maior parte das receitas. Para ilustrar este ponto, em 2020 um estudo da área descobriu que sob o atual regime de publicidade digital, apenas metade de gastos de publicidade realmente chegou aos promotores, enquanto 15% do dinheiro estava desaparecido.[16]

3.2 First-party and third-party data

Existem várias formas de publicidade baseada na vigilância com potenciais riscos e danos que podem variar. Algumas formas de publicidade atuais envolvem a transferência de gigantescas quantidades de dados pessoais para várias entidades terceiras third-party sem o conhecimento ou consentimento dos consumidores, criando uma série de riscos para privacidade e segurança. Ou seja, o termo third-party aplica-se ao que é tipicamente chamado de publicidade com base em entidades terceiras que podem não ter autorização para usar os dados.

A escala da partilha de dados e dos atores envolvidos no serviço da publicidade baseada *tracking* com dados de terceiros é gigantesca. Por exemplo, um único anunciante pode enviar centenas de biliões de "pedidos de oferta" *bid requests*, contendo potencialmente quantidades significativas de dados pessoais para milhares de site ou *apps* por dia. 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]

Outros agentes deste de marketing digital baseado em monitorização, tentam reduzir os riscos limitando a partilha de dados com terceiros. Alguns destes atores, particularmente as grandes plataformas digitais, usam os dados pessoais que têm recolhido junto dos seus consumidores através dos seus próprios serviços.[18] Isto pode ser chamado de publicidade com base em "dados da primeira entidade", *first-party data*. O ator que recolhe os dados pessoais muitas vezes tem uma relação “direta” com o consumidor, por exemplo, no caso em que o operador de uma rede social ou pesquisa da web recolhe informações sobre os seus utilizadores. Embora alguns possam argumentar que esta forma pode ser menos invasiva numa perspetiva de privacidade, uma vez que menos as empresas podem aceder aos dados, este tipo de publicidade baseada na vigilância pode implicar graves riscos relacionados, por exemplo, com a manipulação, discriminação para além de levantar questões de desconfiança, *antitrust*.[19]

Apesar de grandes empresas como a Google ou Facebook muitas vezes dependam dos "dados da primeira entidade", *first-party data*, e partilhem menos dados sobre os seus consumidores com terceiros, este acordo não sana/retira os problemas para os consumidores. A criação de perfis publicitários intrusivos levantam também questões de privacidade, liberdade de escolha e incentivos à manipulação. Como *digital gatekeepers*, estas empresas recolhem dados sobre os consumidores

num grande número de serviços, tanto nas suas próprias plataformas como em toda a web. Por exemplo, quando os consumidores que usam um dispositivo móvel Android com um navegador Chrome, bem como ao usar o Google Maps ou Gmail, estes são rastreados pela Google através destes serviços. Isto oferece oportunidades para criar perfis de consumo altamente detalhados.[20] Para além disto, em alguns casos, entidades terceiras de dados disfarçam-se como entidades de primeira, para contornar as medidas restritivas contra entidades terceiras de dados.[21] Os esforços de alguns atores da indústria para conter o rastreio dos consumidores levou a uma corrida ao "armamento" de ferramentas e práticas por parte das empresas da publicidade digital, a fim de evitar ser bloqueadas.[22]

É portanto, crucial olhar para a publicidade baseada na vigilância de um ponto de vista holístico – os riscos e efeitos nocivos desta tecnologia não se limitam à publicidade com base em dados de entidades terceiras. Não é linear afirmar que os dados em entidades terceiras são um problema e os dados consentidos na primeira entidade como sendo bons.

4. Efeitos negativos da publicidade baseada na vigilância

Apesar da publicidade com base na monitorização dos utilizadores da web seja por vezes apresentada como uma troca, onde os consumidores são diretamente expostos à publicidade direcionada em troca de serviços "gratuitos", esta é uma premissa instável. Embora muitos serviços online sejam apresentados como "grátis" para o consumidor, as receitas destes serviços são impulsionadas pela venda do interesse/atenção que o consumidor dá, ilustrado pelos 400 mil milhões de dollars que a Google lucrou em receitas publicitárias no primeiro trimestre de 2021.[23]

No entanto, vários estudos indicam que a maioria dos consumidores não estão confortáveis com a recolha de dados pessoais.[24] Um inquérito populacional, realizado em nome do Conselho Norueguês do Consumidor, mostrou que consumidores Noruegueses estão particularmente preocupados com a vigilância comercial.[25] Apenas um em cada dez inquiridos tem uma reação positiva para que os atores comerciais recolham informações online pessoais sobre eles, enquanto que apenas um em cada cinco pensou que servir anúncios com base em informações pessoais é aceitável.

Outras pesquisas também indicaram que os consumidores geralmente não querem publicidade com base em dados pessoais, e um estudo descobriu que apenas 17% dos inquiridos vem o rastreamento online para fins publicitários como ético.[26] Para cimentar 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 serem usados para lhes direcionar anúncios.[27] Nos Estados Unidos, uma pesquisa mostrou que quatro em cada cinco consumidores apoiariam a proibição de vigilância baseada em publicidade.[28] Num outro indicador de preferências dos consumidores, apenas 4% a 6% dos utilizadores optaram por aceitar o rastreamento, *tracking*, depois da Apple ter introduzido um sistema de *opt-in* para o *tracking* ou monitorização de anúncios em aplicações.[29]

Embora a perspetiva de que os anúncios monitorizam as nossas atividades possa ter um "fator assustador" significativo, muitas das questões problemáticas relacionadas com o *tracking* na publicidade são "invisíveis". Por exemplo, é impossível para os consumidores saber que dados pessoais sobre eles são retidos, como é processado, transferido ou explorado, e por quem. É

impossível para o indivíduo saber porque alguns dos consumidores estão excluídos de ver certos anúncios ou mensagens. A manipulação é tão mais eficaz quando os consumidores não sabem se, ou como, estão sendo manipulados e muitas vezes não sabem que estão numa situação vulnerável. No ambiente digital, cada consumidor é potencialmente vulnerável. Há poucas medidas que os consumidores podem tomar para limitar estes efeitos nocivos, além de abdicar de uma grande quantidade de serviços digitais úteis e importantes.

Para os devidos efeitos deste documento, o Conselho Norueguês do Consumidor analisou um determinado número de efeitos negativos que são criados ou ampliados pela publicidade baseada em vigilância. A falta de transparência no sistema dominante é um problema abrangente que contribui para efeitos nocivos graves relacionados com violações de privacidade, manipulação e discriminação. Estes são assuntos importantes que não podem apenas ser resolvidas por maior transparência ou melhor informação para os consumidores. Como agravante, a falta de transparência e controlo das empresas intervenientes neste sistema contribuiu para a criação de incentivos financeiros e modelos de negócio para desinformação e fraude em larga escala.

Esta forma de markting baseada em invasão de privacidade também tem efeitos nocivos significativos nos atores empresariais. Os comportamentos de anticoncorrencia e os seus efeitos servem para alicerçar posições dominantes dos atores, enquanto que, cadeias de fornecedores 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. A falta de confiança traduz-se numa adoção mais lenta ou menor pelos consumidores das novas tecnologias. Para além disto, é também difícil para os consumidores distinguir entre atores 'bons' e 'maus' na esfera digital, o que significa que os atores legítimos, entre eles, muitas pequenas e médias empresas, são diretamente afetadas pelas ações de empresas sem escrúpulos. Isto, por sua vez, prejudica tanto os consumidores como as empresas. Todas estas questões são explicadas nas secções seguintes.

4.1 Falta de transparência

A individualização e personalização da publicidade baseada na vigilância faz com que diferentes indivíduos vão ver diferentes anúncios com base num número de fatores como o tempo, o contexto, a demografia, as características pessoais, etc.[30] Um novo anúncio é mostrado para cada visita de página, e muitas vezes apenas para alguns indivíduos em certos períodos de 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, em contraste com o marketing que não se baseia na vigilância. Noutras formas de publicidade, por exemplo, quando um anunciante compra espaço de publicidade diretamente a partir de um emissor, como um jornal ou emissor de TV, é fácil contactar o meio emissor para verificar o que o foi impresso ou mostrado num canal de TV num determinado tempo.

Sistemas algorítmicos avançados podem tornar-se as chamadas "caixas negras", onde os dados são alimentados e os resultados são extraídos, enquanto que as inferências ou implicações por trás dos resultados são opacas. Isto pode ofuscar a base de certas decisões como fatores decisivos e outros aspetos potencialmente problemáticos da tecnologia. Como será detalhado em baixo, isto levou a práticas discriminatórias ocultas. Esta obscuridade torna-se também difícil para as autoridades de

supervisão no levantamento de sanções perante infrações à lei, que podem ter consequências em cascata para várias violações de direitos e 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 em particular, em que segmento foram colocados, e como os dados pessoais são partilhados e usados. Mesmo que esta informação fosse acessível de qualquer forma com significado, iria ser difícil ou mesmo impossível para os consumidores fazer uso dela devido à complexidade técnica, o contexto da prática/industria, e porque, na realidade, eles raramente têm uma opção de escolha.[31]

Como é que a falta de transparência será resolvida através de uma proibição?

Uma proibição contra a publicidade baseada na vigilância libertaria-nos de anúncios que são direcionadas e colocadas com base em dados sobre consumidores individuais. Se isto acontecesse, seria mais fácil "navegar pela web" e controlar os anúncios, uma vez que não seriam mais individualizados e fugazes. Plataformas de anúncios ou plataformas de redes sociais poderiam, por exemplo, estabelecer mais facilmente registos de todos os anúncios que exibem, tornando mais fácil controlar o conteúdo e garantir que a segmentação contextual não é usada de forma inadequada para explorar vulnerabilidades dos consumidores.32 Isto contribuiria para aplicação mais eficaz contra práticas comerciais desleais, violações de privacidade, e muito mais.

4.2 Violações da privacidade e proteção de dados

Com o objetivo de adaptar estratégias de marketing a indivíduos ou grupos, e exibir "o anúncio certo para a pessoa certa", um grande número de empresas recolhem e processam gigantescas 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 (mesmo pelas rede domésticas, *tracking* através de Wi-Fi).

No início de 2020, o Conselho Norueguês do Consumidor publicou o relatório *Out of Control* em que revelou como um grande número de empresas recolhe, usa e partilha dados pessoais sobre os consumidores sempre que visitam aplicativos e websites.[33] Esta informação é agregada, muitas vezes por vários proprietários do site ou aplicação e várias entidades terceiras. Os dados são utilizados para fins relacionados com marketing e serviços personalizados, mas também podem ser usados (inadvertidamente ou não) para fins de discriminação, exclusão e manipulação.

Os consumidores são constantemente manipulados para aceitar um rastreio abrangente através de técnicas comportamentais ou características de design mais obscuras, "padrões negros" *dark paterns*,[34] forçados a sistemas de vigilância comerciais, a fim de aceder serviços necessários[35], e são geralmente expostos à recolha de dados sem o seu conhecimento e consentimento (válido). Esta gigantesca quantidade de dados também significa que tentativas de uso de pseudónimos ou de anonimização no acesso a informação têm-se provado ineficazes.[36]

O universo da recolha e partilha de dados é tão vasto que torna-se praticamente impossível saber como os dados pessoais podem ser usados. Como consequência, no contexto de publicidade baseada em vigilância, torna-se difícil de exercer os direitos fundamentais previstos na Carta dos Direitos Fundamentais da EU (*Charter EU*) e posteriormente fazendo parte do Regulamento Geral

de Proteção de Dados (RGPD), incluindo os direitos a ser informado, ter acesso, retificar e eliminar dados ou para contestar decisões que afetem as nossas vidas.

Como é que os riscos de violações da privacidade e proteção de dados podem ser resolvidos por uma proibição?
Os riscos da publicidade baseada na vigilância para a privacidade e proteção de dados são já amplamente regulados na Europa através do *ePrivacy Diretive* e do RGPD. Após a entrada em aplicação do RGPD em 2018, a execução da lei tem sido, infelizmente lenta e em alguns casos inexistente, com estrangulamentos significativos na aplicação transfronteiriça. Simultaneamente, há poucos indicadores de que a proliferação da economia de vigilância tenha abrandado, apesar duma regulação mais forte. Isto resultou numa lacuna na aplicação transfronteiriça que precisa de ser urgentemente abordada.[37]

Um veto à da publicidade que constantemente nos monitoriza seria positivo para complementar os direitos fundamentais à privacidade e proteção de dados pessoais que estão protegidos ao abrigo da *Charter*, do RGPD e da *ePrivacy Diretive*. Apesar da introdução do RGPD, muitos intervenientes na economia de vigilância têm operado em grande parte sob, “a norma" - negócios do costume. Embora se tenha observado que alguns atores introduziram mudanças relativamente pequenas na forma como pedem o consentimento para o tratamento de dados pessoais. Outros simplesmente tentaram mover-se para uma base legal diferente para o tratamento de dados.[38]

O fosso da 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 interdição geral pode forçar uma transformação estrutural mais abrangente aos modelos de negócio de vigilância. Como complemento a uma interdição, é necessário reforçar a aplicação da lei e procedimentos pelas autoridades, tanto no RGPD como *ePrivacy Diretive* (ou uma nova *ePrivacy* Regulamento que substituirá a diretiva)[39], e na próxima Lei dos Serviços Digitais.

4.3 Manipulação

O aumento do marketing baseado na constante recolha de dados pessoais contribuiu para a tentativa manipulação de indivíduos e grupos a uma escala sem precedentes. Empresas na posse de grandes quantidades de dados podem usar sistemas algorítmicos nas tentativas de decisão para quando os indivíduos estão mais suscetíveis a comportar-se de determinadas formas ou a reagirem de forma induzida a imagens, sons ou mensagens específicas.

Isto pode implicar, por exemplo, que os consumidores são expostos a anúncios de beleza ou produtos de dieta quando a sua auto-confiança é baixa 40 ou, para que os anúncios de jogo online sejam direcionados para os consumidores que lutam contra os vícios. 41 Estas temáticas são exacerbadas pela proliferação da comercialização de produtos e serviços nocivos para as crianças. 42 A automação torna o processo ainda mais obscuro, e a otimização de mensagens pode ter efeitos negativos se for prejudicial e não ético, contudo, os métodos eficazes são automatizados.

A publicidade pode explorar as vulnerabilidades dos consumidores mesmo sem observar diretamente as referidas vulnerabilidades. Por exemplo, através da utilização dos chamados “públicos semelhantes” *lookalike audiences*, os anunciantes podem agregar e construir grupos de consumidores com certas características, a fim de chegar a novos consumidores que partilham as

mesmas características.[43] Desta forma, a publicidade para os produtos farmacêuticos pode, por exemplo, ser mostrada a grupos de consumidores que têm características comuns com 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]

Por meio desta publicidade baseada na vigilância, todos os consumidores ficam vulneráveis por defeito; em teoria podemos ser alvo nos nossos momentos mais vulneráveis a fim de otimizar os efeitos do marketing.[46] O bombardeamento constante de publicidade em espaços digitais também serve para quebrar as defesas enraizadas 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 interdição?
Uma interdição geral desta publicidade baseada na observação/monitorização não resolverá todas os assuntos relacionadas com o marketing manipulador, uma vez que todo o marketing pode potencialmente ser usado para manipular os consumidores. Apesar disto, uma interdição desta má forma de publicidade, contribuirá para acabar com os anúncios individualizados que são otimizados para chegar aos consumidores em situações vulneráveis, bem como, mitigar os efeitos em curso para as "vulnerabilidades por padrão" criadas através da aplicação constantemente de melhorados perfis de persuasão.
A manipulação que acontece através de outras formas de publicidade, como o conteúdo marketing[49], deve ser resolvida através de meios diferentes para além da interdição de vigilância publicitária, como por exemplo através de disposições previstas na Lei dos Serviços Digitais[50] e uma revista *Unfair Commercial Practices Directive.*

4.4 Discriminação

Para além de criar novas oportunidades para comunicar com "a pessoa certa", a publicidade baseada em *tracking* 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 descreveu o modelo de negócio baseado na vigilância de empresas como a Google e o 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 segmentação.[52]

A segmentação e orientação podem ser usadas para não mostrar certos anúncios a pessoas específicas ou grupos de consumidores. Por exemplo, os anunciantes podem escolher mostrar anúncios de habitações apenas para pessoas que se encaixam no seu perfil ideal, para indivíduos que querem fazer com que vivam num certo bairro e excluir indivíduos "indesejáveis" que, no entanto, pode ser capazes de se dar ao luxo de viver lá. Da mesma forma, potenciais empregadores podem escolher a que tipo de pessoas são mostradas certas ofertas de emprego, que pode, por exemplo, excluir potenciais candidatos femininos, quer deliberadamente ou através da discriminação algorítmica.[53] Na realidade, estas escolhas vão necessariamente excluir alguns indivíduos ou grupos.[54] Isto é amplificado pelo nível de obscuridade e a impossibilidade de saber quem está a ver e qual anúncio.

É impossível para os consumidores saberem que anúncios de emprego ou habitação não estão ver. Enquanto o marketing tradicional pode ser observado olhando para o conteúdo e analisado em retrospetiva, isto é muitas vezes impossível se o anúncio é apenas mostrado a um determinado consumidor ou grupo num determinado momento. Se a discriminação está a acontecer como parte de processos algorítmicos automatizados, torna-se muito difícil descobrir e remediar a questão. Assim, este estado de vigilância publicitária pode contribuir para esconder práticas de discriminação ou exclusão porque as questões problemáticas acontecem dentro da "caixa preta" *black-box*. Esta, é uma invasão ao direito à não discriminação, que é um direito humano fundamental.

Estas formas de discriminação e exclusão não se devem necessariamente a um ato deliberado de malícia por parte do anunciante; os processos algoritmos, otimizando os anúncios, podem estar automaticamente a facilitar estas práticas problemáticas.55 Conduzindo a discriminação automatizada, por exemplo, fazendo da geolocalização de um *proxy* (identificador) para atributos pessoais/privados, tais como a etnia, a orientação sexual ou as crenças religiosas, porque os modelos estatísticos mostram que alguns grupos de pessoas têm sobreposição de atributos.56

Por outras palavras, mesmo que um sistema explicitamente proíba direcionar *adds* aos 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 continuamente corre o risco de criar novos proxies/identificadores com atributos à medida que o sistema evolui e decide que indivíduos devem ver determinados 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 e diferenciação entre consumidores, dificultar a comparação de preços, e fazer com que os consumidores estejam receosos em comparar preços, porque pode afetar a final preço do produto ou serviço.58

Como é que as práticas discriminatórias seriam resolvidas com um veto?
Um veto geral da publicidade baseada na vigilância facilitaria a observação e sanção de práticas de marketing discriminatórias e de exclusão. Isto contribuiria para um mercado publicitário onde as práticas discriminatórias seriam mais efetivamente corrigidas, o que ajudaria a proteger os direitos fundamentais dos consumidores.59

4.5 Desinformação

A falta de transparência em grande parte na indústria da publicidade baseada na vigilância significa que muitos anunciantes não sabem onde os seus anúncios estão a ser exibidos. Isto cria danos reputacionais para marcas e anunciantes, uma vez que eles perdem o controlo sobre se, os seus anúncios, estão a ser exibidos em conjunto com desinformação ou conteúdo problemático.

O risco de danos reputacionais levou a que algumas categorias de websites ou palavras-chave fossem postos numa "lista negra", o que criou novas questões para os criadores de conteúdo honesto, produtores e editores.60 Por exemplo, isto causou grandes problemas e enormes perdas de receitas para muitos editores quando um número de anunciantes não desejava colocar os seus anúncios em sites que escreviam sobre COVID-19.61 Práticas semelhantes, têm danificado editores criando conteúdo para minorias e para potencialmente grupos vulneráveis, por exemplo, através de

palavras-chaves relacionadas com LGBTQ+ por estarem na lista negra.62 Isto envolve dinheiro sendo desviado de editores respeitáveis em favor de fontes menos respeitáveis. Consequentemente, o conteúdo de baixa qualidade é incentivado, criando oportunidades de fraudes e corrupção.

O conteúdo sensacionalista está provado criar um alto grau de envolvimento, levando muitas pessoas a clicar em links para artigos ou conteúdo que são enganosos ou manifestamente falsos.63 Isto leva a receitas publicitárias para os atores que criam e espalham desinformação, o que significa que a publicidade baseada na vigilância oferece incentivos financeiros para criar tal conteúdo.64 O uso de vigilância publicitária é um, não o único, modelo de negócio que incentiva a criação e difusão de desinformação online.65 Além disto, a tecnologia por trás da publicidade invasiva pode ser usada para espalhar desinformação, com efeitos potencialmente devastadores para os seres humanos e a sociedade.66

Como é que a prevalência da desinformação online será resolvida através de uma proibição?
Uma proibição da publicidade baseada na vigilância não será o remédio perfeito para a prevalência de desinformação online. No entanto, uma proibição geral irá perturbar os modelos de negócio de um grande número de websites ou aplicações e outros atores que criam e espalham desinformação.

Uma cadeia de negócio mais transparente vai ajudar aos anunciantes saber onde os seus anúncios são exibidos. Isto significa que as marcas podem ter mais controlo sobre os seus anúncios e se estes são usados para financiar desinformação. Uma proibição deve no entanto, ser complementada por uma aplicação consistente e firme na proteção dos dados, mercados de concorrência e direito do consumidor.67

4.6 Efeitos anticoncorrenciais

No modelo de publicidade discutido neste documento, alguns atores podem obter vantagens competitivas através da recolha de dados em websites e serviços.68 A crescente concentração do mercado da publicidade digital está a diminuir valor dos dados de primeira entidade, *first-party data* dos editores e criando uma corrida até ao mais pequeno detalhe. Na prática, as empresas *adtech* podem recolher dados sobre consumidores de um site (por exemplo, um jornal online), combiná-los 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 noutros sites que lhes oferecem um preço mais baixo para colocações dos anúncios escolhidos.69

Apesar das receitas dos anúncios da publicidade baseada em vigilância tenham crescido durante nos últimos anos, a maior parte das receitas foram apenas para algumas plataformas.70 Ambas as plataformas como o Google e o Facebook é estimado deterem cerca de dois terços do mercado de anúncios digitais nos Estados Unidos71 e cerca de 80% no Reino Unido.72 Isto significa que o dinheiro foi movido para longe dos anunciantes 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, a Google controla muitos aspetos da cadeia de valor, e funciona como um comprador, vendedor e espaço de mercado.74 Se a Google manipular as suas ferramentas para beneficiar os seus serviços de anúncios e dificultar a concorrência de tecnologias rivais, estes efeitos de anticoncorrência não só prejudicariam potenciais concorrentes, mas também resultaria numa menor escolha e preços mais elevados para os consumidores.75

Estes efeitos anticoncorrenciais podem-se tornar mais enraizados se as plataformas dominantes afastarem-se de permitirem o uso e a recolha de dados de por terceiros. Mesmo que medidas como limitar o número de atores que podem aceder aos dados pessoais, o que seria positivo do ponto de vista da privacidade, pode também contribuir para que o pequeno número de atores dominantes ainda alicercem a sua posição como "donos da informação".76

No cenário atual, é difícil para os modelos de negócios alternativos da publicidade digital competirem com os atores dominantes. Isto tem muitas causas, incluindo os efeitos da rede, anticoncorrência, comportamento de atores 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, muitas soluções técnicas vinculadas a soluções de publicidade 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 restrição?
Uma restrição geral da publicidade baseada na vigilância poderia contribuir para nivelar o campo de jogo entre editores/anunciantes e plataformas dominantes, o que seria um estimulo para um melhor mercado competitivo para a publicidade. Contudo, as posições dominantes do Facebook e da Google também devem ser abordadas por outros meios, nomeadamente através da aplicação da regulamentação anticoncorrência, *antitrust*. Qualquer intervenção regulatória deve ser complementada com cumprimento da lei da concorrência ao nível de acordos anticoncorrenciais (por exemplo, entre os diferentes intervenientes na cadeia de fornecimento da publicidade) e para evitar o abuso de posições dominantes.

A proibição da publicidade baseada na vigilância também poderia ajudar os consumidores ao contribuir para uma maior liberdade de escolha e pluralidade dos meios de comunicação, e criar um terreno para nova inovação.

4.7 Fraude e perda de receitas

Apesar dos defensores da publicidade baseada em vigilância, por vezes defendam a capacidade de medir a eficiência dos anúncios, estas medições não são necessariamente precisas. A fraude de anúncios é um problema generalizado em toda a indústria, a ser usada para inflacionar fortemente o número de visualizações de anúncios e cliques. A automação e escala do marketing, e o número enorme 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 significa também que os consumidores podem facilmente ser expostos a fraudes e esquemas através de anúncios direcionados.80 Isto, leva a que os consumidores sejam prejudicados, financeiramente e de outras formas, e danos de reputação para os anunciantes que acabam por hospedar anúncios criminais.81

A complicada rede de atores na indústria da publicidade baseada na vigilância tem levado a muitos anunciantes e editores ficarem com uma visão geral limitada de para onde vai o seu investimento nos anúncios, o que, por sua vez, gerou uma grande indústria de fraude baseada em anúncios.82 Este tipo de fraude é frequentemente executada por ter anúncios mostrados para *bots* em vez de seres humanos, o que por sua vez reduz o preço que os editores/promotores podem pedir para o

espaço de anúncios e faz com que os anunciantes paguem por anúncios que nenhum consumidor realmente viu.83 Por outras palavras, os atores honestos acabam por pagar pela publicidade que nunca atinge uma audiência de modo algum.

O uso de intermediários levou a grandes quantidades de receitas publicitárias irem para terceiros.84 Isto significa, por exemplo, que o dinheiro que de outra forma ia chegar a um jornal local está sendo engolido por atores de terceiros, e em alguns casos, não pode ser rastreado.85 O que deu origem a perguntas sobre se a publicidade baseada na vigilância é financeiramente sustentável para editores, anunciantes.86

O aumento da fraude de anúncios levou ao surgimento de um grande mercado de ferramentas de deteção fraude. 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 às 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 publicação dos anúncios. Estes números foram provados serem imprecisos ou totalmente falsos, o que pode ter graves consequências para empresas.88 Outras ferramentas que se destinavam a prevenir a fraude de anúncios e fornecer aos anunciantes segurança também foram encontradas conter falhas significativas.89 A luta contra a fraude de anúncios tornou-se uma espiral negativa onde os anunciantes, como bem como marcas e consumidores, são todos perdedores.

Como é que as questões relacionadas com a fraude serão resolvidas através de uma interdição?
Uma interdição geral da publicidade baseada na vigilância levaria a maior transparência na cadeia estrutural e, provavelmente, reduziria a quantidade de fraude de anúncios. Esta por sua vez diminuiria a necessidade de instrumentos de deteção de fraude dispendiosos e invasivos, que seria uma bênção para os fundos monetários dos editores e anunciantes, bem como para privacidade e segurança do consumidor. A interdição deve ser complementada com outras medidas com intuito de combater a fraude, tais como a obrigação para os mercados online de verificar a 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 a serem partilhados e distribuídos 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 da publicidade.90

Nestes sistemas, não há uma distinção real entre consumidores "normais" e indivíduos em papéis críticos. Por exemplo, a emissora pública norueguesa NRK revelou como os dados pessoais recolhidos por 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 o risco de os dados pessoais ser espalhados como resultado de *hacking* ou violação de dados. Isto significa que os criminosos podem ser capazes de aceder a informações pessoais que podem ser usadas para roubo de identidade, fraude, e fins de chantagem. Os dados que foram descarregados ou vazados também podem ser mal utilizados para identificar, rastrear e prejudicar indivíduos e grupos vulneráveis[93] ou em tentativas de influenciar ou interferir em eleições democráticas.

Além de violações de dados que conduzem a riscos de segurança, a publicidade digital tem vindo a ser um vetor para a propagação de código malicioso, como *malware* ou vírus.[94] Ou seja, alguns blocos de publicidade podem incluir *scripts* que infetam o dispositivo do consumidor, podendo levar a atores maliciosos aceder ao dispositivo, danificar o dispositivo ou, de outra forma, interferir com as operações do dispositivo.

Como podem os riscos de segurança ser resolvidos com uma proibição?
Uma proibição geral da publicidade baseada na vigilância iria estrangular grandes partes do fluxo de dados e a recolha de dados pessoais. Isto ajudaria a diminuir o risco potencial para falhas de segurança e o uso indevido destes dados. Resumindo, se os dados não forem recolhidos ou armazenados, não podem ser utilizados para prejudicar consumidores ou instituições.

4.9 Falta de confiança

Embora as temáticas relativas a violações de privacidade e segurança online tenham recebido atenção pública significativa nos últimos anos, os consumidores são muitas vezes deixados com poucas alternativas e continuam a usar serviços problemáticos. Algumas plataformas não têm concorrência, o que significa que os consumidores não podem mudar para um serviço diferente, mesmo que preferissem. Noutros casos, a complexidade e escala das práticas problemáticas são tão vastas que os consumidores não podem realisticamente compreender os danos, proteger-se ou tomar uma ação preventiva. Isto leva à desilusão, fadiga e falta de confiança nos fornecedores de serviços digitais, impactando a economia digital para além da publicidade.[95]

Apesar da maioria dos consumidores tenham poucas, ou mesmo nenhuma, maneiras de se proteger contra a vigilância comercial online, e não se pode esperar que tome medidas, a falta de confiança nos serviços digitais tem sido um fator importante no aumento de ferramentas de bloqueio e rastreio de publicidade. 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 dos atores honestos estão bloqueados, o que leva tanto a anunciantes como a editoras perderem 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, ele teria que passar centenas de horas todos os anos a ler documentação legal e combater padrões negros projetados para influenciar a sua autonomia, decisões e escolhas.

O uso de padrões obscuros para forçar os consumidores a aceitar o rastreio muda o equilíbrio da informação e poder para a desvantagem do consumidor.[96] A soma destas práticas significa que os consumidores estão constantemente a ser induzidos para fazer escolhas que não têm forma prática ou realista de controlar, compreender ou relacionar-se. Esta situação absurda também contribui à falta de confiança nos serviços digitais.

Devido às cadeias opacas de fornecimento de sistemas de publicidade baseados em vigilância, é difícil também para os anunciantes terem controlo onde os seus anúncios são exibidos. Isto levou a um grande número de casos em que os anúncios foram exibidos ao lado de e usados para financiar conteúdo extremo ou odioso, levando associações negativas para a marca/anuncio.97

Em acréscimo, a falta geral de confiança pode reduzir a propagação e o uso de serviços úteis, e têm um efeito negativo sobre as empresas que tomam privacidade e segurança a sério.98 Isto pode ter sérios efeitos de "gelar" o comportamento do consumidor, que pode impedir os consumidores de utilizarem serviços importantes relacionados para a saúde mental99 ou de procurar 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 as pequenas e médias empresas que querem competir em fatores como o desenvolvimento de tecnologias de preservação de privacidade.

Como é que a falta de confiança nos serviços digitais pode ser resolvida através de uma proibição?
Banir na generalidade a publicidade baseada na vigilância não será uma cura para restaurar a confiança nos serviços digitais. Os escândalos são muito numerosos, e têm ocorrido repetidamente ao através de um longo período de tempo. Vai levar tempo para restaurar a confiança. No entanto, uma proibição contribuiria para um nivelar do campo de jogo onde as receitas monetárias dos anúncios, em grande parte, teria como destino os atores honestos. Por si só, isto pode contribuir para que os consumidores já não tenham a sensação ou noção que os prestadores de serviços e marcas estão a olhar sobre o seu ombro on-line e deixarem de achar que são tratados como mercadorias que são vendidas ao licitador mais alto. Pode também restaurar a confiança, tranquilizando os consumidores de que as marcas não estão a patrocinar conteúdo de ódio.

4.10 Tecnologia ineficiente

Tem sido contestado se, além de criar e ampliar um conjunto de problemas sérios, a tecnologia por trás da publicidade baseada na vigilância é na verdade eficaz como uma ferramenta de marketing. Mesmo com as inovações em áreas como inteligência artificial, muitas vezes apresentada como revolucionária para a indústria da publicidade, vale a pena questionar se os efeitos de marketing da tecnologia não estarão a ser sobrevalorizados.101 Isto é exemplificado por estudos que mostram que publicidade baseada em vigilância, em muitos casos, não teve efeitos benéficos em retorno, taxas de conversão ou receitas editoriais.102

Estudos têm demonstrado que as empresas que vendem tecnologias para publicidade estão a exagerar significativamente na eficácia das tecnologias e no alvo real que está longe de ser preciso.103 Embora a prática de criar perfis, *profilling*, com base em colecionar dados possa ser precisa em certas circunstâncias, em outros casos as inferências desenhadas podem ser imprecisas ou plenamente erradas.104

Há também desafios relacionados com os anunciantes visarem os consumidores que já estão a planear a compra ou que até já compraram o produto anunciado. Pode ser difícil, ou mesmo impossível, para um anunciante distinguir efetivamente entre uma venda feita por causa de um anúncio exibido ou uma venda que apesar do anúncio ser exibido, o consumidor iria fazer a compra independentemente.105 Por outro lado, a publicidade online é muitas vezes dependente da prática

de clicar nos anúncios pelos consumidores, e o volume elevado de publicidade pode levar à maioria do material de marketing transformar-se em ruído de fundo.106

Apesar de uma grande parte das tecnologias da publicidade digital poderem ter efeitos limitados, isto não significa que as decisões baseadas em fracas tecnologias serão melhores para os consumidores do que decisões baseadas em tecnologias precisas. A imprecisão da tecnologia não é um fator atenuante se os consumidores estão sujeitos a discriminação, manipulação ou exclusão.

Existem também ineficiências sérias no uso do poder computacional e energia na publicidade baseada em vigilância. Apesar do consumo de energia dos *data centers* não ser um problema exclusivo da publicidade, diversos estudos têm demonstrado que as tecnologias de publicidade digital têm uma pegada de carbono significativa.107 O impacto ambiental da publicidade baseada na vigilância é agravado pela uso da inteligência artificial e a prevalência de *bots* usados para fraude de anúncios.108

Como pode a tecnologia ineficiente ser resolvida através de uma restrição?
Uma restrição geral da publicidade baseada na vigilância limitará as oportunidades tecnologias de vender a "banha da cobra" que prometem muito mais do que podem entregar a anunciantes e editores. Isto pode reduzir as perdas de receitas para anunciantes e editores e ajudar a proteger os consumidores contra decisões baseadas em tecnologias defeituosas e suposições.

O impacto ambiental da publicidade baseada na vigilância pode ser reduzido desta pegada de carbono excessiva, mas outras medidas complementares são necessárias para lidar com os níveis de emissão dos centros de dados e a inteligência artificial.

5. Legislação em vigor

Como descrito acima, o banir da publicidade baseada na vigilância não é uma cura ou solução para tudo. Os serviços digitais já estão sujeitos a uma série de regras e regulamentos na UE, e uma proibição seria complementar para o enquadramento legal existente. Na secção seguinte, a existente proteção de dados europeia e direitos dos consumidores é analisada em relação aos prejuízos decorrentes da vigilância publicitária.

5.1 Legislação da privacidade e proteção de dados na UE

O Regulamento Geral de Proteção de Dados (RGPD) regula o processamento de dados pessoais. A proteção de dados pessoais é considerada um direito humano fundamental e o RGPD visa principalmente capacitar os indivíduos com o controlo dos seus dados pessoais e proibir o tratamento de dados pessoais sem uma base legal válida. Como regra geral, a utilização de dados pessoais para *profiling* e *tracking*, especialmente quando isto envolve a partilha contínua de dados pessoais, requer um consentimento válido.109 Isto também foi afirmado pelas autoridades de proteção de dados europeia.110

O trabalho feito pelo Conselho Norueguês do Consumidor no domínio da publicidade digital mostra que a indústria de publicidade baseada em vigilância opera em formas que envolvem recolha ilegal,

partilha e uso de dados pessoais. Estas práticas estão generalizadas e são complicadas de entender, mesmo para especialistas. A soma destas práticas resulta em todos os consumidores ficarem vulneráveis por defeito perante a face da publicidade baseada em vigilância. Portanto, não é razoável afirmar que os consumidores entendem o que estão a consentir ao aceitarem o rastreio e *profiling* para fins publicitários. Se for este o caso, o processamento de dados pessoais para fins de publicidade baseados em vigilância tem-se provado na maioria dos casos não estar em conformidade com o RGPD. Isto foi também afirmado pela Autoridade de Proteção de Dados Norueguesa *Datatilsynet*, quando anunciou a sua intenção de multar a aplicação online de encontros *Grindr* por processamento 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 online, 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 persistem mesmo que os dados pessoais não sejam transferidos do dispositivo do utilizador. Nestes casos, tanto o RGPD como a diretiva *ePrivacy* podem ser insuficientes para lidar com os problemas. Daí medidas complementares, como a proibição geral sobre a publicidade baseada na vigilância, podem ser necessárias para combater estes problemas mais amplos.

5.2 Diretiva relativa às práticas comerciais desleais

A diretiva relativa às práticas comerciais desleais *Unfair Commercial Practices Directive*, UCPD) estabelece um quadro europeu para que marketing, práticas comerciais e termos de utilização os atores comerciais possam participar em diferentes mercados. As autoridades de proteção do consumidor são responsáveis pela aplicação desta lei e pela garantia que os consumidores estão protegidos.

A UCPD é neutra em tecnologias, e pode em teoria, ser usada em casos que dizem respeito à publicidade baseada na vigilância. O marketing direcionado a indivíduos na forma de publicidade invasiva pode dar origem a dúvidas se a tecnologia que é usada para influenciar uma entidade recetora cruza os limites para o que constitui influência ou pressão injusta e ilegal.

Perguntas podem surgir sobre se certas formas de publicidade alicerçadas em espiar o consumidor cumprem os critérios para práticas comerciais agressivas no âmbito do *Marketing Control Act*.[112] Esta disposição destina-se ao marketing que emprega medidas que são consideradas ofensivas para as reconhecidas normas sociais generalizadas.

No entanto, a UCPD está predominantemente preocupada com o conteúdo e forma das atividades de marketing e materiais. As numerosas questões problemáticas que advêm da utilização da publicidade baseada na vigilância não estão necessariamente ligadas ao conteúdo do marketing, mas sim nos meios de entrega de anúncios, incluindo o processo de decidir que anúncio mostrar, a que pessoa, em que tempo. Isto, e a natureza fugaz da publicidade baseada em vigilância, pode significar que a UCPD não é adequada para o fim de regular esta área específica.

Pelo nosso conhecimento, nenhuma decisão sobre publicidade baseada em vigilância foi emitida pelas autoridades de defesa do consumidor.

5.3 Questões de execução

Embora o RGPD estabeleça requisitos rigorosos para o tratamento de dados pessoais, o regulamento não foi o suficiente para parar a recolha generalizada ilegal de dados e perfis de consumidores. As razões para esta deficiência estão nas empresas que não cumpriram as regras e por ter sofrido sérios estrangulamentos de execução transfronteiriça e falta de fiscalização.

O RGPD introduziu novos mecanismos de execução que procuraram facilitar a aplicação transfronteiriça, mas até agora isso não funcionou como desejado. Por exemplo, um grande número de queixas legais foram transferidas para a Comissão de Proteção de Dados Irlandeses, uma vez que muitas das grandes empresas tecnológicas têm a sua sede Europeia 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 uma rápida decisão ou coima administrativa é relativamente pequena.

A aplicação da UCPD contra infrações na área da vigilância publicitaria não teve, pelo que sabemos, ocorrido. Penalizar infrações isoladas é um processo demorado e só acontece após a ocorrência de uma infração e os danos nesta fase já foram causados. Na prática, isto significa que um grande número de empresas estão a escapar a lei. O facto do marketing ser personalizado e fugaz, uma vez que é apenas mostrado a pessoas particulares em determinados momentos no tempo, faz com que o controlo e aplicação da lei seja difícil. Além disso, a forma invasiva e problemática da publicidade baseada em vigilância pode não necessariamente violar a UCPD, uma vez que o conteúdo e o contexto de um certo anúncio pode estar fora do enquadramento da lei mas ainda assim ser prejudicial na forma como o anúncio foi entregue ou como o destinatário foi escolhido.

A falta de execução do RGPD levou também a uma situação em que um grande número de atores têm sido capazes de continuar a operar ilegalmente sem enfrentar quaisquer consequências significativas. Modelos onde os perfis de utilizadores são criados e armazenados localmente nos dispositivos do consumidor podem ou não reduzir riscos de privacidade, mas a utilização de personalização e individualização ainda tem problemas relacionados com discriminação, manipulação ou exclusão, e também é muito difícil de controlar ou verificar.

Uma vez que, investigar os casos individuais destas violações requer tempo, recursos consideráveis e acontecem depois do ato, é pertinente considerar se são necessárias medidas mais abrangentes para travar a utilização da publicidade baseada em vigilância. Ao invés de considerar casos individuais de marketing, deve ser considerada uma interdição geral da publicidade baseada na vigilância. Isto contribuiria para uma aplicação mais eficiente e rápida, e enviaria uma forte mensagem para o marketing e para a indústria da publicidade online, *Adtech*.

6. Conclusão

A publicidade baseada na vigilância causa violações dos direitos fundamentais, fraude generalizada e perda de receitas e tem contribuído para uma série de efeitos negativos individuais e sociais. Apesar dos repetidos avisos, multas, escândalos e revelações, a indústria tem mostrado pouca

vontade de alterar significativamente as suas práticas, e é questionável se alterações significativas 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 terem acontecido. É, portanto, oportuno perguntar se publicidade baseada em vigilância deve ser banida totalmente, de modo a evitar o problemas que estão a ser causados em primeira instância. Uma interdição contribuiria também para um equilíbrio do campo de jogo na publicidade digital e maximizar receitas para anunciantes e editores que atualmente estão nas mãos de apenas alguns atores.[114]

Um veto geral da publicidade baseada na vigilância vai forçar muitos atores da indústria a mudar os seus modelos de negócio. Estimularia o crescimento de 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 mais valia para os consumidores, para as empresas e para a sociedade em geral.

Incentivamos os decisores políticos de ambos os lados do Atlântico a decretar regulamentos rigorosos para minimizar os inúmeros danos resultantes da publicidade baseada na vigilância. Políticas eficazes, regulação e execução para abordar o vigilância comercial que penetra o nosso dia-a-dia há muito que são necessárias. Como temos discutido ao longo de todo este relatório, os benefícios percetíveis da publicidade baseada na vigilância são superados de longe pelos prejuízos criados e, a proibição, é portanto a solução certa.

7. Links

[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-business-model-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.html
[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
[9] For an example of this industry argument, see 'What would an internet without targeted ads look like'. Interactive Advertising Bureau Europe. https://iabeurope.eu/knowledge-hub/iab-research-

what-would-an-internet-without-targeted-ads-look-like/
[10] ‘What is Vendor Relationship Management?’. Doc Searls. https://www.capgemini.com/2015/08/what-is-vendor-relationship-management/
[11] ‘To track or not to track? Towards privacy-friendly and sustainable online advertising’. Karolina Iwanska. https://en.panoptykon.org/privacy-friendly-advertising
[12] Existem diferentes tipos de contexto publicitário. Alguns destes podem ser parcialmente baseados no tratamento de dados pessoais e na criação de perfis de utilizador, e podem ser usados para contornar a proteção de privacidade percebida pelo indivíduo. Ao longo deste relatório, usamos o termo "publicidade contextual" para nos referirmos a tipos de anúncios contextuais que não dependem do rastreio e perfis dos consumidores.
[13] ‘Can Killing Cookies Save Journalism?‘. Gilad Edelman. https://www.wired.com/story/can-killing-cookies-save-journalism/ ‘After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue‘. Jessica Davies. https://digiday.com/media/gumgumtest-new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/
[14] ‘Update (Six Months of Data): lessons for growing publisher revenue by removing 3rd party tracking‘. Johnny Ryan. https://brave.com/publisher-3rd-party-tracking/
[15] ‘After GDPR, The New York Times cut off ad exchanges in Europe — and kept growing ad revenue‘. Jessica Davies. https://digiday.com/media/new-york-times-gdpr-cut-off-ad-exchanges-europe-ad-revenue/
[16] ‘A‘ is for ad money oddly gone missing: Probe finds middlemen siphon off half of online advertising spend‘. Thomas Claburn. https://www.theregister.com/2020/05/07/ad_tech_fees_sucked/
[17] ‘Two years on from complaint to the Irish Data Protection Commission, the RTB data breach is the largest ever recorded, and appears to have worsened.‘. Johnny Ryan. https://www.iccl.ie/wp-content/uploads/2020/09/1.-Submission-to-Data-Protection-Commissioner.pdf
[18] However, this is often combined with third-party data or data collected through third party platforms, for example through tracking pixels. See for example ‘Missed by Filter Lists: Detecting UnknownThird-Party Trackers with Invisible Pixels’. Imane fouad, Nataliia Bielova, Arnaud Legout, Natasa Sarafijanovic-Djukic. https://sciendo.com/article/10.2478/popets-2020-0038
[19] ‘Google’s FLoC Is a Terrible Idea‘. Bennett Cyphers. https://www.eff.org/deeplinks/2021/03/googles-floc-terrible-idea
[20] ‘Online platforms and digital advertising market study‘. Competition and Markets Authority. https://www.gov.uk/cma-cases/online-platforms-and-digital-advertising-market-study
[21] ‘Facebook to release first-party cookie option for ads, pull web analytics from Safari‘. Ginny Marvin. https://marketingland.com/facebook-to-release-first-party-pixel-for-ads-web-analytics-from-browsers-like-safari-249478
[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] ‘Alphabet reports big earnings beat as revenue grows 34%‘. Jennifer Elias. https://www.cnbc.com/2021/04/27/alphabet-goog-earnings-q1-2021.html
[24] See, for example, ‘Nordmenn og deling av persondata‘. Norsk Regnesentral. https://www.nr.no/sites/default/files/files/NR-Rapport_Nordmenn-og-deling-avpersondata_ALerT2019.pdf
[25] ‘Surveillance-based advertising: Consumer attitudes to surveillance-based advertising’. Norwegian Consumer Council.

https://fil.forbrukerradet.no/wpcontent/uploads/2021/06/surveilance-marketing-survey.pdf
[26] ‘The Dark Side of Customer Data‘. RSA. https://www.rsa.com/enus/company/news/the-dark-side-of-customer-data
[27] ‘Do people really want personalised ads online?‘. Global Witness. https://www.globalwitness.org/en/blog/do-people-really-want-personalised-ads-online/
[28] ‘Accountable Tech Frequency Questionnaire‘. Accountable Tech. https://accountabletech.org/wp-content/uploads/Accountable-Tech-FrequencyQuestionnaire.pdf
[29] ‘iOS 14.5 Opt-in Rate - Daily Updates Since Launch‘. Estelle Laziuk. https://www.flurry.com/blog/ios-14-5-opt-in-rate-att-restricted-app-tracking-transparencyworldwide-us-daily-latest-update/
[30] The nuances and distinction between individualization and personalization is explored in ‘EU Consumer Protection 2.0: Structural asymmetries in digital consumer markets‘. Natali Helberger, Orla Lynskey, Hans-W. Micklitz, Peter Rott, Marijn Sax, Joanna Strycharz, p. 94. https://www.beuc.eu/publications/beuc-x-2021-018_eu_consumer_protection.0_0.pdf
[31] ‘10 Reasons Why Online Advertising is Broken‘. Karolina Iwańska. https://medium.com/@ka.iwanska/10-reasons-why-online-advertising-is-brokend152308f50ec
[32] Such ad registries would have to avoid a number of pitfalls in order to be useful. See for example ‘Platform ad archives: promises and pitfalls’. Paddy Leerssen, Jef Ausloos, Brahim Zarouali, Natali Helberger, Claes H. de Vreese. https://policyreview.info/articles/analysis/platform-ad-archives-promises-and-pitfalls
[33] ‘Out of Control‘. Forbrukerrådet. https://www.forbrukerradet.no/out-of-control/
[34] ‘Dark Patterns‘. Forbrukerrådet. https://www.forbrukerradet.no/dark-patterns/
[35] ‘Offentlige nettsteder sporer oss‘. Teknologirådet. https://teknologiradet.no/offentligenettsteder-sporer-oss/
[36] ‘Oracle’s BlueKai tracks you across the web. That data spilled online‘. Zack Whittaker. https://techcrunch.com/2020/06/19/oracle-bluekai-web-tracking/
[37] The GDPR enforcement gap is described in detail in ‘The Long and Winding Road: Two years of the GDPR: A cross-border data protection enforcement case from a consumer perspective‘. BEUC. https://www.beuc.eu/publications/beuc-x-2020-074_two_years_of_the_gdpr_a_cross-border_data_protection_enforcement_case_from_a_consumer_perspective.pdf
[38] ‘Facebook's GDPR bypass reaches Austrian Supreme Court‘. Noyb. https://noyb.eu/en/facebooks-gdpr-bypass-reaches-austrian-supreme-court
[39] ‘Shaping Europe’s Digital Future. Proposal for ePrivacy Regulation‘. European Commission. https://digital-strategy.ec.europa.eu/en/policies/eprivacy-regulation
[40] ‘Facebook told advertisers it can identify teens feeling “insecure” and “worthless”‘. Sam Levin. https://www.theguardian.com/technology/2017/may/01/facebook-advertisingdata-insecure-teens
[41] ‘What a Gambling App Knows About You‘. Adam Satariano. https://www.nytimes.com/2021/03/24/technology/gambling-apps-tracking.html
[42] ‘Facebook allows advertisers to target children interested in smoking, alcohol and weight loss‘. Josh Taylor. https://www.theguardian.com/technology/2021/apr/28/facebook-allows-advertisers-totarget-children-interested-in-smoking-alcohol-and-weight-loss
[43] ‘About Lookalike Audiences‘. Facebook. https://www.facebook.com/business/help/164749007013531?id=401668390442328
[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
[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
[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.
[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/
[65] 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 [66] '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
[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
[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
[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
[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
[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
[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/
[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
[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
[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/
[112] Lei de Controlo de Marketing, secção 9, secção 6.
[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
[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

Autor da tradução: *zcavaleiro AT protonmail DOT com*
Zito Cavaleiro
Engenheiro de Automação de Tecnologias de Informação
Professor de Matemática e Ciências da Natureza