revista Fronteiras – estudos midiáticos
24(3):98-108 setembro/dezembro 2022
Unisinos – doi: 10.4013/fem.2022.242.09

A experiência da Google como panóptico[*]

The experience of Google as a panopticon

Ana Regina Rego[**]
anareginarego@gmail.com

RESUMO
O artigo apresenta questões importantes no debate sobre o poder das plataformas digitais e sua ascendência sobre os usuários, assim como, sobre empresas e governos. A vigilância considerada um operador econômico por Foucault retorna à cena como uma estratégia de grande relevância no sucesso do modelo de negócios das *big Techs*. A tecnologia a serviço do capitalismo termina por proporcionar usos da experiência humana como capital. É, portanto, na convergência entre vigilância, controle e biopoder como estratégias do capital que o presente trabalho científico se estrutura e analisa rastreadores de dados comportamentais da Google em aplicativos de uso comum na sociedade.

Palavras-chave: Google; panóptico; vigilância; atenção; rastreadores.

ABSTRACT
The article presents important issues in the debate about the power of digital platforms and their ascendancy over users, as well as over companies and governments. Surveillance, considered an economic operator by Foucault, returns to the scene as a strategy of great relevance in the success of the business model of big Techs. Technology at the service of capitalism ends up providing uses of human experience as capital. It is, therefore, in the convergence between surveillance, control and biopower as strategies of capital that the present scientific work is structured and analyzes Google's behavioral data trackers in applications of common use in society.

Keywords: Google; panopticon; surveillance; attention; trackers.

[*] Este texto faz parte de pesquisa científica desenvolvida com o apoio do CNPq.
[**] Universidade Federal do Piauí (UFPI). Campus Universitário Ministro Petrônio Portella - Ininga, Teresina - PI.

Introdução

> *A moral reformada; a saúde preservada; a indústria revigorada; a instrução difundida; os encargos públicos aliviados; a economia assentada, como deve ser, sobre uma rocha, o nó górdio da Lei sobre os pobres não cortado, mas desfeito_ tudo por uma simples ideia de arquitetura! Tudo isso arrisquei-me a dizer ao repousar a pena; tudo isso deveria eu, talvez, ter dito ao tomar a pena, se desde o início eu tivesse visto a totalidade do caminho que se estendia diante de mim.* **Tratava-se de um novo modo de garantir o poder da mente sobre a mente***, em um grau nunca demonstrado; e em um grau igualmente incomparável, para quem assim o desejar, de garantia contra o exagero. (BENTHAM, 2019, p.17, grifos nossos).*

É assim que Jeremy Bentham inicia o prefácio do livro *O Panóptico* em que propõe um novo princípio construtivo que privilegiaria a vigilância de todos, em todas as etapas da estrutura, inicialmente proposta para as penitenciárias, mas adaptável para casas de indústrias, casas de trabalho, casas para pobres, manufaturas, hospícios, hospitais e escolas. A proposição de Bentham concentrava-se na construção de dois edifícios circulares e concêntricos. O primeiro interno seria uma torre central de onde se poderia vigiar, diuturnamente, o segundo edifício exterior, onde ficariam as celas com os presos, expostas permanentemente aos inspetores da torre central.

Foucault (2002) aponta a vigilância como uma estratégia utilizada na condução da repressão e punição da criminalidade, mas também a situa em outros ambientes, como o escolar e o das fábricas, onde uma medida disciplinar se impunha. Desse modo, a vigilância torna-se uma necessidade constante na economia de produção. É nesse contexto, que Foucault (2002, p.147) enfatiza que "a vigilância se torna um operador econômico decisivo, na medida em que é ao mesmo tempo uma peça interna no aparelho de produção e uma engrenagem específica do poder disciplinar".

Para Foucault (2002, p.169) o panóptico passa a funcionar como um tipo de laboratório de poder. "Graças a seus mecanismos de observação, ganha em eficácia e em capacidade de penetração no comportamento dos homens; um aumento de saber vem se implantar em todas as frentes de poder [...]".

Conforme Autor (2020), os mecanismos de vigilância tornavam o poder disciplinar discreto porque este funcionava silenciosamente, mas ao mesmo tempo impositivo e indiscreto, tendo em vista que se apresentava de modo ubíquo e alerta com vistas a manter e controlar tanto os indivíduos de uma fábrica, escola ou prisão, como também a vigiar os próprios fiscais de cada sistema disciplinar.

Em Deleuze (1992) a vigilância se situa no contexto de uma sociedade do controle, que extrapolaria o ambiente da sociedade disciplinar, sobretudo, porque na análise foucaultiana, os ambientes denunciados pelo autor como ideais para instalação da disciplina a partir da vigilância, eram *fechados* e controlados. Contudo, os movimentos de vigilância com vistas ao controle social e mercadológico, se tornaram mais abrangentes e pautados pelas ações do Estado e do Mercado frente à sociedade. O controle seria nessas bases um aprimoramento da disciplina a ser aplicada em um ambiente amplo. Como enfatiza Sodré (2021, p.79), a vigilância da sociedade disciplinar foucaultiana e o controle trabalhado por Deleuze guardam similaridades. Sociedade do controle "é tão só a forma acabada da domesticação social não violenta em termos físicos, mais próxima dos conceitos foucaultianos de *governamentalidade* ou dispositivo". A vigilância e o controle para Deleuze (1992) estariam potencialmente a serviço do capital.

O aprimoramento da vigilância levou à descoberta do que Zuboff (2020) denomina de capital de predição que segundo a autora, possui dupla finalidade, uma mercadológica de aprimoramento dos produtos de cada plataforma e de vendas às empresas que anunciam em seus espaços e com as quais mantém contrato unilateral, e outra que estaria voltada para a moldagem das sociedades aos parâmetros pensados por seus criadores, a exemplo, de um mundo ideal, mas para poucos, de Larry Page e Mark Zuckerberg. Esse excedente do capital de predição comportamental seria, na visão da autora, o principal capital de cada *big Tech*.

Para Zuboff (2020) as plataformas caminham no sentido de não permitir aos humanos algo que lhes é peculiar, ou seja, a própria falibilidade, o erro, a dúvida, o medo, a dor, a angústia, isso na tentativa de orientar as decisões presentes e futuras dos humanos. Obviamente que tal perspectiva desenhada por Larry Page e Mark Zuckerberg e outros, e denunciada por Zuboff (2020), Foer (2018) e Bratton (2016) possui espacialidade definida e não pode ser pensada para todo o globo, tendo em vista que grande parte da população mundial não se encontra inserida digitalmente, economicamente e educacionalmente, nem mesmo para se colocar disponível para tamanha manipulação com vistas a um poder mercadológico totalitário que esnoba o Estado Nação em alguns ambientes e em outros se insere neste, criando um poder híbrido. Por outro lado, há que se ponderar que existem forças de resistência

e em atuação nos países em que as plataformas digitais possuem grande poder, logo nenhuma realidade futura é simplesmente dada, mas disputada no presente.

Diante do exposto, este artigo se articula no sentido de trazer para o debate questões importantes e concernentes à vigilância das plataformas sobre seus usuários e do poder que estas adquirem em cada sociedade. Os pensamentos de Foucault e Deleuze já mencionados, são aqui situados como pano de fundo para compreensão do atual processo de interação/exploração da vida pelas plataformas e portanto, é no momento de abordagem deste fenômeno no presente texto, que autores como Koselleck, Zuboff, Bourdieu, Martins, Foer, Boden, Rothblatt, Sodré e Bratton, além de Plantin, Nieborg, Helmond, Moazed e Johnson, nos subsidiam do ponto de vista contextual e teórico. Na primeira parte do texto trabalhamos a experiência humana como capital e na segunda nos voltamos para a Alphabet/Google como dispositivo central de um processo capitalista e seus usos da economia comportamental, assim como da potencialização dos elementos de vigilância e trazemos a análise de três aplicativos de uso constante e suas interfaces com as plataformas da Alphabet, Meta e outras, com vistas a identificar rastreadores e dispositivos de vigilância.

A experiência humana como capital

Quando Koselleck (2015) elaborou as categorias meta-históricas espaço de experiência e horizonte de expectativas chamou atenção para o fato de que elas têm potência para estabelecer as condições de histórias possíveis. Abarcam possibilidades históricas que falam da condição humana e a história ganha através de Koselleck, metodologias de compreensão por um prisma antropológico. Enquanto a experiência é passado atual, a expectativa é futuro presente, onde o ainda-não prevalece e se delineia. Para Koselleck, as categorias não são coincidentes, nem tampouco a expectativa é completamente previsível na experiência. Na falibilidade humana residem as incertezas, as imprevisões, as dúvidas, os medos, o que nos impele a lutar no presente por um futuro enquanto esperança.

A potência do *ser-afetado-pelo passado*[1] histórico, mas também relacional e antropológico, por um lado, e a ignorância e a ausência de relação com a experiência anterior, por outro, podem ser definidores da luta no presente pelo passado e pelo futuro. Em Marx (*apud* Arendt, 2011) a história passa a ter um novo objetivo, não se trata mais de compreender o passado, mas de analisar as ações que podem mudar o futuro ou projetá-lo através dos movimentos sociais e da luta de classes. Em Koselleck (2014) a história não trata do acontecimento passado em si, mas das possibilidades na relação futuro-passado. A experiência humana em que se guarda as condições da experiência histórica é o que relaciona o presente com o passado, ao passo em que projeta o futuro.

Zuboff (2020) lembra que o livre-arbítrio está no centro das relações humanas e se coloca como definidor de acertos e erros, o que nos impele a modificar as experiências em prol de um futuro melhor, ou reforçá-las, obviamente, de acordo com a visão de mundo de cada grupo político/social/econômico. A liberdade de escolha, o poder de decidir o caminho é, na visão da autora, primordial à humanidade. Contudo, há que se ponderar que a perspectiva para a liberdade de escolha, como nos lembra Sen (2010), pressupõe um desenvolvimento voltado para a liberdade e, portanto, de inclusão das sociedades excluídas nos direitos fundamentais.

Nesse sentido, consideramos aqui como recorte para ambientar nosso debate e posterior análise, a ação do capitalismo tecnológico em um mundo incluído digitalmente, consciente de que os tentáculos das *big Techs* se espalham por todo o planeta, muito embora essa atuação se dê em diferentes proporções.

Assim é que nos referimos aqui à experiência humana que se lança nas plataformas digitais, por uma teórica, livre e espontânea vontade, para nós, não verdadeira, tendo em vista as imposições mercadológicas e sociais para um novo modo de vida em um novo *lócus* para o existir, onde socialidades acontecem e afetividades são desveladas. As velhas estratégias da vigilância e do controle já mencionadas acima, são ativadas em sua máxima potência com vistas a manter as populações disponíveis para a chamada mineração de dados, que em verdade se trata de extração de experiências, memórias, momentos, prazeres, dores, angústias, enfim, extração da vida.

Entretanto, essa extração da vida não é realizada, conforme Zuboff (2020) , Foer (2018) e Bratton(2016) somente com um viés econômico voltado para fins mercadológicos que trabalham infinitamente a retroalimentação de um capitalismo de produção imediato, há por trás da extração da experiência humana um viés na crença real na possibilidade de transformação comportamental das sociedades, com o intuito de "aprimoramento" das formas

1 – Conceito foucaultiano trazido por Ricoeur (2010) para o desenvolvimento da Hermenêutica da Consciência Histórica.

de dominação humana por parte do capital tecnológico que abomina a livre concorrência e outras características de um momento anterior, enquanto deseja que a humanidade caminhe de acordo com valores específicos. Larry Page da Alphabet (Google, YouTube...), Mark Zuckberg da Meta (Facebook, Instagram, WhatsApp ...), dentre outros, não somente acreditam, como propagam suas crenças no futuro que consideram melhor para o planeta, em que a eliminação das desigualdades não é pauta primordial.

Para muitos o que move o mundo é o capital econômico, contudo, nossa visão converge para a de Bourdieu (1998, 2008) considerando o mundo social como multidimensional e composto de campos "relativamente autônomos" cuja subordinação ao campo econômico se dá de modo relacional às disputas internas e externas aos campos envolvidos. Desse modo, e, ainda em conformidade com Bourdieu, também consideramos a pluralidade de capitais conforme o campo em que se produz e reproduz, implicando em um poder relacional que tanto explica as práticas do campo, como define o campo de poder que estrutura o lugar dominante. Como bem nos diz Foucault (1996, 1998, 2002) o poder não se detém, se exerce, a partir dos processos que possibilitam o biopoder e das redes que o estruturam.

O capital mobilizado pelas plataformas digitais que se alimentam da produção de conteúdo dos usuários e da experiência destes, extrapola a relação capital-trabalho de Marx, como também os diversos capitais propostos por Bourdieu na constituição de um poder simbólico, mas perpassa ambos os sentidos, tendo em vista que os explora, de um lado, na relação usuário-mercado presente e, de outro, na extração da experiência humana, onde as fórmulas dos capitais constitutivas de cada campo se relevam.

Como nos diz Bourdieu (1998, p.140) a incerteza

> *é o que dá fundamento à pluralidade das visões do mundo, ela própria ligada à pluralidade dos pontos de vista, como o dá a todas as lutas simbólicas pela produção e imposição da visão do mundo legítima e, mais precisamente, a todas as estratégias cognitivas de preenchimento que produzem o sentido dos objetos no mundo social ao irem para além dos atributos diretamente visíveis pela referência ao futuro e ao passado.*

Obviamente que o ambiente de Bourdieu não é o mesmo de Zuboff e dos demais, mas nos serve de referência crítica. Como nos detalha Foer (2018), em 2015 a controladora da Google tornou-se Alphabet, o que na concepção do autor revela uma pretensão de tornar-se tão necessária à humanidade e sua tecnologia tão revolucionária, como o foi, o alfabeto e a invenção da escrita. Naquele momento, a Google para além de possuir a maior ferramenta de busca do mundo e a maior biblioteca, já era um dos principais pilares da infraestrutura da internet e ao mesmo tempo era proprietária de uma gama de empresas que abarcam de *software* a *hardware*, de mídias sociais a rede de TVs e até empresa automobilística (FOER, 2018, p. 39) levando seus tentáculos em todas as direções, do mercado tangível ao intangível. Há ainda que se ressaltar que seu maior domínio e, portanto, campo de poder até o momento ilimitado, onde se localiza o seu maior capital é o das *nuvens*. Lá encontra-se o conhecimento e a experiência humana, além das informações governamentais e mercadológicas de outros.

Bratton (2016) ao explorar os efeitos do capitalismo tecnológico sobre a geopolítica mundial, aponta para novas *governamentalidades* e novas soberanias, mas principalmente, para velhas e novas disputas, como a que ocorre entre a Google e o governo Chinês que já se arrasta há mais de 20 anos, pela disputa da camada *Cloud*, onde o conhecimento e a experiência humana em todas as suas dimensões encontra-se armazenada e a partir de onde, o poder é hoje, exercido.

Obviamente que as tensões entre China e EUA abarcam as questões econômicas, ambientadas nas disputas mercadológicas em todos os níveis, assim como, territoriais, mas o espaço intangível e teoricamente não estatal e em muitos sentidos, apátrida, não pode ser desconsiderado, como parte das lutas que se anunciam. Para Bratton (2016) existe, entre os hackers do exército Popular da Libertação (China) e o Google, um conflito fundamental sobre a geografia política. Para este autor trata-se de uma tensão entre dois tipos de *governamentalidades* e duas distintas geometrias de território.

Foer (2018, p.40) detalha que no *core business* da Google há um projeto em especial que se sobressai, o que se destina ao desenvolvimento de Inteligência Artificial que possa replicar o cérebro humano. "Essa é a essência das tentativas de montar um banco de dados completo do conhecimento global e dos esforços para treinar algoritmos para encontrar padrões, ensiná-los a discernir imagens e entender línguas". Para este autor, a IA da Google é a principal fonte de seu poder, tendo em vista que esta é treinada para pensar como humanos, e, portanto, precisa identificar as nossas intenções. Recentemente o engenheiro

Blake Lemoine[2] foi demitido da Google por conta de suas declarações em relação à IA da Alphabet que, em suas palavras, teria adquirido consciência e sentimentos.

Os grandes empresários do Vale do Silício não são os únicos a apostar na Inteligência Artificial e em todo o escopo de possibilidades que se anunciam como irreversíveis, mas, principalmente, como elemento primordial que corre em dois sentidos que se interrelacionam. De um lado, a AI é vista por Boden (2020) e Rothblatt (2016) como uma grande aliada da humanidade nas mais diversas áreas que vão dos avanços na ciência e na medicina, às possibilidades tecnológicas que ajudam no combate a devastação do meio ambiente e no combate à fome. Entretanto, a AI apesar de ter seus méritos reconhecidos desde as descobertas de Alan Turing é também vista com desconfiança por Weeb (2020), Zuboff (2020), Foer (2018) e Bratton (2016), considerando os usos que as plataformas fazem da Inteligência Artificial, o que é visto com suspeição quando se trata da vigilância, monitoramento e mineração da experiência humana, assim como no que se refere ao desenvolvimento de produtos que se tornam a cada dia dispositivos de complemento do humano e, ao mesmo tempo, de mais vigilância e controle. A suspeita leva sempre a um comum, qual seja, a dominação econômica que se faz presente, talvez ganhando contornos hegemônicos mais potentes e menos visíveis. Para Zuboff (2020, p. 384), "assimetrias sem precedentes de conhecimento e poder nos prendem a uma nova desigualdade marcada por sintonizadores e sintonizados, pastores e pastoreados, a matéria-prima e seus mineradores, os responsáveis por experiências e suas desavisadas cobaias". Um abismo do conhecimento separa assim, os que tem desejo de futuro e os que se mantém reféns das atrações econômicas e financeiras das plataformas.

No centro do processo capitalista e tecnológico a experiência humana comumente compartilhada pelo afetar do sensível e agora extraída de nós pelas plataformas digitais, é o capital em negociação presente e futuro, mas não só em negociação, como também é o alicerce das bases de um horizonte de expectativas, que inclui a humanidade e pretende excluir o que nos torna humanos.

Vale destacar ainda a questão estrutural das plataformas e o processo de plataformização, que em si, não são objeto neste estudo, mas ao que nos dedicamos em outro momento. Aqui nos centramos mais nas relações e consequências da vida nas plataformas pelas perspectivas econômica, sociológica e filosófica do fenômeno já apresentadas. Nesse percurso, esclarecemos que a análise que realizamos a seguir surge como gesto desvelador dos meandros da vigilância e dominação, entretanto, é válido perceber que enquanto Plantin *et al* (2016) consideram diferenças contextuais e materiais entre infraestrutura tecnológica e plataformas, Helmond (2019) considera que redes sociais como o Facebook, são modelos de infraestruturas onde outros atores possam produzir e potencializar a visibilidade nos demais ambientes da web. Ao passo que Poell, Nieborg e Van Dijck (2020) procuram estabelecer o processo de construção e uma espécie de ontologia do fenômeno de plataformização. Contudo, a perspectiva para plataformas que aqui adotamos vem de Moazed e Johnson (2016) que definem como plataformas as estruturas tecnológicas que se configuram como modelos de negócios abertos e estruturados para proporcionar o encontro entre oferta e procura de um escopo negocial que extrapola o mercado de tangíveis e chega ao mercado das mentes e da experiência humana.

Google, a economia comportamental e a vigilância intermitente- observando aplicativos de uso comum e suas interfaces com rastreadores

É neste contexto, situado por Moazed e Johson (2016) que a Google é citada por Zuboff (2020) e Foer (2018) como um divisor de águas entre um capitalismo de produção e um novo capitalismo, que Zuboff denomina de vigilância, o que é contestado por Martins (2022) que argumenta que a vigilância é uma estratégia do capitalismo. Para Zubof (2020, p.401) no entanto, "sob o capitalismo de vigilância, os meios de produção servem aos meios de modificação comportamental", enquanto para Martins (2022) a vigilância está vinculada aos processos de hegemonia e tem tripla utilidade, a saber: atua na potencialização dos mecanismos de dominação social, dá maior amplitude a "subsunção do trabalho no capital" e, direciona o fluxo dos produtos e serviços.

Como vimos anteriormente, a vigilância é uma estratégia muito utilizada por diversas instâncias de poder e aparelhos do mercado e do Estado para desenvolver modelos de dominação cada vez mais potentes, seguros e precisos.

2 – https://g1.globo.com/tecnologia/noticia/2022/07/23/google-demite-engenheiro-por-ter-dito-que-programa-de-inteligencia-artificial-da-empresa-tem-consciencia.ghtml

No contexto da vida digital, a psicologia comportamental é acionada duplamente, ou seja, internamente na arquitetura relacional que interliga usuários e plataformas e, externamente através dos atrativos da economia e para que atue com eficácia a vigilância se faz necessária.

Como nos revelam Rêgo e Barbosa (2020), em 2012, Michal Kosinski, doutor em Psicometria por Cambridge, mostrou que com menos de 70 likes de um usuário no Facebook era possível saber a cor da pele, orientação sexual, filiação partidária, religião, relacionamentos, dentre outras informações. Posteriormente, bastavam 300 curtidas para saber de uma pessoa mais do que seu parceiro e acima disso, mais do que a própria.

Outra visada nos revela que a entrada da psicologia comportamental no cenário plataformizado atual também se dá através dos processos desencadeados pela economia comportamental desenvolvida por Thaler (2019), cuja tese é de que as pessoas realizam escolhas orientadas por questões subjetivas e culturais que em grande medida, podem se opor à racionalidade. A intencionalidade da pesquisa de Thaler denominada por este de economia comportamental termina por trazer para o campo econômico traços de humanidade, como gostos, dúvidas e principalmente, estudo dos direcionamentos comportamentais a partir de interveniências psicológicas.

Na união da psicologia comportamental com a economia comportamental localizamos novamente a estratégia da vigilância e de todas as formas de atração para atenção constante, assim como, para a manutenção de modos intencionais de disponibilidade dos usuários para a extração da experiência humana, a ser negociada em mercados do presente e do futuro. Por outro lado, a partir das ações da Cambridge Analytica e dos estudos de Kosinski o direcionamento das ações dos usuários tornou-se possível de modo efetivo. É nesse ponto que Zuboff (2020) destaca a economia da ação das plataformas, que se utiliza de estratégias de atração aos usuários para mantê-los conectados e poder direcionar suas ações.

A Google tem surgido nas pesquisas e nos debates como uma das *big Techs* mais especializadas em vigiar e extrair a experiência humana e com ela negociar nos mercados atuais e futuros. Segundo Foer (2018, p. 55) a Google fez ressurgir as redes neurais que envolvem processos de Inteligência Artificial baseados no cérebro humano, fazendo com que os algoritmos processem informações e fixem os métodos de aprendizagem. A aquisição da empresa inglesa DeepMind, especializada em redes neurais foi um passo importante no processo de transformação da AI da Google denunciada pelo engenheiro Blake Lemoine.

A teia negocial que tem a Alfabeth no centro, se estrutura em diversas direções como já mencionado ao longo do texto. O Google Workspace é um espaço pensado para disponibilizar inúmeros produtos Google a cada usuário. Os produtos vão dos alertas do Google, passando por Chromecast, Desenhos do Google, Documentos do Google, Drive, Google Academic, Google Earth, Google Finance, Google Meet, Google Fotos, Google Play, Google tradutor, Google Play books, Maps, Notícias até o YouTube, dentre outros. O Google Workspace pode ser contrato em edição individual ou *Business e Enterprise,* destinado a empresas e instituições e vendido em diversos tipos de pacotes, conforme as necessidades de cada empresa ou instituição e são comercializados em diversos patamares de preços. No Google Workspace as ações dos usuários ficam registradas nos mínimos detalhes, desde a agenda de reuniões e atividades diárias até a gravação das aulas, palestras etc.. Também ficam registrados os passos do usuário pela rede e pelos produtos que utiliza.

Para além disso, a relação dos usuários com a Alphabet extrapola o extenso ambiente deste e se estende a milhares de aplicativos que estão disponíveis para nosso uso diário e que mantém uma conveniente relação com a Google. Para que possamos visualizar, ainda que minimamente, o alcance da Alphabet em nossas vidas, escolhemos 3 aplicativos de uso comum, com vistas a observar o relacionamento dos aplicativos com a Google e os rastreadores que ficam disponíveis e que monitoram, vigiam e extraem dados dos usuários.

Dito isto, vale ponderar que a amostra intencional (Laville e Dione, 1999) escolhida em aplicativos de uso constante por parte da autoria do texto, se compõe de 2 aplicativos mercadológicos e 1 aplicativo do Governo brasileiro. A intenção é observar e identificar o uso dos rastreadores da Google e de outras plataformas nos programas escolhidos. Vale destacar que a análise foi realizada nas três primeiras semanas de julho de 2022 e reflete o panorama do momento, que pode ser modificado por cada aplicativo a cada atualização e aperfeiçoamento, contudo, como o que nos interessa especificamente é a identificação dos rastreadores da Google e de outras plataformas, as mudanças futuras não interferem em nosso processo analítico final.

O processo analítico desenvolvido em parceria com o cientista de dados, Alexandre Teles, compõe-se de cinco etapas, a saber: em primeiro lugar **download dos arquivos de aplicação** considerando que aplicativos Android são distribuídos através da Google Play Store em formato APK (https://pt.wikipedia.org/wiki/APK**).** Este passo permite a realização da análise estática. Em segundo

lugar, foi realizada a **instalação e análise de interfaces das aplicações.** De posse dos arquivos de instalação e dos metadados de aplicação, os softwares foram instalados em um emulador Android de forma que se pudesse interagir com as aplicações e verificar qualitativamente questões relevantes de *compliance* e melhores práticas de gestão de dados e privacidade. Depois, aplicamos **engenharia reversa** tendo em vista que para efetuar a análise estática das aplicações é necessário ter acesso ao seu código fonte em todo ou parte. Aplicações não ofuscadas por ferramentas como ProGuard[3] podem ser facilmente processadas e suas classes automaticamente extraídas do Bytecode Java[4] obtido na etapa de descompressão dos arquivos APK. As etapas necessárias para este processo são executadas de forma automática pela ferramenta APKPerm[5], desenvolvida pelo Instituto Nacional de Ciência e Tecnologia em Democracia Digital. O quarto passo, consiste na **análise de permissões, uso de permissões e rastreadores,** momento mais importante da nossa observação e motivo desta investigação nos aplicativos. Uma vez obtidos os arquivos fonte dos aplicativos por meio do processo de engenharia reversa, foram analisadas as permissões de sistema utilizadas pela aplicação, como elas são apresentadas e solicitadas ao usuário, como o aplicativo as utiliza, quais as bibliotecas de terceiros incluídas no software e quais ferramentas de rastreamento são utilizadas. Por último realizamos uma **análise heurística[6]** objetivando identificar por meio da JoeSandbox[7] comportamentos suspeitos da aplicação durante o processo de instalação e execução, analisando atividade de rede, do sistema de arquivos do dispositivo e a presença de técnicas de programação comumente associadas à aplicativos maliciosos como a ofuscação de métodos e o uso de reflexões.

Os aplicativos analisados em nossa amostra foram *Doctoralia* voltado para serviços de saúde, *123Milhas* especializado em venda de passagens áreas e o *Gov.Br*, aplicativo do Governo Federal que reúne diversas interfaces de relacionamento do cidadão e do funcionário público com o governo. Sendo o primeiro um aplicativo internacional, o segundo nacional e o terceiro pertencente ao Estado brasileiro.

Iniciando pelo Doctoralia que é um aplicativo para agendamento de consultas médicas e gerenciamento de agenda para usuários e provedores dos serviços de saúde. O Doctoralia foi desenvolvido pela Empresa Docplanner Group (https://www.docplanner.com/) e tem sua sede em Varsóvia, Polônia. Os Termos de uso deste programa podem ser localizados em https://www.doctoralia.com.br/termos-e-condicoes e sua Política de Privacidade pode ser localizada em https://www.doctoralia.com.br/privacidade .

No que concerne à privacidade e proteção de dados, no Doctoralia nenhum documento foi disponibilizado na página do aplicativo no Google Play contrariando as instruções para publicação de aplicativos na loja, mas os termos podem ser acessados a partir da tela de cadastro do aplicativo. Contrário às exigências dos termos de serviço da Google, não há destaque no processo de registro para as políticas de dados.

A sobreposição de termos de serviço e políticas de privacidade entre os provedores de autenticação (Google, Facebook e Apple) e o aplicativo em uso, não é claramente apresentada ao usuário, do mesmo modo que o documento de privacidade não apresenta em detalhes os vários acordos de uso de dados entre os provedores de autenticação e o desenvolvedor da plataforma.

A análise estática nos permitiu analisar o código fonte do aplicativo por meio de engenharia reversa, a fim de obter informações sobre rastreadores, permissões e acesso a informações do usuário. O aplicativo analisado apresenta em seu arquivo *.manifest* as permissões necessárias ao seu funcionamento. Por outro lado, dentre as permissões efetivamente solicitadas ao usuário, todas estavam presentes no arquivo *.manifest* em conformidade com as melhores práticas para desenvolvimento de aplicativos Android. Permissões não apresentadas no manifesto do aplicativo, mas solicitadas posteriormente, podem representar cenários onde certas permissões são solicitadas de forma suspeita com o intuito de obter maior acesso a informações pessoais do usuário. Dentre as permissões solicitadas, entretanto, algumas são categorizadas como "perigosas" e exigem autorização do usuário na primeira vez em que o aplicativo utilizar uma função que requeira tais permissões, tais como, acesso a câmera, localização, armazenamento de dados, dentre outros.

Ao longo da observação, não foram encontrados

3 – É um aplicativo de vigilância da Contronics.

4 – Código de um programa escrito na linguagem Java.

5 – Ferramenta de análise e rastreamento do pacote Android (APK)

6 – A análise heurística realiza-se por meio da quantificação de proximidade a um determinado objetivo.

7 – Ferramenta de análise profunda de malware/comportamentos suspeitos etc.

no código, usos suspeitos das permissões solicitadas. Quando analisadas em conjunto com as permissões solicitadas no manifesto do aplicativo e o código-fonte da aplicação não foram encontradas atividades suspeitas por parte das bibliotecas de terceiros e rastreadores. No entanto, os rastreadores relacionados a seguir encontram-se presentes no aplicativo analisado, a saber: 1. Google Analytics que coleta informações gerais de acesso (localização, horário, demografia, etc), 2. Google Firebase Analytics que coleta informações sobre o comportamento do usuário (uso de telas, conversão de campanhas pagas, eventos personalizados etc.) e proporciona ao proprietário do aplicativo os dados necessários para acompanhar seus usuários através de relatórios e gráficos (dashboard), enquanto se movimentam pelo programa. 3. Adjust que coleta informações de *target marketing*, aquisição de usuários e monetização. 4. Google Tag Manager que faz o gerenciamento de *tags* de rastreamento, acompanhamento de campanhas de marketing, conversão etc. 5. Bugsnag que realiza monitoramento e comunicação de erros, estabilidade de aplicação.

O 123Milhas foi a segunda aplicação escolhida para observação direta e se apresenta como um aplicativo de compra de passagens áreas com uso de milhas de diversos programas de recompensas. O 123Milhas v4.5.9 encontra-se disponível em https://play.google.com/store/apps/details?id=com.a123milhas.app, Pacote: com.a123milhas.app. O proprietário do programa é a 123 VIAGENS E TURISMO LTDA (https://123milhas.com/) com sede em Belo Horizonte, Brasil. Os Termos de uso: https://123milhas.com/termos-condicoes, assim como, a Política de privacidade: https://123milhas.com/politica-de-privacidade, podem ser acessadas nestes links.

No que se refere à privacidade e proteção de dados**,** destacamos que nenhum documento foi disponibilizado na página do aplicativo no Google Play o que contraria as instruções para publicação de aplicativos na loja, e os termos também não podem ser facilmente acessados a partir da tela de cadastro do aplicativo. Uma vez aberto, o aplicativo apresenta automaticamente a tela inicial, sem que o usuário tenha sido apresentado às políticas de privacidade e gestão de dados. Vale ressaltar que a coleta de dados por meio dos rastreadores presentes na aplicação já se encontra ativa e o usuário não concordou com qualquer termo que autorize o processo, ainda. Por outro lado, contrariamente às exigências dos termos de serviço da Google, não há destaque no processo de registro para as políticas de dados.

Para efetuar o login por meio de plataformas de terceiros o usuário necessita primeiramente realizar o seu cadastro na plataforma do 123Milhas. No entanto, contrário à experiência web a aplicação não oferece a opção de login com OAuth[8]. Ainda que a opção de autenticação OAuth não esteja presente no aplicativo móvel no momento do teste, a existência desta opção na versão Web apresenta a mesma problemática de sobreposição de termos de serviço vistas na análise do aplicativo Doctoralia.

Vale ressaltar aqui que a aplicação apresenta práticas de transparência relevantes e em *compliance* em conformidade com as exigências dos termos de serviço da Google e da Lei Geral de Proteção de Dados na experiência Web, mas não em sua versão móvel.

A análise estática mostrou que o aplicativo analisado apresenta em seu arquivo *.manifest* as permissões necessárias ao seu funcionamento, contudo, dentre as permissões efetivamente solicitadas ao usuário, nem todas estavam presentes no arquivo *.manifest* da aplicação, tais como, acesso a câmera e a conta do usuário. As duas permissões solicitadas encontram-se no grupo de permissões de risco. Também relacionamos como permissões de risco solicitadas por esta aplicação a solicitação de acesso à localização.

Por fim, quando analisadas em conjunto com as permissões solicitadas no manifesto do aplicativo e o código-fonte da aplicação, não foram encontradas atividades suspeitas por parte das bibliotecas de terceiros e rastreadores. Vale destacar, no entanto, que a aplicação da 123Milhas deixa atuantes os rastreadores: 1. AppsFlyer**:** análise de uso de aplicação, retenção de usuário, retorno de investimento em marketing, etc. 2. Google Firebase Analytics que acessa informações sobre o comportamento do usuário e de negócios. 3. Adjust que coleta informações de *target marketing*, aquisição de usuários e monetização. 4. Facebook Login: biblioteca compartilhada para fluxo de autenticação com o Facebook e 5. Facebook Share**:** biblioteca compartilhada para fluxo de compartilhamento com o Facebook.

O último aplicativo em análise é o Gov.br v3.2.34 com versão liberada em 10 de julho de 2022 e disponível em https://play.google.com/store/apps/details?id=br.gov.meugovbr . Pacote: br.gov.meugovbr.

Esse aplicativo dá acesso a dados e documentos pessoais nas plataformas governamentais brasileiras e

8 – OAuth é um padrão aberto para autorização, comumente utilizado para permitir que os usuários da Internet possam fazer logon em sites de terceiros usando contas de um provedor de identidade, como Google, Facebook, Microsoft, Twitter, etc.—mas, sem expor credenciais de autenticação, como senhas.

encontra-se vinculado ao Ministério da Economia / Serpro do Brasil. Os Termos de uso e a Política de privacidade podem ser acessados neste link: https://www.gov.br/governodigital/pt-br/governanca-de-dados/conecta-gov.br/termos-de-uso-e-de-politica-de-privacidade.

Sobre privacidade e proteção de dados do usuário, o Gov.br atua em conformidade com as diretrizes de publicação de aplicativos na Google Play, e apresenta claramente suas políticas de privacidade e uso de dados em sua página na loja. Todavia, contrário às melhores práticas de gerenciamento, o aplicativo não apresenta em sua interface nenhum link ou botão de acesso às configurações de privacidade, termos de uso ou política de privacidade da plataforma. O processo de autenticação na plataforma ocorre fora do aplicativo ou mesmo de uma *WebView* e direciona o usuário para um fluxo efetuado no navegador padrão do dispositivo.

Apesar do uso extensivo de dados biométricos do usuário, a aplicação não apresenta informações concisas sobre como os dados serão processados ou usados, se serão vendidos ou compartilhados com terceiros. Mesmo sendo uma aplicação governamental, o controle de dados do usuário quando não essenciais para a execução do aplicativo é uma garantia estabelecida na LGPD e deve ser obedecida.

Na análise estática o aplicativo analisado apresentou em seu arquivo *.manifest* as permissões necessárias ao seu funcionamento. Entretanto, dentre as permissões efetivamente solicitadas ao usuário, mais de 30 permissões, não estavam presentes no arquivo *.manifest* da aplicação e que vão de acesso a contas, mensagens recebidas, histórico das chamadas telefônicas, calendário, contatos, sensores de corpo, dentre outras.

Dentre as permissões inseridas no grupo de risco apenas as seguintes foram explicitamente requeridas no *.manifest* da aplicação, a saber: acesso a câmera, áudio, e armazenamento externo de dados do usuário.

O volume de permissões do grupo de risco não presentes no manifesto da aplicação é preocupante especialmente porque muitas das permissões requeridas fornecem acesso a dados não essenciais para o funcionamento da aplicação, como sensores corporais ou o histórico de ligações do usuário. O fato destas permissões não estarem claramente definidas no arquivo de manifesto impedem que o usuário tenha uma noção transparente das permissões requeridas pela aplicação no momento de instalação e podem representar um risco à privacidade do usuário.

Isto reflete a análise de especialistas que afirmam que apesar do Governo Federal está avançando no uso da Inteligência Artificial em prol de suas instituições e estruturas, o processo em si, não possui transparência, tal percepção tem sido feita através de pesquisa realizada a cada dois anos pelo Centro Regional de Estudos para Desenvolvimento da sociedade da Informação-CETIC.BR[9].

Vale destacar que apesar do excesso de permissões solicitadas e ainda que muitas estejam no grupo de alto risco à privacidade e proteção de dados do cidadão, não foram encontrados no código, usos suspeitos das permissões solicitadas.

Por fim, quando analisadas em conjunto com as permissões solicitadas no manifesto do aplicativo e no código-fonte da aplicação não foram encontradas atividades suspeitas por parte das bibliotecas de terceiros e rastreadores. No entanto, apesar de ser um aplicativo governamental o Gov.br mantém os rastreadores: 1. Google CrashLytics: realiza monitoramento e comunicação de erros, estabilidade de aplicação. 2. Google Firebase Analytics: coleta informações sobre o comportamento do usuário e de negócios (uso de telas, conversão de campanhas pagas, eventos personalizados, etc).

Ilação

Nesse momento, vale ponderar que todos os aplicativos analisados foram desenvolvidos dentro da Google e, portanto, devem obedecer às boas práticas previstas no Termos de uso de serviços da Google[10], por outro lado, para disponibilizar a seus usuários o acesso ao aplicativo através da conta pessoal da Google, a aplicação deve atender aos Termos e condições da API de autenticação de contas do Google.

Destaca-se que o ambiente em que foram desenvolvidos é terreno da Alphabet que desde os primeiros momentos já conhece cada aplicação e os usos que esta pretende oferecer aos usuários.

Para além de todos os rastreadores localizados nos

9 – TIC Governo Eletrônico 2021. Disponivel em: < https://cetic.br/media/docs/publicacoes/2/20220725170710/tic_governo_eletronico_2021_livro_eletronico.pdf> . Acesso em 10 ago 22.

10 – https://www.gstatic.com/policies/terms/pdf/20220105/it7r24p9/google_terms_of_service_pt-BR_br.pdf

três[11] aplicativos analisados em interface com a Google e outros provedores de acesso e autenticação, como o Facebook, há um rastreador comum disponibilizado em todos eles, a saber: Google Firebase Analytics que, como dito, coleta informações sobre o comportamento do usuário e de negócios. Contudo outros rastreadores do Google também foram localizados de forma pontual em algum aplicativo, tais como: Google Analytics que coleta informações gerais de acesso (localização, horário, demografia, etc), Google Tag Manager que realiza gerenciamento de tags de rastreamento, acompanhamento de campanhas de marketing, conversão, etc. e Google CrashLytics que faz o monitoramento e comunicação de erros, e estabilidade da aplicação.

A presença do Google Firebase Analytics em todos os aplicativos é significativa da força da Google e de sua preponderância na relação com os usuários empresariais e governamentais. A negociação com os aplicativos desenvolvidos em todo o mundo em seu domínio, se dá a partir de suas diretrizes e envolve a utilização de outros produtos e rastreadores comuns da Google. O Google Firebase Analytics funciona para os Apps de modo similar ao Google Analytics para sites e possui cinco principais seções: Propriedades do Usuário, Eventos, Dashboard, Conversões e Audiência. E ao tempo em que possibilita aos proprietários dos aplicativos o conhecimento pleno de seu público, também coleta os dados dos usuários dos aplicativos desenvolvidos em sua plataforma e que se utilizam desta ferramenta.

Obviamente que outras plataformas digitais e empresas do Vale do Silício também estão na mesma disputa por informações comportamentais dos usuários. O Facebook, considerado um "abutre de dados" também está presente com seus rastreadores, além de outros rastreadores como Adjust, Apple e Microsoft, dentre outras.

Retornamos a Foucault (2002) primeiro com o panóptico tendo em vista que este se apresenta como um princípio de uma anatomia política que para Foucault tem como objetivo a disciplina. *Surveiller et punir* se dedica potencialmente a analisar os mecanismos da disciplina em uma tecnologia política de regulação dos corpos, o que nos leva aos caminhos de desvelamento do biopoder que adota Foucault (1999), revelando sua dupla face que se situa no poder sobre as vidas (regulação da sexualidade) e sobre a morte (gestão do racismo), é nesse momento em que o biopoder revela sua face mais abrangente confluindo para o capitalismo como elemento fundamental de sua estrutura, o que por sua vez, se converte em ferramenta estratégica do que Foucault (2012) denomina de biopolítica que a partir da vigilância e disciplina, ao que Deleuze (1992) acrescenta o controle, passou a se ocupar com efetividade da saúde, higiene, natalidade, longevidade e raça da população. Como nos detalha Foucault (2012) ao falar sobre o neoliberalismo e as formas de *governamentalidades*, o biopoder se consolidou como uma estratégia, mas também como uma ferramenta que tinha como intuito garantir "uma inserção controlada dos corpos" no sistema capitalista. Para Foucault (2012) a economia política e a prática limitativa governamental terminam por consolidar uma duplicação de atos governamentais sobre o povo.

Guardadas as devidas proporções o biopoder é hoje exercido também pelas plataformas que como nos lembram Moazed e Johnson (2022) operam, principalmente, como modelos de negócios abertos e que se situam tanto frente aos milhões de usuários espalhados por todo o mundo, como frente ao mercado que precisa se adequar às suas normas e condições para poder alcançar o público certo, obter visibilidade e lucratividade.

Todavia, o biopoder atual ultrapassa a gestão da vida e da morte e se lança sobre a gestão da experiência sensível, a partir da transformação das afetividades e sociabilidades em métricas como parte relevante da experiência presente e da atenção dos usuários que terminam por influenciar no processo de valoração dos conteúdos disponibilizados digitalmente.

A Google como panóptico mantém o caráter silencioso do processo de vigilância e por se manter assim, delega aos usuários a decisão de se expor ou de se manter em postura de privacidade e como no passado, mantém o olho vigilante que se revela a cada palavra falada perto de um dispositivo móvel ou visita a um site. As plataformas digitais que se consolidam em redes sociais trazem, como nos lembra Brattan (2016), outro comportamento do usuário frente ao panóptico. Se no modelo de Bentham (2019) os vigiados mantinham-se comportados considerando a possibilidade da vigilância, no modelo das redes sociais os usuários ofertam sua intimidade exatamente porque tem ciência da vigilância permanente, não somente das plataformas em suas vidas (embora nem sempre de modo consciente e pleno) mas também por parte dos demais usuários que compõe sua rede de amigos, seguidores, inscritos ou contatos.

A vigilância das *big Techs* em torno dos usuários

11 – Durante a pesquisa analisamos mais 3 aplicativos: Trivago, Linkedin e Booking. Todos apresentaram o rastreador Google Firebase Analytics e a análise não veio para o texto por conta dos limites do artigo na Revista.

cuja experiência extraída origina tanto o capital de negociação com os mercados presente e futuro, como o capital acumulado em cima do qual se gerencia o conhecimento humano e o coloca em relação direta com a Inteligência Artificial em prol de um poder que instrumentaliza o comportamento humano com "propósitos de modificação, predição, monetização e controle" (ZUBOFF, 2020, p. 402) em prol da gestão deste em suas estruturas, servindo portanto, ao neoliberalismo que na visada de Chauí (2022) seria o novo poder totalitário.

Referências

ARENDT, Hannah. 2011. *Entre o passado e o futuro*. São Paulo: Perspectiva, p.348

BENTHAM, Jeremy.2019. *O panóptico*. Belo Horizonte: Autêntica, p.202

BODEN, Margareth.2020. *Inteligência Artificial*. São Paulo: Ed. Unesp, p.249

BOURDIEU, Pierre.2008. *A Distinção*: crítica social do julgamento. Porto Alegre: Zouk, p.556

BOURDIEU, Pierre.1998. *O poder simbólico*. Rio de Janeiro: Bertrand Brasil, p. 306

CHAUÍ, Marilena. *Neoliberalismo*: a nova forma do totalitarismo. Disponível em https://aterraeredonda.com.br/neoliberalismo-a-nova-forma-do-totalitarismo/. Acesso em: 05/08/ 2022.

BRATTON, Benjamin. 2016. *The Stack*. Massachusetts: MIT, p. 398

DELEUZE, Gilles. 1992. *Conversações*. Rio de Janeiro: Ed. 34, p. 226.

FOER, Franklin.2018. *O mundo que não pensa*. Rio de Janeiro: LeYa, p.235

FOUCAULT, Michel.2012. *Nacimento de la biopolítica*. Buenos Aires: Fondo de Cultura Económica, p.401

FOUCAULT, Michel.1996. *Microfísica do poder*. Rio de Janeiro: Ed. Graal, p.293

FOUCAULT, Michel.2002. *Vigiar e punir*. Petrópolis: Vozes, p.262

FOUCAULT, Michel.1999. *História da sexualidade*. A vontade de saber. v.1. Rio de Janeiro: Ed. Graal,p.245

HELMOND, Anne.2019.A plataformização da web. In: JOCELI, Janna. *Métodos digitais*. Lisboa: ICNOVA Edição- Universidade NOVA de Lisboa,p.72

KOSELLECK, Reinhart.2014. *Estratos do tempo*. Rio de Janeiro: Contraponto, p.351

KOSELLECK, Reinhart.2015. *Futuro passado*. Rio de Janeiro: Contraponto, p.366

LAVILLE, Christian e DIONNE, Jean.1999. *A construção do saber*. Belo Horizonte: Ed UFMG, p. 344

MARTINS, Helena. 2022. *A vigilância no capitalismo contemporâneo*. IN: *Revisa E-Compós*, v.25, p.1-22

MOAZED, Alex e JOHNSON, Nicholas L.2016. *Modern Monopolies*: what it takes to dominate the 21st-Century Economy. New York, NY: St. Martin's Press.

PLANTIN, Jean-Christophe et al (2016).Infrastructure studies meet platform studies in the age of Google and Facebook.In: *New Media & Society*. Disponível em: Infrastructure studies meet platform studies in the age of Google and Facebook - LSE Research Online. Acesso em: 30/11/22

POELL, Thomas; NIEBORG, David B.; VAN DIJCK, José.2020. *Plataformização.* In; Fronteiras, 22(1):2-10 janeiro/abril

RÊGO, Ana Regina. 2020. Vigilância, controle e atenção. In: *Organicom*, ano 17, n.34, p.82-92

RÊGO, Ana Regina e BARBOSA, Marialva.2020. *A construção intencional da ignorância*. Rio de Janeiro: Mauad, p.190

ROTHBRATT, Martine.2016. *Virtualmente humanos*. São Paulo: Cultrix, p.360

SEN, Amartya.2010. *Desenvolvimento como liberdade*. Cia das Letras, p. 461

SODRÉ, Muniz.2021. *A sociedade incivil*. Petrópolis: Vozes, p. 271

RICOEUR, Paul. *Tempo e narrativa*. v.3. São Paulo: Cia das Letras, 2010.

THALER, Richard.2019. *Misbehaving*: a construção da economia comportamental. Rio de Janeiro: Intrínseca, p. 356

WEEB, Amy.2020. *Os nove titãs da IA*. Rio de Janeiro: Alta Books, p.320

ZUBOFF, Shoshana. 2020.*A era do capitalismo de vigilância*. Rio de Janeiro: Intrínseca, p.796.