Vigilância cega, o que as pegadas digitais podem revelar sobre o indivíduo

João Carlos Rebello Caribé
Mestrando em Ciência da Informação pelo convênio Universidade Federal do Rio de Janeiro/Instituto Brasileiro de Informação em Ciência e Tecnologia (UFRJ-IBICT). Novembro de 2018,
(joao.caribe@icloud.com)

Resumo
Quando se fala em vigilância, logo vem a mente a imagem de uma câmera, um observador por trás dos monitores. É um modelo naturalizado no século XX, que com o advento do big data, está se tornando obsoleto.

O modelo de vigilância do Panóptico de Benthan, descrito por Foucault (2014) em "Vigiar e Punir", se baseia no par ver-ser-visto, a partir de um ponto de observação central, com o vigilante tendo ampla visão do vigiado e este nenhuma visão do vigilante, presumindo assim a sua vigilância.

Com a emergência da mobilidade e do capitalismo de vigilância (Shoshana Zuboff, 2015), surgiram novas sistematizações de modelos de vigilância. Zigmunt Bauman (2013) em "Vigilância Líquida", apresenta o modelo do Panóptico pessoal, onde o indivíduo torna-se vigilante de si e seus pares, carregando seu próprio Panóptico, materializado como seus smartphones e dispositivos conectados. O que Bauman descreve, dialoga com o que Fernanda Bruno (2013), em "Máquinas de ver, Modo de Ser. Vigilância Tecnologia e Subjetividade" descreve como Vigilância Distribuída, que tira a centralidade da vigilância, principal característica do Panóptico.

Sandra Braman (2006) no livro "Change of State - Information, Policy, and Power", apresenta o Panspectro, como o modelo de vigilância adequado ao advento do big data. Segundo a autora, o foco do Panspectro não é o indivíduo em particular, seu foco está nos dados, e sua ação focal se dá em resposta a padrões.

O volume de dados produzidos voluntária e involuntariamente, pelo indivíduo, na Internet configuram o novo petróleo, o Facebook, por exemplo, teve uma receita bruta de U$ 40,6 bilhões em 2017, Alphabet, holding da Google, faturou U$ 110 bilhões, no mesmo período.

Panspectros, treinados com modelos, através de machine learning, constroem a partir dai, por deep learnig, padrões sofisticados, que respondem de forma lateral, distinta da lógica humana, com extrema precisão a perguntas feitas na tela panspectral. Yoyou Wu et al (2015) demonstra em “Computer-based personality judgments are more accurate than those made by humans” como os julgamentos baseados em computador são mais precisos que os feitos por humanos.

As pegadas digitais que o indivíduo produz permitem produzir informações valiosas de sua individualidade, seus gostos, temores, e até revelar seus mais sombrios segredos.

Palavras-chave: Big data, capitalismo de vigilância, vigilância distribuída, panspectro, panóptico.

Introdução

Em 2008, ativistas, acadêmicos, coletivos e políticos uniram-se na luta contra o "AI5 digital", um projeto de lei de combate à cibercrimes do Senador Eduardo Azeredo. O PL84/99, conhecido por AI5 digital, criava uma camada de vigilância na internet, obrigando os provedores de internet registrarem além do log de acesso[1], todas as páginas na Internet que foram visitadas, com dia e hora, e ainda produzir uma identificação positiva da conexão, ou seja, associar um número de IP de conexão à uma identidade real. Estes dados estariam disponíveis aos poderes públicos, como a policia e o judiciário, sem necessidade de ordem judicial, por até três anos, além de outros absurdos. O projeto criava um "estado policial", inclusive invertendo o principio da presunção de inocência.

Desta ameaça surgiu o Mega Não[2], idealizado por Daniel Pádua e João Carlos Caribé, um metamanifesto que concatenava todos os eventos e ações daqueles que combatiam o projeto. O Mega Não publicou uma petição on-line que obteve mais de 100 mil assinaturas, tornando-se noticia, sendo usada no congresso, por deputados e senadores, como argumento pela rejeição do projeto de lei, tornando-se a primeira petição on-line a criar um fato político no Brasil.

Esta luta ganhou forte apoio de um número crescente de parlamentares, que conseguiram retirar do projeto de lei todos os pontos polêmicos. O movimento culminou com a convocação, durante o FISL (Forum Internacional de Software Livre), pelo presidente Lula[3], por uma constituição da Internet, surgindo assim o Marco Civil. Esta história foi linda, e foi sistematizada e contada pela Anna Carolina Papp em sua monografia intitulada "Em nome da Internet"[4].

1 Do panóptico ao panspectro, o vigilante cego

O que se estava combatendo em 2008 era a instalação de um panóptico virtual pelo Estado, "que tudo via e tudo registrava na Internet". O foco da vigilância estava no indivíduo e seus hábitos de navegação, uma vigilância rasa, visando saber quando o indivíduo conectou, e que sites visitou, não permitindo saber muito sobre ele, apenas o sobre o que lhe interessava, como esquematizado na figura a seguir.

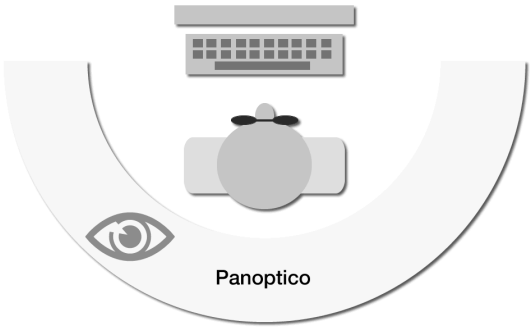

Figura 1 - Modelo de vigilância na internet em 2008, o panóptico sobre um indivíduo

A figura 1 é a representação esquemática de um indivíduo, com um dispositivo computacional à sua frente e o visor do panóptico por trás, representando a visibilidade sobre os seus ombros. Um modelo onde o vigilante "enxerga" as atividades do indivíduo. O panóptico remete à idéia de visibilidade, é um modelo conceitual derivado de uma proposta

de modelo prisional de Jeremy Bentahm, dialogando com o conceito de vigilância consolidado no imaginário da sociedade do século XX.

O panóptico é uma maquina de dissociar o par ver-ser visto, ou seja, os indivíduos no anel periféricos são totalmente visíveis, enquanto o vigilante no ponto central nunca é visto, o efeito mais importante do panóptico é induzir no indivíduo um estado permanente e consciente de visibilidade (FOUCAULT, 2014). O controle, segundo Foucault, se da pela presunção da vigilância. A interpretação do modelo panóptico e sua aplicabilidade no contexto atual deve munir-se de cautela, pois como diz Fernanda Bruno (2013), ainda que elementos importantes do dispositivo panóptico persistam e mesmo se ampliem, a suposição de que se trata apenas de uma ampliação implica em perder de vista o essencial, que as mudanças mais importantes nos modelos de vigilância se dão em seu modo de funcionamento.

A vigilância anteriormente sólida e estável, esta agora liqüefazendo e permeando em espaços antes impenetráveis, como descrevem Bauman e Lyon:

> Uma série de teóricos tem observado as maneiras pelas quais a vigilância, antes aparentemente sólida e estável, se tornou muito mais móvel e flexível, infiltrando-se e se espalhando em muitas áreas da vida sobre as quais sua influência era apenas marginal (BAUMAN e LYON,2013).

Para Bauman e Lyon, a arquitetura das tecnologias eletrônicas permitem formas de controle com diferentes faces, inclusive compartilhando as características ligadas ao consumo e entretenimento, apontando para a vigilância e auto vigilância como novas perspectivas comportamentais do indivíduo frente às tecnologias, que inclusive sentem-se felizes e motivados a compartilhar detalhes íntimos de suas vidas pessoais tais como fotos, fatos, eventos e pensamentos. A tecnologia vem transformando o vigiado servidor do vigilante, através da auto vigilância, vinte e quatro horas por dia e sete dias por semana como destacam os autores. Bauman e Lyon utilizam o conceito de panóptico pessoal como o dispositivo que torna o indivíduo vigilante de sí e de seus pares, pavimentando o conceito de que a vigilância atua de forma descentralizada.

Hoje em dia o indivíduo vigia-se, carregando consigo um dispositivo computacional de alta eficiência, equipado com câmera de foto e vídeo, microfone, GPS, acelerômetro, giroscópio, magnetrômetro, sensores de luz e proximidade, além de outros recursos. Estes dispositivos estão conectados vinte e quatro horas por dia, sete dias por semana, durante o ano inteiro, mesmo enquanto este indivíduo está dormindo. Mas a questão da vigilância contemporânea não reside apenas neste dispositivo, a conectividade entre diferentes dispositivos configuram em um modelo muito mais eficiente e permeável.

A vigilância esta se tornando mais ubíqua ao incorporar-se aos diversos dispositivos tecnológicos, como destaca Fernanda Bruno (2013), reforçando a necessidade do estudos destes dispositivos, suas capacidades e interconectividade. Para a autora, o conceito de vigilância distribuída, não se confunde com uma estrutura com sistemas centralizados e hierarquizados, como na estrutura panóptica, ainda que hajam práticas, tecnologias e discursos pontuais relacionados a estes princípios.

Fernanda Bruno descreve o modelo de vigilância contemporânea como um modelo de vigilância distribuída. Ao demonstrar que a vigilância cognitiva pode ter um caminho inverso

no conceito da cognição distribuída, ou seja, um processo transindividual, coletivo e distribuído entre múltiplos agentes, humanos e não humanos, concluiu que:

> Esta perspectiva inspira a noção de vigilância distribuída, que se espraia por muitos e diversos agentes, tecnologias, contextos, práticas, sem constituir uma atividade ou processo unificado que possa ser plenamente atribuído de intenções ou prescrições de um centro de ordenação ou controle. (BRUNO, 2013)

Ainda que a autora utilize a definição ambígua e ampla de dispositivo, como o elemento tecnológico de vigilância e como a própria prática, como encontrado nos trabalhos de Foucault, o estudo que segue, se deu sobre o dispositivo tecnológico, abrindo-se para uma perspectiva da prática.

O principio da vigilância distribuída rompe com a centralidade do modelo panóptico, tornando-o um modelo obsoleto para fundamentar a compreensão dos modelos de vigilância do século XXI. A vigilância deslocou do modelo panóptico com o vigilante centralizado, para o modelo de vigilância distribuída, onde diversos dispositivos computacionais se tornam dispositivos de vigilância. Mas o grande passo esta na compreensão do deslocamento do foco da vigilância, do indivíduo para os dados que ele produz.

As relações de vigilância contemporâneas passam pelo modelo de um vigiando muitos do panóptico, muitos vigiando um, o modelo sinóptico onde muitos vigiam muitos, e a auto vigilância. Entretanto manter-se nesta lógica onde há sempre um par vigilante e vigiado pode ignorar a vigilância sobre os dados que estes indivíduos produzem. Sandra Braman (2006) descreve o panspectro, um mecanismo de controle que não segue esta lógica. O panspectro pode gerenciar quantos assuntos forem necessários, ao mesmo tempo, ele esta focado nos dados, analisa seus padrões e o objeto de vigilância nunca sabe quando, como ou porque ele pode ser tornar visível à tela panspectral.

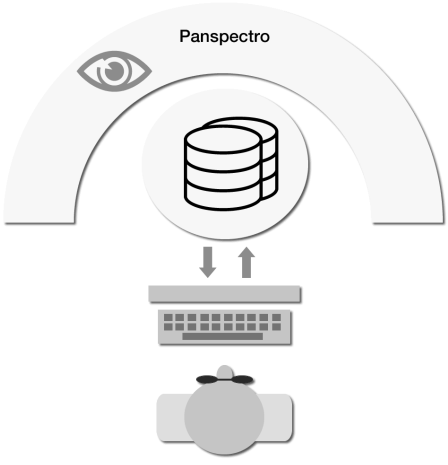

Figura 2 - Modelo de vigilância, o panspectro

A vigilância do panspectro, como demonstra o diagrama acima, se dá sobre os dados produzidos pelos diversos dispositivos, sendo acionados sempre que algum dado distancia do padrão, ou aproxima de padrões de vigilância preestabelecidos.

O panspectro segue a lógica da vigilância sobre os padrões, sejam eles desviantes ou não. Desviantes como sistematizados por Howard Becker (2014), onde o comportamento desviante é aquele que não segue determinados padrões de conduta, entretanto como ressalta

Becker, ao estudarmos um padrão desviante, é importante investigar quem são os responsáveis por determinar aquele, como desviante. Estes responsáveis, podem ser os viesses dos próprios algoritmos de mineração de dados ou dos próprios dados. Este viés dos algoritmos pode ser resultante dos próprios responsáveis por sua codificação, como destaca Cathy O'Neil (2016), os algoritmos codificam os preconceitos. Atividades de vigilância voltadas para indivíduos ou populações humanas envolvem, de modo geral, três elementos centrais: observação, conhecimento e intervenção (BRUNO), e não podem estar sujeitas às falhas humanas codificadas em algoritmos opacos, que tomam decisões que, na maioria das vezes, não aceitam apelações.

O modelo de vigilância neste ponto, é um modelo complexo, que envolve todos os modelos citados, e pela perspectiva dos dispositivos como esquematizado na figura a seguir.

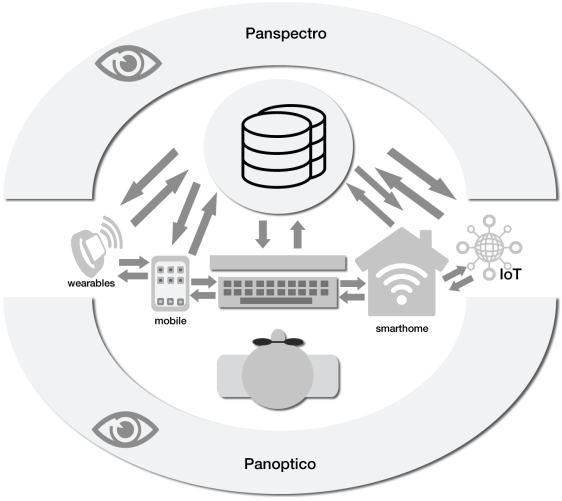

Figura 3 - Modelo de vigilância contemporâneo, o modelo complexo

Existem, atualmente, em torno de 12,3 bilhões de dispositivos conectados como smartphones, tablets, computadores, wearables, IoT e etc. Para chegar a este número partiu-se do Internet World Stats[5], que em Dezembro de 2017, indicava que 4,1 bilhões de pessoas tinham acesso a Internet. Considerando que o relatório da Cisco[6] projeta que em 2020, existirão em média 3,4 dispositivos conectados à Internet por usuário, e considerando a média de 3 dispositivos, existem hoje, mais de 12,3 bilhões de dispositivos conectados, com seus sensores, atuadores e habilidades, coletando, tratando, armazenando e enviando uma quantidade gigantesca de dados sobre o indivíduo.

2 Capitalismo de vigilância

É importante destacar que o big data não é uma massa homogênea de dados disponíveis à qualquer um, cada nuvem possui seu conjunto de dados obtidos através dos diversos dispositivos, e estas em geral não compartilham os dados entre si.

No livro Cypherpunks, Julian Assange (2013) demonstra preocupação com o crescimento da quantidade de nuvens, para ele data center gigantescos estão sendo instalados nos Estados Unidos, em geral todos muito próximos por questões de incentivos fiscais e infraestrutura. Na sua opinião, é mais conveniente para a NSA, "espetar" suas "escutas" nestes data centers, do que monitorar os dispositivos de cada usuário.

Os dados são o novo petróleo[7], o Facebook teve uma receita bruta de U$ 40,6 bilhões em 2017[8], Alphabet, holding da Google, faturou U$ 110 bilhões, no mesmo período[9], por estes números é possível imaginar o tamanho do mercado. A pesquisadora Shoshana Zuboff (2015) popularizou o conceito de "capitalismo de vigilância" que denota um novo tipo de capitalismo monetizado por dados adquiridos por vigilância. A autora atribui o surgimento desta nova forma de capitalismo ao acoplamento de vastos poderes digitais e a indiferença e narcisismo intrínseco do capitalismo financeiro dentro da ótica neoliberal, frente à nova dependência da arquitetura global de mediação digital que produz o big data, e uma nova expressão de poder que ela chama de "Big Other". O capitalismo de vigilância foi descoberto e consolidado pelo Google, e posteriormente adotado pelo Facebook e outros, e se baseia inclusive no uso de mecanismos ilegítimos de extração, mercantilização e controle de comportamento para produzir novos mercados. Segundo Zuboff, a Internet era um mundo gentil e promissor, agora é onde o capitalismo esta desenvolvendo de forma perversa e avassaladora pela extração de dados, ameaçando a liberdade e a privacidade.

2.1 Os cardeais do algoritmo

As empresas proprietárias das nuvens, como o Google, Facebook dentre outros, são o que Cathy O'Neil (2016) denomina de "cardeais do algoritmo", aqueles que detêm total controle sobre os algoritmos, que operam com estes dados, que em sua maioria são totalmente opacos ao usuário.

Estes cardeais do algoritmo são poderes privados, que possuem cada vez mais conhecimento e controle sobre o indivíduo, configurando o que Sandra Braman qualificou como "Estado Informacional". O Estado informacional sabe cada vez mais sobre o indivíduo que em contrapartida sabe cada vez menos sobre o Estado, produzindo uma matriz de força totalmente desproporcional. Entretanto o poder do Estado é limitado aos mecanismos legais para ter acesso aos dados, que são propriedade dos cardeais do algoritmo, configurando um modelo neoliberal como descreve Zuboff.

3 A vigilância cega

O indivíduo está sendo digitalizado, os dados que produzem estão possibilitando aos cardeais do algoritmo, conhecerem mais sobre ele, do que ele mesmo. Maria Wróblewska (2018) descreve este fenômeno de forma crítica ao chamar o Facebook de caixa preta:

> Eles são responsáveis pela nova forma de trabalho e exploração. A caixa preta é, na verdade, uma fábrica. Você, o usuário, não é um cliente. Você se torna apenas uma matéria-prima, biomassa humana convertida em um perfil digital vendável no mercado de ações da Internet - no Facebook Ad Manager. (WRÓBLEWSKA, 2018, tradução nossa).

O documentário "Monologue of the Algorithm: how Facebook turns users data into its profit" produzido por Maria Wróblewska, para o Panoptykon Foundation, apresenta de forma impressionante como os dados são obtidos e tratados pelo Facebook na construção de perfis extremamente precisos, com o objetivo de oferecer conteúdo e publicidade dirigida.

A vigilância cega se dá a partir dos dados produzidos de forma voluntária e involuntária pelo indivíduo. Estes dados são obtidos, armazenados, tratados e comparados na busca de padrões, padrões estes que são usados pelo panspectro em sua atividade de vigilância.

A mineração dos dados em busca de padrões e repostas produzem o valor do big data. Os padrões muitas vezes são obtidos de dados elementares, por exemplo, através do simples registro das coordenadas GPS, é possível identificar onde um indivíduo reside e trabalha, qual trajeto que costuma fazer regulamente entre estes lugares. Estes padrões são construídos de forma recursiva e utilizam inúmeras técnicas, com o apoio de profissionais de diferentes especializações com matemática, física, geografia, psicologia, informática, sociologia, ciência da informação, comunicação, engenharia, dentre outros.

3.1 Identificando personalidades

Toda sociabilização nas plataformas de redes sociais é mediada por complexos algoritmos. Estes algoritmos, ou melhor conjunto de algoritmos, cuidam de registrar tudo que o usuário faz, cada clique, like, comentário, compartilhamento, leitura, amizades, seguidores, grupo, página, absolutamente tudo é registrado. Todos estes registros são comparados com inúmeros outros que foram coletados de outros usuários, criando um perfil tão preciso, que bastam 300 curtidas para o Facebook saber mais sobre um indivíduo do que sua(seu) parceira(o). Tudo isto tem por objetivo entreter o usuário, e vender estes perfis precisos como critérios de publicidade dirigida.

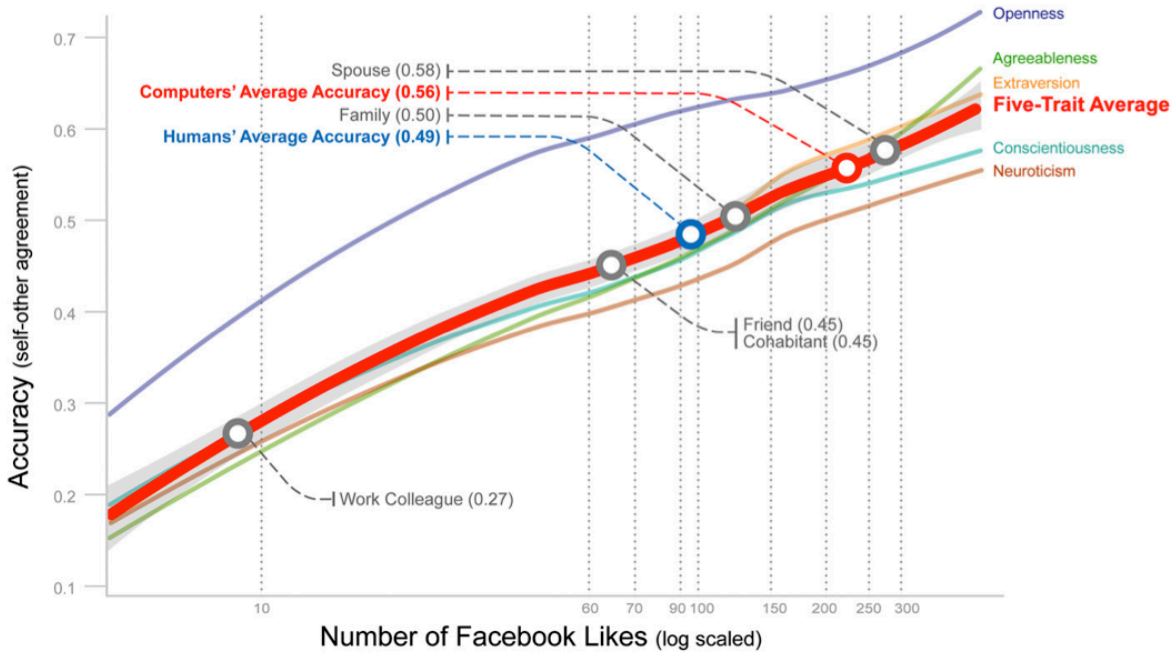

Figura 4 - Numero de Likes do Facebook
Fonte - Wu et al (2015) - Reprodução

O estudo de YouYou Wu et al (2015) da Universidade de Cambridge, demonstra que o julgamento de personalidade baseado em computadores é mais preciso que por humanos. No gráfico a seguir (figura 4), a linha central mais grossa é a média dos traços de personalidade do modelo de personalidade de cinco fatores, utilizado na psicologia para identificar elementos da personalidade dos indivíduos. O projeto utilizado para este estudo continua disponível, chama-se Apply Magic Sauce[10]. Para chegar a conclusão, Wu fez o teste convencional, através de questionários, para mais de 17.000 voluntários, que em seguida conectaram o Apply Magic Sauce às suas contas no Facebook. Utilizando o processo de "machine learning", os pesquisadores "ensinaram" aos algoritmos com base nos padrões do

teste convencional e do resultado da leitura de likes no Facebook, estabelecendo padrões de traços de personalidade para cada uma das páginas “curtidas”. Após a experiência, o algoritmo aprendeu a identificar os traços de personalidade com base nos likes, por um processo de comparação conhecido por homofilia. Por exemplo, Wu cita que indivíduos com grande abertura para novas experiências, tendem a curtir páginas sobre Salvador Dali, meditação ou palestras no TED.

Padrões de personalidade podem ser obtidos a partir de outros dados, Jennifer Golbeck (2016), no estudo “Predicting personality from social media text”, descreve como usou a técnica de psicolingüistica para analisar as personalidades de indivíduos com base em suas publicações em redes sociais, apresentando resultados precisos utilizando um aplicativo baseado no modelo de personalidade de cinco fatores.

3.2 Identificando emoções

A interação interpessoal é muitas vezes intrincada e cheia de nuances, e o sucesso é muitas vezes dependente de uma variedade de fatores. Esses fatores variam amplamente e podem incluir o contexto, humor e tempo da interação, bem como as expectativas dos participantes. Para isto o ser humano é naturalmente provido de habilidades para perceber a receptividade de seu interlocutor e ajustar a mensagem de acordo, há um julgamento emocional nesta equação, que o indivíduo faz de forma nativa, uns possuem mais habilidades que outros, estes possuem uma inteligência emocional mais apurada. James Pao (2017), concluiu que o ser humano produz uma expressão facial distinta para cada uma das sete principais emoções: raiva, desprezo, desgosto, medo, felicidade, tristeza e surpresa. O sistema descrito por Pao utiliza “unidades de ação” que descrevem movimentos de certos músculos faciais e grupos musculares para classificar as emoções, permitindo respostas precisas na leitura emocional a partir de fotos e imagens obtidas. Pao acredita que o recurso de leitura emocional possa permitir uma experiência mais gratificante ao usuário nos espaços de interação mediada por algoritmo, uma vez que estes algoritmos poderão ser dotados de inteligência emocional.

O Facebook registrou pelo menos três patentes ligadas a reconhecimento de emoções no período de 2014 e 2015[11]. A tecnologia funciona baseada na forma como o usuário interage com o teclado, touch pad, mouse, tela touch screen e outros dispositivos de entrada, além das câmeras dos dispositivos. Fatores como velocidade e intensidade com que se usa o teclado, ou se o smartphone esta ou não em movimento oferecem elementos para rastrear as emoções dos usuários. Uma das patentes permite o usuário usar a webcam para substituir automaticamente uma selfie por um emoticom de acordo com seu estado emocional, entretanto este reconhecimento continua ativo através da câmera, mesmo que o usuário não a esteja utilizando.

O desenvolvimento da industria de vigilância também inclui o reconhecimento facial, não só para identificar indivíduos, mas também para identificar suas emoções. A empresa Russa NTechLab desenvolveu uma tecnologia capaz de reconhecer as pessoas e suas emoções[12], inclusive em sistemas de CCTV, o que significa que o indivíduo e seu estado emocional podem ser rastreados, mesmo sem seus dispositivos.

4 Conclusão

Em um dez anos o modelo de vigilância passou por duas importantes transformações: A primeira foi a migração do conceito de visibilidade do par ver-ser-visto do panóptico, para o panspectro focado nos dados que o indivíduo produz voluntária e involuntariamente. A segunda é que passou de um modelo de vigilância a partir de um ponto central, para uma vigilância distribuída com alta permeabilidade.

Algumas hipóteses para este processo profundo de mudança são além da evolução tecnológica, o rápido crescimento rápido da penetração dos smartphones no mercado. No Brasil foi de 5% em 2008 para 87% em 2017[13], somados à oferta franqueada de acesso a aplicativos de redes sociais, fomentado pelo emergente capitalismo de vigilância.

Atualmente, dispositivos como smartphones, vestíveis e IoT, através de seus diversos sensores coletam dados sobre o indivíduo de forma continua, permanente e simultânea. Estes dados podem ser modelados e comparados para produzir informações precisas sobre o indivíduo. O indivíduo pode estar assistindo à TV em sua casa, com seu smart watch no pulso, e durante a exibição de uma determinada publicidade, seus dados fisiológicos podem estar sendo medidos, processados e enviados, medindo sua reação emocional.

Aplicações de redes sociais como o Facebook constroem perfis extremamente precisos dos indivíduos, além do perfil psicométrico, seus interesses, particularidades, relacionamentos, renda familiar, padrão de consumo, biometria facial, e até seu estado emocional.

A inteligência artificial já conta com a inteligência emocional, o trabalho de James Pao, e as patentes do Facebook de leitura emocional corroboram com esta possibilidade, que na prática se resume ao sistema de publicidade dirigida da linha 4 do metrô de São Paulo[14].

Não havendo limite para estes processos, perfis cada vez mais precisos dos indivíduos e seus relacionamentos serão construídos o ponto de dar às ciências humanas uma precisão próxima das exatas.

A emergência do Estado Informacional, fomentado pelo capitalismo de vigilância, produzem a coleta, processamento, transmissão e armazenamento de dados, de forma indiscriminada, objetivando a obtenção de lucro com a venda de perfis, para publicidade dirigida, transformando o indivíduo em mera “biomassa” humana. Este processo esta rompendo as barreiras entre os laboratórios e o mundo real, algoritmos, apresentam informações aos usuários de forma única, utilizando-se da prática do vinculo duplo, para ultraja-lo e obter deste maior interação, produzindo uma montanha russa emocional.

O surgimento de legislações de proteção de dados pessoais como a GDPR na Europa e a LGPDP no Brasil, permitem estabelecer limites a estas questões.

Por fim, nos da academia temos de compreender e assumir nossa responsabilidade sobre o futuro da humanidade frente a dicotomia beneficio x ameaça da tecnologia. Seja através do estabelecimento de limites éticos nos resultados e na utilização de sua pesquisa.Seja através da divulgação cientifica ampla geral e irrestrita, adequando seu trabalho ao público alvo, abolindo o formalismo, e buscando formas de explica-lo ao mais humilde cidadão

Referências

ASSANGE, J. et al. **Cypherpunks: liberdade e o futuro da internet**. Boitempo, 2013.
BAUMAN, Zygmunt; DAVID, Lyon. **Vigilância Líquida**. Zahar, 2013.
BECKER, Howard S. **Outsiders**. Zahar, 2014.
BRAMAN, Sandra. **Change of State: Information, Policy, and Power**. The MIT Press, 2006.
BRUNO, Fernanda. **Máquinas de ver, modos de ser: vigilância, tecnologia e subjetividade**. Sulina, 2013.
FOUCAULT, Michel. **Vigiar e Punir**. Almedina, 2014.
GOLBECK, Jennifer. **Predicting personality from social media tex**t. Transactions on Replication Research, v.2-2: p.1–10, 2016.
O'NEIL, C. **Weapons of math destruction: How big data increases inequality and threatens democracy**. United States: Crown Publishing Group (NY), 2016.
PAO.James. **Emotion detection through facial feature recognition**. Technical report, Stanford, 2017.
WRÓBLEWSKA, Maria. **Monologue of the Algorithm: how Facebook turns users data into its profit**.(12/01/2018) disponível em https://en.panoptykon.org/articles/monologue-algorithm-how-facebook-turns-users-data-its-profit-video-explained acesso em 02/02/2018
WU, Youyou; KOSINSKI, Michal; STILLWELL,David. **Computer-based personality judgments are more accurate than those made by humans**. 2015.
ZUBOFF, S. Big other: Surveillance capitalism and the prospects of an information civilization. *Journal of Information Technology*, [s.l.], v. 30, nº 1, p. 75–89, 2015.

Bibliografia consultada

GOLBECK, Jennifer; ADALI, Sibel. **Predicting personality with social behavior: a comparative study**. Soc. Netw. Anal. Min.,2014. doi: 10.1007/s13278-014-0159-7
KAPPLER, Karolin; SCHRAPE, Jan-Felix; ULBRICHT, Lena; WEYER, Johannes. **Societal Implications of Big Data**. KI - Künstliche Intelligenz v.32. p.55-60 (2018)
SHARE LAB. **Facebook Algorithmic Factory (1,2 e 3)**. Disponível em: https://labs.rs/en. Acesso em: 10/03/2017.
STEINER, Christopher. **Automate This: How Algorithms Came to Rule Our World**. Portfolio Hardcover, 2012.

Notas

[1] Log de acesso registra o IP e timestamp (registro contendo data, hora, minutos e segundos) para cada conexão

[2] Mega Não - https://meganao.wordpress.com/

[3] Veja em: http://softwarelivre.org/portal/fisl/veja-escute-e-leia-na-integra-o-discurso-do-presidente-lula-no-fisl-10 acesso em: 10/12/2017

[4] Disponível em: https://issuu.com/annacarolinapapp/docs/em_nome_da_internet

[5] Veja em: https://www.internetworldstats.com/stats.htm

[6] Veja em: http://www.telecompetitor.com/3-4-device-connections-per-person-worldwide-2020-cisco-highlights-11th-visual-networking-index/

[7] Conforme matéria na revista The Economist - https://www.economist.com/news/leaders/21721656-data-economy-demands-new-approach-antitrust-rules-worlds-most-valuable-resource acesso em 26/02/2018

[8] Veja em: https://investor.fb.com/investor-news/press-release-details/2018/Facebook-Reports-Fourth-Quarter-and-Full-Year-2017-Results/default.aspx acesso em 12/02/2018

[9] Veja em: https://abc.xyz/investor/ acesso em 12/02/2018

[10] Veja em: https://applymagicsauce.com/

[11] https://www.digitaltrends.com/social-media/facebook-patents-emotion-tracking/

[12] Veja em: http://mashable.com/2017/07/28/russia-facial-recognition-emotion-ntechlab-findface/

[13] Fontes: IBOPE inteligência http://www.ibopeinteligencia.com/ , Deloitte https://www2.deloitte.com/br/pt.html , Teleco http://www.teleco.com.br/smartphone.asp

[14] Leitura Facial Metrô: https://jornal.usp.br/atualidades/novas-portas-da-linha-4-amarela-contam-com-reconhecimento-facial/