JOÃO CARLOS REBELLO CARIBÉ

Seminários Interdisciplinares em Informação e Conhecimento - *Cultura do Algoritmo: informação, comunicação e conhecimento sob a lógica da tecnologia digital*

Prof. Paulo César Castro

O organismo de vigilância, a digitalização do indivíduo, da sociedade e a prática da previsibilidade

Artigo

Janeiro de 2018

O organismo de vigilância, a digitalização do indivíduo, da sociedade e a prática da previsibilidade

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). Graduado em Propaganda e Marketing pela Universidade Estácio de Sá.

Resumo

A sociedade está cada vez mais conectada e dependente de seus dispositivos computacionais, e suas úteis e empolgantes habilidades. Aos poucos o indivíduo está terceirizando sua autonomia, e alimentando um gigantesco organismo de vigilância, que paulatinamente está aprendendo mais sobre o indivíduo do que ele mesmo. Por causa desta prática, padrões cada vez mais precisos são criados sobre o indivíduo, e sobre a sociedade, a ponto de concluir que um metaverso esta sendo construído, com cópias em modelos matemáticos destes indivíduos. Neste metaverso simulações e avaliações complexas poderão ser executadas, dando aos cardeais do algoritmo o poder da verdade e o poder da premunição.

Palavras-chave
Algoritmo, redes sociais, sociabilização, estado informacional, big data, deep learning, machine learning, tracker, reconhecimento facial, reconhecimento emocional, técnicas preditivas, capitalismo de vigilância, dispositivo de vigilância, vigilância distribuida, vigilância liquida, panspectro, panóptico.

Introdução

O presente artigo está centrado no estudo epistemológico da privacidade, com foco na avaliação e sistematização do potencial de vigilância a partir das tecnologias atuais, e na exploração das possibilidades a partir desta avaliação, com o objetivo de demonstrar a viabilidade de estabelecer predições comportamentais dos indivíduos.

O Mega Não

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

Desta ameaça surgiu o Mega Não, idealizado por Daniel Pádua e João Carlos Caribé, um metamanifesto que concatenava todos os eventos e ações daqueles que combatiam o projeto. Este grupo de trabalhou duro, didaticamente elucidou milhares de brasileiros à cerca dos riscos do projeto de lei. O Mega Não publicou uma petição on-line que obteve mais de 100 mil assinaturas, tornando-se noticia, sendo usada no congresso, por políticos progressistas, 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),

[1] Log de acesso registra o IP e timestamp para cada conexão

pelo presidente Lula[2], por uma constituição da Internet, surgindo assim o Marco Civil. Segundo Lula, a regulação da Internet não poderia começar pela porta da cadeia, mas, pela garantia dos direitos do cidadão. Esta história foi linda e foi sistematizada e contada pela Anna Carolina Papp em sua monografia intitulada "Em nome da Internet"[3].

Este movimento mobilizou milhares de pessoas, que estavam preocupadas com sua privacidade na Internet. O risco do Estado saber quando os cidadãos conectavam e confirmando suas identidades, além do registro de todo site visitado na Internet, e registrando tudo isto por três anos, parecia ser um verdadeiro pesadelo.

As primeiras janelas de vigilância

Em 2008, a preocupação era com a vigilância do Estado sobre o cidadão, entretanto, desde que o protocolo HTTP foi criado, diversos dados sempre foram compartilhados com os servidores de internet. A maioria dos ativistas sabia disto, mas não demonstraram a mesma preocupação com a vigilância privada.

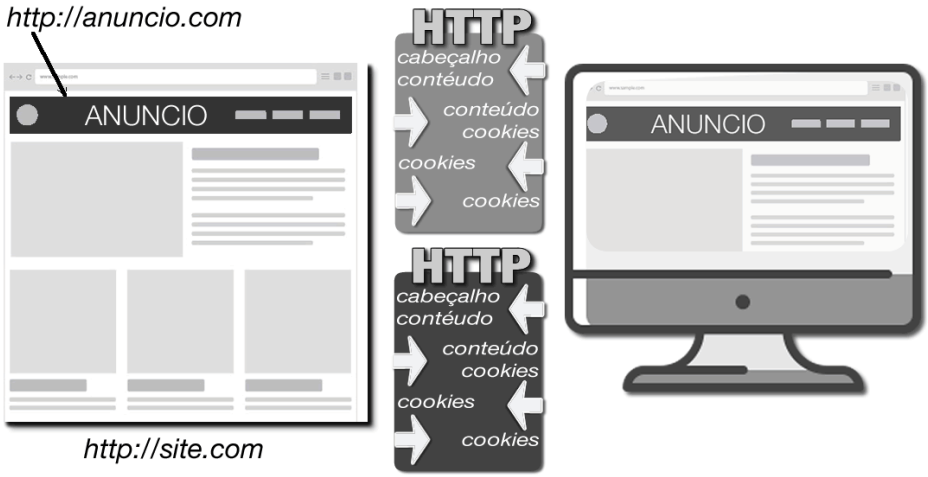


Figura 1: Esquema de conexão HTTP com duas sessões

Em uma simples conexão HTTP (explicada em detalhes no anexo 1), ou seja, ao acessar um site, o usuário (cliente) envia um cabeçalho com diversas informações como número de IP, dados do computador e navegador, recebendo em troca o conteúdo solicitado, e na mesma operação o servidor acessa e grava um cookie, que é um

---

[2] 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

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

pequeno arquivo com até 4Kb de dados, no computador do cliente. Os cookies em geral são utilizados para identificar se uma visita ao site veio do mesmo cliente, mas também são usados para criar personalização, gerenciar dados de uma sessão de comércio eletrônico, ou podem ser usados para registrar um ou mais códigos que permitam identificar o cliente em um banco de dados. Com o número de IP do cliente, é possível determinar de forma geral sua localização.

Quando o site exibe um banner, é como se literalmente ele abrisse uma janela para o anunciante impactar o cliente, conforme ilustra a figura 1 acima. Toda troca de informações HTTP citadas anteriormente se dão também com o anunciante, apesar dele não poder acessar o cookie do site, pode acessar o seu próprio cookie e grava-lo. E este mesmo cookie estará disponível para o anunciante, em qualquer outro site em que um de seus anúncios seja exibido, desta forma é possível ao anunciante identificar e registrar os interesses do cliente. Este cookie em especial é conhecido tecnicamente por "tracking cookie", ou simplesmente "tracker".

Por este artifício, soluções como o AdSense[4] do Google permitem identificar o site que o cliente está visitando, assim como o conteúdo da página, uma vez que a publicidade é exibida de acordo com este conteúdo, e para isto a página inteira é carregado e analisado pelo Google em frações de segundo. Os anúncios do AdSense do Google são inseridos de forma a permiti-los executarem diversos algoritmos por Javascript, uma linguagem de programação, que possibilitam entre outras coisas identificar o tempo despendido na página, os movimentos e interações do mouse, teclado e rolagem de tela. É importante observar que o Javascript adicionou novas habilidades além do cabeçalho HTTP, esta característica será abordada adiante quando falarmos da **profundidade** nos dispositivos de vigilância.

Se este usuário (cliente) tiver uma conta Google (Gmail, Google Plus ou Youtube), o Google fará uma identificação positiva, agregando todas as informações obtidas à sua conta pessoal. Isto permite aprimorar e exibir publicidade de acordo o histórico registrado, e cria um vínculo inseparável entre o código usado para rastrear o

---

[4] Veja em: http://adsense.google.com/ o AdSense foi lançado pelo Google em 2003. acesso em 03/12/2017

usuário no cookie do AdSense e a conta Google. Ao inserir o código do AdSense ou de qualquer outro parceiro de publicidade, o site estará literalmente abrindo uma janela para o Google.

O Google AdSense também oferece o serviço de Remarketing que rastreia o comportamento dos usuários em sites de compras e pesquisa de preços, oferecendo posteriormente publicidade com os produtos pesquisados. Isto explica o Facebook exibir publicidade oferecendo o mesmo produto que este usuário pesquisou.

É importante notar que toda esta informação está sendo registrada, e são dados importantes sobre o indivíduo, obtidos de forma invisível e involuntária.

Modelos de vigilância

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.

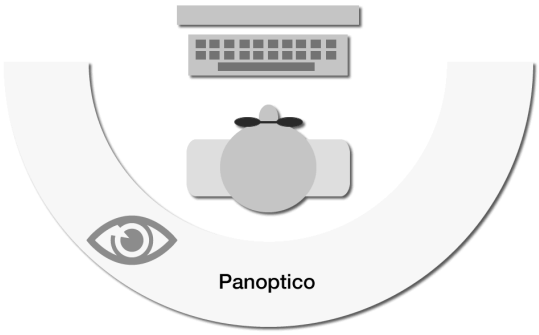


Figura 2: Modelo de vigilância na internet em 2008, o panóptico sobre um indivíduo

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 (FOCAULT, 2014). O panoptismo presume a vigilância, o controle se dá por esta premissa. A interpretação do modelo 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.

Como veremos adiante, com a análise dos dispositivos e suas configurações como potenciais dispositivos de vigilância, aliados a pluralidade de usos, pontos de coleta e armazenamento de dados, a adoção de um único modelo como referencial interpretativo das formas de vigilância contemporâneas certamente não abarcará todas as possibilidades e induzirá a uma miopia contextual.

A vigilância anteriormente sólida e estável, esta agora liqüefazendo e permeando em espaços antes impenetráveis, como sintetizam 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. 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.

De fato, hoje o indivíduo auto 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, 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.

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.

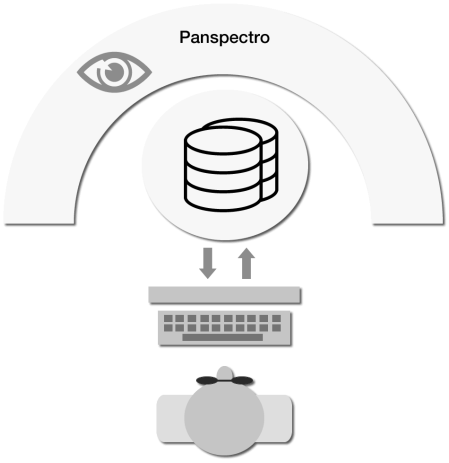


Figura 3: Modelo de vigilância, o panspectro

A vigilância do panspectro, como demonstra o diagrama acima, se dá sobre os dados produzidos pelos diversos dispositivos de vigilância 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 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 fazer daquele um comportamento desviante. Estes responsáveis, no contexto deste

artigo, podem ser os viesses dos próprios algoritmos de mineração de dados. Este viés dos algoritmos pode ser resultante de mal entendido, ou viés 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 que iremos estudar é um modelo complexo, que envolve todos os modelos citados, e pela perspectiva dos dispositivos como esquematizado na figura a seguir, que considera apenas os dispositivos computacionais, e que em uma segunda análise, em outro artigo, deverá considerar também os dispositivos não computacionais como os sistemas tradicionais de vigilâncias, produzindo dados e agregando ao modelo complexo.

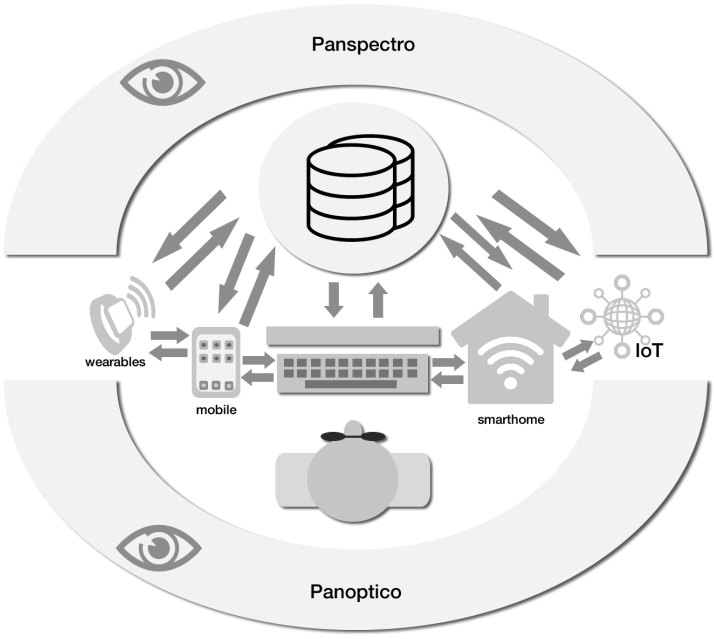


Figura 4: Modelo de vigilância contemporâneo, o modelo complexo

Anatomia dos dispositivos

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 intenções ou prescrições de um centro de ordenação ou controle. (BRUNO, 2013)

Ainda que Fernanda Bruno 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.

Com o objetivo de sistematizar e estabelecer referenciais para este trabalho, foi realizada uma pesquisa[5] nas especificações técnicas de diversos dispositivos, compreendidos como hardware no contexto da informática. A pesquisa se deu nos sites dos fabricantes e noticias, de diferentes dispositivos conectados fixos, móveis, vestíveis (wearables), IoT (Internet das coisas), e de casas inteligentes (smarthome). Esta pesquisa levou ao entendimento, após a tabulação, análise e estruturação dos dados pesquisados, que os dispositivos possuem cinco elementos em comum em sua estrutura: sensores, atuadores, conectividade, memória e habilidades, como representado esquematicamente na figura a seguir.

Figura 5: Anatomia de um dispositivo

Os **sensores**, são responsáveis pela obtenção dos dados, podem ser teclados, câmeras, microfones, GPS, giroscópios, acelerômetros, dentre outros. **Atuadores** são formas de interação a partir do dispositivo, por exemplo, a câmera de fotografia de um

[5] Veja a pesquisa no Anexo 2

smartphone, o sensor de luz ambiente informa ao dispositivo a luminosidade, e este, usando suas habilidades, aciona ou não o flash, através de um atuador. Alguns sensores como as câmeras, por exemplo, podem ter tanto a função de sensor como atuador, conforme as características das habilidades que estão em uso. **Conectividade**, é a forma como o dispositivo conecta com outros e/ou com redes locais e a Internet. Nas tecnologias pesquisadas a conectividade se dá através de rede celular (3G/4G), Bluetooth e Wi-Fi. A **memória**, RAM[6] e ROM, são onde os dados são transitoriamente gravados, e onde os algoritmos são gravados e executados. **Habilidade** neste contexto é uma capacidade específica de processamento de dados e controle do dispositivo. As habilidades permitem, através de seus algoritmos, produzir novos dados a partir de outros, assim como controlar os sensores, atuadores e a conectividade. Um exemplo é um aplicativo para medir o ritmo cardíaco em um smartphone, o aplicativo é a habilidade, que aciona a luz do flash que ilumina o dedo em contato com a lente da câmera, permitindo converter uma leitura visual em registro de ritmo cardíaco, destacamos que neste exemplo a câmera teve uma atuação ambígua de sensor e atuador.

As habilidades de um dispositivo podem ser classificadas em três tipos conforme o ambiente onde o algoritmo é executado: própria, hospedeira e remota. A **habilidade própria** é aquela nativa do dispositivo, como um sistema operacional, ou firmware[7] quando se trata de dispositivos menos complexos. Uma **habilidade hospedeira** é um aplicativo ou software que pode ser instalado e desinstalado do dispositivo adicionando novas funcionalidades. Já uma **habilidade remota** é quando um algoritmo é executado remotamente em outro dispositivo, e o resultado do processamento retorna ao dispositivo de origem. Um exemplo de habilidade remota são os sistemas de ditados, onde o dispositivo “ouve” a fala e transcreve. Todo processamento de conversão se dá remotamente, o audio é enviado para um servidor (dispositivo) remoto, que possui as bases de dados e algoritmos capazes de decodifica-lo, retornando o texto para o dispositivo. Este exemplo é interessante, pois demonstra que o dispositivo deve possuir obrigatóriamente uma habilidade própria ou hospedeira, pois neste exemplo, ela atuaria

---

[6] Memória RAM - Memória de Acesso Aleatório: https://pt.wikipedia.org/wiki/RAM Memória ROM - Memória Somente Leitura: https://pt.wikipedia.org/wiki/Mem%C3%B3ria_somente_de_leitura

[7] Firmware é o conjunto de instruções operacionais programadas diretamente no hardware de um equipamento eletrônico, são operações de baixo nível e alguns dispositivos permitem sua atualização. https://pt.wikipedia.org/wiki/Firmware

na operação de conversão do audio analógico para digital, preparo e envio deste audio para a conectividade, e no retorno, do recebimento do texto da conectividade e seu envio para o atuador (tela).

Metadispositivos

Uma característica importante dos dispositivos frente ao descrito, é a possibilidade de interconexão, que possibilita expandir suas capacidades e campo de ação, permitindo aos dispositivos compartilharem seus elementos e dados. Um exemplo são os relógios inteligentes (smart watch), dispositivos vestíveis (wearables), que possuem sensores e habilidades para obterem dados fisiológicos e físicos tais como batimento cardíaco e, identificação e gestão de atividade física, e trabalham conectados com o smartphone, dando a ele a capacidade de obter e tratar estes dados. É interessante observar que os dispositivos neste exemplo estão compartilhando suas habilidades, sensores, atuadores e dados, de forma distribuída e coordenada. Ainda dentro deste entendimento podemos conceber a idéia de um dispositivo com elementos distribuídos e escaláveis, tal como um sistema de segurança que possui um dispositivo central, com habilidade, memória e conectividade; alguns dispositivos com conectividade, habilidades, memória e sensores de movimento; outros com conectividade, habilidades, memória e câmera de video; um dispositivo com conectividade, habilidades e atuadores, que irão acionar as trancas e o alarme sonoro. Estes dispositivos interconectados configuram um novo dispositivo, que pode ser compreendido como um **metadispositivo**, que permite ao detectar o movimento, iniciar a gravação de vídeo, acionando as trancas e o alarme sonoro, e simultaneamente notificando no smartphone do proprietário, e transmitindo o video, que esta sendo capturado.

Este é o princípio da Internet das Coisas (IoT), que se configura com diversos dispositivos interconectados, transformando em metadispositivo, de forma escalar e infinita, pois um metadispositivo é na prática um dispositivo interconectado a outros dispositivos sem necessariamente atender à uma lógica hierárquica. Ao aprofundar neste entendimento, percebe-se que a IoT não está relacionada apenas aos dispositivos interconectados com objetivos específicos, este conceito se amplia a todo e qualquer dispositivo conectado, qualquer dispositivo é na prática uma “coisa”.

O organismo

Um único dispositivo pode enviar dados para diferentes servidores nas nuvens, por exemplo, cada habilidade hospedeira (aplicativo) pode possuir sua própria nuvem, e o dispositivo também pode usar uma ou mais nuvens proprietárias para tarefas como backup e sincronização de dados, como ilustrado na figura a seguir.

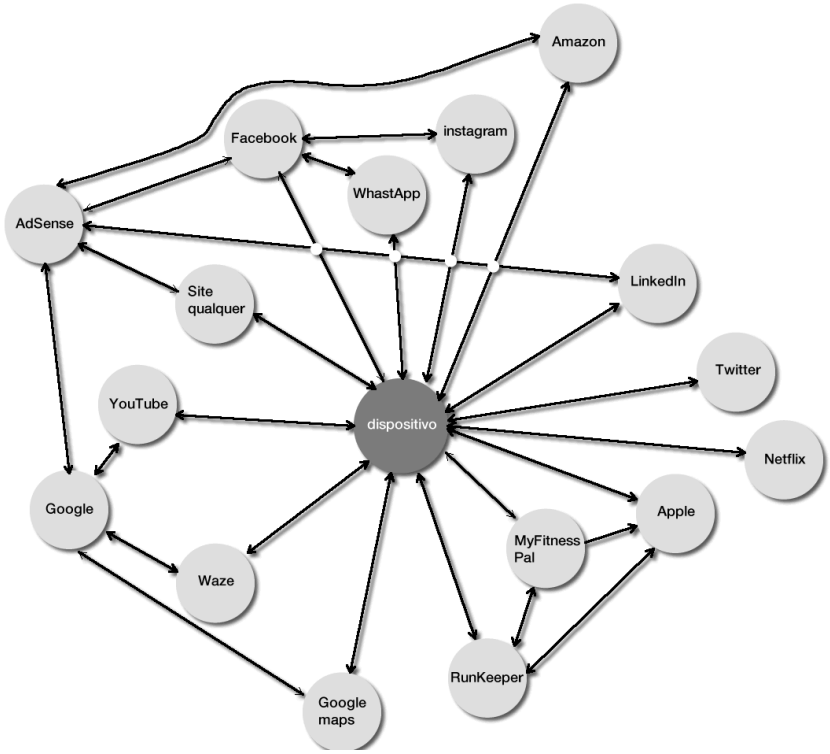


Figura 6: Modelo estrutural de conectividade de um dispositivo

Observa-se algumas particularidades nesta figura. É possível visualizar graficamente como o AdSense acessa e compartilha dados, e como é possível o remarketing. A imagem ilustra como os dados de um cliente específico podem ser compartilhado entre diferentes serviços. Outro ponto interessante é como aplicativos (habilidades hospedeiras) podem compartilhar dados entre si, como no caso do aplicativo de atividade física "RunKeeper", que envia os dados das atividades físicas como calorias queimadas, distância percorrida e tipo de atividade para o aplicativo "MyFitnessPal" que é um aplicativo de controle alimentar, permitindo assim uma perfeita contabilidade de calorias diárias. Ambos aplicativos compartilham, entre si, diversos dados, inclusive o diário alimentar com um terceiro aplicativo o "Apple Health", que concentra todos os dados fisiológicos e médicos do usuário. Os dados são

compartilhados entre as habilidades dos dispositivos e destes para as nuvens de dados específica de cada aplicativo.

A figura 6 representa uma rede de interconexão hipotética de um único dispositivo, suponhamos que seja um smartphone, adicione um tablet, um computador, uma smart TV, todos conectados à uma rede doméstica, à qual estão conectados os demais dispositivos da casa, e de outros coabitantes, formando um "clique"[8] . Ao imaginar-se distanciando desta rede, percebe-se outras redes, outras conexões, formando clusters e mais clusters, e em uma observação mais distante, visualiza-se esta rede imaginária com um verdadeiro grafo, uma complexa rede composta de dispositivos e metadispositivos, conectados a dispositivos remotos (nuvens), que concentram os dados coletados. Muitos dispositivos são moveis, trocando de ponto de conexão e produzindo dados dinâmicos de seus portadores como posicionamento, aceleração, altitude, imagens, etc... Mesmo deslocando, e mesmo sem conectividade, estes dados são passíveis de registro pelos sensores dos dispositivos.

As nuvens são dispositivos remotos, onde sensores e atuadores são as interfaces de conexão com os usuários, o Google, o Facebook e muitos outros se enquadram nesta categoria.

Ao imaginar um afastamento suficientemente a ponto de visualizar todo planeta, mas sem perder de vista as interconexões dos dispositivos, metadispositivos e nuvens, o resultado seria como um grafo, muito mais complexo que o grafo hipotético da figura a seguir que possui pouco mais 800 nós. Segundo o Internet World Stats[9], em Dezembro de 2017, 4,1 bilhões de pessoas tinham acesso a Internet, considerando que o relatório da Cisco[10] projeta que em 2020, existirão em média 3,4 dispositivos conectados à Internet por usuário, e considerando a média de 3 dispositivos, teríamos um grafo com mais de 12,3 bilhões de nós e um número muito superior de conexões, o grafo resultante seria tão denso que pareceria uma esfera opaca.

---

[8] Divisões na rede em ARS (análise de redes sociais), clique é um conjunto de atores com conexões estreitas, cluster um conjunto de relações similares, quando plotadas formam grafos que representam uma rede com nós e conexões.

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

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

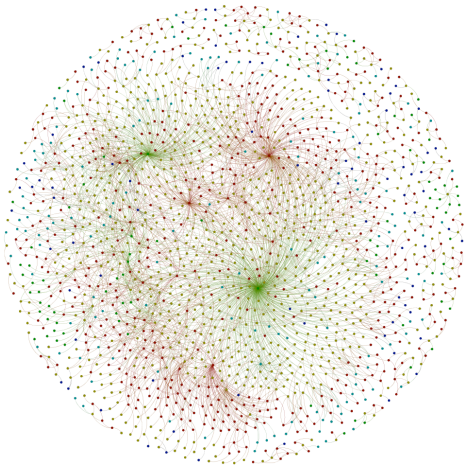


Figura 7: Grafo hipotético de um organismo

Este grafo composto de bilhões de dispositivos e metadispositivos conectados à milhares de dispositivos remotos (nuvens), é o que se pode chamar de **organismo de vigilância**, cujo potencial de vigilância está relacionado a cinco campos potenciais dos dispositivos.

Os cinco campos potenciais de vigilância dos dispositivos

Ao longo do desenvolvimento da pesquisa sobre os dispositivos, do estudo de diversos artigos, e da leitura de noticias e textos na Internet sobre o tema privacidade e vigilância, surgiram diversos fatores que influem no potencial de vigilância. Estes fatores depois de tabulados e categorizados resultaram em cinco campos potenciais de vigilância. Cinco campos que possuem variáveis que influem positivamente ou negativamente no potencial de risco à privacidade, compreendido neste artigo como potencial de vigilância. Os potenciais de vigilância podem servir de referencial estratégico para a construção de políticas de dados. É importante destacar que o potencial de vigilância de um dispositivo significa a possibilidade de vigilância. Os campos potenciais são o técnico, mercadológico, legal, de segurança e comportamental.

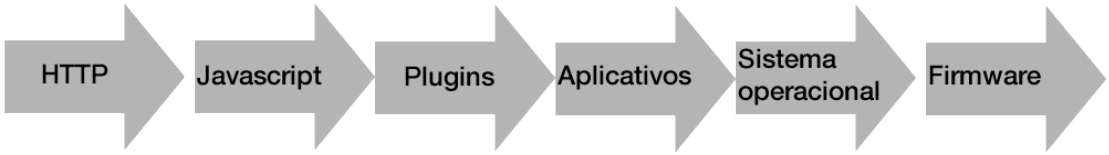
O potencial técnico

Evolução tecnológica e qualidades técnicas tornam os dispositivos mais eficientes, e mais potencialmente invasivos. O potencial técnico se divide em dois aspectos: capacidade e profundidade.

A **capacidade** está relacionada as qualidades técnicas e evolução tecnológica do dispositivo, estas variáveis estão relacionadas ao tamanho e velocidade de acesso da memória, à capacidade de processamento do dispositivo e à velocidade e duração da conectividade.

A capacidade também esta relacionada as qualidades técnicas dos elementos do dispositivo, por exemplo, quanto maior a resolução da câmera, melhor a imagem e uso que se faz dela, o mesmo se da para cada componente do dispositivo.

A **profundidade** esta relacionada às habilidades hospedeiras, é subordinada à uma política de sandbox. Sandbox, ou caixa de areia, é um mecanismo de segurança computacional que serve para separar e limitar os programas em execução (habilidade hospedeira), geralmente controlando e limitando o acesso dela a determinados recursos,



dados, sensores e atuadores.

Figura 8: Profundidade do sandbox

A figura acima demonstra o nível de profundidade, da esquerda (raso) para a direita (profundo). O HTTP e Javascript como já visto anteriormente possuem acesso limitado aos recursos do dispositivo. O HTTP apenas ao cookie, e o Javascript a alguns sensores e atuadores de entrada e saída como tela, teclado, mouse e touchscreen. O Plugins, funcionam através dos navegadores e permitem acesso a outros sensores e atuadores como câmera, memória, microfone e auto falante. O acesso à memória, sensores, atuadores e conectividade por parte dos aplicativos (habilidade hospedeira), é limitado pelas especificações do sistema operacional, a habilidade hospedeira pode inclusive acessar algoritmos do sistema operacional. O sistema operacional, possui acesso pleno aos componentes do dispositivo, pois é ele quem o gerência, e o mais profundo dos níveis fica com o firmware, este consegue acessar até mesmo recursos do dispositivo que não foram habilitados para o sistema operacional.

Em termos práticos, uma habilidade remota executada em um navegador de internet, o Facebook, por exemplo, só terá acesso aos recursos que o navegador permitir, mesmo com o plugin, este acesso será restrito e controlado. Ao executar o Facebook no dispositivo como uma habilidade hospedeira, o acesso será bem mais invasivo, com acesso a sensores e atuadores, e dados de outros aplicativos como agenda de eventos, caderno de endereços, dentre outros.

O potencial mercadológico

Uma das hipóteses levantada durante a pesquisa dos dispositivos, e pela cronologia da maior parte da bibliografia, era de que o potencial de vigilância cresceu com o surgimento das tecnologias e habilidades dos diversos dispositivos. Para responder à isto, foi realizada uma pesquisa da cronologia do surgimento de tais tecnologias e habilidades, e conclui-se que todos surgiram anos antes de seus efeitos serem percebidos e/ou estudado, inclusive os dispositivos vestíveis (wearables) que surgiram em 2010, conforme figura a seguir.

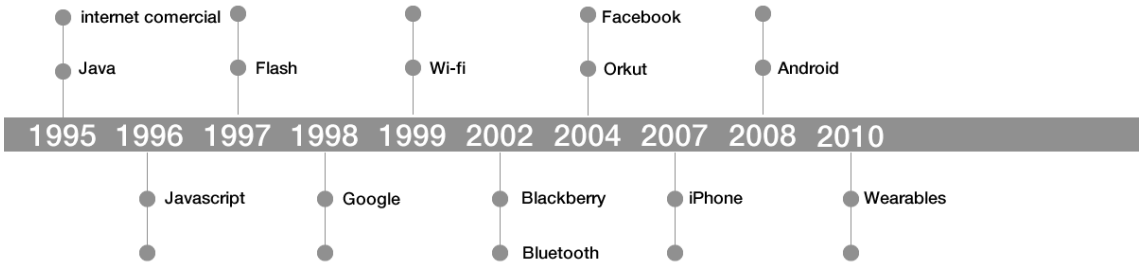


Figura 9: Linha do tempo do surgimento dos principais dispositivos e habilidades

Por exemplo, o Facebook foi lançado em 2004, mas só se tornou popular no Brasil a partir de 2011. Outro exemplo são os smartphones, surgiram em 2002 com o Blackberry, mas começaram a ganhar popularidade em 2007 com lançamento do iPhone, ainda assim, em 2010, apenas 7% da população brasileira possuía smartphone, somente a partir de 2015, que a penetração chegou à 57%. Desta forma pode-se concluir que o potencial de vigilância dos dispositivos está direta e proporcionalmente relacionado à lógica do mercado, ou seja ao ciclo de vida da tecnologia, tornando-se

maior à medida que aumenta sua penetração no mercado, conforme ilustra a figura a seguir.

Figura 10: Ciclo de vida do smartphone no Brasil[11]

O aumento do potencial de vigilância é diretamente proporcional à penetração da tecnologia no mercado. O que se conclui disto, é que um conjunto de dados sozinho não representa risco, o risco está na sua combinação com outros conjuntos de dados, dai a importância da escala. Quanto maior a escala de uso de uma tecnologia, maior o volume de dados que seus dispositivos produzem, e mais preciso são os resultados de sua mineração.

Apesar do potencial de vigilância estar relacionado ao ciclo de vida do dispositivo, os dados coletados permanecerão enquanto poderem ser armazenados e tratados, principalmente se forem compartilhados ou mesclados, mesmo que o dispositivo entre em declínio e seja retirado do mercado.

Ainda dentro do potencial mercadológico, práticas como aquisições e fusões de empresas, e acordos operacionais podem estabelecer novos usos dos dados coletados, inclusive possibilitando novas combinações, produzindo novos dados sobre os usuários e seus padrões. Esta pratica também pode dar novas habilidades aos dispositivos, a partir de uma nova perspectiva de coleta e uso de dados. Por exemplo ao comprar o

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

Waze, a Google passou a ter acesso a todos os dados de trânsito que cada usuário produz.

O potencial legal

O potencial de risco à privacidade de um dispositivo e/ou habilidade hospedeira e remota, é inversamente proporcional à transparência com que seus fabricantes tratam seus dados. Uma política de dados clara, descrevendo como os dados serão utilizados, que dados serão enviados para as nuvens, como serão criptografados, quem terá acesso a eles, se serão compartilhados, como serão armazenados, e qual o risco de serem obtidos de forma ilícita, reduz o risco à privacidade.

O robô aspirado iRobot esteve no centro de um escândalo[12], quando um dos executivos do fabricante falou em uma entrevista da intenção de compartilhar a planta baixa das casas de seus proprietários, como resposta, o fabricante criou e publicou, em seu site, uma política de privacidade e de dados exemplares[13].

A política de proteção de dados pessoais esta no centro da estratégia de governança de algoritmos[14], e como este artigo quer demonstrar, também está no centro da estratégia de proteção da privacidade. A comissão européia é pioneira, e já possui um marco legal na proteção de dados pessoais[15], no Brasil o principal projeto tramitando no congresso é o PL5276/2016, vem ganhando forte apoio da Coalizão Direitos na Rede[16], com a campanha de conscientização “Seus Dados São Você”.

O potencial de segurança

A segurança dos dados é uma enorme responsabilidade dos fabricantes dos dispositivos, habilidades embarcadas e remotas (aplicativos). Segundo o manual do CERT.Br[17], a segurança deve prever, perda - através de uma política de backup e

---

[12] Veja em: https://www.nytimes.com/2017/07/25/technology/roomba-irobot-data-privacy.html

[13] Veja politica de privacidade: http://www.irobot.com.br/Privacy-Policy e política de segurança de dados: http://www.irobot.com.br/Data-Security

[14] Veja em: https://www.politics.org.br/edicoes/o-que-%C3%A9-governan%C3%A7a-de-algoritmos

[15] Veja em: https://www.politico.eu/article/europe-data-protection-privacy-standards-gdpr-general-protection-data-regulation/

[16] Veja em: https://direitosnarede.org.br/c/seus-dados-sao-vc/

[17] Veja em: https://www.cert.br/docs/seg-adm-redes/

restauro de dados, roubo e acesso indevido dos dados - adotando uma boa política de criptografia e controle de acesso aos centro de dados, uma boa estratégia de firewall, e precauções contra engenharia social, bem como impedir o uso de rastreadores (crawlers) nas interfaces de acesso pela Internet. Tais práticas reduzem substancialmente o potencial de vigilância pelo risco à segurança (potencial de segurança).

O potencial comportamental

A competência do usuário para usar os dispositivos e as habilidades hospedeiras (aplicativos) é inversamente proporcional ao potencial comportamental de vigilância. A falta de competência crítica, leva o usuário a colocar seus dados, e sua privacidade em risco. Há, por exemplo, as opções de configurações de habilidades hospedeiras (aplicativos), que solicitam acesso a sensores e aos dados de outros aplicativos, por exemplo, aplicativos que solicitam acesso ao GPS, câmera, microfone em um smartphone. Há também o caso onde aplicativos compartilham dados entre si em um mesmo dispositivo, um exemplo é o aplicativo Health da Apple, que integra com outros aplicativos de saúde como o RunKeeper (controle de atividades físicas) e o MyFitness Pal (controle alimentar), possibilitando a integração de dados entre eles.

A CodingRights, tem o projeto “Chupadados”[18], um projeto elucidativo sob vários tópicos relacionados aos riscos aos dados pessoais, assim como o CERT.Br[19] possui inúmeras cartilhas e livros, todos gratuitos, para adultos e crianças sobre segurança na Internet e proteção de dados pessoais. A tarefa de educar o usuário é do fabricante, mas inúmeras organizações e até algumas empresas estão atuando neste tema, quanto maior a competência crítica do usuário, menor o potencial comportamental de vigilância.

Big data, big money e big other

A estrutura composta por dispositivos, metadispositivos e finalmente a união destes aos inúmeros data centers (nuvens) configurou o **organismo de vigilância**, uma complexa rede com mais de 12,3 bilhões de dispositivos e alguns milhões de nuvens.

---

[18] Veja em: https://chupadados.codingrights.org/

[19] Veja em: https://www.cert.br/

Considerando que somente um smartphone tem em média dez sensores diferentes, e considerando que os usuários utilizam diariamente diversas aplicações (habilidades hospedeiras), é possível imaginar a quantidade de dados criados e manipulados pelo **organismo**. O relatório Cisco Visual Networking Index: Forecast and Methodology, 2014–2019[20] permite dar a dimensão deste volume. Segundo o relatório, em 2016, **96 bilhões de Gigabytes** transitaram **mensalmente** pela Internet. Este número cresce tão rapidamente que o relatório prevê que o volume de dados que trafegará na Internet em 2021 será 127 vezes maior que todo conteúdo existente na Internet em 2005.

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 dispositivos que possuem suas habilidades hospedeiras ou remotas instaladas, e estas em geral não compartilham os dados entre si, este compartilhamento pode se dar através dos mecanismos citados no potencial mercadológico.

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. Para Assange, para a NSA é mais conveniente "espetar" suas escutas nestes data center do que monitorar os dispositivos de cada usuário.

Os dados são o novo petróleo[21], o Facebook teve uma receita bruta de U$ 40,6 bilhões em 2017[22], Alphabet, holding da Google, faturou U$ 110 bilhões, no mesmo período[23], por estes números é possível imaginar o tamanho do mercado. Em 2012 o Boston Consulting Group projetou[24] que a economia da Internet atingiria U$ 4,2 trilhões em 2016, somente no G-20.

---

[20] Veja em: https://www.cisco.com/c/en/us/solutions/collateral/service-provider/visual-networking-index-vni/complete-white-paper-c11-481360.pdf acesso em 27/02/2018

[21] 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

[22] 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

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

[24] Veja em: https://www.bcg.com/publications/2012/technology-digital-technology-planning-internet-economy-g20-4-2-trillion-opportunity.aspx acesso em 02/12/2017

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.

Os cardeais do algoritmo

As empresas proprietárias das nuvens, como o Google, Facebook dentre outros, são o que Cathy O’Neil 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. Os mecanismos legais podem ser transparentes ou opacos, estes através de agências governamentais de segurança como a NSA nos EUA e a ABIN no Brasil.

A mineração do big data depende de algoritmos cada vez mais complexos, que em sua maioria estão protegidos por patentes e segredos de negócios, e consequentemente

totalmente opacos, por esta razão Braman descreve, no Estado informacional, o empoderamento da iniciativa privada.

A digitalização do indivíduo

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

> They are responsible for the new form of labour and exploitation. The black box is, in fact, a factory. You, the user, is not a client. You become just a raw material, human biomass converted into a sellable digital profile on Internet stock market – in Facebook Ad Manager. (WRÓBLEWSKA, 2018).

O documentário "Monologue of the Algorithm: how Facebook turns users data into its profit" produzido pela Maria Wróblewska para o Panoptykon Foundation (WRÓBLEWSKA, 2018), apresenta de forma impressionante como os dados são obtidos e tratados pelo Facebook na construção de perfis extremamente precisos, mas o que motiva o indivíduo a produzir dados de forma espontânea, alimentando estes metadispositivos de vigilância?

A prática do self-tracking

A maior parte destes dados são compartilhados espontaneamente pelos usuários, segundo Bauman e Lyon, o indivíduo se tornou um servo da auto vigilância, é o que reforça o artigo "Societal implications of Big Data" de Karolin Kappler et al (2018). resumindo de forma concisa a questão, apontando os benefícios e riscos do big data. Para Kappler, a prática da auto vigilância tem algumas motivações gerais: **Auto-reflexão** - Como conseqüência da incerteza generalizada da vida moderna, o self-tracking tornou-se uma nova fonte de significado e reconhecimento social; **Otimização** - o self-tracking contribui para uma melhor compreensão do próprio corpo e ajuda a identificar opções de otimiza-lo; **Emancipação** - como a auto-avaliação leva à otimização, e como conseqüência o indivíduo torna-se mais independente da opinião de

especialistas sobre si, seu corpo e sua saúde; **Condescendência** - As novas normas sociais, que designam ao indivíduo a responsabilidade por si e pelo próprio corpo, promovem as práticas da auto-avaliação (KAPPLER et al, 2018).

Segundo os autores, o melhor entendimento do indivíduo e da sociedade sobre seus hábitos e sua fisiologia, através da análise do big data, com ajuda dos especialistas, pode levar à melhoria da qualidade de vida, inclusive na prevenção e tratamento precoce de doenças físicas e mentais. Também mostram o quanto a análise do big data pode melhorar as cidades, e seus fluxos diários de indivíduos em seus transportes, permitindo inclusive uma gestão dinâmica, e em tempo real, do controle de vias e semáforos. A análise de padrões também permite a previsão de delitos com base na repetição de padrões de delitos anteriores. Por fim os autores relatam que críticos são céticos do fato de que, sem uma regulamentação adequada, o big data pode ameaçar as liberdades individuais e os princípios democráticos, e recomenda que a regulamentação se dê em cinco domínios, dialogando com os potenciais de vigilância descritos anteriormente: Domínio da regulamentação do Estado, através de leis e normas de proteção de dados pessoais; domínio das auto-regulamentações corporativas, através de princípios e normas de aquisição, tratamento e armazenamento de dados de terceiros e garantia do anonimato; domínio da regulação através da sociedade civil, através do suporte de agências de proteção aos direitos dos consumidores; Domínio da auto-regulamentação profissional, através de normas de conduta e ética no principio da profissão; Domínio através da auto proteção, através da capacitação do usuário para proteger seus dados.

Padrões digitalizados

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. Se o dispositivo registra mesma coordenada durante a noite e em boa parte do final de semana, provavelmente este é o lugar de residência do indivíduo. Se o dispositivo costuma estar em determinada coordenada GPS durante o horário comercial,

provavelmente este é o local de trabalho. Outros dispositivos deslocando-se na mesma periodicidade para esta mesma coordenada, indicam ser colegas de trabalho. Se neste local, todos costumam conectar à mesma rede Wi-Fi, a certeza é ainda maior. Habilidades hospedeiras como o Facebook, WhatsApp acessam todas estas informações e muitas outras. Ao todo o aplicativo do Facebook acessa 43 recursos do dispositivo e o WhatsApp ,34, uma lista completa pode ser encontrada no anexo 3. Este simples exemplo permite ilustrar o potencial de vigilância que os algoritmos podem produzir a partir dos dados gerados pelos dispositivos, criando, comparando e combinando padrões.

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.

A vigilância Intrapessoal

A vigilância esta se deslocando para dentro do indivíduo, esta se tornando intrapessoal, é possível aos cardeais do algoritmo, saber dados fisiológicos, médicos, alimentares e psicológicos. Profissionais que lidam com estes dados seguem um código de ética e confidencialidade, mas uma vez que estes dados são obtidos por dispositivos, há um hiato legal, que pode produzir danos ao indivíduo e à sociedade.

Este nível de conhecimento do indivíduo e da sociedade, pode estabelecer no cruzamento exaustivo dos dados, resultados positivos, respostas para muitas questões que seguem em aberto, pelo conhecimento profundo de uma ampla gama de informações, mas o preço a se pagar pode ser a própria privacidade, liberdade e autonomia, o indivíduo perderá o domínio sobre si, a busca por um equilíbrio se torna necessária.

Identificando personalidades

Toda sociabilização nas 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, até mesmo as meta informações das fotos enviadas, como coordenadas GPS e dados da câmera. 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) (figura a seguir). Tudo isto tem por objetivo entreter o usuário, e vender estes perfis precisos como critérios de publicidade dirigida.

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.

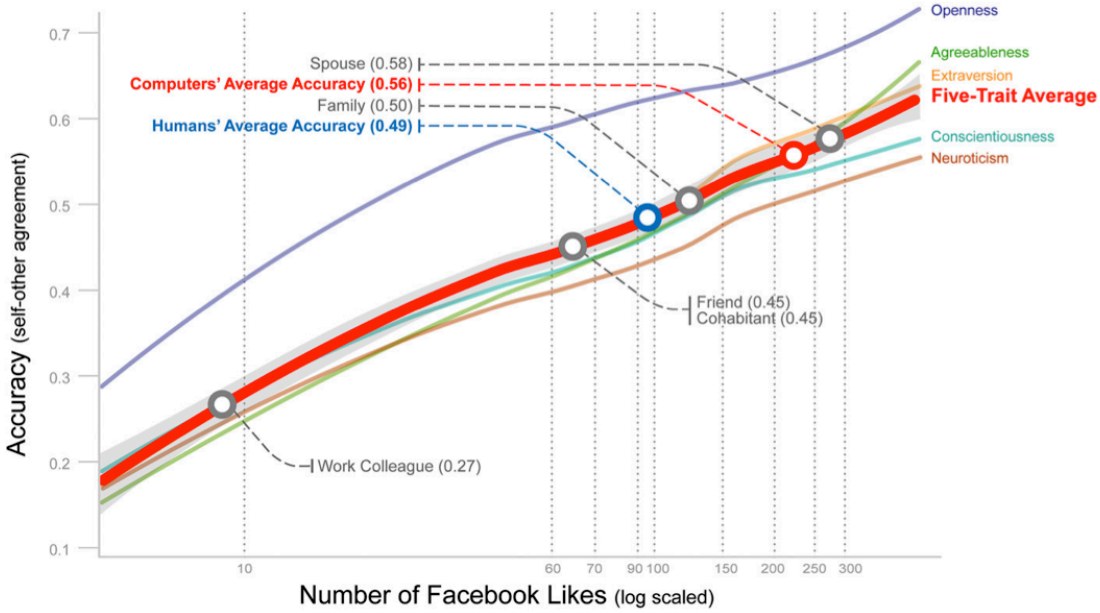


Figura 11: Numero de Likes do Facebook, Wu et al (2015) - Reprodução

No gráfico 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[25]. 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,

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

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. Golbeck(2014) também apresenta um estudo descrevendo como prever uma personalidade com base no comportamento social do indivíduo, inclusive nas redes sociais.

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 de 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[26]. 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[27], inclusive em sistemas de CCTV, o que significa que o indivíduo e seu estado emocional podem ser rastreados, mesmo sem seus dispositivos.

O pré crime

Sandra Braman descreve a possibilidade do indivíduo ser incriminados, num modelo de pré-crime com base em padrões e estatísticas de “provas” que o indivíduo produz involuntariamente contra si mesmo.

> Uma vez que a evidência do estado de espírito e das pretensas intenções de se envolver em determinada atividade, em vez de comportamentos reais, são agora usadas para fins de justiça criminal, é possível inclusive incriminar-se inconscientemente e irrefletido de intenções e comportamentos reais. (BRAMAN,2006, Tradução nossa)

Práticas preditivas não são novidade, em 2016 alguns bancos americanos estavam testando uma vigilância biométrica, através de sensores que avaliavm a temperatura corporal e batimentos cardíacos, e os associando à imagens do circuito fechado de TV de um indivíduo, como forma de prevenção de ilícitos[28]. Outro caso mais recente vem do Canadá, o governo canadense utilizará inteligência artificial para vasculhar as redes

---

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

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

[28] Veja em: http://fortune.com/2016/03/22/biometric-sensors-banks/ acesso 12/11/2017

sociais em buscas de traços que indicam tendências suicidas[29] em seus cidadãos, com o objetivo de prevenir e salvar vidas.

Outro interessante exemplo citado por O'Neil é o PredPol, sistema de mapeamento adotado pela policia de Santa Cruz, California. Este baseia-se no mapeamento das regiões e dados atualizados de crimes, desta forma permite prever onde haverá mais possibilidade de novos crimes. O problema é que isto acaba produzindo um ciclo de feedback pernicioso, pois ao mandar patrulhar as áreas suspeitas indicadas pelo PredPol, os policiais produzem ocorrências que alimentam a base de dados e a possibilidade de novas previsões nas mesmas regiões.

e-clones e e-sociedades

A precisão na construção de perfis com base no big data, a partir de um número crescente de indicadores, pode, em algum momento traçar perfis pessoais e psicológicos tão precisos que darão às ciências humanas uma precisão próxima a das ciências exatas. O indivíduo está sendo digitalizado, sua essência esta sendo codificada na forma de precisos modelos matemáticos. Estes clones digitais (e-clones) permitirão sofisticadas simulações, em números, detalhes e circunstancias nunca antes imaginados. Estas simulações poderão produzir novos padrões sociais codificados (e-sociedades), ou ainda serem utilizadas na prática foresene com e-clones dos suspeitos, testemunhas e vítimas em busca de novos elementos ou veredicto. As possibilidades são ilimitadas.

Estas simulações poderão prever comportamentos de indivíduos sob determinadas circunstâncias e contextos simulados, até mesmo determinar a probalidade deste cometer um crime. Neste ponto o cardeal do algoritmo terá o “dom da premonição” com tamanha precisão que a vida poderá imitar a arte, tornando o Minority Report realidade.

Com este nível de conhecimento do indivíduo, e dos novos padrões sociais codificados, a intensidade e precisão da vigilância do panspectro sobre os comportamentos desviantes poderá chegar a níveis alarmantes. Uma outra questão, é que os e-clones certamente sobreviverão aos indivíduos, como lidar com estes fatos novos é uma questão urgente e necessária.

---

[29] Veja em: http://gizmodo.uol.com.br/canada-ia-suicidio/ acesso em 02/03/2018

Bibliografia

ASSANGE, J. et al. **Cypherpunks: liberdade e o futuro da internet**. São Paulo: 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.

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) https://doi.org/10.1007/s13218-017-0520-x

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.

STEINER, Christopher. **Automate This: How Algorithms Came to Rule Our World**. Portfolio Hardcover, 2012.

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**. PNAS, 112 N4: 1036–1040, 2015. doi: doi/10.1073/pnas.1418680112.

Anexos
Anexo 01 - Modelo HTTP

Cada vez que um site na Internet (http://site.com no exemplo), é acessado, inicia-se uma troca de informações, conforme a figura acima. O navegador do usuário (cliente) requisita o conteúdo ao site na Internet (servidor), e simultaneamente, envia uma série de informações conhecidas por "cabeçalho HTTP"[30]. Neste processo, o servidor envia o conteúdo solicitado e requisita ao cliente os web cookies[31] (cookies), que são pequenas porções de dados que o servidor envia ao navegador do cliente, o navegador armazena estes dados que serão enviados ao servidor na próxima visita. Os cookies podem conter qualquer tipo de dado até 4Kb, que são acessíveis apenas pelo site que os criou. Em geral são utilizados para identificar se uma visita ao site veio do mesmo cliente, mas também são usados para criar personalização, e gerenciar dados de uma sessão de comércio eletrônico, ou podem ser usados para registrar um ou mais códigos que permitam identificar o cliente em um banco de dados em uma próxima sessão.

Informações do cabeçalho usualmente enviadas:

O cliente envia que "agente" esta usando (modelo do computador; versão do sistema operacional, versão e modelo do navegador de internet); que tipos de conteúdo ele aceita; que idiomas o "agente" está habilitado a reconhecer, se o cliente veio a partir da referência de um link, este endereço de referência também é informado; o endereço IP do cliente e algumas outras Informações.

Isto significa que o servidor consegue saber a localização aproximada de onde o cliente está acessando, como de que país, cidade e até o bairro, através do endereço IP[32]. Se esta usando um computador e navegador de internet atualizado, e o idioma compatível, desta forma em sites multi-idiomas, pode enviar o conteúdo adequado ao idioma adequado, tipo de navegador e sistema operacional do cliente. È desta forma que o servidor identifica se o cliente é um computador, tablet ou celular.

Conexão com múltiplas sessões HTTP

Quando o site exibe um banner, é como se literalmete ele abrisse uma janela para o anunciante impactar o cliente, conforme ilustra a figura a seguir. Toda troca de informações HTTP citadas anteriormente se dão também com o anunciante (http://anuncio.com), apesar dele não poder acessar o cookie do site.com, pode acessar o seu próprio cookie anuncio.com e grava-lo.

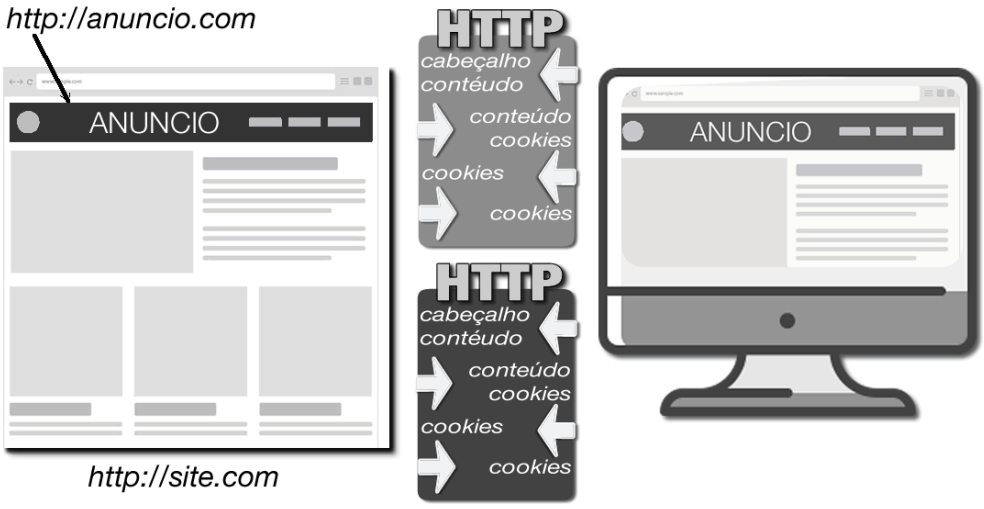
Um projeto interessante é o Trackography, que apresenta uma interface dinâmica que permite ver e compreender os trackers usados nos principais sites de noticias do mundo e de um país à escolha, acesse https://trackography.org/

---

[30] Cabeçalhos HTTP - https://developer.mozilla.org/en-US/docs/Web/HTTP/Headers para saber que dados o computador envia, acesse: http://myhttpheader.com/

[31] Cookies - https://developer.mozilla.org/en-US/docs/Web/HTTP/Cookies

[32] Geolocalização por IP - https://www.iplocation.net/



Entretanto há detalhes importantes neste processo. Primeiro que a publicidade é contextualizada de acordo com o conteúdo da página que esta sendo exibida, isto dá ao anuncio.com a capacidade de contextualizar o interesse do cliente e certamente registra isto em um banco de dados. Segundo que o cookie que o anuncio.com acessa no cliente é o mesmo, independente do site em que esteja sendo exibido. Isto explica, por exemplo, porque um usuário recebe promoções de produtos que tenha visto em outros sites.

Este é o princípio do Remarketing[33], que é um recurso geralmente oferecido pelo anunciante, neste exemplo "anuncio.com". Supondo que o site seja de comércio eletrônico e o usuário pesquisa produtos, mas não conclui a compra, isto fica registrado no banco de dados do "anuncio.com". Em outro momento, este mesmo usuário acessa o Facebook - que hipoteticamente usa o remarketing do "anuncio.com" - e fica impressionado em ver uma publicidade oferecendo exatamente o produto que ele havia pesquisado.

Anexo 02 - Sensores, habilidades, conectividade e atuadores nos principais dispositivos conectados

O levantamento foi realizado no período de 01 e 10 de Fevereiro de 2018, nos sites dos fabricantes, conforme relação abaixo.

Apple Watch 3	https://www.apple.com/apple-watch-series-3/
iPhone X	https://www.apple.com/iphone-x/specs/
Ipad	https://www.apple.com/ipad/compare/
Galaxy S8+	http://www.samsung.com/br/smartphones/galaxy-s8-g955/SM-G955FZKRZTO/
Galaxy Tab S3	http://www.samsung.com/br/tablets/galaxy-tab-s3/SM-T825NZKPZTO/
Gear Fit 2 Pro	http://www.samsung.com/br/wearables/gear-fit2-pro/SM-R365NZKAZTO/
Nokia Thermo	https://health.nokia.com/br/en/thermo
Nokia Body+	https://health.nokia.com/br/en/body-plus
Nokia BPM+	https://health.nokia.com/br/en/blood-pressure-monitor
Echo Plus	https://www.amazon.com/dp/B075RWFCHB/ref_=fs_ods_fs_aucc_sr
iRobot 900	http://www.irobot.com.br/Robos-domesticos/Vacuum-cleaning
Netatomo CAM	https://www.netatmo.com/product/security/welcome/specifications
Baby Monitor	https://www.fredicctv.com/product/dog-wifi-camera/

[33] Veja em: https://www.academiadomarketing.com.br/o-que-e-remarketing/

Tabela: Sensores, habilidades, conectividade e atuadores nos principais dispositivos conectados

	Mobile					Wearables		IoT Saúde			Smarthome			
Sensores, habilidades, conectividade e atuadores	iPhone X	iPhone 6S	Galaxy S8+	Ipad	Galaxy Tab S3	Apple Watch 3	Gear Fit 2 Pro	Nokia Thermo	Nokia Body +	Nokia BPM+	Echo Plus	iRobot 900	Baby Monitor	NET atomo Cam
GPS	☑	☑	☑	☑	☑	☑	☑							
GPS indoor	☑	☑												
Altimetro barométrico	☑	☑	☑	☑	☑	☑	☑							
Acelerômetro	☑	☑	☑	☑	☑	☑	☑							
Sensor geo magnético			☑		☑									
Giroscópio	☑	☑	☑	☑	☑	☑	☑							
Sensor de proximidade	☑	☑	☑											
Sensor de luz ambiente	☑	☑	☑	☑	☑	☑					☑			
Sensor de pressão de toque														
assistente inteligente	☑	☑	☑	☑	☑						☑			
Microfone	☑	☑	☑	☑	☑						☑		☑	☑
Auto falante	☑	☑	☑	☑	☑						☑		☑	☑
Audio e mic via bluetooth	☑	☑	☑	☑	☑	☑	☑				☑			
Câmera frontal	☑	☑	☑	☑	☑								☑	☑
Câmera traseira	☑	☑	☑	☑	☑									
Biometria facial	☑													☑
Biometria digital		☑	☑	☑	☑									
Biometria pela íris			☑											
Reconhecimento por voz											☑			
Controle pela voz											☑			
Sensor de ritmo cardiaco						☑	☑			☑				
Sensor de pressão arterial										☑				
Sensor de umidade relativa							☑							
Identificação e gestão de atividade física						☑	☑							
Conectividade com equipamentos de ginástica						☑								
Monitor de sono						☑	☑							
Sensor de temperatura								☑						
Sensor de peso									☑					
Sensor de massa muscular									☑					
Sensor de massa óssea									☑					
Sensor de % de água									☑					
Sensor de % de gordura									☑					
Visão noturna													☑	☑
Controle de PAN/TILT remoto													☑	
Integração com hand free											☑			
Mapeia espaços												☑		
Identifica objetos e pisos												☑		
Detector de movimento													☑	☑
HUB SmartHome ZigBee											☑			☑
3G/4G	☑	☑	☑	☑	☑	☑								
Wi-fi	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑
Bluetooth	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑	☑			☑

Anexo 03 - Permissões dos aplicativos Facebook e WhatsApp

Dados obtidos no projeto Browsing Histories - Metadata Explorations da Share-Lab, no link https://labs.rs/en/raw-data-documents-tools/ . Dados em inglês. Os dados se referem ao acesso de recursos que o Facebook app (Facebook como habilidade hospedeira e o WhatsApp app (WhatsApp habilidade hospedeira possuem e/ou solicitam acesso no dispositivo.

Facebook app permissions

Permission	Type of Permission
retrieve running apps	Device & app history
find accounts on the device	Identity
add or remove accounts	Identity
read your own contact card	Identity
read your contacts	Contacts/Calendar
modify your contacts	Contacts/Calendar
read calendar events plus confidential information	Contacts/Calendar
add or modify calendar events and send email to guests without owners' knowledge	Contacts/Calendar
precise location (GPS and network-based)	Location
approximate location (network-based)	Location
read your text messages (SMS or MMS)	SMS
write call log	Phone
directly call phone numbers	Phone
read call log	Phone
test access to protected storage	Photos/Media/Files
modify or delete the contents of your USB storage	Photos/Media/Files
take pictures and videos	Camera/Microphone
record audio	Camera/Microphone
view Wi-Fi connections	Wi-Fi connection information
read phone status and identity	Device ID & call information
receive data from Internet	Other
download files without notification	Other
adjust your wallpaper size	Other
create accounts and set passwords	Other
run at startup	Other
prevent device from sleeping	Other
view network connections	Other
install shortcuts	Other
change your audio settings	Other
read Google service configuration	Other
toggle sync on and off	Other
draw over other apps	Other
expand/collapse status bar	Other
full network access	Other
change network connectivity	Other
set wallpaper	Other
send sticky broadcast	Other

Permission	Type of Permission
read battery statistics	Other
reorder running apps	Other
connect and disconnect from Wi-Fi	Other
read sync settings	Other
control vibration	Other

WhatsApp permissions

Permission	Type of Permission
In-app purchases	In-app purchases
retrieve running apps	Device & app history
find accounts on the device	Identity
add or remove accounts	Identity
read your own contact card	Identity
read your contacts	Contacts/Calendar
modify your contacts	Contacts/Calendar
approximate location (network-based)	Location
precise location (GPS and network-based)	Location
receive text messages (SMS)	SMS
send SMS messages	SMS
test access to protected storage	Photos/Media/Files
modify or delete the contents of your USB storage	Photos/Media/Files
take pictures and videos	Camera/Microphone
record audio	Camera/Microphone
view Wi-Fi connections	Wi-Fi connection information
read phone status and identity	Device ID & call information
receive data from Internet	Other
read sync statistics	Other
create accounts and set passwords	Other
run at startup	Other
prevent device from sleeping	Other
view network connections	Other
install shortcuts	Other
use accounts on the device	Other
uninstall shortcuts	Other
change your audio settings	Other
read Google service configuration	Other
toggle sync on and off	Other
modify system settings	Other
full network access	Other

Permission	Type of Permission
connect and disconnect from Wi-Fi	Other
read sync settings	Other
control vibration	Other