

**A VIGILÂNCIA ALGORÍTMICA NA SOCIEDADE DE CONTROLE [[1]](#footnote-1)**

**Maria Rita Pereira Xavier[[2]](#footnote-2); Alexsandro Galeno Araújo Dantas[[3]](#footnote-3)**

1. **Introdução**

O presente referencial teórico se baseia em preceitos que auxiliam o entendimento do smartphone como um artefato tecnológico de comunicação, entendido como um elemento heterogêneo de vigilância digital, aqui chamado de dispositivo de vigilância algorítmica. O pressuposto é o de que esse artefato possui a capacidade de produzir ou acelerar certos processos de subjetividade, a partir de um dispositivo de vigilância inserido em uma sociedade de controle. (DELEUZE, 1992).

Entende-se o smartphone[[4]](#footnote-4) como um dispositivo tecnológico em si, no sentido de máquina de comunicação, captura de informações e alteração de condutas através da programação de algoritmos. A justificativa é a de que a sua atuação é bastante ampla, servindo de suporte e/ou meio de captura de dados, através do uso de rastreadores (*trackers*) algorítmicos de informação, que atuam em aplicativos diversos. Os smartphones são dispositivos que estariam inseridos em um dispositivo de vigilância mais abrangente. São artefatos utilizados para servir de suporte ou meio de captura de dados, através do uso de rastreadores de informação, em forma de algoritmos, atuando por meio de aplicativos diversos. São dispositivos dentro de dispositivos, tal qual bonecas matrioscas[[5]](#footnote-5), os smartphones são dispositivos inseridos em um dispositivo de vigilância mais abrangente.

Definindo-a sociedade de controle[[6]](#footnote-6), o intuito deste artigo é compreender a sociedade contemporânea do ponto de vista da “captura da informação, armazenamento, cruzamento e recombinação de dados,” a partir de práticas que por meio da comunicação permeiam “a constituição de saberes, a criação de conhecimento, os processos de invenção e os modos de produção.” (KANASHIRO, 2016, p. 21). A partir dessa ideia, é possível pensar sobre a forma na qual se passou a estabelecer a coleta de dados por meio de smartphones:

[...] alguns dispositivos mencionados não estão direta ou intencionalmente voltados para o exercício da vigilância *stricto sensu*. Em muitos casos, a vigilância é um efeito colateral ou característica secundária de um dispositivo cuja função primeira é outra. (BRUNO, 2013, p. 31).

A vigilância que se depreende desse regime de vigilância e a produção (condução) de subjetividades que intento verificar podem ser apreendidas através da perspectiva de que o smartphone pode não ter sido, originalmente, pensado para a função de vigilância, mas não há dúvidas de que, nos termos de Foucault (1996), esse foi um preenchimento estratégico que surgiu através de um efeito colateral tal qual proposto por Bruno (2013). As corporações da internet e da telefonia adquiriram uma capacidade de coleta que extrapola os mecanismos de captura do Estado herdados do período industrial, a partir de informações de instituições disciplinares. O mercado das tecnologias de informação (TICs) adquiriu uma captura de dados que incluem os aspectos disciplinares, mas que os superam na medida em que captam “uma dimensão fragmentada dos dados que habita as visões de mundo, as dúvidas e incertezas, os desejos e as aspirações muitas vezes ainda não realizados.” (KANASHIRO, 2016, p. 21).

1. **A vigilância algorítmica**

Para uma empreitada nos estudos de vigilância, faz-se mister retomar a obra de Foucault, de modo a entender os caminhos que precisarão ser seguidos rumo ao entendimento das transformações desse campo. De acordo com Foucault, (2004 apud BRUNO, 2013), na passagem da soberania, na idade média, para a disciplina e o poder, a partir do séc. XVIII, o direito à morte é deslocado para um poder que gerencia a vida e se torna uma administração eficaz e uma gestão calculada da vida pelo Estado, a chamada biopolítica. Isso é fundamental para estabelecer uma diferenciação em relação as práticas de hoje, em que o Estado não mais detém o monopólio da informação, do monitoramento, da identificação e da classificação.

Atividades de vigilância voltadas para indivíduos ou populações humanas envolvem, de modo geral, três elementos centrais: observação, conhecimento e intervenção. A *observação* (visual, mecânica, eletrônica, digital) implica a inspeção regular, sistemática e focalizada de indivíduos, populações, informações ou processos comportamentais, corporais, psíquicos, sociais, entre outros. Isso para permitir a *produção de conhecimento* sobre os vigiados (extração de padrões, regularidades ou cadeias causais, por exemplo). As informações apreendidas pela observação devem ser convertidas em conhecimento a respeito dos que estão sob vigilância, de modo a permitir que se haja sobre suas escolhas, subjetividades, comportamentos. Nem a observação nem o conhecimento gerado se caracteriza como vigilância se não houver a perspectiva de *intervir* sobre os indivíduos ou populações em foco. Essa intervenção é da ordem do governo, entendido como a arte de conduzir condutas. (FOUCAULT, 2004 apud BRUNO, 2013, p. 18).

Os estudos de vigilância são aqueles que problematizam as práticas de captura contínua e rotineira de dados, processamento, armazenamento, análise, cruzamento, apropriação e gerenciamento de informações. De forma mais concisa Bruno (2013, p. 18) diz que “uma atividade de vigilância pode ser definida como a observação sistemática e focalizada de indivíduos, populações ou informações relativas a eles, tendo em vista produzir conhecimento e intervir sobre os mesmos, de modo a conduzir suas condutas”.

A análise de discursos e práticas atravessa a construção e utilização de tecnologias que dizem respeito ao controle de acesso, à vigilância, ao monitoramento e identificação de pessoas, e à formação de bancos de dados e de perfis sobre a população. São exemplos de artefatos tecnológicos de vigilância digital: as câmeras de monitoramento, os controles de acesso, as etiquetas de identificação por rádio frequência (RFID), a utilização da internet nas diversas finalidades, o uso de celulares, smartphones, geolocalizadores (GPS), a constituição e exploração do *big data*, entre outros. (KANASHIRO, 2016, p. 20). Este campo de estudos tem particular interesse pelas transformações que incluem as mudanças no capitalismo, nas racionalidades governamentais, no exercício do poder, nos modos de ver, pensar, sentir e conhecer. As reflexões a respeito da contemporaneidade se baseiam nas transformações que constituem tais tecnologias, mas buscam não “recair no determinismo tecnológico ou na afirmação de que a tecnologia é razão ou causa explicativa suficiente para as mudanças. (KANASHIRO, 2016, p. 21).

Desde o 11 de setembro de 2001, houve uma recomposição e um agravamento das práticas e discursos de vigilância. De lá para cá, também se deu o aumento e a consolidação do uso da internet, especialmente dos produtos de corporações como Google e Facebook; a reelaboração de termos de privacidade e de uso de serviços na internet; a ampliação de ferramentas de marketing e de comércio eletrônico; e as tensões a respeito de questões como propriedade intelectual, direito autoral, acesso e compartilhamento de informação se acirraram. Nesse período, ainda testemunhamos os vazamentos de documentos pela *Wikileaks*[[7]](#footnote-7) e as denúncias encabeçadas por seu fundador, Julian Assange, e Eduard Snowden a respeito do uso de programas de vigilância pela Agência nacional de segurança dos Estados Unidos, que têm como base dados recolhidos por empresas de internet e telefonia. (KANASHIRO, 2016).

Para Bruno (2013), a vigilância de sistemas informacionais não está centrada no olhar, mas sim sobre rastros e dados, pois se interessa bem mais em antecipar tendências de preferências e interesses do que em exercer práticas que visam corrigir ou reformar. Assim, estamos lidando com um dispositivo que tem na sua composição “mecanismos de rastreamento, monitoramento e arquivo de informação; sistemas de classificação e conhecimento dos rastros pessoais; procedimentos de individualização; e formas performativas e proativas de controle sobre as ações e escolhas dos indivíduos”. (BRUNO, 2013, p. 148)

Nessa perspectiva, TUFEKCI (2017) afirma que as preocupações em torno da vigilância digital ainda giram em torno de metáforas do passado e diz que “1984”, de George Orwell, não é mais a distopia correta para o século 21. Posto que o medo não deve vir do que a inteligência artificial em si vai fazer conosco, mas de como as pessoas no poder vão usar a inteligência artificial para controlar e manipular de novas formas, muitas vezes ocultas, sutis e inesperadas. Isto porque boa parte da tecnologia com capacidade para ameaçar a liberdade e a dignidade a curto prazo está sendo desenvolvida dentro de empresas que transformaram em negócio a captura, a venda de dados e a venda da atenção para anunciantes e outros. São as corporações que nos rodeiam no cotidiano, tais como Facebook, Google, Amazon, Alibaba, Tencent, Samsung, Apple, por exemplo.

A seguir, especificar-se-á mais detalhadamente como atuam as principais técnicas de persuasão, interpretação, coleta, monitoramento e perfilização de dados, conhecidas como *profiling* e *tracking*.

* 1. ***Profiling***

Aqueles que disseminam a ideia de que para se manter livre de vigilância basta não criar perfis em redes sociais ou não usar os serviços dessas grandes corporações não poderiam defender considerações mais falsas ou simplistas. No atual cenário, não há mais fora, não é possível se ausentar dos sistemas de informação e comunicação, todos estão incluídos independentemente de serem usuários de determinados serviços ou não. (KANASHIRO, 2016). Por oportuno, cabe elucidar a crítica ferrenha de Agamben (2009) ao identificar esse movimento:

A futilidade daqueles discursos bem-intencionados sobre a tecnologia, que afirmam que o problema dos dispositivos se reduz aquele de seu uso correto. Esses discursos parecem ignorar que, se todo dispositivo corresponde a um determinado processo de subjetivação (ou, neste caso, de dessubjetivação), e de tudo impossível que o sujeito do dispositivo o use "de modo justo". Aqueles que tem discursos similares são, de resto, a seu tempo, o resultado do dispositivo midiático no qual estão capturados. (AGAMBEN, 2009, p. 7).

Nesta perspectiva, Golumbia (2015 apud KANASHIRO, 2016, p. 22) apresenta a ideia de *crowdforcing* como uma lógica de mapeamento de parte da população, que acaba envolvendo mesmo os que não tiveram dados mapeados. É uma prática que pode guiar valores de serviços, por exemplo, ao premiar os que disponibilizam os dados com descontos e punir os não mapeados com preços mais altos.

No Brasil, essa prática acontece quando as seguradoras de carro diferenciam usuários que aceitam colocar geolocalizadores nos carros dos que não aceitam. (KANASHIRO, 2016). Um fenômeno ainda mais comum envolve muitas redes de farmácia, que estabelecem preços diferentes entre os clientes que realizam cadastro e os que não o fazem. Já se tornou banal, inclusive, que não só farmácias, mas lojas, supermercados, etc. tenham esses dados sem que o cliente nunca tenha entrado em determinado estabelecimento. Isto porque ao fazer o cadastro as pessoas não estão cientes de que há a prerrogativa de compartilhamento das informações com outras redes. O grupo pão de açúcar, recentemente, criou um programa em que basicamente trocava dados e preferências de consumo, através de um aplicativo, por descontos personalizados para os clientes.

Os hábitos de consumo dos quase 12 milhões de membros de seus programas de fidelidade, o Pão de Açúcar Mais e o Clube Extra. A moeda de troca do Pão de Açúcar era um tesouro que estava enterrado debaixo de uma camada de algoritmos: o grupo abriu para a indústria toda a base de dados de seus programas de fidelidade. Os fornecedores têm acesso ao perfil de quem consome (e de quem ignora) seus produtos, e podem fazer ofertas “nichadas”. (VIRI, 2017, p. 1).

Ao privilegiar o grupo que fornece informações, a prática segue a lógica do *crowdforcing*, termo que reitera uma “pressão coletiva que torna falsa a opção de estar fora de um determinado sistema.” (KANASHIRO, 2016, p. 23). A partir desses exemplos bastante próximos, é possível inferir o quanto a atuação do dispositivo de vigilância se dá pelo monitoramento sistemático, automatizado e à distância de ações e informações de indivíduos por meio da coleta digital de dados. Ainda que, tal qual os dispositivos modernos, a finalidade é conhecer para depois intervir nas condutas.

Isso se dá através de mecanismos de monitoramento e rastreamento de ações, informações e comunicações. Especialmente, através da elaboração de bancos de dados, a partir dos quais se estabelece perfis computacionais por meio de uma prática conhecida como *profiling*. (BRUNO, 2013). Os rastros digitais podem ser organizados de forma infraindividual ordenados segundo o modelo *top-down*, que utiliza parâmetros como idade, gênero e profissão de modo preestabelecido, ou ainda segundo o modelo *bottom-up* que gera classes como:

Frequentadores do site Y que clicam nos links tipo X”. Essa categoria é submetida (...) a mineração de dados, técnica estatística aplicada que consiste num mecanismo automatizado de processamento de grandes volumes de dados cuja função central é a extração de padrões que geram conhecimento, é um procedimento conhecido como *“descoberta de conhecimento em bases de dados*”. (BRUNO, 2013, p. 158, grifo do autor).

Esse conhecimento segue processos indutivos que se baseiam em algoritmos programados para extrair padrões e regras de correlação entre elementos. Os mecanismos mais comuns são os de tipo associativo, como o *profiling*, que através de similaridade, vizinhança ou afinidade associam no mínimo dois elementos e depois diferenciam tipos de indivíduos ou grupos. Desse modo, características e padrões podem ser relacionados a certos tipos de comportamento. (BRUNO, 2013).

Trata-se de uma nova racionalidade estatística que cria força através do tratamento automatizado de informações com aspecto massivo, tal qual o *big data*, mas que não busca causas para os fenômenos. De fato, “ancora-se na observação puramente estatística das correlações (independente de toda lógica) entre dados coletados de uma maneira absolutamente não seletiva numa variedade de contextos heterogêneos”. (ROUVROY; BERNS, 2010, p. 4 apud BRUNO, 2013, p. 159). Os perfis são projeções algorítmicas, são menos sobre indivíduos identificáveis e mais sobre “ações, condutas, escolhas de modo que podem ser suscitadas, desviadas, orientadas e conjuradas. Esse conhecimento é mais da ordem futuro, das regras de similaridade e da exterioridade”. (BRUNO, 2013, p. 163).

No entanto, ainda que os dados sejam coletados de modo massivo e aleatório, TUFEKCI (2017, sem pág.) nos lembra que os algoritmos podem realizar inferências aleatórias e facilmente distinguir “etnia, posição religiosa e política, traços de personalidade, inteligência, felicidade, uso de substâncias viciantes, separação dos pais, idade e gênero, só a partir das curtidas no Facebook”. E mais:

Além de serem capazes de identificar manifestantes mesmo que seus rostos estejam parcialmente ocultos. Esses algoritmos podem detectar a orientação sexual das pessoas só pelas fotos de perfil de seus relacionamentos. Essas são inferências probabilísticas, então não estarão 100% corretas, mas não vejo os poderosos resistindo à tentação de usar essas tecnologias só porque há alguns falsos positivos. [...] E a tragédia é a seguinte: estamos construindo uma infraestrutura de vigilância autoritária só para que as pessoas cliquem em anúncios. E esse não será o autoritarismo do Orwell. Essas estruturas estão organizando o modo como funcionamos e estão controlando o que podemos ou não fazer. E muitas dessas plataformas financiadas por anúncios se vangloriam de serem gratuitas. Nesse contexto, o produto que está sendo vendido somos nós. (TUFEKCI, 2017, sem pág.).

Essa infraestrutura de vigilância tem como base uma taxonomia dos bancos de dados, que pode ser interpretada como uma máquina epistêmica e individualizante. O perfil é uma categoria correspondente à probabilidade de manifestação de um fator – comportamento, interesse, traço psicológico – de acordo com um quadro de variáveis. O intuito é a categorização de conduta para simular comportamentos futuros, de modo que aqui não se aplica a divisão norma/desvio, as regularidades expressam tendências e potencialidades e não fletem uma natureza ou uma lei. O que é inadequado não é corrigido, mas sim incorporado aos cálculos futuros de definição de perfil. (BRUNO, 2013). O desvio aparece não como erro, mas como possibilidade de um acerto cada vez mais preciso do algoritmo.

Nesse cenário, a privacidade é um fator que se encontra em momento de disputa, no qual os discursos, forças e práticas estão num embate por determinar o sentido, o valor e a experiência da privacidade. Os dados publicados de forma voluntária geram uma segunda camada de dados. Por meio de bancos de dados e *profiling*, é possível gerar mapas e perfis de consumo, interesse, comportamento, sociabilidade, preferências políticas que podem ser usados para marketing, administração pública, indústria do entretenimento, indústria da segurança, etc. O que fica evidente é que o controle do indivíduo sobre os próprios dados é muito restrito e a noção jurídica de privacidade não dá conta da complexidade das questões sociais, políticas e cognitivas envolvidas. (BRUNO, 2013, pp. 129-130).

Esse é um processo de vigilância que não se concentra fortemente na identificação dos indivíduos, o rastreamento de dados opera em níveis menos visíveis – o do rastro digital, do plano infraindividual ou supraindividual –, de modo que o interesse está mais concentrado em desenvolver uma forma de exercício do poder sem a prioridade da identificação. O que, por outro lado, pode acender uma discussão sobre o que é considerado como privacidade ou informação pessoal. (BRUNO, 2013).

* 1. ***Tracking***

Diante dessa caracterização estabelecida com o auxílio de Bruno (2013), especialmente sobre o *profiling*, há a possibilidade de se afirmar que o *big data*, a mineração de dados e o estabelecimento de perfis é um dos caminhos a serem seguidos por esta pesquisa. A tentativa é cartografar a produção de subjetividades da perspectiva do uso de smartphones, como artefatos que alimentam a coleta desses rastros digitais ao facilitar e induzir determinados usos. O que nos leva à discussão sobre *tracking* e a inserção de rastreadores em aplicativos através da diversificação de funções. Um mesmo algoritmo pode ter, ao mesmo tempo, uma função de detecção de erros e de rastreamento, por exemplo.

A vigilância digital opera em vários níveis, as informações pessoais e as publicações divulgadas voluntariamente se encontram em uma camada mais superficial e explícita. Outro nível vigia a navegação, busca, simples cliques em links, downloads, produção ou reprodução de conteúdo – deixam vestígios mais ou menos explícitos, suscetíveis de serem capturadas. (BRUNO, 2013). Já o nível ainda mais profundo fica por conta dos algoritmos rastreadores, a maior parte funciona derivando um código de identificação do dispositivo móvel ou navegador web, que depois é compartilhado com terceiros para traçar o perfil do usuário com maior precisão. Nessa prática, são recolhidos dados bastante variados sobre os usos de aplicativos, geolocalização, preferências, métricas de performance, etc. (GRAUER, 2017).

De acordo com Bruno (2013), em 2010, 68% dos rastreadores já atuavam no campo do marketing online e da publicidade direcionada, embora o monitoramento de rastros pessoais na Internet também já despertasse o interesse de domínios variados. Tais como “segurança, entretenimento, saúde, gestão do trabalho e recrutamento pessoal, consultoria e propaganda política, desenvolvimento de produtos e serviços, vigilância e controle, inspeção policial e estatal, etc.” (BRUNO, 2013, p. 124). Sobre a forma que as grandes corporações, como Facebook e Google, atuam no dispositivo de vigilância, a autora disserta:

Não existem redes sociais, por exemplo, isentas de práticas de vigilância ainda que essa não seja sua função potencial, os sistemas de monitoramento são parte integrante tanto da eficiência dessas plataformas que rastreiam, arquivam e analisam as informações disponibilizadas pelos usuários, que encontram na vigilância mútua e consentida, com pitadas de voyeurismo, um dos motores desta sociabilidade. Não existem sistemas de busca, tal qual o Google, já que com sua maquinaria estritamente informacional, os algoritmos de monitoramento das informações e ações dos indivíduos no ciberespaço são constituintes dos parâmetros de eficiência de qualquer motor de busca. (BRUNO, 2013, p. 31).

A arquitetura da persuasão que o Facebook construiu é a responsável por sua capitalização de mercado perto de 500 bilhões de dólares. Todavia, é importante ressaltar que a estrutura para quem vende sapatos também é a mesma para quem vende política. O algoritmo não faz diferenciação, aquele que serve para nos tornar mais influenciáveis a anúncios, também serve para organizar o fluxo de informações políticas, pessoais e sociais. (TUFEKCI, 2017). De acordo com GRAUER (2017), o Google também tem interesse particular em permitir o livre uso dos rastreadores nos aplicativos distribuídos pelo Google Play[[8]](#footnote-8). Posto que um dos rastreadores mais difundidos é desenvolvido por sua plataforma de publicidade *DoubleClick*, feita para direcionar os anúncios por localização e em diferentes dispositivos e canais. A plataforma também segmenta usuários com base no comportamento online, vinculando-os a informações pessoalmente identificáveis, além de oferecer compartilhamento de dados e integração com vários sistemas de publicidade. Assim, o rastreador da *DoubleClick* é facilmente encontrado em vários aplicativos populares.

A Exodus, por exemplo, é uma plataforma privada de audição para aplicativos Android, que tem como objetivo detectar comportamentos que podem ser perigosos para a privacidade do usuário, tais como publicidades, rastreadores e estatísticas. Tem sido usada em parceria com o laboratório de privacidade da Universidade Yale como forma de detectar práticas de vigilância algorítmicas. Segundo Grauer (2017, p. 1), as funções dos rastreadores descobertos pela Exodus incluem “segmentar usuários com base em dados de terceiros, identificar atividade offline por meio de aprendizagem de máquina, rastrear comportamento em diversos aparelhos; identificar e correlacionar usuários isoladamente; e segmentar usuários que abandonam carrinhos de compras”. No modelo da plataforma, basta clicar no ícone do aplicativo desejado para que ele seja escaneado quanto a presença de rastreadores (*trackers*). Através da Exodus é possível analisar diversos aplicativos, no que concerne a presença de *trackers*, bem como o relatório de qual seria sua função oficial e as suas funções extras, digamos assim. Na tabela, a seguir, é possível identificar os modos como os rastreadores coletam e monitoram os dados de maneiras bastante diversificadas. As informações são de pesquisa realizada pelo Laboratório de privacidade da Faculdade de Direito de Yale, através do desenvolvimento da plataforma Exodus.

Tabela 1 Rastreadores encontrados em aplicativos pelos pesquisadores do Privacy Lab da Universidade de Yale através da plataforma Exodus Privacy. Fonte: GRAUER (2017).

|  |  |  |
| --- | --- | --- |
| RASTREADOR *(TRACKER)* | APLICATIVO | FUNÇÕES DE VIGILÂNCIA |
| *CRASHLYTICS (GOOGLE)* | *Tinder; OKCupid; Spotify*  *Uber; Superbright LED e LED Light (aplicativos de lanterna);* | Vincula usuários através de múltiplos cookies e dispositivos. |
| *HOCKEYAPP (MICROSOFT)* | *Microsoft Outlook; Skype;*  *Weather Channel;* | [Rastreia os usuários ativos diariamente e mensalmente](https://www.hockeyapp.net/features/user-metrics/), o número líquido de novos usuários e as contagens de sessões. |
| *APPFLYER* | *Tinder;*  *Superbright LED;*  *Weather Channel;* | [Identifica dispositivos por seus IDs](https://www.appsflyer.com/product/mobile-ecosystem/); [rastreia usuários em diferentes conjuntos de dados](https://www.appsflyer.com/product/marketing-analytics/) e [quais usuários instalam quais aplicativos](https://www.appsflyer.com/product/overview/). |
| *BRAZE* | *OKCupid;*  *Lyft;* | [Rastreia os usuários por local](http://www.prweb.com/releases/2013/10/prweb11275487.htm), segmenta-os em diferentes dispositivos e canais, e [veicula publicidade direcionada com base nas ações dos consumidores](https://www.braze.com/product/cross-channel-personalization) |
| *SALESFORCE DMP* | *OKCupid;* | Permite aos vendedores utilizar [aprendizagem de máquina](https://www.salesforce.com/blog/2017/05/krux-is-now-salesforce-dmp.html) (*machine learning*) para revelar personas (profiling), usa uma ID entre diferentes dispositivos. Analisa comportamentos para adivinhar quando o usuário está dormindo. Usa [algoritmo de combinação probabilística](https://konsole.zendesk.com/hc/en-us/articles/115009397188-Cross-Device-Identity-Management-CDIM-FAQ) para correspondência de identidades entre dispositivos. |
| *SCORECARDRE*  *SEARCH* | *Accuweather;*  *Weather Channel;*  *Spotify;* | [Rastreia dados de utilização](https://www.scorecardresearch.com/privacy.aspx), informações sobre navegação web e comportamento de uso de aplicativos; estabelece relações entre navegadores e dispositivos. |
| *FLURRY* | *Microsoft Outlook;*  *Weather Channel;*  *Superbright LED e LED Light;* | Rastreia as métricas de performance de dispositivos e aplicativos, analisa as interações dos usuários, identifica interesses, armazena perfis de dados como personas, agrupa e correlaciona dados de usuários e injeta anúncios, inclusive de vídeo. |
| *TUNE* | *Foca em usuários que utilizam o compartilhamento de caronas;* | Segue o comportamento online e offline dos [em diferentes dispositivos](https://www.tune.com/solutions/tune-marketing-console/our-difference/) e também [rastreia o comportamento de usuários dentro dos aplicativos](https://developers.tune.com/sdk/measuring-in-app-events/), identifica usuários de forma específica e rastreia sua localização. |
| *APPNEXUS* | *Superbright LED, entre outros aplicativos;* | [Utiliza aprendizagem de máquina para fazer publicidade direcionada](https://www.appnexus.com/en/buyers). |
| *DOUBLECLICK,*  *TEEMO,*  *BRAZE,*  *SALESFORCE,*  *DMP* | *Tinder; OkCupid; Lyft, Uber, Spotify; Weather Channel e Accuweater; Superbright LED e LED Light;* | Coletam grandes volumes de dados. |

Segundo Grauer (2017), foram identificados 44 tipos de rastreadores em mais de 300 aplicativos para smartphones com Android[[9]](#footnote-9). Os aplicativos analisados já foram baixados bilhões de vezes. Os pesquisadores da faculdade de Direito de Yale, estão tentando reproduzir os resultados da Exodus e já divulgaram relatórios sobre 25 rastreadores. Até agora só foi possível analisar aplicativos Android, mas imagina-se que os rastreadores também estejam presentes sistema da Apple, o IOS, pois as empresas distribuem aplicativos para ambas as plataformas.

Para encontrar os scripts de rastreamento, os pesquisadores da Exodus desenvolveram uma plataforma de auditoria customizada para o ecossistema Android, que pesquisou os aplicativos em busca de “assinaturas” digitais extraídas de rastreadores já conhecidos. Uma “assinatura” pode ser um conjunto de palavras-chave sinalizadoras ou uma cadeia de bytes, encontrados num arquivo de aplicativo, ou uma representação matematicamente derivada do próprio arquivo (um “*hash*”).” (GRAUER, 2017, p. 1).

Os níveis de invasão dos rastreadores variam, embora todos capturem mais informação do que deveriam. Segundo Bruno (2013), o valor econômico, estratégico e heurístico dos rastros digitais está concentrado no tipo de conhecimento gerado a partir deles. O que nos leva a pensar sobre os desdobramentos dessa vigilância em nível de rastros para as formas de controle vigentes que atuam em prol do capitalismo, através da acumulação de dados no *big data*.

1. **A importância do big data para a vigilância algorítmica**

Para a vigilância, a importância do *big data* vai além da sua capacidade de armazenamento de dados, o seu valor está na potência de conhecimento gerada pela quantidade de dados. Os sistemas de classificação da vigilância digital intentam governar condutas através de uma taxonomia específica que é distinta dos procedimentos modernos. Os processos algorítmicos de vigilância seguem uma lógica própria que é iniciada nas plataformas online, como sites, aplicativos e redes sociais, de modo que, à princípio, a maior quantidade possível de vestígios e traços de dados seja coletada, para que no passo seguinte do processo, haja uma mineração para distinguir que tipo de informações foram recolhidas e para que intuitos servirão. De acordo com Bruno (2013),

Sob o gigantesco fluxo de rastros pessoais em plataformas participativas, apresenta-se processos como *dataveillance* (vigilância de dados), *data mining* (mineração de dados) e *profilling* (perfilagem), que monitoram e classificam os dados, construindo saberes que sustentam uma vigilância proativa sobre indivíduos e populações. (BRUNO, 2013, p. 127).

Do ponto de vista da máquina algorítmica, o conteúdo não é o principal ponto, mas sim a movimentação do usuário e o seu comportamento, a indiferença formal do algoritmo destitui os indivíduos de escolhas da suas próprias ações, o algoritmo em si não se importa com o os sujeitos pensam, diferentemente da disciplina que tinha um investimento sobre o que o sujeito falava sobre si, com o intuito de entender quem ele era, muito valor era dado ao que ele pensava sobre si (os seus gostos, escolhas, preferências e desejos).

The extractive processes that make big data possible typically occur in the absence of dialogue or consent, despite the fact that they signal both facts and subjectivities of individual lives. These subjectivities travel a hidden path to aggregation and decontextualization, despite the fact that they are produced as intimate and immediate, tied to individual projects and contexts (NISSEMBAUM, 2011 apud ZUBOFF, 2015, p. 79).[[10]](#footnote-10)

Para Zuboff (2015) o que torna esses dados tão valiosos para os anunciantes são possíveis sinais de subjetividades que possam ter sido capturados. Na vigilância algorítmica há um efeito performativo muito acentuado, que passa por um modelo de autoridade produtor de um certo tipo de controle que não passa pelo consentimento dos indivíduos. Se na sociedade disciplinar os dados eram populacionais, em um contexto de consentimento; presença física; biopolítica e do nível Estatal. Isto é muito distinto do que acontece na sociedade de controle, em que a correlação entre os dados é a responsável por gerar um padrão comportamental.

Os dados passaram a ser transacionais, em um panorama dominado pelo *small data*, que se apoia na extração, análise, personalização e experimento contínuo. Trata-se de dados transformados na captura que são coletados em transações econômicas; através de sensores acoplados a objetos, pessoas e lugares; por meio de banco de dados governamentais e corporativos. O *big data* se institui a partir de duas escalas: os vestígios/rastros e a escala gigantesca que se dá pela quantidade massiva de dados coletados. (ZUBOFF, 2015). A principal intenção é captar os rastros de subjetividade, as formas de expressão e comunicação em ambientes informacionais, a mina de ouro está na riqueza de detalhes.

Individual needs for self-expression, voice, influence, information, learning, empowerment, and connection summoned all sorts of new capabilities into existence in just a few years: Google’s searches, iPod’s music, Facebook’s pages, YouTube’s videos, blogs, networks, communities of friends, strangers, and colleagues, all reaching out beyond the old institutional and geographical boundaries in a kind of exultation of hunting and gathering and sharing information for every purpose or none at all. It was mine, and I could do with it what I wished! These subjectivities of self-determination found expression in a new networked individual sphere characterized by what Benkler (2006) aptly summarized as non-market forms of ‘social production. (ZUBOFF, 2015, p. 79).[[11]](#footnote-11)

Nessa perspectiva, nada é trivial para a coleta, o princípio é o de coletar todo o possível, porque os dados nunca são excessivos e se transformam em “*data exaust”[[12]](#footnote-12)* e (ainda) não são limitados tal qual matérias-primas naturais; a lógica atual é: colete primeiro, analise depois. A correlação se faz suficiente porque não há a necessidade de entender os porquês ou os motivos das ações, não há perguntas sobre as causas quando só o padrão de fato importa. O nexo que perpassa esse entendimento é o de que é possível produzir, ou conduzir, comportamentos sem precisar entende-los completamente, os mecanismos de *profilling* não funcionam com distinções entre verdadeiro/falso, a produção de comportamentos importa mais do que o erro ou acerto. A indiferença fica clara no exemplo do sistema de recomendação do *spotify*[[13]](#footnote-13), quando uma música é recomendada e o usuário a escuta, o objetivo do algoritmo já foi atingido, não importando se a pessoa gostou ou não do que lhe foi recomendado.

Segundo Zuboff (2015) essa é uma das formas do capitalismo de informação que intenta “prever e modificar o comportamento humano como meio de produzir receitas e controle de mercado”. Já que as origens do *big data* remontam a um projeto de extração baseado na indiferença formal em relação às populações, que são tanto a fonte de dados quantos os alvos finais desse processo. De acordo com Zuboff (2015):

Big data, I argue, is not a technology or an inevitable technology effect. It is not an autonomous process, as Schmidt and others would have us think. It originates in the social, and it is there that we must find it and know it. […] big data is above all the foundational component in a deeply intentional and highly consequential new logic of accumulation that I call surveillance capitalism. (ZUBOFF, 2015, p. 75).[[14]](#footnote-14)

O *big data* tornou-se a peça fundamental para entender o quebra-cabeças da vigilância na sociedade de controle. Nessa perspectiva, é possível dizer que se as coletas de dados estão cada vez menos interessadas em características identitárias, é porque estão mais centradas nos aspectos subjetivos, que antes eram de difícil acesso e agora se encontram nos rastros digitais imersos na inumerável quantidade de dados disponíveis no *big data*.

But when it comes to information technology, automation simultaneously generates information that provides a deeper level of transparency to activities that had been either partially or completely opaque. It not only imposes information (in the form of programmed instructions), but it also produces information. (ZUBOFF, 2015, p. 76).[[15]](#footnote-15)

Assim, uma característica fundamental para a análise do dispositivo de vigilância contemporânea é o fato dele ser “atravessado por jogos do ver e do ser visto, nos quais as subjetividades encontram um domínio privilegiado de investimentos e cuidados. Não é, portanto, de se surpreender que para esta subjetividade, a vigilância apresente-se como aceitável, chegando a ser por vezes requerida. (BRUNO, 2013, p. 47)”. Assim, na seção a seguir nos deteremos um pouco sobre esses aspectos. Esse fato nos redireciona para a ideia de que a coleta de dados para a montagem de perfis de aspectos subjetivos, são a matéria-prima ideal para a produção de meios que consigam atingir a subjetividade, de modo a exercer intervenções sobre as condutas. Em outras palavras: é preciso conhecer para conquistar; posto que, se hábitos, interesses e ações são investigados e analisados também são passíveis de serem usados para estabelecer maneiras de capturar e conduzir a subjetividade.

**Referências**

AGAMBEN, G. **O que é um dispositivo?** In O que é contemporâneo? E outros ensaios. Trad. Vinicius Nicastro Honesko. Chapecó: Argos, 2009.

BRUNO, Fernanda. **Máquinas de ver, Modos de ser**: Vigilância, tecnologia e subjetividade. Porto Alegre: Sulina, 196p., 2013.

DELLEUZE, Gilles. “**Post-scriptum sobre as sociedades de controle**”, In Conversações 1972-1990, trad. Peter Pál Pelbart. Rio de Janeiro: Editora 34, 1992.

FOUCAULT, M. **Microfísica do poder**. Org. Roberto Machado. Rio de Janeiro: Graal, 1996.

\_\_\_\_\_. **Nascimento da biopolítica**. São Paulo: Martins Fontes, 2004.

\_\_\_\_\_. **Vigiar e punir**. Rio de Janeiro: Vozes, 1997.

GRAUER, Yael. **Aplicativos populares para celular estão cheios de rastreadores**. In The Intercept, 2017. Disponível em:<https://theintercept.com/2017/12/04/aplicativos-populares-para-celular-estao-cheios-de-rastreadores/> Acesso em: 04. Dez. 2017.

KANASHIRO, Marta M. **Vigiar e resistir**: a constituição de práticas e saberes em torno da informação. Cienc. Cult., São Paulo, v. 68, n. 1, p. 20-24, mar. 2016. Disponível em: <http://cienciaecultura.bvs.br/scielo.php?script=sci\_arttext&pid=S000967252016000100010&lng=en&nrm=iso>. Acesso em: 03. Dez. 2017.

ORWELL, George. **1984**. 29ª ed. São Paulo: Ed. Companhia Editora Nacional, 2005.

TUFEKCI, Zeynep. **Estamos criando uma distopia só para fazer as pessoas clicarem em anúncios**. In official TED conference, 2017. Disponível em: https://www.ted.com/talks/zeynep\_tufekci\_we\_re\_building\_a\_dystopia\_just\_to\_make\_people\_click\_on\_ads?language=pt-br#t-842171 Acesso em: 04. Dez. 2017

ZUBOFF, Shoshana. ***Big Other***: *Surveillance Capitalism and the Prospects of an Information Civilization. Journal of Information Technology 30*, nº. 1, pp. 75-89, 2015.

\_\_\_\_\_. ***Big Other***: capitalismo de vigilância e perspectiva para uma civilização de informação. In: Tecnopolíticas da vigilância: perspectivas da margem / organização: Fernanda Bruno, et al. 1 edição - São Paulo: Boitempo, 2018.

VIRI, Natalia. **Pão de Açúcar descobre um tesouro nos algoritmos**. In *Brazil Journal*. Disponível em: http://braziljournal.com/pao-de-acucar-descobre-um-tesouro-nos-algoritmos Acesso em: 04.Dez. 2017

1. Artigo apresentado ao Eixo Temático 10. Privacidade, vigilância e controle de dados, do XI Simpósio Nacional da ABCiber. [↑](#footnote-ref-1)
2. Pesquisadora é doutoranda em Ciências Sociais da Universidade Federal do Rio Grande do Norte. É Mestre em Ciências Sociais (UFRN) e participa do Grupo de Pesquisa em Comunicação Marginália (UFRN). E-mail: [mariaritax\_@hotmail.com](mailto:mariaritax_@hotmail.com). O presente trabalho foi realizado com apoio da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior - Brasil (CAPES) - Código de Financiamento 001. [↑](#footnote-ref-2)
3. Pesquisador é professor da Universidade Federal do Rio Grande do Norte. É Doutor em Ciências Sociais (PUC-SP) e participa do Grupo de Pesquisa em Comunicação Marginália (UFRN). E-mail: alexgalenno@gmail.com [↑](#footnote-ref-3)
4. Com o intuito de evitar desentendimentos no que se refere ao conceito na filosofia do dispositivo, optou-se por se referir ao smartphone como artefato móvel de comunicação. [↑](#footnote-ref-4)
5. A matriosca é um tipo de boneca russa que encaixa outras menores dentro de si. [↑](#footnote-ref-5)
6. Deleuze, G. **Post-scriptum das sociedades de controle**. In Conversações. Rio de Janeiro, Editora 34, 2000. [↑](#footnote-ref-6)
7. Fundada por Julian Assange, em 4 de outubro de 2006, na Islândia, a WikiLeaks é uma organização transnacional sem fins lucrativos, sediada na Suécia, que publica, em sua página, postagens de fontes anônimas, documentos, fotos e informações confidenciais, vazadas de governos ou empresas, sobre assuntos sensíveis. [↑](#footnote-ref-7)
8. Google Play é um serviço de distribuição digital de aplicativos, jogos, filmes, programas de televisão, músicas e livros, desenvolvido e operado pela Google. [↑](#footnote-ref-8)
9. Sistema operacional móvel do Google. [↑](#footnote-ref-9)
10. Tradução em português: Os processos extrativos que tornam o “big data” possível normalmente ocorrem na ausência de diálogo ou de consentimento, apesar de indicarem tanto fatos quanto subjetividades de vidas individuais. Essas subjetividades percorrem caminhos ocultos para agregação e descontextualização, apesar de serem produzidas como íntimas e imediatas, ligadas a projetos e contextos individuais. ”. (ZUBOFF, 2015). [↑](#footnote-ref-10)
11. Tradução em português: «as necessidades individuais de auto-expressão, voz, influência, informação, aprendizagem, empoderamento e conexão reuniram em poucos anos uma ampla gama de novas capacidades: pesquisas do Google, música do iPod, páginas do Facebook, vídeos do YouTube, blogs, redes, comunidades de amigos, estranhos e colegas, todos ultrapassando as antigas fronteiras institucionais e geográficas em uma espécie de exultação de caça, coleta e compartilhamento de informações para todos os propósitos, ou mesmo para nenhum. Isso era meu, e eu posso fazer com isso o que eu quiser! Essas subjetividades de autodeterminação encontraram expressão em uma nova esfera individual em rede caracterizada pelo que Benkler (2006) resumiu adequadamente como formas não-mercantis de “produção social”». (ZUBOFF, 2018). [↑](#footnote-ref-11)
12. “Esses dados são adquiridos, tornados abstratos, agregados, analisados, embalados, vendidos, mais e mais analisados e vendidos novamente. Esses fluxos de dados foram rotulados pelos tecnólogos como “data exhaust”. Presumidamente, uma vez que os dados são redefinidos como resíduos, a contestação de sua extração e eventual monetização é menos provável.” (ZUBOFF, 2018). [↑](#footnote-ref-12)
13. Spotify é um serviço de streaming de música, podcast e vídeo que foi lançado oficialmente em 7 de outubro de 2008. É o serviço de streaming mais popular e usado do mundo. Ele é desenvolvido pela startup *Spotify AB* em Estocolmo, Suécia. Fonte: Wikipedia [↑](#footnote-ref-13)
14. Tradução:«O *big data* não é uma tecnologia ou um efeito tecnológico inevitável. Tampouco é um processo autônomo, como Eric Schmidt e outros querem que acreditemos. O *big data* tem origem no social, e é ali que devemos encontrá-lo e estudá-lo. [...] O“big data” é acima de tudo o componente fundamental de uma nova lógica de acumulação profundamente intencional e com importantes consequências, que chamo de capitalismo de vigilância.» (ZUBOFF, 2018). [↑](#footnote-ref-14)
15. Tradução em português: «porém, na tecnologia de informação, a automação gera simultaneamente informação que proporciona um nível mais profundo de transparência a atividades que pareciam parcial ou totalmente opacas. A automação não somente impõe informação (sob a forma de instruções programadas), mas também produz informação.» (ZUBOFF, 2018). [↑](#footnote-ref-15)