UNIVERSIDADE DO VALE DO RIO DOS SINOS - UNISINOS
UNIDADE ACADÊMICA DE GRADUAÇÃO
CURSO DE COMUNICAÇÃO DIGITAL

FABRICIO BARILI

COMUNICAÇÃO MÓVEL:
A Evolução da Infraestrutura e dos Dispositivos em Confronto com a Privacidade

São Leopoldo
2019

FABRICIO BARILI

COMUNICAÇÃO MÓVEL:
A Evolução da Infraestrutura e dos Dispositivos em Confronto com a Privacidade

Projeto de pesquisa apresentado como requisito parcial para obtenção do título de Graduado em Comunicação Social, pelo Curso de Comunicação Digital da Universidade do Vale do Rio dos Sinos – UNISINOS.

Orientadora: Prof.ª Dra. Maria Clara Aquino Bittencourt

São Leopoldo

2019

Dedico este trabalho aos meus pais Luiz Antônio Barili e Adi Maria Barili que, privando-se de inúmeros prazeres da vida, proveram durante toda a minha trajetória acadêmica condições financeiras e emocionais, mesmo que isso custasse a eles suor e dor. Agradeço também à minha irmã, Fabiane Barili, por ter indicado este curso e me auxiliar em uma fase importante da minha vida oferecendo moradia e companheirismo. A Deus, que nas suas infinitas definições, fez eu nascer em um local privilegiado, podendo usufruir de sortes que, ao ter contato com outras realidades, comecei a dar valor. Agradeço, por fim, a todas as pessoas – colegas de trabalho e de classe – que marcaram presença nesses quatro anos e tornaram o caminho mais leve, prazeroso e memorável.

AGRADECIMENTOS

A elaboração deste trabalho, com toda a certeza, não teria este resultado sem a contribuição importante de profissionais extremamente capacitados, empáticos e com uma vontade imensa de compartilhar o conhecimento.

Inicialmente, agradeço à minha orientadora Professora Doutora Maria Clara Aquino Bittencourt, por sua disponibilidade e por aceitar acompanhar este trabalho de perto, oferecendo tranquilidade e excelentes apontamentos durante todo este ano. Ao professor Doutor Gustavo Fischer, pelo tempo disposto para conversar sobre a forma de executar a metodologia escolhida, a fim de esclarecê-la. Aos demais professores e colegas da Unisinos pelas inúmeras trocas, recomendações de matérias e livros que identificavam serem importantes para a elaboração deste projeto.

"[...] Corrida pra vender os carros
Pneu, cerveja e gasolina
Cabeça pra usar boné
E professar a fé de quem patrocina

Eles querem te vender
Eles querem te comprar
Querem te matar de rir
Querem te fazer chorar

Quem são eles?
Quem eles pensam que são?
Quem são eles?
Quem eles pensam que são?

Terceira do Plural – Engenheiros do Hawaii
Compositor: Humberto Gessinger

Sempre que ouvia a letra desta música, eu imaginava que "eles" eram os donos das indústrias do cigarro e petróleo, utilizando toda a máquina da mídia para vender seus produtos: cigarro e combustível. Hoje, após realizar este trabalho, atualizo esta visão para o senhor dos dados que, de fato, nos compram ao criarem as suas plataformas digitais e nos vendem aos anunciantes para nos fazer rir e chorar. Quem são eles? E quem eles pensam que são para fazer isso conosco?

RESUMO

Este trabalho propõe uma construção arqueológica da comunicação móvel, a partir das redes de telefonia sem fio, para discutir como a privacidade é afetada a partir da transformação no modo de coleta de dados dos indivíduos que utilizam diferentes dispositivos de comunicação. São recuperados os modos de funcionamento de tecnologias, como o telefone sem fio, o celular e os *smartphones*, ao mesmo tempo em que se discute conceitos de privacidade e privacidade digital, nos ambientes *on* e *offline*, com o objetivo de entender também conceitos de monitoramento e vigilância, que atravessam os termos apresentados previamente e interferem na privacidade das pessoas que hoje se comunicam pelas redes digitais.

Palavras-chave: Comunicação móvel. Privacidade digital. Monitoramento. Vigilância.

LISTA DE FIGURAS

SUMÁRIO

1 INTRODUÇÃO

A história da telefonia celular inicia no ano de 1947, com a empresa Bell, também conhecida como AT&T, desenvolvendo o primeiro protótipo de um telefone acoplado em um veículo, permitindo ao motorista e aos ocupantes a realização de ligações telefônicas durante deslocamentos. A tecnologia tinha como base o uso de estação de rádio base (ERB), cuja função era realizar a conexão entre os aparelhos e a companhia telefônica (ESTAÇÃO, 2017).

A Motorola, expoente na comunicação entre dispositivos por ondas de rádio – inventora do Walkie-Talkie[1] – para não ficar fora do mercado, destinou suas energias para desenvolver o primeiro telefone móvel. Diferentemente da sua concorrente, o foco era na pessoa, possibilitando que ela pudesse realizar ligações ao se deslocar pelas ruas. Apesar de o início dos estudos e propostas de uma comunicação móvel ter sido na década de 50, foi somente em 1973 que a primeira ligação foi realizada por um telefone sem fio com sucesso. A Motorola, liderada por Martin Cooper, conseguiu tal feito com o DynaTAC 8000. Mesmo com o êxito da operação, o modelo somente foi comercializado em 1983.

No Brasil, a primeira companhia a oferecer o serviço foi a Telecomunicações do Rio de Janeiro (TELERJ), no Rio de Janeiro, em 1990, ganhando maior expressão após a privatização da telefonia, no ano de 1998 (HISTÓRIA, 2019). A adoção no país foi tão grande que, em 2016, um estudo do Instituto Brasileiro de Geografia e Estatística (IBGE) revelou que mais de 92% dos lares já contavam com pelo menos uma pessoa dona de uma linha de telefonia móvel (TECNOLOGIA E GAMES, 2019).

Em 2007, com o lançamento do primeiro Iphone, da Apple, deu-se início a uma larga produção e criação de outros *smartphones*[2]. Tal popularização atingiu boa parte da população brasileira, resultando, em 2018, o total de 94,6% dos brasileiros acima dos 10 anos conectados à internet por meio destes aparelhos (AGÊNCIA DE NOTÍCIAS IBGE, 2018).

Com a evolução tecnológica, os celulares ganharam maior poder de processamento, comparando-se a computadores pessoais. Tal evolução criou uma

[1] WALKIE-TALKIE. *In:* Wikipedia: A enciclopédia livre. Wikimedia**,** 2019. Disponível em: https://pt.wikipedia.org/wiki/Walkie-talkie 2019). Acesso em 10 jul. 2019.
[2] *Smartphones* são aparelhos de telefonia móvel com poder computacional, e assim, capazes de instalar *softwares* e realizar operações de maior complexidade.

linha de dispositivos móveis: os *smartphones*, com inserção de *hardwares* diversificados – como câmera fotográfica de maior resolução, bússola, acelerômetro e giroscópio – e o desenvolvimento de aplicações específicas para eles, os chamados aplicativos móveis. Já, os Apps3, como mensageiros instantâneos e redes sociais, proporcionaram uma interação específica do usuário com o celular, além de diversificar o tipo de dados produzidos nestes e por estes aparelhos.

O vínculo social do dispositivo móvel com seu portador pode ser notado na afirmação de Chuck (2013), quando ele cita que a pessoalidade do *smartphone* é algo extremo, pois ele não é compartilhado: está no bolso ou bolsa de cada indivíduo e é utilizado para ações pessoais, como envio de mensagens de texto, ligações para amigos ou familiares, e também para conectar-se às redes sociais, o que nos dá a real dimensão da pessoalidade dos dados gerados por meio destes dispositivos.

Como toda operação mediada por *software*, ela produz um conjunto de informações sempre que executada, como explica Sérgio Amadeu da Silveira:

> Uma fechadura digital aberta por um cartão magnético ou por biometria não somente destrava a porta como também registra o horário exato em que isso aconteceu. Também pode registrar qual cartão magnético ou digital abriu a porta, no caso de existir mais que um. A parte física do dispositivo é comandada por sua parte lógica gerando um conjunto de informações que ficam armazenadas em um *software* (SILVEIRA, 2017 n. p.).

A natureza da coleta se dá através de duas principais formas: pelos aplicativos, a coleta é específica, transacional, ou seja, conforme o uso. Como explica Zuboff (2018), existem formas de coleta de dados provenientes de fluxos, que surgem de transações mediadas por computador. O próprio funcionamento do celular pode ser gerador de dados, como explica: “seu celular está constantemente calculando a localização de qual torre está mais próxima. Não que a companhia telefônica se importa onde você esteja, mas ela precisa saber onde o seu telefone está para encaminhar as chamadas para você” (SCHNEIER, 2015, p. 16) e completa: “Se você realmente usa esse telefone, produz mais dados: números discados e chamadas recebidas, mensagens de texto enviadas e recebidas, duração da chamada, e assim por diante” (SCHNEIER, 2015, p. 16). Já, pelos *smartphones,* a coleta pode ser simplesmente através do seu uso e portabilidade, como explica Schneier: “[...] um

[3] Apps é sinônimo de aplicativos. São *softwares* desenvolvidos especialmente para *Smartphones* e, em geral, desempenham funções específicas, como: mensageiros, redes sociais, *games* e ferramentas para gerenciar arquivos.

smartphone também é um computador e todos os seus aplicativos produzem dados quando você os usa – e, às vezes, até mesmo quando não os está usando" (SCHNEIER, 2015, p. 16)[4].

A localização, o tempo de permanência em determinado local, os sons e as imagens podem ser percebidos e captados sem que o usuário tenha ciência do exato momento que está ocorrendo. Alguns deles são coletados e gerados de forma passiva, seja para a manutenção do sistema, como é o caso do Waze[5], ou também via alguns artifícios criados especialmente para a coleta indevida de dados e informações destes usuários, comprometendo de forma crítica a privacidade digital.

Nos últimos anos, fomos surpreendidos por grandes escândalos envolvendo corporações e governos, em que estes abusaram do seu poder, de vulnerabilidades de sistemas e tecnologias para obter informações privilegiadas e confidenciais de uma população em massa. Os casos mais recentes e famosos foram as denúncias de Edward Snowden, ex-funcionário da NSA, envolvendo a agência, e o escândalo que envolveu o atual presidente norte-americano Donald Trump, o Facebook e a *Cabridge Analytica*.

O primeiro caso, relatado pelo *The Guardian*, revelou ao mundo o poder de vigilância que a agência norte-americana de inteligência FBI tinha dos cidadãos não somente do seu país, mas do mundo. Por meio do programa PRISM[6], plano de vigilância global da NSA iniciado em 2007, o governo tinha acesso a inúmeros dados, como mensagens trocadas por e-mail, postagens em redes sociais, conteúdos de mensageiros, histórico de pesquisas, entre outros. Não precisamos entrar em termos técnicos, mas estimativas afirmam que, por dia, um dos braços do projeto PRISM coletava mais de 200 milhões de SMS's[7].

O segundo caso veio à tona em 17 de março de 2018. Novamente, o jornal *The Guardian* publicava uma notícia sobre uma empresa de Londres que havia coletado e

---

[4] If you actually use that phone, you produce more data: numbers dialed and calls receibed, text messages sent and received, call duration, and so on. If it's a smartphone, it's also a computer, and all your apps produce data when you use them - and sometimes even when you're not using them. Tradução nossa.

[5] Aplicativo de mobilidade. Utiliza o deslocamento do usuário para alimentar a base de informação do trânsito local.

[6] PRISM (Programa de Vigilância). *In:* Wikipedia: A Enciclopédia livre. Wikimedia. Disponível em: https://pt.wikipedia.org/wiki/PRISM_(programa_de_vigil%C3%A2ncia). Acesso em 02 mai. 2019.

[7] NSA collects millions of text messages daily in 'untargeted' global sweep. *In:* The Guardian. Disponível em https://www.theguardian.com/world/2014/jan/16/nsa-collects-millions-text-messages-daily-untargeted-global-sweep. Acesso em 02 mai. 2019.

utilizado os dados pessoalmente identificáveis[8] de mais de 50 milhões[9] de usuários de uma rede social. O escândalo envolvia a empresa britânica Cambridge Analytica, o Facebook e as eleições americanas. Na ocasião, a empresa de consultoria foi acusada de obter de forma ilegal, e por uma falha no Facebook, acesso à contas e informações dos usuários da rede social, através de um *game* disponibilizado na plataforma. Segundo o Facebook, mais de 87 milhões de contas poderiam ter sido comprometidas devido à prática adotada pela empresa britânica[10]. O número salta de 50 para 87 milhões na atualização da reportagem do The Guardian, o que indica não ver total dimensão do impacto deste vazamento.

Um outro exemplo do comprometimento da privacidade, além do caso da Cambridge Analytica, foi de um grupo de soldados norte-americanos que utilizava um aplicativo para monitoramento de suas corridas e acabou por divulgar uma possível base militar secreta[11]. Nessa situação, o percurso registrado periodicamente possibilitou que os seguidores deduzissem a existência de alguma instalação naquele local.

Esses casos demonstram o quanto as empresas que detém conhecimento sobre as tecnologias, inclusive as que produzem, conseguem realizar um ato de vigilância em massa nunca antes visto, como afirma Schneier (2015): “Não é ‘siga aquele carro’, mas sim ‘siga todos os carros[12]’’. Sem distinção entre os motivos que levaram tais coletas serem necessárias, a questão é que as revelações, em especial a última, geraram enorme repercussão e reativaram uma preocupação no mundo inteiro acerca da privacidade digital. O termo passou a ser amplamente pesquisado[13] logo após a divulgação da notícia – mas parou de ser procurado pouco tempo depois.

A privacidade digital é um direito e define-se como a expectativa de que o indivíduo possa ter total controle de quando, como e em que medida as informações

---

[8] Referem-se a informações que podem ser usadas para identificar, contatar ou localizar uma única pessoa. Na ocasião, foram divulgados os endereços de e-mail das pessoas envolvidas.
[9] REVEALED: 50 million Facebook profiles harvested for Cambridge Analytica in major data breach. *In:* The Guardian. Disponível em: https://www.theguardian.com/news/2018/mar/17/cambridge-analytica-facebook-influence-us-election. Acesso em: 02 mar. 2019.
[10] FACEBOOK says Cambridge Analytica may have gained 37m more users' data. *In:* The Guardian. Disponível em: https://www.theguardian.com/technology/2018/apr/04/facebook-cambridge-analytica-user-data-latest-more-than-thought. Acesso em 02 mar. 2019.
[11] APLICATIVO de corrida revela supostas bases militares nos EUA. *In:* G1. Disponível em: https://g1.globo.com/mundo/noticia/aplicativo-de-corrida-revela-supostas-bases-militares-dos-eua.ghtml. Acesso em: 05 mar. 2019.
[12] It’s not “follow that car”; It’s “follow every car.” (SCHNEIER, 2015, p. 32)
[13] Resultado do volume de pesquisa sobre o termo “Privacidade Digital”. Google Trends. Disponível em: http://bit.ly/2VwcaSi. Acesso em 02 fev. 2019.

pessoais sejam disponibilizadas a terceiros, conforme cita Lins (2000). Esse direito está embasado em três diferentes pontos: a ciência e permissão do usuário que está provendo os dados; a utilização destes dados, que deve ter o propósito claro e informado; e a possibilidade de o usuário solicitar a revisão ou exclusão dos seus dados da base a qualquer momento.

No entanto, o tema é debatido no Brasil há anos. Em março de 2000, um estudo da Câmara dos Deputados, realizado por Lins (2000), já avisava sobre a fragilidade da privacidade digital, tendo em vista três fatores: a estruturação dos dados; o amplo acesso aos dispositivos eletrônicos que produzem tais dados; e a padronização dos dispositivos.

Mas não é somente a atual tecnologia que permite esta vasta coleta de dados. O mais básico dos celulares possibilitava que as empresas soubessem onde o seu cliente estava. Segundo Schneier (2015) estamos, diariamente, ao utilizar o nosso celular, realizando uma “barganha”. Essa barganha nos beneficia com a possibilidade de fazer e receber chamadas telefônicas quase em qualquer lugar, em troca de a companhia saber onde estamos. Olhando por este ponto de vista, pode parecer estranho, mas é assim que funciona a telefonia móvel: a operadora necessita saber qual antena está mais próxima para fornecer sinal.

Para Schneier (2015) isso permite uma forma de vigilância tão rica e variada que todo esse material, produzido pelo celular, pode “pintar” uma imagem temporal nossa muito melhor do que nós mesmos. O autor ainda afirma que estudos realizados no ano de 2012 foram capazes de presumir onde um indivíduo poderia estar nas 24 horas seguintes, com uma precisão de até 20 metros.

Tendo a minha atenção sido chamada para essa situação, a minha curiosidade, vontade de estudar e aprofundar conhecimentos me levaram a procurar respostas. Assim, uma pesquisa por plataformas digitais fora iniciada durante a fase de projeto de TCC. Na busca pela palavra-chave ‘privacidade’, no periódico do Capes, encontrei diversos artigos hospedados, das mais diversas naturezas. Com a segmentação das publicações entre 2010 e 2018 — data da mais recente — obtive mais de 1500 resultados. Há textos que abordam a privacidade no campo da saúde, discorrendo sobre a relação médico-paciente, DST’s; mas há também os que dialogam com legislação, *marketing*, o uso da internet e redes sociais.

Ao tornar mais profunda a pesquisa e utilizar os termos “privacidade + digital” o número foi reduzido drasticamente, totalizando 384 resultados. A abordagem dos

temas, apesar de mais específica, continua diversa. Alguns tratam sobre a privacidade e o modo de usar plataformas digitais, outros sobre a perspectiva de uso de aplicativos e não somente da navegação, ou ainda, sobre legislação e proteção de dados.

Sobre privacidade digital, alguns autores a abordam no aspecto jurídico, procurando demonstrar como a legislação está amparando os cidadãos brasileiros — mencionando, inclusive, o Marco Civil da Internet. Outros autores falam sobre a privacidade em plataformas mais específicas, como as redes sociais, relacionando a forma com que jovens se expõem no Facebook. Neste ponto em específico, a privacidade é tida como o ato de alguém invadir a conta ou artefato tecnológico de outro, não referindo-se à coleta de dados pelos desenvolvedores das plataformas mediante o seu uso.

Para aproximar ainda mais do objeto empírico — a privacidade digital em decorrência dos dispositivos móveis — adicionei em minhas buscas a palavra "dispositivo móvel", tornando a pesquisa extremamente específica. O número de artigos resultantes foi menor, apenas 34. Os assuntos dos artigos que apareceram na pesquisa abordam a privacidade digital em dispositivos móveis nos seguintes aspectos: aplicativos para redes sociais, comportamento do consumidor, consumo de informação, regulamentação da comunicação móvel por parte das operadoras, e também estudos de causa-efeito da tecnocultura instaurada pela mobilidade, como é o caso de um artigo da Lisiane Barea Sandi e Amarolinda Zanela Saccol – amnbas da Unisinos – que aborda a relação entre os TIMS[14] e os seus utilizadores.

De todos os resultados, alguns chamaram mais atenção por se aproximarem de pontos específicos do meu objeto de pesquisa, dos quais separei:

a) Monitoramento, classificação e controle nos dispositivos de vigilância digital (BRUNO, 2008);

b) *Smart Surveillance* em aplicações recentes no Brasil: um estudo de caso nas cidades de Recife e Curitiba (BATISTA; FARINIUK; MELLO, 2016);

c) A estética política das mídias locativas; (SANTAELLA, 2008);

d) Sou o que eu consumo? Smartphones e o Self Estendido a Luz de Paradoxos Tecnológicos (MARTINS; OLIVEIRA; CORSO, 2018);

e) Cidadão Sensor e Cidade Inteligente: Análise dos Aplicativos Móveis da Bahia (LEMOS; ARAUJO, 2018).

[14] Tecnologias da Informação Móveis e Sem Fio.

O primeiro texto, *Monitoramento, classificação e controle nos dispositivos de vigilância digital,* refere-se a um contexto de protestos contra a vigilância de dados e violação da privacidade por diversos serviços de Internet, trazendo, num panorama geral e muito esclarecedor, as formas de monitoramento, classificação e criação de perfis digitais.

Bruno (2008) retrata muito bem os tipos de dados coletados, dividindo-os grosseiramente, segundo ela, em dois grupos: os dados relativamente estáveis e os dados circunstanciais. Interessante essa distinção pois ela influencia diretamente no estudo deste trabalho, quando unimos essas duas classificações em um dispositivo móvel. O primeiro, relativamente estável, são os dados geodemográficos, biométricos, relativos a gênero, entre outros. Esses aspectos trazem informações importantes de quem está portando um dispositivo móvel, por exemplo, principalmente se pensarmos que cada vez mais os *smartphones* estão dotados com leitores de impressão digital como forma de autenticar o portador do aparelho. O segundo grupo, dos dados circunstanciais, revela muito do comportamento de quem está portando o dispositivo móvel, por serem dados do tipo comunicacional, transacional, social, psicológico, entre outros.

O texto segue discorrendo sobre as etapas que constituem a cadeia produtiva da vigilância digital: coleta, armazenamento, classificação e conhecimento, individualização e identidade e, por fim, a predição, o controle e a performance.

Em resumo, o texto explica muito bem conceitos como vigilância digital, *Data mining*[15] e *profiling*[16]*.* Para o presente estudo, eles são de extrema importância, pois mostram as grandes possibilidades de controle e monitoramento a partir das informações coletadas e processadas. Será de muita utilidade para este trabalho os conceitos de vigilância, reforçando que cada meio possui a sua especificidade de coleta e tratamento de dados, bem como, as suas consequências, tanto na justificativa quanto na fundamentação teórica.

No entanto, a autora aborda todas essas questões por meio da interação com serviços digitais: sites de busca, de relacionamento, redes sociais e serviços de

[15] Mineração de dados: técnica estatística aplicada que consiste num mecanismo automatizado de processamento de grandes volumes de dados, cuja função central é a extração de padrões que gerem conhecimento (BRUNO, 2008, p. 12).
[16] Produção de perfis computacionais: processo que segue uma lógica indutiva que visa “determinar indicadores de características e/ou padrões de comportamento que são relacionados à ocorrência de certos comportamentos” (BENNETT, 1996 *apud* BRUNO, 2008, p. 12).

streaming. O que pretendo, aqui, é mostrar como se dá todo este processo de coleta na telefonia móvel, analisando a infraestrutura de rede (TDMA, GSM, 3G, 4G, entre outras) e a evolução dos dispositivos móveis (como: adoção de GPS, conexões *Bluetooth*, câmera, acelerômetro).

Outro texto que separei para analisar foi *A estética política das mídias locativas***,** escrito por Lucia Santaella. O artigo tem como finalidade apresentar a estética das mídias locativas que surgiram através das novas formas de comunicação, interação e conexão. Sob esta perspectiva de transformação de espaços, a autora fala dos lugares e não-lugares com as suas definições e características. Estes dois territórios, mesmo que em proporções, tempo e motivações diferentes, mantém o humano como presente, circulando e ativo, diferentemente de outro espaço citado pela autora: o cibernético. Esse último retira o corpo do homem e deixa as relações "sobre a geração de modelos de realidade sem origem e sem destino, sobre a atrofia do corpo físico, plugado e inerte enquanto a mente navega pelos espaços da virtualidade." (SANTAELLA, 2008, p. 129–130). O texto serve como referência para reforçar como se dão as relações do ciberespaço e da sociedade e "que não importa qual forma o corpo virtual possa adquirir, sempre haverá um corpo biológico junto, ambos inseparavelmente atados" (SANTAELLA, 2008, p. 130).

Outro ponto trazido pela autora que é de extrema relevância para o campo da comunicação móvel e das mídias locativas é a sua categorização. Ela aborda rapidamente o trabalho realizado por Lenz, em 2007, ao retratar dezenove categorias (cada uma com subcategorias e diversos projetos) mas, no seu texto, revela a categorização feita por André Lemos, por sua vez, mais sucinta: realidade aumentada móvel, mapeamento e monitoramento, *geotags*, anotação urbana e games *wireless,* que utilizam uma ou mais dessas funções (SANTAELLA, 2008).

Ao trazer pontos que tangem as mídias locativas, o texto auxilia muito no desenvolvimento do presente projeto, pois reforça a dependência do dispositivo móvel e do corpo virtual a um corpo biológico, como a própria autora afirma. Sendo assim, somando com o primeiro texto da Fernanda Bruno, assimilamos que as informações provenientes de um *profiling* que foram coletados pelo dispositivo móvel podem, de fato, representar muito bem o seu portador.

Separei também uma pesquisa realizada após a Copa do Mundo Fifa 2014, nas cidades de Recife e Curitiba, locais nos quais ficaram resquícios de iniciativas tecnológicas utilizadas para segurança e gestão tecnológica dessas cidades. O texto

inicia afirmando que os conceitos de segurança, defesa, vigilância e a prática de coletar informações vem evoluindo ao longo do tempo, impulsionado pela mudança tecnológica. Também recorda sobre o termo *Big Brother,* cunhado em 1940 por George Orwell, que se referia a um ambiente no qual os indivíduos eram constantemente vigiados. Para dar mais tangibilidade à realidade, os autores lembram que após os atentados de 11 de setembro os países ao redor do mundo passassem a adotar a "ideologia da segurança", conforme afirma Batista (2016).

Para a importância deste estudo, há alguns conceitos, como *smart cities*[17]*, smart spaces*, em que há a adoção de tecnologias de vigilância, cada vez menores e mais populares. Em certo ponto, os autores falam de um "inteligenciamento urbano", definido por tornar cada vez mais tecnológicos os ambientes, ao deixá-los repletos de dispositivos que se tornam invisíveis no espaço urbano. Importante seguir o raciocínio de Batista (2016), quando ela afirma que esses dados se tornam dados em rede com enorme facilidade, visto a pesquisa que será apresentada ao longo deste projeto.

Retomando André Lemos, no artigo *A comunicação das coisas: teoria ator-rede e cibercultura,* é importante vermos que "torna difícil a separação de pessoas e máquinas, pois as associações entre ambas se tornam dinâmicas, alternadas e híbridas" (BATISTA; FARINIUK; MELLO, 2016, p. 109). Sendo assim, em resumo, o texto nos auxilia ao demonstrar o poder de vigilância que as cidades, cada vez mais conectadas, têm sobre os seus cidadãos.

Toda essa forma de poder, controle e vigilância servem a vários propósitos. Um deles é o *Marketing* que, cada vez mais, tenta se aproximar do consumidor a fim de oferecer o melhor produto na hora que o usuário der indícios. Nesta vertente, encontrei o artigo: *Sou o que eu consumo? Smartphones e o Self Estendido a Luz de Paradoxos Tecnológicos*. Este artigo, presente na revista Remark – Revista brasileira de *Marketing* – tem como objetivo investigar o envolvimento dos usuários com os seus *smartphones,* e se tal relação pode representar um *self* do seu portador.

Os resultados obtidos no estudo citado acima são essenciais para a presente análise, pois indicam "que certos usuários de *smartphone* possuem forte apego emocional ao seu aparelho, considerando-o uma extensão da sua própria identidade" (MARTINS; OLIVEIRA; CORSO, 2018, p. 329). Também foi observado o desconforto dos entrevistados na ausência do dispositivo móvel comunicacional.

[17] Redes urbanas – complexas e de alta densidade – que podem ser gerenciadas a partir da utilização de tecnologias (KITCHIN, 2014 apud BATISTA; FARINIUK; MELLO, 2016, p. 107).

O texto traz conceitos como o de *self estendido*, da área do comportamento do consumidor, e mostra como se dá essa relação de posse e afeto entre o *smartphone* e o seu portador. Para endossar a aproximação do dispositivo móvel com o seu portador, trago uma afirmação de Martins, Oliveira e Corso (2018): “Além dos aspectos comunicacionais, o aparelho celular tornou-se fonte de entretenimento e cada vez mais as pessoas vem construindo vínculos físicos e emocionais com esse tipo de aparelhos”. Prossigo, aprofundando a discussão entre autores que abordam a atualização do *self estendido* com a mediação das relações pessoais, mas isso vai para outro campo, o qual não abordarei neste primeiro momento. Mesmo assim, não posso deixar de mencionar este aspecto pois ele, de certa forma, implica no comportamento do usuário e induz na forma com que ele age e reage nos relacionamentos digitais: “o self é muito mais ativamente gerenciado, construído em conjunto, interativo, abertamente desinibido, confessional, com múltiplos manifestos, e influenciado por aquilo que nós e os nossos avatares fazem online” (MARTINS; OLIVEIRA; CORSO, 2018, p. 331).

Como o título do artigo já previa, o autor encontra paradoxos sobre os efeitos que os dispositivos causam em seus usuários, tais como: controle e caos, liberdade e escravização, novo e obsoleto. Em um primeiro momento, o estudo pode parecer irrelevante, no entanto, posso aproveitar de alguns desses paradoxos para compreender os efeitos de forma mais ampla na sociedade.

Por fim, separei o texto de André Lemos e Nayra Veras de Araujo, intitulado *Cidadão Sensor e Cidade Inteligente: Análise dos Aplicativos Móveis da Bahia.* O artigo é resultado de um mapeamento de aplicativos para dispositivos móveis, disponíveis aos cidadãos da cidade de Salvador. A intenção dos autores é estudar como o governo da Bahia, em especial na cidade de Salvador, está utilizando os m-government[18] como importantes ferramentas para a comunicação pública, articulando governo e cidadão por meio destes, e defende: “os aplicativos podem ser excelentes mediadores para incentivar processos comunicacionais multilaterais que primem não só pela comunicação governo-cidadão, mas também na relação cidadão-governo e cidadão-cidadão” (LEMOS; ARAUJO, 2018, p. 2).

[18] Refere-se a um conjunto de estratégias conduzidas por setores públicos, usando as tecnologias e dispositivos de comunicação móveis (computação nas nuvens, internet sem fio, smartphones e tablets), ampliando os canais de serviços e as formas de acesso a informações (WENDY LI, 2016 apud LEMOS; ARAUJO, 2018, p. 3).

Algumas das definições importantes encontradas no texto é a do “cidadão sensor”, sendo seu papel fornecer dados para o Estado. Os autores explicam o porquê da criação de aplicativos pelos setores públicos para os cidadãos:

> Criar aplicativos é, na maioria dos casos, produzir mecanismos de extração de dados do cidadão, seja em suas ações cotidianas mais banais, como pegar um ônibus, seja em uma participação mais ativa na vida pública, como participar com opiniões na definição do orçamento municipal, ou enviando sugestões e queixas sobre os problemas de infraestrutura urbana (LEMOS; ARAUJO, 2018, p. 2).

Esta produção textual auxilia em meu estudo, pois aborda a utilização dos dispositivos móveis pelo poder público para um relacionamento direto com o cidadão. Também porque há um questionamento interessante acerca do cidadão-sensor e o seu relacionamento com o Estado, que não pode ser deixada de lado, e reforça ainda mais as questões de poder, vigilância e controle. Lemos e Araújo (2018), ao trazerem a fala de Scruggs, definem a natureza da relação sujeito-sensor e o Estado em duas formas: a primeira é que, nem sempre, o cidadão fornece seus dados espontaneamente. Assim, ficam lacunas abertas de dados e o universo total de cidadãos não é, de fato, tão exato. O segundo ponto é que essa governança, que é possível a partir dos dados fornecidos, carrega um potencial autoritário sobre a própria população que os forneceu.

Assim, os artigos, estudos e pesquisas relacionados para este trabalho de conclusão nos fazem perceber que: a preocupação com a coleta de dados, vigilância e poder não é algo de hoje e só tem ganhado maior potência e velocidade através das tecnologias digitais; as mudanças na sociedade advindas da penetração dos dispositivos móveis são transformadoras e permitem uma série de categorizações, de acordo com a sua utilização; as tecnologias de vigilância e monitoramento estão sendo cada vez mais utilizadas pelo poder público, a fim de gerir sua infraestrutura e combater a criminalidade; há um forte sentimento de apego e afeição entre o *smartphone* e o seu portador, definindo pelo seu uso, um selfie estendido e, por fim, o papel do m-*governmen*t em criar aplicativos móveis para estimular o cidadão-sensor a produzir dados e informações para si.

Diante deste cenário, questiona-se: como a evolução da conexão móvel e dos dispositivos, celulares e *smartphones* permitiram o aperfeiçoamento das coletas e como isso afeta a privacidade dos indivíduos? Em função do contexto apresentado,

tanto mercadológico quanto acadêmico, sobre o uso de *smartphone*, monitoramento e vigilância, parece fundamental estudar como a privacidade digital é comprometida em função dos tipos de coletas de dados realizados através do seu uso.

Para compreender a forma com que as evoluções tecnológicas da telefonia móvel – seja pela sua infraestrutura ou pelo desenvolvimento dos dispositivos – implicam diretamente na privacidade do seu portador, e também atendendo aos objetivos gerais, defino como objetivos específicos:

a) Contextualizar aspectos relativos à estrutura da telefonia móvel e a outras formas de conexão disponíveis para celulares e *smartphones*;

b) Identificar e descrever o funcionamento técnico dos diferentes *hardwares* presentes nos *smartphones*, permitindo o esclarecimento de quais dados podem ser coletados;

c) Relacionar essas tecnologias com o comportamento dos atores móveis para discutir questões que comprometam a privacidade.

O que me move a realizar este trabalho é, primeiramente, um fascínio pela tecnologia digital. As possibilidades que ela trouxe para a nossa geração, a troca de conhecimento e, principalmente, a geração de dados e produção. Mas isso não é de hoje. A comunicação e a tecnologia marcaram fortemente a trajetória da minha vida. Dada a realidade brasileira, eu fui agraciado muito cedo, em 2000, com um computador pessoal. Mesmo sendo compartilhado com meu pai e minha irmã, eu já tinha acesso à tecnologia e, poucos anos mais tarde, à conexão pela Internet.

Aos 12 anos, recebi uma proposta de bolsa de estudos, a qual me inseriu num primeiro curso de informática. Ele foi o propulsor para a área de programação, inserindo-me, mais tarde, na área da computação, o que aumentou ainda mais o meu interesse por tecnologia. Mas nem toda a tecnologia bastava para mim. Se fosse somente ela, eu estaria graduado em Ciências da Computação pela Unisinos. O que me faltava era o lado humano, a comunicação em si, e isso fez-me pairar por outras áreas, até chegar naquela que estou hoje.

Percebi que eu tinha uma facilidade em encontrar pessoas pela Internet quando necessitei recuperar um vestido de uma então namorada, que o havia emprestado para uma ex-colega de trabalho. Na ocasião, eu estava munido de apenas nome, sobrenome, possível cidade e um perfil em uma rede de relacionamentos. Por meio dos motores de busca, cruzamento de informações disponíveis abertamente na Internet e um pouco de empirismo, acabei encontrando uma MEI (Microempresa

Individual) registrada no nome dela. Posteriormente, localizei o telefone e, assim, recuperei o vestido.

Ora, se essas informações são alcançadas, é porque alguém gerou e disponibilizou na rede. Seja por exposição pessoal de quem abertamente cria um perfil em redes social e disponibiliza ali suas informações, ou por empresas e governos como Facebook, Cabridge Analytica ou NSA, que têm o poder e a inteligência de coletar, armazenar e analisar dados que dependam de enorme processamento intelectual.

Mais recentemente, o escândalo que envolvia a NSA, o Facebook, a Cambridge Analytica e as eleições norte-americanas causaram em mim uma certa inquietação. Quais formas de coletar dados são possíveis pelas tecnologias de uso em massa? Como essas grandes corporações e instituições usufruem da sua influência, monopólio e poder para vigiar os cidadãos do mundo? O que nos resta fazer para evitar ou amenizar tal invasão à nossa privacidade?

No campo acadêmico, percebi que há diversos estudos liderados por grandes nomes, como André Lemos, Fernanda Bruno e Sérgio Amadeu da Silveira, cujos trabalhos tangem as áreas de cibercultura, mobilidade, monitoramento, controle e vigilância. Estes campos, somados à popularização da telefonia e comunicação móvel, da rede onipresente na sociedade, dos diversos movimentos que surgem na intenção de proteger os dados[19] e, principalmente, de expor a forma banal com que os dispositivos móveis são capazes de fornecer dados sobre nós[20] faz-se necessário compreender a forma com que essa prática vem evoluindo e se aperfeiçoando.

Para a realização da proposta de pesquisa, acredito ser necessária a implementação de uma metodologia que possibilite encontrar traços, através do tempo, que demonstrem as diferentes maneiras de coletar os dados por meio dos dispositivos. Assim, proponho um estudo aprofundado sobre o caminho que a infraestrutura de rede e os dispositivos de comunicação móvel percorreu no Brasil, bem como o seu impacto na sociedade. Busco resgatar os elementos tecnológicos, técnicos e culturais que surgiram, sucumbiram, perpetuaram e se reconfiguraram ao

[19] LGPD, no Brasil; GPDR, na Europa; e o projeto Solid desenvolvido por Sr. Tim Berns Lee, o criador da Web.
[20] *THE CHOREOGRAPHY of Everyday Movement*. *In:* Teri Rueb. 2001. Disponível em: http://terirueb.net/the-choreography-of-everyday-movement-2001/. Acesso em 07 abr. 2019.

longo da história das telecomunicações. Para isso, a metodologia escolhida, ou a forma de agir sobre os objetos, foi a arqueologia das mídias.

A arqueologia das mídias mostra-se uma metodologia interessante para este estudo, por sua forma de olhar para caminhos alternativos de uma história “não linear e que contesta a distribuição estabelecida entre vencedores e perdedores em narrativas midiáticas teleológicas, sejam elas de inventores, invenções e técnicas” (GODDARD, 2017, p. 17).

Assim como Parrika (2017, p. 4) propõe para a arqueologia, atuarei para encontrar “uma maneira de compreender os fundamentos culturais de artefatos e tecnologias” e, complementando com a definição do que Zielinski (1999 *apud* PARIKKA, 2017, p. 4) afirma “[..] a tecnologia não é um fluxo de determinantes culturais que condiciona a existência consciente e inconsciente dos sujeitos de maneira unidimensional [...]”. Com isso, pretendo mostrar quais os fatores que as mudanças das tecnologias de comunicação móvel e de dispositivos interferiram na forma como as pessoas se comunicam e se relacionam com os dispositivos.

Um dos resultados interessantes da aplicação deste modo de pesquisa é o rompimento da ideia de que há uma inovação que torna obsoleta uma tecnologia anterior, vencendo-a. O movimento é atuar na investigação a fim “de questionar o que é tido como certo ou aceito como 'verdade' até escavar pioneiros esquecidos, [...] e outros materiais e dimensões negligenciados” (STRAUVEN, 2013, p. 83 *apud* PARIKKA, 2017, p. 5).

Muito mais do que olhar para a tecnologia, a arqueologia atua “como processo de redescoberta não apenas dos objetos tecnológicos da cultura mas, sobretudo, da subjetividade artística nesses tempos marcados pela multimídia” (MACHADO, 2001, p. 202). Para isso, o olhar volta-se à sociedade da época, onde essa tecnologia estava presente, e analisa seus limitantes, seus potencializadores e seus efeitos ou, como Zielinski, citado por Machado (2001, p. 202) diz, “é a possibilidade de reconsiderar as potencialidades do tempo, das quais as tecnologias transformadas em mídias são produtos imediatos”.

O olhar arqueológico também é útil pois ele aborda “de forma crítica os dispositivos e a sua construção de um dado ambiente que nos é invisível” (ARAUJO, 2017, p. 164). O autor prossegue a afirmação reforçando que tais mídias não ficam isoladas, sendo criadas e utilizadas na sociedade e não em um ambiente inerte. O autor, em *Arqueologia das mídias pela literatura*, aborda a metodologia aqui aplicada,

apresentando a intrínseca relação das mídias com a sociedade, cultura e política, e nos dá a entender que a invisibilidade de um meio padronizado é tão grande que este somente é percebido ao “tornar-se obsoleto”. Como cita McLuhan, “um novo meio bombardeia as mídias e a consciência, despindo as velhas formas de experiência até deixá-la em pele e osso, ou em códigos básicos” (MCLUHAN, 1966 p.79 apud ARAUJO, 2017, p. 160).

Importante observar a fala de McLuhan, em 1966, trazida por Araújo (2017), abordando a nova revolução tecnológica que torna evidente as características antes invisíveis, durante a sua utilização massiva. A consistência e controle do conhecimento que temos dá-se quando não a estamos utilizando cotidianamente.

Como base para este estudo, observarei fontes e conteúdo de publicações em diferentes fontes, tais como, livros, publicações e estudos de diferentes áreas, a fim de trazer à luz visões complementares acerca do tema e dos capítulos construídos. Tomando por base autores que sejam relevantes dentro de cada tema, por suas inúmeras publicações e resenhas em sites de compra de livros, tornarei eles os guias deste trabalho.

No primeiro capítulo, abordarei a comunicação e mobilidade. Primeiramente, definirei o que é a comunicação, o ato de comunicar e algumas necessidades que foram aparecendo ao longo da história da comunicação, tornando-a mais complexa. Passarei pelas definições de comunicação sem fio, até chegar à comunicação móvel, de fato. Após adentrar neste tema, passarei a demonstrar quais foram os passos que a telefonia móvel deu desde a sua primeira estrutura analógica, até a atual rede comercial no Brasil, a 4G. Também explicarei no primeiro capítulo as fases dos dispositivos de comunicação, partindo do telefone sem fio doméstico, radiotransmissores, os primeiros telefones celulares e, posteriormente, os atuais *smartphones*. Nesta jornada, abordarei quais foram os principais diferenciais em cada etapa que separa de uma “versão anterior”, e como elas impactaram na sociedade.

O segundo capítulo é majoritariamente jurídico. Por tratar de privacidade, achei importante definir e conceituar o tema, visto que ao longo do estudo eu percebi que ela passou por diferentes modificações. Os autores utilizados trazem desde o primeiro conceito da privacidade, em um mundo sem conexão com a Internet, passando por uma sociedade da informação, até termos a sociedade digital, informatizada e conectada, necessitando de um olhar mais atento às definições previamente instituídas. Neste capítulo, pretendo esclarecer e atentar aos possíveis atos ilícitos

cometidos por empresas de tecnologia e como isso pode, de certa forma, implicar em falhas contra a nossa privacidade.

Já, no terceiro capítulo, abordo os conceitos da área da comunicação. Monitoramento e vigilância foram os termos escolhidos, pois esses tratam de atos contra o indivíduo, um estado de observação constante, imparcial e desigual em que há uma parte com total acesso às nossas vidas, e pouco da nossa parte para lidarmos contra. Ainda no referido capítulo, considero o que está de acordo com a área da área da comunicação na qual estou inserido, e pretendo utilizar ele como consolidador dos capítulos anteriores mostrando, de fato, como as evoluções apresentadas no primeiro capítulo e as terminologias de privacidade, definidas no segundo, causam efeitos sobre o nosso cotidiano.

2 COMUNICAÇÃO E MOBILIDADE

A comunicação pode ser definida como “um mecanismo que se atribui a um processo artificial, ou seja, meio pelo qual a pessoa se utiliza de artifícios para atingir seus objetivos.” (SANTOS, 1992 p. 24). O fato de ser algo artificial, e que, portanto, não natural, é o que difere o humano dos demais animais. A comunicação, segundo DeFleur (1966), foi um fator que “levou ao desenvolvimento crescente de complexa tecnologia, e a mitos, lendas, explicações, lógica, hábitos, e às regras complexas para o comportamento que possibilitou a civilização.”

Essa complexidade se constitui, a todo o momento, da descoberta de “ferramentas e instrumentos simbólicos com o intuito de organizar sua evolução a contento, criando o aperfeiçoamento à curiosidade de interagir com os demais semelhantes” (SANTOS, 1992 p. 24), tendo como meio para isso os sons, palavras, desenhos, escritas, sinais sonoros entre outros.

Uma dessas formas de comunicação que estará presente neste projeto é a comunicação móvel. Ela torna-se interessantemente paradoxal, dadas as suas vantagens e desvantagens descritas por Martins, Oliveira e Corso (2018). Entre as características apontadas pelos autores, está a autonomia e flexibilidade na comunicação e realização de atividades, a possibilidade de manter o fluxo da comunicação evitando a interrupção enquanto há o deslocamento e a pessoalidade do dispositivo, uma vez que esse permite uma comunicação privada.

Por outro lado, ela nos prende a desenvolvedores e empresas prestadoras de serviços, torna mais forte as empresas que detém os principais *softwares* de comunicação, restringe o seu funcionamento pela disponibilização da rede, a tecnologia presente, e, também, a disponibilidade ou não de plano de dados para a maioria das suas aplicações. Assim, a comunicação móvel e o *status* de ubiquidade dependem de uma série de fatores tecnológicos, sociais, financeiros e de interesses para que seja, de fato, aplicável.

2.1 MOBILIDADE E UBIQUIDADE

A soma da mobilidade com a comunicação gerou novas perspectivas sobre o processo informacional da comunicação. O usuário passa a produzir e consumir conteúdo em qualquer local. A conexão está em todo o lugar e não há necessidade

de esperar um momento para acessar a Internet, sendo este “um dos ícones da sociedade atual, no que se refere aos processos comunicacionais, ampliando a circulação de informação através dos dispositivos móveis” (HENRIQUES, 2016, p. 1).

A ubiquidade, na comunicação, define-se como algo que pode ser alcançado pelo estado de conexão generalizada a quem possui dispositivos móveis (MANTOVANI; MOURA, 2012, p. 64). A forma com que os autores abordam o termo pode ser entendida como a onipresença de algo. Mantovani e Moura (2012) citam Pellegrino, esclarecendo sobre o *status* ubíquo, afirmando que seria o dom divino da onipresença, podendo estar em qualquer lugar e a qualquer momento, sem as limitações da comunicação face-a-face. Santaella (2014) reforça que o conceito de ubiquidade não significa somente a mobilidade. Para ela, a comunicação ubíqua se dá no momento em que ela ocorre, em qualquer lugar e a qualquer momento, pelos aparelhos eletrônicos espalhados no ambiente.

Outro ponto importante da ubiquidade é a sua invisibilidade. Ao estar intrínseco à cultura de uma sociedade, a ubiquidade torna-se parte dela e é incorporada aos meios (BATISTA; FARINIUK; MELLO, 2016, p. 10). Esses dispositivos “estarão em todos os lugares e em todos os momentos, auxiliando o ser humano sem que ele tenha consciência disso” (KAHL et al., 2011, p. 1) ganhando um *status* de “*calm technology*”, ou seja, tecnologia discreta e controlada, segundo MONT’ALVERN (2010), ao citar Weiser e Brown. Esses dispositivos, trabalhando de forma conectada e descentralizada, criam uma forma de conexão a serviço do homem, sem que a sua presença seja percebida ou entre em fricção com as atividades cotidianas — inclusive, torna-se parte delas. MONT’ALVERNE (2010) compara essa invisibilidade com a que ocorreu com a escrita e a eletricidade.

Interessante observar que essa invisibilidade e permeabilidade da tecnologia ubíqua na sociedade moldou o comportamento humano. Isso permitiu que os portadores de tecnologia trocassem informações com a rede, promovendo uma reorganização dos espaços, da comunicação e da mobilidade. Esses espaços reorganizados moldam as relações com o tempo, criando um ambiente diferenciado e alterando noções de presença e virtualidade. A ideia de estar em um lugar, por exemplo, é uma dessas mudanças em que o ambiente móvel se torna híbrido, pois há uma onipresença da conexão móvel entre indivíduos, e entre indivíduos e objetos (HENRIQUES, 2016).

A mobilidade, tão fundamental para o assunto deste trabalho é pensada por Lemos (2011) em três dimensões: a primeira segue a linha definida por Deleuze e Guattari (1997 apud LEMOS, 2011), como a desterritorialização por excelência; a segunda, como física (deslocamento de corpos e objetos); a terceira é a informacional-virtual (informação). Lemos (2011) afirma ainda que a mobilidade não é neutra, revelando-se em formas de poder, seja por controle, monitoramento e/ou vigilância. Hoje, a mobilidade tornou-se "globalizada" e "virtualizada", característica das redes telemáticas e dos dispositivos de conexão móvel e sem fio, e vem criando territorializações e, por consequência, novos sentidos de lugar. Como Lemos (LEMOS, 2011) afirma, um simples ato de enviar um SMS, uma foto, ou mesmo postar em uma rede social usando um telefone celular, revela essa nova relação sinérgica, algo que era impossível na era dominada pelas "*mass media*".

Uma das mais drásticas mudanças tecnológicas nos meios de comunicação do terceiro milênio, segundo Beiguelman e La Ferla (2011), a comunicação móvel configurou uma nova interface cultural. Ela está presente em diversas dimensões da vida quotidiana: relações de trabalho, campo da arte e do lazer, relações familiares, setores governamentais, marketing e nas formas de vigilância.

Com o seu uso, surge a espacialização e a hiperlocalização, resultante da relação dinâmica entre dispositivos, informação e lugares, a partir de trocas infocomunicacionais contextualizadas (LEMOS, 2011). O resultado dessa ação é o *upload* informacional – toda a informação produzida no ambiente físico é enviada para a nuvem e, com a internet das coisas[21], pode-se fazer o *download* dessa informação para apropriar-se novamente nos espaços físicos.

Importante olharmos, por meio da escavação das mídias, os elementos que culminaram em um estado de comunicação móvel e ubíqua, partindo dos primeiros exemplares de uma comunicação móvel até os exemplos mais contemporâneos. Para isso, passaremos a conhecer os aspectos da comunicação móvel aplicadas à comunicação sem fio, os aparelhos móveis, celular e *smartphone*, e os diferentes tipos de redes móveis que estiveram presentes na sociedade.

[21] Internet das coisas (em inglês: *Internet of Things*, abreviadamente, IoT) é um conceito que se refere à interconexão digital de objetos cotidianos com a internet, e a conexão dos objetos, mais do que das pessoas, à internet. INTERNET das coisas. *In:* Wikipedia: A enciclopédia livre. Disponível em: https://pt.wikipedia.org/wiki/Internet_das_coisas. Acesso em: 13 abr. 2019.

2.2 COMUNICAÇÃO SEM FIO

Uma das primeiras iniciativas de uma comunicação sem fio da história recente deu-se pelo brasileiro Padre Roberto Landell de Moura. O porto-alegrense é conhecido por ter conseguido, em 1900[22], realizar a primeira transmissão de som e sinais telegráficos por ondas eletromagnéticas. No ano seguinte, ele obteve a patente de um aparelho destinado à transmissão fonética a distância, com fio e sem fio, através do espaço, da terra e do elemento aquoso (WIKIPEDIA, 2019).

Anos se passaram e as primeiras utilizações deram-se nos rádios de comunicação utilizados em automóveis na década de 30. Como Mont'alverne (2010) relata na sua dissertação de mestrado pela UFBA, os dispositivos estavam acoplados nos veículos de bombeiros e carros policiais da cidade de Detroit, Nova York, e em outras cidades dos Estados Unidos. A forma de operação permitia a comunicação unilateral. O aparelho disponível nos veículos apenas recebia um sinal sonoro e dependia que os ocupantes saíssem e fossem até o telefone fixo mais próximo para ligarem à central.

O próximo passo, em 1937, deu-se pelo desenvolvimento das duas vias de comunicação, o que permitia aos ocupantes do veículo transmitirem voz e sons pelo aparelho veicular. O "Motorola", que era o nome do aparelho, tornou-se o padrão da comunicação móvel, ganhando apelo público ao chamar de *mobileers* a comunidade de usuários, acarretando a troca do nome da empresa fabricante, que passou de Galvin Manufacturing Corporation para Motorola (MONT'ALVERNE, 2010).

Com o início da segunda guerra mundial, a Motorola passou a fabricar versões portáteis do aparelho, os *Walkie-Talkies*[23] e *Handie-Talkies* (MONT'ALVERNE, 2010). Em 1956, na Suécia, a Sony Ericksson lançou o CB *Radio*, *Citizen's Ban Radios*, permitindo a comunicação sem fio de curta distância entre os civis (MONT'ALVERNE, 2010). Este sistema ficou conhecido como Rádio Cidadão e na década de 70 tornou-se popular, sendo utilizado na comunicação entre carros e caminhões, o PX.

---

[22] A data é controversa. Vários testemunhos afirmam que ele vinha realizando testes bem-sucedidos em ambas as modalidades de transmissão desde 1893 ou 1894, mas a documentação sobre esses primeiros experimentos é carente e a data é disputada. O seu primeiro registro inconteste, documentado publicamente, é de 3 de junho de 1900. ROBERTO Landell de Moura. *In:* Wikipedia: A enciclopédia livre. Wikimedia. Disponível em: https://pt.wikipedia.org/wiki/Roberto_Landell_de_Moura. Acesso em 08 mai. 2019.

[23] Rádio transmissor e receptor de uhf de ponto a ponto, portátil. WALKIE-TALKIE. *In:* Wikipedia: A enciclopédia Livre. Wikimedia. Disponível em: https://pt.wikipedia.org/wiki/Walkie-talkie. Acesso em 11 mai. 2019.

O funcionamento de tais aparelhos era por ponto a ponto, ou seja, eles eram os emissores e receptores do sinal, não havendo estrutura mediando a comunicação, o que limita o alcance e ocasionava em uma série de possíveis interferências e cruzamento de linhas devido à limitação de bandas[24] operacionais.

Por mais sem fio que fosse, ele não era móvel. De certa forma, o aparelho que possuía um “endereço” – endereço podemos referenciar aqui como uma frequência de operação – em um determinado local, não possuiria a mesma identificação em outra área daquela que estava destinado à operar, tornando, portanto, uma comunicação sem fio mas ‘pertencente à um local’ limitando a mobilidade e não permeando, de fato, a sociedade.

2.3 COMUNICAÇÃO MÓVEL

“As tecnologias mais profundas são aquelas que desaparecem. Elas se entrelaçam no tecido da vida quotidiana até se tornarem indistinguíveis” (WEISER, 1991 apud LEMOS, 2005). É com essa menção feita por Lemos, citando Mark Weiser, pai da ubiquidade, que iniciamos uma a discussão sobre comunicação móvel.

A comunicação móvel, diferentemente da comunicação sem fio, define-se por “uma rede de comunicações por rádio que permite mobilidade contínua por meio de muitas células” (ALENCAR, 2004, p. 301). A possibilidade de comunicar-se em mobilidade deu-se com a evolução da telefonia nos anos 70. Inicialmente, o telefone sem fio foi projetado para funcionar dentro das residências, conforme afirma Alencar (2004). Tal aparelho apenas removia o cabo que o prendia à parede, permitindo que o interlocutor se deslocasse pela residência por distâncias consideráveis.

Os telefones fixos sem fio atuavam com até oito canais, sendo assim, em um determinado espaço, poderiam existir apenas oito destes operando sem problemas. Caso surgisse um novo integrante, um dos demais sofreria interferência. Outra limitação era que um aparelho móvel dependia de uma única estação de recepção,

[24] Banda é uma subsecção do espectro eletromagnético usado para as frequências de radiocomunicação. Normalmente, a entidade nacional reguladora (como a FCC nos EUA, a ANACOM, em Portugal, e a ANATEL no Brasil) determina o uso destas bandas na forma de canais, cada faixa usada para um determinado propósito. BANDA (rádio). In: Wikipedia: A Enciclopédia livre. Wikimedia. Disponível em: https://pt.wikipedia.org/wiki/Banda_(r%C3%A1dio). Acesso em 11 mai. 2019.

ou seja, não havia *handoff*[25], sendo este um dos principais diferenciais da telefonia móvel: a possibilidade de se deslocar sem perder a comunicação.

O telefone celular padrão inicial pode ser descrito por Steuernagel como “uma única peça que serve como *handset* e inclui um teclado, *display*, microfone, mini autofalante ou *speaker*, um mini-rádio receptor e transmissor, antena e uma bateria removível e recarregável”. (STEUERNAGEL, 2000, p. 9).

De fato, como afirma Steuernagel, esses aparelhos eram ditos como maravilhas da engenharia. Seu formato era retangular e alguns, mais cobiçados, eram os modelos *flip*[26]. Eles dominavam a imaginação popular aparecendo, inclusive, no filme *Star Trek*.

Jeszenksy faz a sua avaliação da mudança que provocaria na sociedade:

> O desenvolvimento dos serviços de comunicação móvel quebrou o paradigma de que para se comunicar é necessário estar fisicamente conectado a uma estrutura com fio. Com o acesso de rádio móvel é possível estabelecer comunicação caminhando, dentro de veículos, ou em qualquer lugar aceito pelo sistema. Desse modo, os sistemas de comunicação móvel permitiram simplificar consideravelmente as atividades pessoais e profissionais, trazendo agilidade, flexibilidade, aumento de produtividade e, também, aumento da segurança (pessoal) (JESZENSKY, 2007, p. 568).

Para experienciar toda essa flexibilidade, mobilidade e comunicar-se em movimento, o *handoff* era uma funcionalidade essencial e somente era possível devido ao funcionamento da estrutura e organização das antenas celulares e dos protocolos de comunicação. O funcionamento da rede móvel consistia, e ainda consiste, em lotear a área que será coberta em muitas áreas menores, contrapondo o sistema anterior, sem fio, que utilizava altas frequências para aumentar o alcance (ALENCAR, 2004). Esse sistema trabalha com menor frequência, logo, menor alcance, mas com maior número de estações de rádio base (ERB), permitindo a reutilizando da frequência entre as diferentes células.

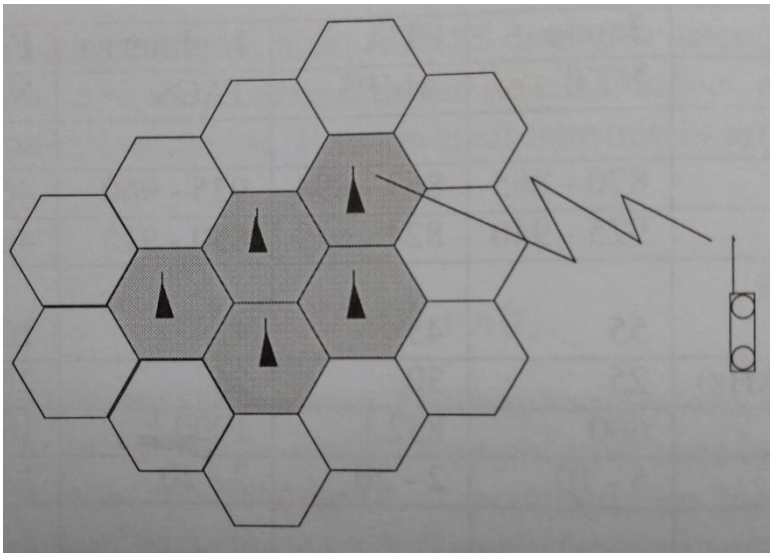
A comunicação entre o dispositivo móvel e a ERB é estabelecida por um protocolo de comunicação. A evolução de tais protocolos[27] analisaremos nos próximos capítulos, que abordarão as redes de transmissão de voz e de dados. A organização

---

[25] *Handoff* é a função que permite manter a continuidade de uma conversação quando o usuário passa de uma célula para outra (ALENCAR, 2004, p. 314).
[26] Os modelos de celular *flip* eram dotados de uma parte que cobria o teclado quando não estava em uso (STEUERNAGEL, 2000).
[27] Pode-se dizer que um protocolo consiste num conjunto de regras que permitem a comunicação entre dispositivos. Grosso modo, protocolo é uma “linguagem” (DA SILVEIRA, 2018, p. 7).

das ERB's (figura 1) dá-se de acordo com a área que deseja cobrir, variando o alcance do sinal. Conforme Alencar (2004) afirma, o raio de abrangência de uma estação pode variar de cinco a dez quilômetros, existindo também estações com alcance de 500 metros e micro-células utilizadas em ambientes internos com alcances ainda menores.

Figura 1 - Descrição do sistema celular



Fonte: Telefonia Celular, por Marcelo Sampaio de Alencar (2004).

Alencar explica como se dá a dimensão de cada célula: elas variam de acordo com a densidade do tráfego. Quanto maior o tráfego, menor a célula. Isso significa que áreas centrais das cidades possuem maior número de ERB's do que em cidades menores ou áreas suburbanas.

Ao deslocar-se de uma célula para outra, a ligação é transferida instantaneamente e automaticamente pela operadora de telefonia, por meio do MTSO[28] (STEUERNAGEL, 2000). Isso permite que a conversa não seja interrompida, provendo a mobilidade ao usuário e suprindo a antiga necessidade de ter uma frequência de banda única em um espaço de pertencimento como se dava nos rádios amadores, PX.

O simples funcionamento da telefonia móvel nos faz refletir sobre um ponto interessante, explicado por Schneider: "Toda a manhã que você coloca seu celular no bolso, está fazendo uma barganha implícita com a empresa: 'eu desejo fazer e receber ligações; em troca, eu permito que esta companhia saiba onde eu estou todo o tempo'"

[28] MTSO: *Mobile Telephone Switching Office.*

(SCHNEIER, 2015, p. 1. Tradução nossa.)[29]. Ou seja, para o ideal funcionamento da rede móvel, as empresas necessitam saber qual antena proverá o melhor sinal para cada aparelho. Sendo assim, há uma noção de espaço que aquele aparelho estava ocupando quando realizou a ligação, mas também por onde ele circulou enquanto estava fora de uso, porém ligado. Levando em conta também os diferentes raios de cobertura de cada ERB, da disposição delas de acordo com a demanda de tráfego e das antenas de menor potência para locais fechados, podemos entender que havia a possibilidade de indicar a posição de cada dispositivo móvel com maior ou menor precisão, de acordo com a configuração e organização das estações.

Cada aparelho possuía um número para ser acionado e que o identificasse tanto para quem recebia a ligação, quanto para a operadora que iria cobrar depois. Para isso, eles possuíam um microchip chamado NAM[30]. Esse *hardware* possuía um número sequencial único, capaz de identificar o celular onde quer que ele estivesse. As informações contidas no NAM eram gravadas ou "queimadas"[31] com uso de equipamentos especiais, e utilizadas pelas MSC[32] para realizar as cobranças pela utilização. Outra utilidade era para identificar quando o usuário estava utilizando o aparelho, quanto ele falou e também para qual aparelho destinar a ligação quando vinha de outra fonte.

A possibilidade de vincular um identificador único a um aparelho e a um usuário permite que as empresas saibam, de fato, onde aquele aparelho esteve. Isso, de certa forma, acarreta numa possível forma de vigilância.

> Seu celular registra onde você mora e trabalha. Ele registra onde você gosta de passar seus finais de semana e finais de tarde [...] Ele rastreia – desde que saiba sobre os outros telefones na sua área – com quem você gasta seus dias, com quem você se encontrou para almoçar e com quem você está dormindo (SCHNEIER, 2015, p. 1–2).

A potencial vigilância, neste caso, existe devido à pessoalidade do celular, que pode existir na sua portabilidade e uso. Como Martin (2013) relata:

> O telefone móvel é um aparelho individual. Ele não é compartilhado como um computador ou assistido em grupo, como uma televisão. Ele está no bolso,

[29] "Yet every morning when you put yout cell phone in your poket, you're making na implicit bargain with the carrier: "I want to make and receive mobile calls; in Exchange, I allow this company to know where I am at all thimes".
[30] *Numeric Assignment Module.*
[31] *Burning the NAM* era o termo utilizado para dizer que a informação era gravada no microchip.
[32] MSC – *Mobile Switching Center*: é a parte responsável pelo *handoff*.

> na mão ou na bolsa das pessoas. O celular está próximo delas e vai aonde elas forem. Depois das chaves e carteiras, as pessoas não saem de casa sem seus telefones celulares. As comunicações feitas por meio do aparelho são pessoais, incluindo mensagens de texto de familiares e amigos, juntamente com as conexões das redes sociais. Para interagir através desses aparelhos pessoais, as empresas precisam ser convidadas a entrar, o que potencializa o verdadeiro marketing pessoal (MARTIN, 2013, p. 22).

Contudo há uma particularidade nesse “aparelho móvel”. Ele não se move sozinho, ele é potencialmente móvel e, sendo assim, indissociável de um motor que o mova, conforme Mariela afirma: “se esse algo não se movesse, estaria em repouso e perderia sua condição de objeto móvel” (YEREGUI, 2011, p. 119).

No que tange à privacidade, a questão é justamente quando este motor de movimento é o ser humano, por mover-se conforme sua vontade ou necessidade, como explica Yeregui (2011):

> Embora o corpo não seja um motor exclusivo, é um dos motores privilegiados nas práticas locativas e o que apresenta questões fundamentais no que diz respeito ao movimento, uma vez que integra a esfera da volição: o corpo se move porque há uma determinação e uma motivação individual – não é uma decisão do sistema (YEREGUI, 2011, p. 125).

Associando isso à pessoalidade do celular relatada por Martin, o motor humano de Yeregui, junto à associação do aparelho a um usuário e a forma de metadados gerados pelo uso e coletados pelas MSC, podemos traçar perfis desse usuário, como Schneier (2015, p. 2) explica:

> Os dados acumulados podem provavelmente pintar uma melhor imagem de como você gasta seu tempo [...]. Em 2012, pesquisadores eram capazes de usar este dado coletado para predizer onde as pessoas poderiam estar nas próximas 24 horas com uma precisão de 20 metros.

A empresa brasileira Algar Telecom lançou em 2011 um serviço chamado “Onde está”, que consistia em informar ao usuário onde estava um outro usuário por meio do envio de uma mensagem SMS à operadora com o número de quem desejava saber (SMAAL, 2011). Conforme a redatora da matéria, Beatriz Smaal (2011), o serviço funciona para os números de um mesmo titular de forma automática, ou seja, no momento que um integrante solicitava o serviço, logo vinha a localização. Para quem não estava sobre o mesmo titular, havia uma requisição prévia, sendo que a segunda parte poderia aceitar ou não informar a sua localização. O que é interessante nesse ponto é a forma clara de que podemos saber, com uma certa precisão, onde

estão os indivíduos apenas por deixarem seus celulares ligados, como explica Beatriz: “A novidade funciona através da triangulação de dados, “usando como referência a posição das antenas da cobertura GSM e 3G da CTBC para informar a localização aproximada de um celular”, explica Luciana Borges. (SMAAL, 2011).

O SMS[33], citado anteriormente, entrou na segunda geração das telecomunicações sem fio, como veremos adiante. Com ele, havia um serviço de confirmação de entrega que possibilitava saber se um determinado aparelho estava na área de cobertura, ligado ou era existente. No Japão, por exemplo, havia uma forma própria de utilização do SMS. Conforme Lemos (2005) relata, era possível saber quais usuários cadastrados nesta plataforma estavam na mesma região, potencializando a rede de contatos do indivíduo.

Outra diferença do SMS para a chamada de voz é o tipo de dado que ele transmite, o texto, sendo esse mais fácil de ser armazenado, estruturado e analisado. Assim, as empresas e governos poderiam saber onde as unidades móveis estavam. A partir desse ponto, elas podem saber com mais facilidade sobre o que elas falam. “A capacidade de coletar, armazenar, utilizar e distribuir informação alheia revela um poder de controle (*power of control*) exercido por alguém, quer seja uma corporação empresarial, um órgão do governo ou mesmo uma pessoa física” (REINALDO FILHO, 2005, p. 24).

Um próximo passo para os celulares foi a conexão entre eles sem a necessidade de terceiros. Inicialmente, o padrão de comunicação entre os dispositivos era o infravermelho[34]. A tecnologia já era utilizada nos controles remotos dos televisores, sendo que até hoje ainda é utilizado com tal finalidade. A limitação era a sua baixa taxa de transferência de dados, bem como, a necessidade de um dispositivo estar apontando para o outro, a fim de obter com êxito a transferência de dados.

Como uma alternativa para isso, surge o *Bluetooth* que, diferentemente do IrDA, utilizava ondas de rádio para a comunicação entre as partes, deixando de lado a necessidade de dispor os dispositivos num mesmo campo de visão. Outra diferença do *Bluetooth* é a inteligência do protocolo, permitindo que a troca de dados seja feita

[33] SMS, acrônimo de *“short messages”,* mensagens curtas enviadas pelo celular para uma pessoa ou grupo de pessoas (LEMOS, 2005, p. 6).

[34] A comunicação via infravermelho utiliza sinais de luz emitidos através de um LED e captados por um sensor instalado no destinatário (MORIMOTO, 2005).

de forma automática e sem a intervenção do usuário, como afirma Alencar (2004). Da mesma forma, cada placa de *Bluetooth* possui seu próprio número de série, o Mac[35].

O alcance depende da classe do *Bluetooth*. A classe 1 permite conexões até 100 metros, a classe 2, até 10 metros e a classe 3, aproximadamente, 1 metro (ALECRIM, 2018). “Embora já existam classes de *Bluetooth* com alcance de 100 metros, a maioria dos dispositivos conta com alcance de 1 a 10 metros, o que, embora seja uma desvantagem, ajuda na segurança dos usuários” (CAMARA, 2012). Para que a comunicação ocorra, a funcionalidade deve estar sempre ativada. Se a condição for verdadeira e o usuário permitir que outros dispositivos o encontrem, ele pode ser encontrado no espaço que está.

A utilização do *Bluetooth* se dá para transferência de arquivos entre celulares, celulares e notebooks, celulares e fones de ouvido, *mobile marketing*, entre outros. Dada a natureza da sua operação, o dispositivo receptor deve estar com o *Bluetooth* sempre ativado para que haja interação. A partir disso, ele pode ser detectado, receber uma solicitação de pareamento e, posteriormente, realizar aplicações como gerenciamento de arquivos, controle de dispositivos e até streaming.

Na juventude do *Bluetooth*, diversas brechas de segurança foram encontradas e diversos movimentos apareceram com a finalidade de evidenciar algumas formas de burlar o sigilo e o isolamento dos indivíduos que detinham esta tecnologia habilitada no celular. Uma das iniciativas que visava mostrar o poder de rastreio pelo *Bluetooth* foi o projeto *Loca.* O funcionamento se dava pela seguinte forma: “Os agentes do projeto, por sua vez, estão equipados com etiquetas. Usando seus celulares, eles detectam outros dispositivos e os registram, deixando uma etiqueta no lugar, com o nome do dispositivo, a data e a hora da detecção.” (YEREGUI. 2011, p. 123). Os dados eram armazenados e disponibilizados em um estande em que as pessoas poderiam escanear seus dispositivos para terem seus trajetos exibidos, e ainda poderiam imprimir os seus próprios movimentos (YEREGUI, 2011).

Outra forma de intervir e aproveitar o modo de funcionamento dessa comunicação é o *Bluejacking* – “mensagens não solicitadas enviadas para dispositivos com *Bluetooth*” (YEREGUI, 2011, p. 123). Com ela, os mesmos autores do projeto *Loca* enviavam mensagens que diziam: “Estamos com dificuldades de monitorar sua

[35] Semelhante ao NAM.

posição: por favor, mova seu dispositivo de rede no ar”[36], por *Bluetooth*, a fim te intrigar os receptores.

Da mesma forma que operam as ERB’s, as antenas *Bluetooth*, se posicionadas da forma correta, podem realizar a triangulação – semelhante ao funcionamento do GPS – e indicar com certa precisão onde o dispositivo se encontra. Para acurar ainda mais a localização, a versão 5.1 desse protocolo permitirá “serviços de localização com o novo recurso de localização de direção” (CARVALHO, 2019) e completa:

> O sistema de posicionamento utiliza o *Bluetooth* para determinar a localização física do aparelho e inclui Sistemas de Localização em Tempo Real (RTLS) para localização em grandes distâncias e Sistemas de Posicionamento Interno (IPS) para utilizar em áreas de baixa cobertura (CARVALHO, 2019 n.p).

Há, também, formas de uso comercial desse *trackeamento* via *Bluetooth*:

> Muitas lojas de varejo estão rastreando clandestinamente as pessoas pelos endereços MAC e os IDs *Bluetooth* – que são basicamente números de identificação – difundidos pelos seus smartphones. O objetivo é gravar com os corredores que eles desçam, com produtos que parem de olhar e assim por diante. As pessoas podem ser rastreadas em eventos públicos por meio dessas duas abordagens (SCHNEIER, 2015, p. 34–35)[37].

Assim, entendemos que a possibilidade de monitoramento dos dispositivos móveis é aumentada, ao passo que as maneiras para realizar tal ato são democratizadas. O que antes era exclusivo de quem fornecia o sinal de telefonia, agora parte para quem tiver um dispositivo capaz de emitir um sinal *Bluetooth*.

Não somente o trackeamento mas o hackeamento dos celulares pode ser feito por *Bluetooth*. *Bluebugging*, *Bluejacking* e *Bluesnarfing* permitem que invasores acessem os celulares das vítimas, controlando e, até mesmo, roubando dados, como contatos e arquivos multimídia.

A evolução dos celulares ocorreu também na quantidade e diversidade de *hardwares* acoplados. Além dos itens descritos por Steuernagel, outros foram se

---

[36] “We are currentl experiencig difificulties monitoring your position: please wave yout network device in the air” (HEMMENT et al., 2006 *apud* YEREGUI, 2011, p.122).

[37] Many retail stores are surreptitiously tracking people by the MAC addresses and Bluetooth IDs - with are basically identification numbers - broadcastly by their smartphones. The goal is to record with aisles they walk down, with products thet stop to look at and so on. People can be tracked at public events by means of both these approaches. Tradução nossa.

juntando ao aparelho, tornando-o complexo, com mais possibilidades e mais presença no cotidiano.

Uma das junções mais relevantes ocorreu em 2000, no Japão. Naquele ano, o celular era integrado, pela primeira vez, a uma câmera digital. O modelo Sharp J-SH04 obteve lançamento e comercialização somente naquele país (MELANINHO; THEREZA, 2018). Isso dava a possibilidade de registrar imagens, mesmo que em baixa qualidade, e armazenar no dispositivo. O compartilhamento podia ser feito por meio de MMS[38] ou por conexões entre celulares, como *Bluetooth* ou IrDA.

A partir desse momento, era possível não apenas registrar uma imagem mas também compartilhar ela sem a necessidade de estar em um computador pessoal, ou seja, era possível compartilhar estando em mobilidade. O fluxo de informação torna-se possível entre os dispositivos móveis, e alguns serviços online permitiam receber e postar os conteúdos.

Os *softwares* de alguns celulares se destacavam, como os modelos Danger Hiptop e BlackBerry 5810, que em 2002 podiam executar comandos simples de voz, como ligar para algum contato, enviar e receber e-mails, acessar *websites*. Esta funcionalidade era restrita a comandos disponíveis no celular e necessitava que o operador cadastrasse as ações previamente — como, “ligue para casa” — e vinculasse elas a um contato.

A possibilidade de executar diversas operações enquanto se desloca modificou a forma com que as pessoas se comunicavam e trabalhavam. Segundo Viera (2015), os dispositivos móveis, com acesso sem fio, deram autonomia e liberdade. Ao poderem acessar as informações a qualquer momento, os usuários foram empoderados, transformando a sociedade como um todo. Não somente a possibilidade de se comunicar, mas também a convergência de diversas funcionalidades distribuídas em outros aparelhos — como agenda de telefone, armazenamento de mídia, câmera fotográfica e telefone em um só aparelho —fizeram com que tanto a comunicação móvel quanto o dispositivo que permitia isso ganhassem importância e destaque no cotidiano. Empresas, governos e a sociedade em geral passaram a adotar regras para uso e restrição. Essas boas práticas são fortes indícios da penetração profunda da tecnologia e dos impactos que isso gerou.

[38] *Multimedia messaging service*, termo inglês que significa serviço de mensagens multimídia.

2.4 TECNOLOGIAS MÓVEIS

Em paralelo à evolução dos dispositivos móveis, ocorriam estudos para melhorar a infraestrutura de comunicação. Não somente a parte física mas os protocolos de comunicação sofreram transformações, passando de um sinal analógico para o digital. Isso permitiu que não somente mais aparelhos atendidos em uma mesma área, mas também outros tipos de dados fossem transferidos.

O primeiro protocolo de comunicação comercialmente utilizado era o *Advanced Mobile Phone System* (AMPS), ou Telefonia de Primeira Geração 1G. Analógico, o seu funcionamento permitia que, em cada faixa de 30kHz, os usuários poderiam realizar as suas ligações telefônicas (ALENCAR, 2004). Isso, em uma faixa de 825 a 894MHz, possibilitava que 832 canais de comunicação fossem explorados pelas empresas.

O sistema AMPS permitia apenas o envio e recebimento de chamadas, ou seja, era uma rede unicamente para voz. Outra característica dessa rede é que nem todos os canais eram para a comunicação. Vinte e um deles estavam reservados para controle da operadora. Esses canais eram a interface entre a operadora e a unidade móvel e possibilitavam estabelecer a comunicação, transmissão de mensagens gerais do sistema, receber mensagens da unidade móvel, entre outras aplicações pontuais (ALENCAR, 2004).

Conforme Alencar (2004) explica, esse número limitado de telefones conectados gera uma série de implicações na organização e disponibilização das antenas. Em áreas mais povoadas, que supera o limite de celulares por canais disponíveis, há duas saídas possíveis para atender a demanda: ou aumentar o número de antenas *omnidirecionais* de baixo alcance para cobrir áreas menores, ou utilizar antenas direcionais dividindo um mesmo setor em dois. Ambos os métodos duplicam o número de canais disponíveis na mesma célula, resolvendo o problema.

Apesar da transferência ser unicamente de voz, vale ressaltar que era possível realizar transferência de dados dos celulares de primeira geração com a utilização de modems específicos, conforme afirma Alencar (2004). Anos mais tarde, por diferentes motivos, houve uma busca para desenvolver um sistema digital de comunicação. Dá-se início à segunda geração da telefonia móvel.

Duas frentes estavam realizando estudos: os Estados Unidos tinham por objetivo manter a compatibilidade com o antigo sistema, o AMPS, e permitir o *roaming* nacional; na Europa, havia sistemas distintos de comunicação e a finalidade era criar um padrão compatível com a rede telefônica fixa e com os padrões ITU (ALENCAR, 2004). O resultado seria um maior número de assinantes por antena, capacidade para expandir a cobertura do sinal analógico e melhoria da transmissão de voz para os assinantes analógicos e digitais (ALENCAR, 2004). Como a mudança era impactante, as duas frentes, europeia e Norte-americana, adotaram medidas distintas para realizar a migração. O padrão europeu, posteriormente adotado no Brasil, era o GSM. Este sistema possibilitou o *roaming* internacional pois era compatível com os diversos padrões existentes, já que era mais abrangente. Isso permitiu que os fabricantes pudessem criar aparelhos menores, mais eficientes e baratos (ALENCAR, 2004).

Tanto o GSM como o TDMA e o CDMA foram tecnologias de transmissão digitais de segunda geração, denominada popularmente por 2G. Como vantagens, ela permitia maior número de pessoas conectadas a uma mesma antena e, posteriormente, consolidou a infraestrutura que viria a ser utilizada para transmissão de dados.

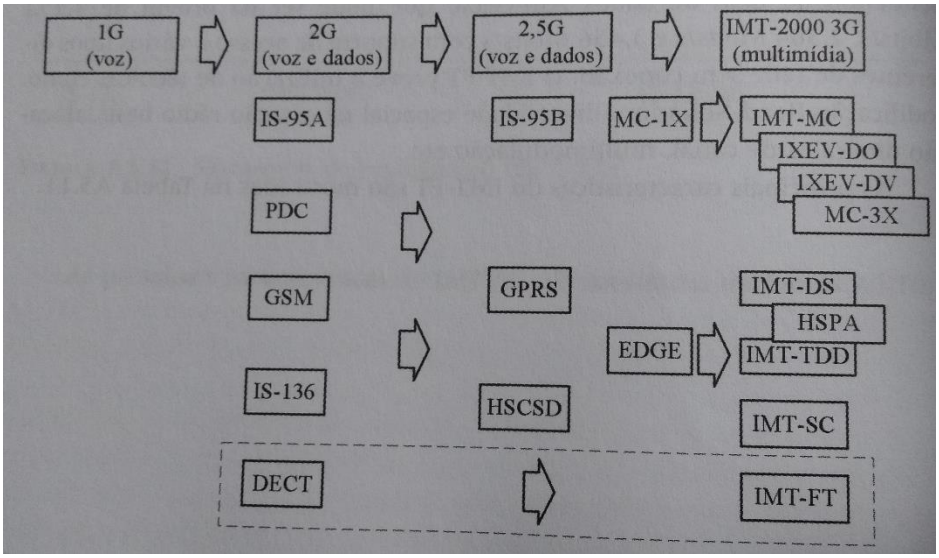
Outro ganho para a comunicação móvel foi a criptografia na comunicação. Além disso, foi na tecnologia GSM que implantaram os chips celulares (ALENCAR, 2004), substituindo o NAM na identificação dos dispositivos, sendo possível trocar de dispositivo sem precisar “queimar a NAM”, como na geração anterior. O sucesso do protocolo acarretou no aumento crescente do número de usuários e da demanda por novos serviços (JESZENSKY, 2007).

Os serviços oferecidos pela rede 2G eram desde SMS, acesso à mensagens eletrônicas, até a tecnologia WAP, entre outros (JESZENSKY, 2007). Contudo, apesar de haver a possibilidade de transferência de dados, o 2G não possuía interface adequada para oferecer transferência de dados ideal para aquela geração. O intuito real era aprimorar os serviços de transmissão de voz.

Mesmo assim, para o sistema GSM, foi desenvolvido um serviço de transferência de dados por pacotes, o GPRS. Esse movimento ficou marcado como a geração 2.5G e permitia transferências de dados máxima de 171,2 kbits/s (JESZENSKY, 2007). A partir desse momento, era possível enviar mensagens multimídia, o MMS, além de acessar websites com a tecnologia WAP. A tecnologia EDGE foi outra iniciativa, ainda dentro da rede 2G, que pretendia aumentar a

velocidade de transferência de dados, sendo considerada como rede 2.75G. Essa nomenclatura foi definida para oferecer uma transição suave entre o sistema 2G e o 3G, como vemos no quadro abaixo:

Figura 2 - Evolução das redes 1G até 3G



Fonte: Sistemas telefônicos, por Paul Jean Etienne Jeszensky (2007).

A entrada da terceira geração de telefonia móvel, a rede 3G, ocorre quando a Internet comercial está se consolidando no cotidiano das pessoas. Isso aconteceu porque a presença do computador doméstico já era uma realidade e a Internet passava a ser importante para a comunicação entre os aparelhos (JESZENSKY, 2007). Somando isso à crescente utilização da tecnologia móvel, há necessidade de avanços que correspondessem à demanda de manter a conexão fora do ambiente doméstico.

Para se ter uma ideia das mudanças que estavam ocorrendo no Brasil, em 2007, “pela primeira vez, o país comercializou mais computadores pessoais do que aparelhos de TV. A internet como mercado publicitário também passou a receita da TV a cabo” (PELLANDA, 2009, p. 16). Além disso, o comportamento social, a vida pessoal e profissional demandavam uma maior mobilidade e dependência do acesso à informação, em paralelo às ações do mercado, que desenvolvia e oferecia aparelhos cada vez menores, portáteis e com maior capacidade de processamento, como Notebooks e Palm-tops, além de um maior número de serviços, como e-commerces, resultaram nessa demanda crescente de transmissão de dados sem fio, conforme elucida Jeszensky (2007).

Um ponto observado por Jeszensky e que é de extrema importância para este estudo é que, na rede 3G, há a convergência entre a Telecom, Tecnologia da Informação e Entretenimento. A primeira, presente desde a primeira geração e aprimorada na segunda, mantém-se quase igual. Mas o ganho que se dá na tecnologia da informação, aliada ao entretenimento, dá à telefonia móvel novas funções sociais, trazendo “avanços nunca antes imaginados na interface homem-máquina, nos serviços multimídia oferecidos, na capacidade do comércio eletrônico, na velocidade de acesso e, principalmente, na forma de comunicação a distância” (JESZENSKY, 2007, p. 568).

Um aspecto marcante com a chegada do 3G foi o esforço mundial para que a nova geração fosse compatível com todos os aparelhos que passariam a ser fabricados. O resultado foi: “várias propostas foram feitas e, após estudos e análises, restaram apenas duas, o W-CDMA (Wideband CDMA – CDMA de Banda Larga) e o CDMA2000” (INATEL, 2019).

Assim, entra o sistema 3G, segundo Jeszensky, considerado como sucessor da rede 2G, oferecendo, além da cobertura global, *roaming internacional*, suporte para voz e novos serviços de banda-larga, como:

a) Acesso à Internet de alta velocidade;
b) Vídeo e imagem de alta qualidade;
c) Videoconferência;
d) Transferência de dados e altas taxas;
e) Aplicações multimídia.

Essas novas possibilidades permitiram a integração do mundo, oferecendo serviços mais sofisticados, possibilitando que qualquer um, em qualquer lugar, pudesse estabelecer comunicação a qualquer hora – “*Anyone, Anywhere, and Anytime”* (JESZENSKY, 2007, p. 568), com estimativa de taxa de transferência de dados da rede 3G de 2Mbits/s ou mais.

No Brasil, a primeira operadora a oferecer o serviço foi a Vivo, em 2004. Somente em 2007 a Claro e a Tim também passaram a ofertar a tecnologia no país. (WIKIPEDIA, 2019). Sua expansão, a partir do ano de 2008, representou a forte inserção da população brasileira à comunicação digital, abrangendo áreas onde, até então, a banda larga não era possível (PELLANDA, 2009). Esse fator, segundo o autor, era devido ao desinteresse econômico das empresas de telecomunicações. Assim, áreas pobres ou distantes, como favelas ou zonas rurais, não eram atendidas

por conexão à *internet*. A tecnologia sem fio, por sua vez, chegaria para incluir essa parcela excluída, inserindo-a na comunicação mediada por ambientes digitais.

Um exemplo relatado por Pellanda (2009) sobre a carência da população brasileira por uma conexão à internet foi a procura massiva aos *modems* 3G — que permitiam conexão à laptops e PC's. Essa busca desenfreada pelo *hardware* fez com que os estoques ficassem vazios, pois a capacidade de alimentação não supriu a demanda. O impacto social dos 140 milhões de usuários brasileiros que migraram do serviço unicamente de voz para voz e dados, possibilitou a emancipação e um maior acesso à informação por parte de uma população anteriormente excluída (PELLANDA, 2009).

Apesar de os modens resultarem em um acesso para computadores pessoais, como *desktop* e *laptop*, a tecnologia 3G permeou a população mudando aspectos sociais e culturais, como explica Pellanda (2009, p. 11):

> O aumento de conexões resultantes da tecnologia móvel no país tem proporcionado diferentes oportunidades e desafios aos hábitos sociais e aos limites entre espaços públicos e privados. O acesso *Always-on* com voz e dados tem aberto caminho para um novo manancial de distribuição e colaboração de informações num contexto onde os aparelhos são "hiper-pessoais", pois eles são realmente usados por uma só pessoa, o que não ocorre necessariamente com o computador pessoal (PELLANDA, 2009.

2.5 A CONVERGÊNCIA DO DESKTOP NO CELULAR: A CHEGADA DOS *SMARTPHONES*

Não somente a população passou por esse processo. Ao passo que a conexão móvel permitiu a troca e compartilhamento de áudio, vídeo e fotos, outras formas de comunicação foram possibilitadas (PELLANDA, 2009). Com isso, os a aparelhos móveis também passaram por uma ressignificação:

> À medida que esses aparelhos começam a incorporar mais funcionalidades, começam a se tornar mais parecidos com computadores. Nessa perspectiva, eles têm uma grande relevância no processo de inclusão digital por serem mais baratos e estarem em condição ubíqua (PELLANDA, 2009, p. 11–12).

A quantidade e diversidade de possibilidades que o celular e a rede permitiam na comunicação "gerou uma demanda pela convergência de todas em poucos aparelhos. Os *smartphones* consistem em uma solução para parte dessa demanda,

com um único dispositivo que agrega funções de comunicação e processamento em geral” (RODRIGUES, 2009, p. 9).

Morimoto (2009, n.p) designa *smartphone* como um aparelho que é capaz de:

a) Rodar um sistema operacional completo e permitir a instalação de aplicativos nativos (e não apenas *widgets* ou aplicativos em java);

b) Comunicar-se com o PC via USB e *bluetooth*;

c) Conectar-se à web via GPRS, EDGE ou de preferência 3G;

d) Rodar um navegador com bons recursos, oferecer um cliente de e-mails, IM e outros aplicativos de comunicação;

e) Tocar MP3, exibir vídeos e rodar jogos.

Diferentemente dos celulares — que eram mais limitados, possuindo somente agenda telefônica e funcionalidades como calendários, jogos e envios de mensagens — os *smartphones* eram vistos como celulares inteligentes, ou seja, a nova geração de celulares “pelas funcionalidades disponíveis e diversas definições, podemos classificar os *smartphones* como dispositivos programáveis que convergem mobilidade e conectividade” (RODRIGUES, 2009, p. 19).

Como coadjuvantes dessa mudança, os aparelhos da empresa *Blackberry* ofereciam serviços de e-mail e envios instantâneos de mensagens. Empresas como Apple, Google, Microsoft, HTC e Nokia passaram a buscar alternativas, permitindo a popularização dos aparelhos por meio da concorrência e da baixa dos preços.

Um ponto interessante e marcante desse novo aparelho era a presença de um sistema operacional, ou plataformas, permitindo o total aproveitamento do potencial fornecido pelos *smartphones* (MORIMOTO, 2009). Symbian, Windows Mobile, Iphone OS, Blackberry OS e Android foram alguns exemplos de sistemas operacionais que deram início ao ciclo dos *smartphones*.

A ideia de um *smartphone*, originalmente, não vem dos anos 2000. Uma primeira versão, considerada por Melaninho e Thereza (2018) como o “avô do *smartphone*”, foi a ideia da IBM, o IBM Simon, “que era capaz de enviar e receber e-mails e fax, efetuar chamadas, enviar e receber mensagens de *pagers*, calendário, agenda, relógio mundial e editor de texto” (MELANINHO; THEREZA, 2018, p. 4).

Até junho de 2007, os aparelhos celulares que usufruíam de uma conexão 3G e que trocavam dados com a rede de internet, porém, não tinham fluidez de interação com a interface. Havia pouca variedade de sistemas de interação, sendo apenas duas

empresas, Nokia e Windows, responsáveis por dar início ao que viria a ser o *smartphone* (MELANINHO; THEREZA, 2018).

Foi em junho de 2008 que Steve Jobs, CEO da Apple, anunciou um produto que reinventaria o telefone[39]. Na ocasião, foi apresentado como um aparelho 3 em 1: um Ipod widescreen com tela *touchscreen*, um telefone revolucionário e um dispositivo inovador de comunicação via internet (STEVE, c2011). O que Jobs apresentava naquela ocasião passaria a ditar a forma que que iríamos interagir com os dispositivos móveis.

Através desses dispositivos, foi possível que seus usuários tivessem, em qualquer lugar, um rápido acesso às informações desejadas. Assim, a importância da computação móvel se tornou mais reconhecida, chegando ao patamar de ser considerada a quarta revolução na computação (MATEUS, LOUREIRO 1998 *apud* BINE; KUK, 2013).

O fato de o *smartphone* possuir uma plataforma indicava "justamente esta combinação intrínseca entre o *hardware*, o sistema operacional e o conjunto de aplicativos que rodam sobre ele" (MORIMOTO, 2009, n. p). Como explica Bine e Kuk "cada um dos Sistemas Operacionais é composto de características próprias, fazendo com que a grande parte dos aplicativos devam ser projetados exclusivamente para a plataforma pretendida" (2013, p. 4).

A intrínseca relação entre *hardware* e *software* é tão determinante que, segundo Morimoto, "faz com que, muito mais do que em qualquer outra área, o sistema operacional e os *softwares* sejam dois fatores cruciais na hora de escolher um *smartphone*; em muitos casos mais importantes até mesmo que os recursos de *hardware* do aparelho" (MORIMOTO, 2009, n. p).

Dos sistemas operacionais já criados, quatro grandes *players* ganharam destaque na presença em *smartphones*. Hoje restam apenas dois, que dominam quase a totalidade do mercado. Blackberry, Windows phone, IOS e Android foram sistemas operacionais que protagonizaram o início da era dos telefones inteligentes.

O que diferenciava os três primeiros do quarto sistema operacional era a variedade de aparelhos distribuídos. O Windows Phone está presente apenas nos aparelhos desenvolvidos pela empresa Nokia. O IOS e o Blackberry são plataformas exclusivas dos respectivos fabricantes. Já o Android, do Google, é um sistema

[39] "Today Apple is going to reinvent the phone" (DAN, 2007).

baseado em Linux e está presente nos demais dispositivos, como Samsung, Motorola, LG etc.

A empresa de Bill Gates não fez o mesmo sucesso nas plataformas móveis tanto quanto fez nos PC's e laptops. Com apenas 7,2% do mercado em 2016, a empresa anunciou o fim do suporte aos smartphones com Windows Phone até o final do ano de 2019 (CANALTECH, 2016).

A Blackberry, que teve seu passado gloriosos entre 2005 e 2010, dominando o mercado dos *smartphones* principalmente nos Estados Unidos, começou a perder mercado com a ascensão dos aparelhos embarcados com Android e IOS. Em 2017, a empresa detinha apenas 0,1% do mercado. Atualmente, a empresa lança dispositivos com SO Android numa parceria formada com a TCL (KLEINA, 2017).

Os sistemas operacionais restantes, Android e IOS, dominam quase que a totalidade dos aparelhos. No quadro abaixo, podemos ver a presença de mercado no ano de 2016 e a projeção para 2020.

Imagem: Presença de mercado dos sistemas operacionais.

Worldwide Smartphone Shipments by OS, Market Share, and Annual Growth (shipments in millions)							
Platform	**2016 Shipment Volume***	**2016 Market Share***	**2016 YoY Growth***	**2020 Shipment Volume***	**2020 Market Share***	**2020 YoY Growth***	**5 Year CAGR***
Android	1,246.2	85.3%	6.7%	1,507.1	85.7%	4.4%	5.2%
iOS	203.8	13.9%	-12.0%	249.2	14.2%	3.4%	1.5%
Windows Phone	7.2	0.5%	-75.2%	1.7	0.1%	-23.2%	-43.4%
Others	3.9	0.3%	-56.5%	0.8	0.0%	-3.9%	-38.7%
Total	**1,461.2**	**100.0%**	**1.6%**	**1,758.8**	**100.0%**	**4.2%**	**4.1%**
Source: IDC Worldwide Quarterly Mobile Phone Tracker, September 1, 2016							

Fonte: (CANALTECH, 2016).

Importante ressaltar este cenário para perceber que a quase totalidade das comunicações realizadas por *smartphones* dependem de apenas duas empresas, Apple e Google. Juntas, elas gerenciam 230 milhões de dispositivos só no Brasil (BRASIL, 2019) e controlam *hardwares* importantes, como *Bluetooth*, GPS, câmera, microfone e sensores, além de funcionalidades como ligações, envio e recebimento de mensagens e armazenamento.

A interação, a partir desse momento, passaria a ser por meio de aplicações desenvolvidas pela empresa criadora do SO, mas também por terceiros, que disponibilizariam, em lojas específicas, *softwares* capazes de realizar funções específicas, como produção, manipulação e distribuição de dados e acesso ao *hardware* do dispositivo. As aplicações, que chamaremos de Apps ou aplicativos variam desde redes sociais, editores de imagens, textos, som e vídeo, mensageiros instantâneos, navegadores, *browsers*, entre outros.

O usuário, por sua vez, atua em uma interface simplificada e que permite uma interação intuitiva e fluída na realização das tarefas. A associação dos periféricos como, por exemplo, GPS, bússola e acelerômetro, permite a elaboração de aplicações baseadas em geolocalização com uma precisão extraordinária, diferente da acuracidade possível na era dos celulares, como explica Schneier:

> Seu telefone provavelmente tem um receptor gps, que produz informações de localização ainda mais precisas do que a localização da torre de celular sozinha. O receptor de GPS em seu smartphone aponta você para dentro de 4 a 8 metros. Torres de celular, para cerca de 610 metros (SCHNEIER, 2015, p. 16)[40].

Outros exemplos indicados por Schneier são importantes para refletir, como: ao registrar uma fotografia, o *smartphone* anexa à ela a localização, data e hora, lente e identificação do aparelho; aplicativos instalados, como Uber e Lyft, armazenam os pontos de embarque e desembarque; apps de leitura, como Amazon Kindle, consegue capturar o tempo de leitura e pontos de atenção, entre outros exemplos.

Para demonstrar alguns dos possíveis dados que podem ser gerados pelo uso ou simples porte do *smartphone*, vamos descrever alguns *hardwares* e as suas contribuições para a produção e coleta de dados de posicionamento e movimentação. É essencial afirmar que a maioria dos periféricos que serão citados estão presente em quase todos os *smartphones* populares, o que exponencia a possibilidade de coletar dados.

O microfone, no contexto dos assistentes pessoais como a Siri, presente nos Iphones, e o Google Assistente, presente nos dispositivos Android, recebe a missão de capturar os comandos que serão executados pelo dispositivo. Dependente do

[40] Your phone probaly has a gps receiver, wich produces even more accurate location information than the cell tower location alone. The GPS receiver in your smartphone pinpoints you to within 16 to 27 feet. Cell towers, to about 2000 feets. (tradução nossa)

sistema operacional para ser ativado, ele necessita estar atentos ao ambiente para ser acionado quando o usuário desejar, como explica o próprio Google: “O Google grava sua voz e outros tipos de áudio, além de alguns segundos anteriores, quando você usa ativações de áudio, ao dizer o comando ‘Ok Google’” (GOOGLE, 2019).

Ainda segundo o Google (2019), essa funcionalidade permite “ajudar a conseguir melhores resultados usando a voz. O Google usa sua atividade de voz e áudio para:

a) Conhecer o som da sua voz;

b) Saber como você diz palavras e frases;

c) Reconhecer quando você diz "Ok Google";

d) Melhorar o reconhecimento de voz em todos os produtos do Google que usam sua voz.

Ao realizar esta operação, os áudios ficam registrados na URL *https://myactivity.google.com/item?restrict=vaa* e podem ser consultados pelo usuário, dando permissão para que ele ative ou desative a qualquer momento.

Essa funcionalidade não é exclusiva dos *smartphones*. Havia celulares, como o BlackBerry 5810, que executavam comandos simples de voz como ligar para um contato. Interessante abordar neste ponto que os comandos de voz nos celulares funcionavam após o usuário pressionar um botão. Mesmo os *headsets*[41] para realizar chamadas por voz ou executar comandos necessitavam de um toque para ativarem o microfone.

A partir desse momento, o aparelho ativava o microfone e aguardava o comando, o que difere de um assistente virtual que tem a possibilidade de receber comandos de voz sem a necessidade de ser acionado fisicamente pelo seu dono. O que antes era um comando que partia de uma ação ativa do usuário por meio de um comando mecânico, agora passa por uma gerência de *software*.

O texto *Não existe mídia digital. SoftCult*, de Lev Manovich, e traduzido por Cícero da Silva (2011), aborda uma questão interessante sobre o *software*. Essas novas formas de acesso à mídia se dão por meio do *software* e, portanto, as escolhas realizadas pelo algoritmo seguem princípios básicos e protocolos que regem o ambiente da computação moderna. Manovich continua discorrendo sobre o *software* quando fala que as novas formas de acesso à mídia, distribuição, análise, geração e

[41] Aparelho dotado de microfone, fone de ouvido que era acoplado à orelha do usuário e possuía conexão sem fio, permitindo a utilização do celular sem utilizar as mãos.

manipulação só existem devido a ele. Isso significa que elas são o resultado de escolhas específicas realizadas por indivíduos, empresas e consórcios que desenvolvem o *software*.

Essas escolhas, portanto, não são totalmente claras e nem possuem abertas a sua forma de operação para ser auditada, então, isso implica na questão da privacidade. Não somente a opacidade do *software*, mas também os rastros deixados por toda essa interação, como explica Sérgio Amadeu da Silveira (2017), que torna o *software* tão importante para a coleta de dados:

> [...] o envio de informações quase sempre é acompanhado de seu registro. Dados são comunicados gerando dados sobre a comunicação efetuada, ou seja, metade dos são constantemente criados. Os registros do que é feito têm como base esses processos de comunicação e controle. Assim, a comunicação em rede produz rastros digitais que Alexander Galloway comparou com “pegadas na neve” (SILVEIRA, 2017, n. p).

O *Global Positioning System* (GPS) é um “sistema de cálculo de posicionamento baseado no uso de sinais enviados por uma rede de satélites” (n. p MORIMOTO, 2009). A disposição desses satélites está de tal forma que, em qualquer ponto do planeta, ao menos quatro deles sejam visíveis. Desenvolvido em 1965 pelo Departamento de defesa norte-americano, o projeto NAVSTAR tinha como objetivo informar o governo estado-unidense sobre qualquer informação geográfica de qualquer lugar do mundo[42]. Inicialmente, seu projeto era apenas para fins militares, tornando-se disponível para uso civil apenas em 1995. A precisão entre as duas versões, militar e civil, são distintas. A primeira, além de ter um tempo de resposta menor, possui uma acuracidade bem maior que a segunda.

O funcionamento do GPS no *smartphone* somente é possível porque ele possui um receptor de sinal que capta e processa as informações enviadas pelos satélites, como explica Morimoto:

> Os satélites transmitem um sinal de alta freqüência, contendo pacotes de informação com indicações precisas da hora em que cada um foi transmitido. Os receptores em terra captam o sinal e usam um sistema de trilateração para calcular a posição, comparando a diferença de tempo entre a transmissão e a recepção de cada pacote, calculando assim a distância de cada satélite. Conforme você se desloca, a distância em relação aos satélites muda, gerando uma pequena diferença no tempo do percurso, que é usada para atualizar a localização (MORIMOTO, 2009 n. p).

[42] HISTÓRIA do GPS. *In:* História de tudo. Disponível em: https://www.historiadetudo.com/gps. Acesso em: 14 set 2019.

O resultado desse cálculo é a posição em latitude e longitude, e com o quarto satélite, segundo Morimoto, é possível calcular a altitude do dispositivo. Como os *smartphones* possuem placas de GPS com menor acuracidade, a localização baseada apenas por satélite torna-se menor. Para isso, existe o A-GPS, que combina com o sinal emitido pelas redes de telefonia móvel para realizar a triangulação. Em ambientes *Indoor*, a tecnologia *Bluetooth* e a rede *Wifi* podem ser utilizadas como alternativa à A-GPS atuando de forma semelhante.

Diversas aplicações usufruem dessa funcionalidade — navegadores como Waze, Google Maps; jogos móveis como Pokemon Go, Ingress; redes sociais como Instagram, Twitter e Facebook. A junção da geolocalização com conteúdo produzido é a *geotagging*. Segundo Morimoto (2009), ela permite que o conteúdo gerado possa ser vinculado ao exato local que foi produzido, abrindo possibilidades em torno de serviços de compartilhamento de imagens, como o o Flickr, permitindo fazer buscas também por locais ou coordenadas, trazendo como resultado conteúdos produzidos em locais específicos.

Muito além da posição atual, o GPS pode ser utilizado juntamente com *softwares* específicos para armazenar o deslocamento do *smartphone* e, consequentemente, do usuário. Para exprimir essa possibilidade, Teri Rueb, em 2001, realizou a obra *The Choreography of Everyday Movement*. A ação consistia em capturar, armazenar, processar e imprimir o deslocamento dos dispositivos através da variação latitudinal e longitudinal, produzindo um metamapa. Segundo Yeregui (2011, p. 126–127) “através da tecnologia de GPS, o projeto busca tornar visíveis nossos movimentos dentro do ambiente da cidade, pondo em evidência padrões sociopolíticos e visões poéticas acerca do tráfego de informações via corpo urbano”.

Mesmo que puramente performática, a obra de Teri é uma contribuição ao projeto *Loca,* já citado, e nos faz refletir sobre o dispositivo se mover. Se ele é potencialmente móvel, há um corpo que atualiza o seu movimento e, consequentemente, é este corpo que está desenhando o mapa, e não o dispositivo.

O acelerômetro tem como principal função transformar energia mecânica em impulsos elétricos. Muito utilizado nas indústrias, sua aplicação tinha como principal objetivo analisar vibrações em máquinas, a fim de prever possíveis rupturas na estrutura. Na geologia, servia para medir abalos sísmicos. Na área médica, para estudos de movimentos de articulações. Nos dispositivos móveis, inicialmente foi acoplado nos *smartphones*, auxiliando na orientação da tela e fazendo com que o

conteúdo ora fosse exibido na vertical, ora na horizontal. Também pode ser utilizado para tornar os *softwares* mais inteligentes, conforme Morimoto:

> No caso dos aplicativos de GPS, o acelerômetro permite que o software detecte arrancadas e freadas, curvas, e assim por diante, variáveis que podem ser usadas para tornar o *software* mais inteligente, detectando quando você perdeu uma curva ou mantendo uma estimativa aproximada da localização quando perde o sinal dos satélites por alguns segundos, por exemplo (MORIMOTO, 2009, n.p.).

Em ambientes internos ele pode contabilizar a quantidade de passos e, portanto, o deslocamento. Assim é possível calcular e prever quanto tempo uma pessoa esteve se deslocando, por quanto tempo permaneceu parada e qual sua velocidade.

Por atuar nos três eixos, o acelerômetro pode indicar o deslocamento não somente horizontal, mas também vertical. Para tanto, subidas e descidas de elevador e inclinação de terrenos podem ser monitoradas, como mostra as experiências realizadas pelos alunos da Universidade Federal do Rio de Janeiro *Experimentos com o Acelerômetro de Tablets e Smartphones*[43].

A câmera fotográfica, incorporada inicialmente no modelo japonês Sharp J-SH04, passou a estar presente nos dispositivos seguintes, tornando-se indispensável. Com a função de registrar imagens e vídeos nos *smartphones,* ela passa a ganhar novas funções, como ler códigos (de barras ou QRCode[44]).

Inserindo algoritmos de inteligência artificial, como o Google Lens[45], é possível a leitura e interpretação de imagens para realizar buscas, identificar elementos e reconhecer faces, inclusive recomendando amigos para taguear as fotos. Além do registro de imagens, a câmera frontal, principalmente, facilita a realização de videoconferências e transmissões ao vivo, quando o usuário pode transmitir a sua face enquanto visualiza a tela e as informações que estão nela.

---

[43] VIEIRA, Leonardo Pereira; AGUIAR, Carlos Eduardo. **Experimentos com o Acelerômetro de *Tablets* e *Smartphones*.** 2013. Disponível em: https://www.if.ufrj.br/~pef/producao_academica/dissertacoes/2013_Leonardo_Vieira/experimentos_acelerometro.pdf. Acesso em: 19 jun. 2019.

[44] Código de barras bidimensional que pode ser escaneado usando a maioria dos celulares equipados com câmera. Esse código é convertido em texto (interativo), um endereço URL, um número de telefone, uma localização georreferenciada, um e-mail, um contato ou um SMS. (CÓDIGO QR..., 2019c).

[45] Google Lens. Disponível em: https://lens.google.com/. Acesso em: 10 jun. 2019.

Com a possibilidade de produção de informação dos *smartphones* cada vez maior, esses aparelhos passaram a ter maior importância, tornando-se cada vez mais presentes no acesso a *websites* e serviços online. No ano de 2015, o acesso por *smartphones* superou os *desktops,* segundo *o Google (BOAS RAZÕES..., 2015c).* Isso se deu pela criação de *sit*es responsivos com *Bootstrap*[46], por exemplo.

Toda essa mudança gerou uma demanda maior por troca de dados, que podia ser tanto pela rede Wifi quanto pela rede móvel. A velocidade média da Internet 3G oferecida no Brasil era de 1Mbps, mas prometia entregar até 21Mbps. Para se ter ideia, uma videoconferência com um vídeo HD utilizando a plataforma Skype necessita de uma conexão de 1,5Mbps tanto para *Download* quanto para *Upload*.

Para atender essa demanda e o crescente tráfego de dados, chegou a tecnologia 4G. Semelhante à 3G, o foco era no aumento da velocidade de transmissão de dados. No Brasil, a proposta de implementação era para a Copa do Mundo de 2014, aproveitando a banda de frequência que ficaria disponível após o desligamento do sinal analógico da televisão.

O foco da rede 4G era o melhor aproveitamento do espectro de rádio, o que permitia aumentar (e muito) a velocidade de transmissão de dados, chegando até 10x mais do que a 3G. Com isso, a possibilidade de utilização variava de apenas compartilhar conteúdo, até fazer *streaming* de áudio, vídeo, chamadas de voz e de vídeo utilizando a rede de dados. A Claro, no Brasil, consegue entregar a velocidade de 28,5 Mbps[47], enquanto a velocidade da internet doméstica, no terceiro trimestre de 2018, tinha a média de 24,9 Mbps[48].

Esse aumento na velocidade fez o comportamento das pessoas ser alterando após a implementação da rede. Diversas aplicações tornaram-se viáveis, permitindo executar funções que dependiam de uma rede *wireless* doméstica ou *indoor* e agora poderiam ser executadas em espaços abertos. Segundo um estudo da Cisco[49], o tráfego de Internet por dispositivos móveis no mundo saltou de pouco mais de 1,4

[46] *Framework front-end* responsivo.
[47] ESTUDO mostra claro com 4G mais rápido do Brasil; velocidade fica estagnada. *In:* Techtudo. Disponível em: https://www.techtudo.com.br/noticias/2018/06/4g-empaca-no-brasil-velocidade-fica-estagnada-diz-opensignal.ghtml. Acesso em 10 jul. 2019.
[48] VELOCIDADE média da banda larga fixa foi de 24,9 MBPS no 3º tri. *In:* Tele Síntese. Disponível em: http://www.telesintese.com.br/velocidade-media-da-banda-larga-fixa-no-brasil-foi-de-249-mbps-no-3o-tri/. Acesso em 10 jul. 2019.
[49] CISCO Visual Networking Index: Forecast and Methodology, 2013–2018. *In:* Anatel. Disponível em: http://www.anatel.org.mx/docs/interes/Cisco_VNI_Forecast_and_Methodology.pdf. Acesso em: 10 jul. 2019.

exabytes em 2013 para quase 16 exabytes em 2018. Nos primeiros anos da análise o crescimento foi mais modesto, mas o aumento se mostrou exponencial ano após ano.

Com isso, podemos presumir que o ganho de velocidade de Internet propiciou um maior número de troca de dados e de produção também. A variedade, proveniente dos dispositivos ou das aplicações utilizadas, também aumentou. Segundo o estudo da Cisco, 29%[50] do tráfego corresponde à *streaming* de vídeo, 20% acesso à Internet (e-mail e dados em geral), 2% do compartilhamento de arquivos e o restante para jogos.

O volume de dados gerados evidência, também, uma maior adoção das tecnologias móveis para a comunicação e a diversidade da forma de se comunicar. A origem da telefonia celular, que só permitia conversas por voz, evoluiu ao longo dos anos. Sua evolução permitiu, além da conversa, a troca de mensagens de texto, troca de arquivos entre celulares sem mediador, envio e recebimento de e-mails com a chegada das primeiras redes de dados, até o consumo e produção de diversos tipos de conteúdo multimídia – incluindo a voz, desta vez digital – alterando a forma de se comunicar em movimento.

A comunicação móvel, do ponto de vista do dispositivo, por si só, seria imóvel. Ela precisa de um motor, de um corpo em uma situação nômade que a desloque de um ponto ao outro. “O aparelho é móvel em estado potencial: somente um motor (no caso, o corpo em movimento) concretiza essa propriedade latente do objeto” (YEREGUI, 2011, p. 119). Essa afirmação dá-nos a perceber a relação extensiva do corpo no seu mais alto grau[51] e reflete a relação homem-dispositivo:

> O sujeito se move pelo espaço com dispositivos capazes de estabelecer comunicações bi e multidirecionais (mais de um aparelho de registro visual e sonoro). Esses dispositivos tecnológicos são terminais, ou seja, situados na periferia e distantes de uma unidade central, e que permitem a saída dos dados solicitados ao sistema global, em que o usuário, mediante um teclado ou outra interface, pode incluir dados. Os terminais são – em um sentido físico, como reminiscências fisiológicas – extremidades. Esses terminais supõem a existência de uma rede. Invisível e selada por um processo dinâmico de polimorfia, a rede é um metamapa (mais do que um simples mapa, uma estrutura que engendra o mapa), em que são construídas situações físicas concretas, dinamicamente definidoras do território. Através da rede, são transportados múltiplos trajetos e itinerários de fluxos de dados [...] (YEREGUI, 2011, p. 121–122).

[50] Ibid.
[51] “Tecnologia extensiva como aquela que opera como prolongação, potencializando funcionalidades e atributos inerentes à corporeidade humana” (YEREGUI, 2011, p. 120).

Ou seja, o dispositivo é um ponto terminal que permite a inserção e o consumo de informações por meio da sua interação. Isso nos permite dizer que há produção de conteúdo nestes dispositivos, e a partir destes:

> Tratar-se-ia das entradas e das saídas de dados, dos processos de intercâmbio, das relações que são construídas no seio da rede, da interação com bases de dados, dos fenômenos de retroalimentação, etc., que definem uma morfologia não tão nítida como a de um itinerário espacial poderia ser (YEREGUI, 2011, p. 123).

Lemos (2011, p. 10) completa:

> A passagem do computador pessoal para os dispositivos portáteis, nos quais confluem o GPS, a telefonia e o audiovisual, remete-nos à produção e à recepção de textos, imagens e sons, aos mecanismos de controle e rastreio e à formação de redes sociais reconfiguradas para os dispositivos locativos.

O desenvolvimento da computação sem fio, pervasiva e ubíqua, como consequência da popularização dos telefones celulares e conexões sem fio (como Wi-fi, Wi-max e *Bluetooth*) proporcionou o surgimento de uma nova fase dentro da sociedade da informação, já iniciada na década de 70 (LEMOS, 2005). “A cibercultura (...) solta as amarras e desenvolve-se de forma onipresente, fazendo com que não seja mais o usuário que se desloque até a rede, mas a rede que passa a envolver os usuários e os objetos numa conexão generalizada”.

Se analisarmos essa mobilidade comunicacional feita por dispositivos informacionais, acabamos por criar os “primeiros endereços não territoriais” (LEMOS, 2011), fazendo com que o sujeito tenha um ponto de recebimento e envio de informações nômade.

> (...) os indivíduos “carregam” consigo seus próprios territórios. Algo disso está se tornando aparente pelo uso crescente de celulares, laptops e memórias móveis, o que permite a cada um levar junto de si sua própria biblioteca e ter comunicação e acesso imediatos sem qualquer referência com a localização (KELLERMAN, 2006, p.64 apud LEMOS, 2011, p. 23).

Toda essa produção informacional ubíqua, pervasiva e, muitas vezes, correlata ao local em que é produzida, proporciona a produção de uma gama informacional enorme: o dado e o metadado. Diferentes experiências artísticas mostram como o uso dos dispositivos de comunicação móvel, que acolherão o *corpus* deste estudo,

permitem que se faça metamapas[52] performáticos, resultantes da utilização de dispositivos móveis.

Lemos (2010) aborda a forma com que a ubiquidade, criada pela onipresença da Internet e dispositivos que se conectam a ela, criou zonas de controle informacional – que ele chama de "território informacional" – e como isso afeta a nossa privacidade:

> O território informacional pode ser pensado como uma nova heterotopia (...) criando funções informacionais (digital/telemática) no espaço físico a partir de banco de dados e dispositivos eletrônicos. Esse território informacional é percebido por autores como "território digital ou bolha" (...), "espaço intersticial" (...), "realidade híbrida, aumentada ou cellspace" (...), "virtual Wall" (...). Em todas essas concepções, o que está em jogo é o controle (territorialização) informacional e, consequentemente, uma nova função dos espaços (públicos e privados). (...) Compreender os novos territórios é fundamental para visualizar os impactos das mídias locativas sobre a privacidade e o anonimato ameaçados por novas formas de controle, monitoramento e vigilância (LEMOS, 2010, p. 4).

Assim, interações que realizamos no nosso dispositivo móvel, em movimento, pode entregar muito mais do que o que estamos executando nele. Somando os *hardwares* presentes e apresentados, acelerômetro, GPS, câmera, microfone e *Bluetooth*, nossos metadados gerados são utilizados como insumos para publicidade e, ao serem analisados, desenham um mapa do nosso comportamento e hábitos extremamente detalhado. Levando em consideração a quantidade de dispositivos móveis presentes no Brasil, a área de cobertura e a crescente cobertura da tecnologia 4G, podemos deduzir que a capacidade de monitoramento e vigilância em massa é presente no cotidiano.

[52] Metamapa para fins de estudo se basearão como uma estrutura referenciada à Deleuze e Guatarri por Yeregui (YEREGUI, 2011).

3 PRIVACIDADE E PRIVACIDADE DIGITAL

Como abordado no capítulo anterior, a massificação da forma de produção de informação e coleta de dados através dos dispositivos móveis pode gerar uma pintura digital, duplo digital, ou ainda identidades projetadas de forma automática, ampla e onipresente. Por propiciar uma visão macro (comportamento coletivo) e uma visão micro (como um indivíduo se comporta), vale entender como se caracteriza a privacidade, de modo geral, e também a privacidade digital, a fim de encontrar quais pontos podem ser considerados como invasão e exposição do indivíduo por meio das informações produzidas por pelos dispositivos.

3.1 PRIVACIDADE

Inicialmente, trago o conceito de privacidade no seu sentido mais básico e primitivo para embasar esta discussão. Segundo Konder (2014) a privacidade, apesar de ter seu conhecimento familiarizado, sofreu dramáticas modificações de significado conforme as circunstâncias históricas. Assim, é preciso sempre analisar o contexto no qual a sociedade está inserida para que se faça uma abordagem adequada de tal termo, pois ela – a privacidade – serve como um “termômetro” que indica os valores, desejos e medos desta sociedade enquanto um direito civil.

O marco inicial na história da privacidade, e que embasa um dos pilares deste projeto de pesquisa, é o caso *Manola vs Mayers* (KONDER, 2014, p. 356), de 1890. Nesse embate, a atriz Marian Manola, ao ter suas roupas íntimas fotografadas pelo fotógrafo do *The New York Times*, Myers, moveu uma ação contra ele. Os juristas da época, Warren e Brandeis, publicariam, naquele mesmo ano, um artigo no qual divulgavam a privacidade como um “amplo direito de ser deixado em paz”. Nessa perspectiva, a privacidade mantinha sua atuação sobre a proteção jurídica para promover a proteção da imagem, do sigilo profissional, de comunicações, de transações bancárias e a inviolabilidade do domicílio (KONDER, 2014). Ainda segundo Konder, toda essa proteção visava proteger o indivíduo da imprensa, que acabara de ganhar maior notoriedade na sociedade civil daquela época.

O conceito de “ser deixado em paz”, em resumo, significava a possibilidade de não ser exposto, ou de permitir que apenas parte das informações fossem divulgadas – apenas o que não causasse constrangimento ou preocupação legítima. A decisão

sobre o que deve ser divulgado parte de quem diz respeito a informação produzida, independente do *status* ou posição social, portanto, um direito fundamental e universal. Esse conceito, segundo Warren e Brandeis (1890), vai além da privacidade burguesa, que assegurava a privacidade do tangível como invasão da propriedade privada. A proteção da privacidade vai para o âmbito imaterial, intangível, dando paz aos interesses espirituais (SALDAÑA, 2012 apud BOFF; FORTES; FREITAS, 2018).

No entanto, a definição de privacidade cunhada por Warren e Brandeis começou a ser questionada, entre as décadas de 60 e 70, após diversas pessoas reclamarem que sua privacidade havia sido corrompida e exigirem que as violações fossem examinadas. Isso se deu pelo fato de a sociedade estar passando por mudanças, exigindo maior cooperação entre as pessoas. Elas deveriam reter informações sobre outras, tornando quase que impossível um indivíduo passar despercebido, sem nenhuma informação sua circulando. Isso ocasionou um questionamento sobre o conceito de privacidade, conforme as palavras de Warner e Stone (BOFF; FORTES; FREITAS, 2018). Segundo eles, o direito à privacidade não podia ser um estatuto imutável, mas sim algo que respeitasse as diferenças e espaços, e estaria diretamente ligado com o que representaria um anonimato.

Tapper (1973, apud BOFF; FORTES; FREITAS, 2018), na década de 70, faz uma visão mais contemporânea sobre a privacidade e aponta duas possíveis formas da sua violação: coleta de informações e a utilização delas. A coleta de informações dividia-se em duas, sendo a primeira de forma lícita – quando o indivíduo as cede voluntariamente. A segunda, de forma ilícita, é extraída sem que a pessoa saiba. O segundo ponto refere-se à utilização dessa informação, tanto na forma quanto no efeito causado naquele que a forneceu. Isso dá-nos uma clareza do que seria uma violação de privacidade, além de ser amplamente útil para o nosso estudo num ambiente digital.

A fim de perceber as diferentes interpretações do termo, concebo como fundamental a análise que se faz sobre o que é considerada privacidade nos estados norte-americanos. Tapper (1973, apud BOFF; FORTES; FREITAS, 2018) afirma que a privacidade consiste no direito de a pessoa fazer escolhas significativas para sua vida sem a interferência de terceiros. Complemento também com a visão da ONU, na Assembleia Geral das Nações Unidas de 1966, sobre a privacidade: o documento afirma que nenhum indivíduo deve ser objeto de interferências arbitrárias na vida privada, familiar e domiciliar. Analisando as duas interpretações, elas dizem muito a

respeito do controle e prezam pela total autonomia dos cidadãos frente às tecnologias. As tecnologias em questão não são apenas as mais recentes, conforme os autores Boff, Fortes e Freitas (2018). As possibilidades da tecnologia da época, meados de 1890, começaram a perturbar e pôr em risco a intimidade dos indivíduos frente à imprensa, o próprio fotógrafo ou qualquer outro que possuísse tal aparato tecnológico que reproduzir imagens ou sons.

O zelo pela privacidade acabou por criar uma espécie de membrana informacional que controla o fluxo de informação surgindo sob esferas privadas em modelos de círculos concêntricos: uma primeira, restrita na intimidade acessível somente à pessoas muito próximas, e uma esfera mais fechada que consistia o segredo máximo a qual somente o seu titular possuía acesso (KONDER, 2014). Neste contexto a privacidade consistia em oferecer alguma solução contra a circulação não autorizada de fotografias pessoais a fim de evitar um possível sofrimento espiritual e angústia (BOFF; FORTES; FREITAS, 2018). No ambiente das redes sociais, vimos esta permeabilidade pelas configurações de privacidade o qual o usuário escolhe um alcance, dentre as possibilidades que a plataforma disponibiliza, das suas informações.

A privacidade nos meios digitais, em um primeiro momento, era tratada de forma semelhante à imprensa, protegendo os indivíduos da divulgação de fatos privados que pudessem ocasionar constrangimento ou dano moral e que fossem obtidos por métodos questionáveis (LINS, 2000). Porém, com a Internet, a situação reconfigura-se e a definição de privacidade precisa passar por um novo olhar. Lins (2000) já apontava que a disseminação das tecnologias, tanto de captura como também de tratamento e análise de dados, potencializava a disseminação e reprodução das informações de forma massiva, muito mais rápido do que na imprensa tradicional. Assim, a preocupação que antes era somente pela circulação da informação, ganha outros aspectos também apontados por Lins: a estruturação das bases de dados, a disseminação da informática e a padronização dos equipamentos e sistemas.

Dos três pontos citados por Lins, abordarei, mais adiante, o primeiro – a estruturação dos bancos de dados – mas aqui chamo a atenção para os dois últimos. A disseminação da informática, neste projeto, podemos relacionar à popularização dos *smartphones* que, como já mencionado, está cada vez mais presente na sociedade e executando uma variedade maior de tarefas, tornando-nos dependentes.

Já a padronização dos equipamentos e sistemas pode ser relacionada às duas grandes empresas que produzem os sistemas operacionais que rodam nos dispositivos móveis, a quase que hegemonia de certos aplicativos nos *smartphones*.

Lins também classifica as formas de ter a privacidade invadida na Internet: coleta de informações diretamente no computador do usuário; coleta de informações no *hardware* de transferência de dados entre teclado/mouse e computador; coleta de informações por meio de um terceiro computador (servidor que presta serviço de acesso à Internet, por exemplo); coleta ou compra de informações por terceiros sem o consentimento do usuário; violação da comunicação por meio de dispositivo de escuta ou interceptação; uso ou roubo de senha, a fim de entrar em alguma rede e obter conhecimento sobre o conteúdo inserido nela.

3.2 PRIVACIDADE DIGITAL

As diversas definições e aplicações da privacidade em um mundo "*offline*" ocorrem também no ambiente "*online*", conforme vimos acima. Para isso, atentarei para algumas visões e definições que se aplicam ao presente trabalho. Começo com a visão que Rohrmann (2000), que entende a privacidade como a forma em que os dados pessoais são disponibilizados, protegidos de ataques, vazamentos ou interceptações. Essa visão, porém, limita-se à proteção dos dados, mas não aborda a utilização desses, a fim de atingir um objetivo. Assim, trago o conceito de Rodotá (2008), ao afirmar que o sujeito não deve ter o seu dado utilizado como forma de colocá-lo em situação de vigilância, ou ter seus hábitos e movimentos perfilados, fazendo com que a sua autonomia de escolha seja comprometida. Assim, acredito que abrangemos dois importantes aspectos sobre a privacidade do indivíduo no ambiente digital: a sua proteção contra exposição involuntária por meio de ataques a bancos de dados e outra contra a utilização massiva do cruzamento dos seus dados, permitindo o esquadrinhamento de seu perfil e possíveis implicações.

No Brasil, no ano 2000, pelo menos, não havia uma legislação clara que abordasse a proteção dos dados. A Lei n. 9.296, de 1996, dava suporte apenas à proteção contra interceptação dos dados transmitidos entre o emissor e receptor, proveniente da forma de comunicação massivamente analógica da época. Na telefonia móvel, o cuidado com o conteúdo transmitido foi uma das grandes preocupações em cada etapa da evolução da rede de telefonia móvel, tornando mais

necessária a mudança do sinal analógico para o digital e da inserção de criptografia dos dados trocados. Com o Marco Civil da Internet, sancionado pela então presidenta Dilma Roussef em 2014, criou-se a responsabilidade pela proteção dos dados armazenados em bancos de dados, protegendo o usuário da Internet de invasões, venda e fornecimento de seus dados sem o seu consentimento, responsabilizando as empresas caso as devidas medidas não fossem tomadas para evitar infrações aos dados dos seus usuários.

Voltando a atenção para o objeto de estudo deste projeto – os *smartphones* – a nossa atenção às novas preocupações em relação à privacidade torna-se pertinente sob aspectos específicos e distintos. O seu alto poder de processamento permitiu a convergência de múltiplas funções – anteriormente divididas em outros aparelhos, como *desktop*, *palmtop*, agenda, secretária eletrônica e navegador GPS – em um mesmo dispositivo. Isso acarretou numa produção de dados e informações, como já abordamos no capítulo anterior, de forma diversificada e em um volume muito maior. Algumas dessas funcionalidades dependem de acessos especiais a *hardwares,* como GPS, microfone e câmera fotográfica, e depende do usuário para permitir ou não. Sob uma ótica da construção dessas aplicações, o indivíduo fica refém dos termos de uso e permissões que as empresas o forçam a aceitar para fornecer seus serviços. Algumas dessas permissões, de fato, fazem sentido (como geolocalização para fornecer o caminho mais curto entre dois pontos). Outras, porém, são questionáveis (como a solicitação de acesso à galeria de imagens, por exemplo, para um game de palavras cruzadas).

Um exemplo do uso sem a ciência do portador foi revelado em abril de 2019[53] quando pesquisadores do Instituto Internacional de Ciências Computacionais (ICSI), do IMDEA *Networks Institute*, da Universidade de Calgary e da empresa AppCensus auditaram mais de 83 mil aplicativos presentes no Google Play[54] e identificaram mais de 13 mil programas que burlavam as permissões concedidas pelos usuários.

Os dados eram obtidos por esses aplicativos a partir da extração não autorizada de arquivos armazenados em *cache*[55]*.*

---

[53] NÃO é só o FaceApp, milhares de aplicativos espionam o usuário mesmo sem permissão. *In:* El Pais. Disponível em: https://brasil.elpais.com/brasil/2019/07/18/tecnologia/1563452146_195128.html. Acesso em: 17 ago. 2019.

[54] Google Play é uma loja de aplicativos que permite usuários de Android baixar e instalar aplicativos nos seus smartphones.

[55] Cache é um tipo de arquivo que armazena informações que são utilizadas com maior frequência no dispositivo, fazendo com que a recuperação seja mais rápida ou não consuma o pacote de dados.

Seja por acessos do tipo *side channel*[56] ou *covert channel*[57] os dados eram obtidos sem o consentimento – e o pior, sem a ciência do usuário. Isso mostra o quão vulnerável os usuários estão ao instalarem diversas aplicações nos seus *smartphones,* sem a preocupação com dados sensíveis presentes nele. Nesse estudo, o principal objeto de captura eram os dados geográficos que eram utilizados com a finalidade de alimentar bancos de dados. Cruzando com o IMEI[58], pode-se saber precisamente quem é o usuário e auxiliar a montar o perfil ideal para segmentar os anúncios.

Outro ponto que nos chama a atenção em relação à privacidade e dispositivos móveis é o comportamento do usuário e como a informação passa a ser produzida. Um indivíduo que, anteriormente, estava preso em lugar estático por estar, necessariamente, dependente de cabos, agora torna-se móvel. Se em outros tempos ele dividia seu computador com outros integrantes da mesma casa, agora dificilmente empresta o *smartphone* para outra pessoa, permitindo muita associação somente a uma pessoa. Essa montanha de dados fornece uma gama de informações para diversos bancos de dados, alguns restritos e outros compartilhados. Conforme a utilização do dispositivo aumenta, também cresce a quantidade desses dados, traçando, em questão de algum tempo, o perfil de cada usuário dentro dessas bases de dados.

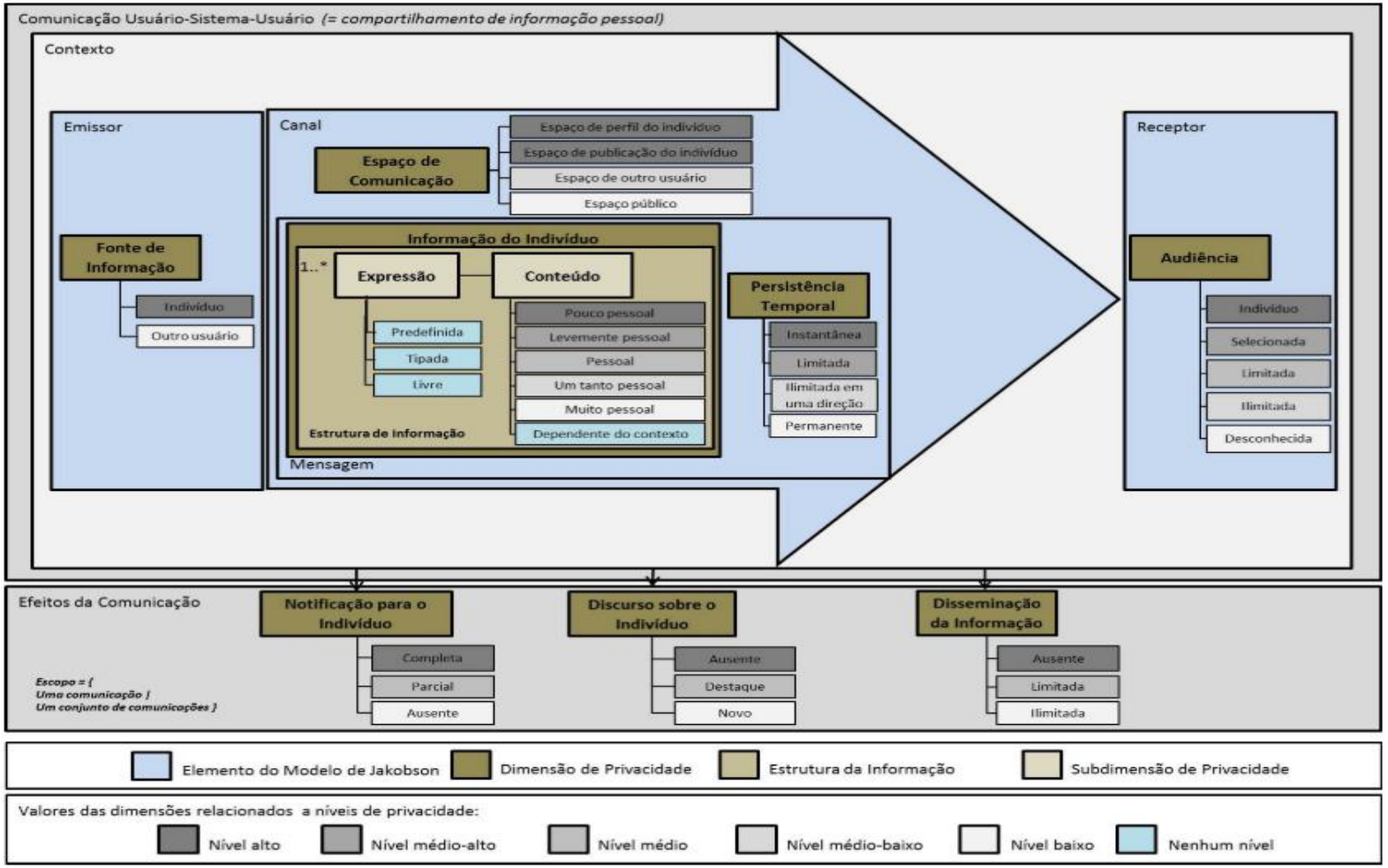
O fato de termos um objeto tão pessoal, conectado, com alto poder computacional e que executa tarefas rotineiras essenciais – do despertador ao comunicador – tornamo-nos parte dele. O *smartphone* passa a ser o nosso *self estendido*[59]*,* carregando consigo toda essa gama informacional. Nossos dados mais sensíveis estão nele e são gerados por ele. Eu não consideraria o dispositivo móvel como sendo uma “extensão do eu” pois trocamos eles após algum período. O que eu levo como, de fato, a propagação da identidade, seria o *login* necessário para acessar o histórico de aplicativos presentes em cada sistema operacional. A Apple e o Android, na sua fase de instalação, sugerem que o portador faça ou efetue o *login* a fim de recuperar as suas informações – aplicativos instalados, senhas armazenadas, contas

[56] Acesso através de vulnerabilidades presentes no *smartphone*.
[57] Acesso através de aplicações de terceiros.
[58] IMEI (*International Mobile Equipment Identity*) número de identificação único e global que identifica o celular globalmente.
[59] Termo formulado em 1998, por Belk, para definir os impactos dos artefatos tecnológicos na forma com que consumimos, comportamos, apresentamos etc. (MARTINS; OLIVEIRA; CORSO, 2018).

de e-mail, fotos, entre outros – antes de finalizar a configuração inicial do sistema. Tal processo, por sua vez, recupera todas as informações e trackeia, de certa forma, o usuário nas suas constantes trocas de dispositivo. Assim, os dados não se perdem e tornam-se atualizados a cada nova interação, não havendo a possibilidade de o usuário optar por não executar tal ação.

Fica evidente que a parte mais frágil dessa relação é o usuário final, assim, torna-se necessário pensar e refletir em formas de equiparar tal desequilíbrio de permissões. Para fornecer embasamento à proteção do usuário, Villela (2016) apresenta um Modelo de Design de Privacidade (MDP) fundamentado na teoria da privacidade e proposto por Atlman e na Engenharia Semiótica. Esse modelo considera como informação pessoal não somente aquela sobre o indivíduo explicitamente revelada, mas também toda informação derivada de análise de discursos e atividades dentro do sistema. Para Villela, um modelo de privacidade ideal é aquele cujo usuário tem o total controle sobre a sua privacidade, e que cada mudança no acesso ou restrição da informação seja executado no exato momento. As definições do que deve ser ou não compartilhado segue a premissa da privacidade, em que o usuário é quem define o que será ou não publicado e com quem será. Esse modelo atua também no controle do alcance do discurso e conteúdo publicado não somente aos dados produzidos por interações na plataforma. A imagem abaixo exemplifica a dinâmica da privacidade, mostrando que o usuário possuiria total controle sobre o alcance das suas informações em todas as etapas da comunicação: da fonte, passando pelo canal e até a chegada ao receptor.

Figura 3 - Estrutura do Modelo de design de privacidade



Fonte: Villela (2016, p. 36).

Muito além da preocupação sobre o escopo que as informações são visíveis, proposto pelo MDP, percebemos a importância do dado produzido quando Schneier (2015) afirma que um dado, sozinho, revela muito sobre nós, mas que o metadado[60] possibilita, ao ser analisado, conhecer muito mais do nosso comportamento, por possuir uma gama de informações amplamente relacional. Ou seja, esses metadados, ao serem combinados uns com os outros e relacionados, tornam possível a identificação de padrões que dificilmente nós teríamos ciência. Assim, o histórico de ligações telefônicas, se analisado por um algoritmo, poderia revelar traços de personalidade, comportamentos e situações não somente de quem está efetuando a ligação, mas também de quem está recebendo. Schneier (2015) traz como exemplo um estudo realizado pela Universidade de Standford, no qual 500 voluntários tiveram seus metadados analisados. Foi analisada a natureza das ligações e alguns perfis resultantes mostraram a relação das pessoas com os locais e o que isso poderia revelar sobre elas. Uma situação como esta mostra a potencial exposição não apenas de um indivíduo, mas de toda uma rede que se relaciona com ele. Como Tapper (1973, apud BOFF; FORTES; FREITAS, 2018) menciona, a forma que esses dados são utilizados também afetam a privacidade do indivíduo. A utilização indevida pode afetar o visitante, expondo-o em situações embaraçosas pelo fato de alguns sites comercializarem os dados de seus frequentadores a terceiros. Pereira, citado por Gregori e Hundertmarch (2013), afirma que a exposição é causada pelo sistema informatizado de computadores, permitindo que haja um esquadrinhamento das pessoas, devassando a sua individualidade. O autor prossegue e afirma que quanto maior a facilitação da tecnologia pela comunicação, maior a possibilidade que estes bancos de dados desvendem a vida do usuário sem a sua autorização e, até mesmo, sem o seu conhecimento.

As novas tecnologias da informação são as grandes responsáveis pela geração e coleta dos metadados. Aproveitando-se da ubiquidade e da computação pervasiva, elas conseguem ficar invisíveis – por puro efeito psicológico (WEISER, 1991 apud BOFF; FORTES; FREITAS, 2018) – levando-nos a absorver informações e executar diversas operações em variados dispositivos, sem a ciência disso. Nesse mesmo caminho, há diversos desenvolvedores atentos em produzir aplicações e *softwares,* a

[60] Metadados são informações que acrescem aos dados e que têm como objetivo informar-nos sobre eles para tornar mais fácil a sua organização. O que são metadados. *In:* Safernet. Disponível em: https://new.safernet.org.br/content/o-que-são-os-metadados. Acesso em 11 ago. 2019.

fim de se aproveitarem dessa gama informacional que pode ser produzida pelos aparelhos móveis.

Esses *softwares* são oferecidos como serviços facilitadores para a nossa vida prometendo entregar conteúdo relevante, e também utilizam fortemente a estrutura de *hardware* e *software* presente nos *smartphones*. O Waze, por exemplo, possui diversas patentes registradas[61] que demonstram a coleta de informações mesmo enquanto o *smartphone* não está sendo utilizado ou a tela está desligada.

No Google Chrome, por exemplo, ao realizar uma busca pelo termo *Café* pelo *Smartphone,* o navegador montou a seguinte URL: https://www.google.com/search ?q=Caf%C3%A9&oq=Caf%C3%A9+&aqs=chrome..69i57j0l3.1601j0j4&client=ms-android-motorola&sourceid=chrome-mobile&ie=UTF-8. Nela, há identificadores que mostram qual o tipo de dispositivo que estou acessando, qual é o sistema operacional e também o fabricante.

Em paralelo, realizei a mesma pesquisa pelo navegador do meu *laptop* e a URL gerada é bem mais simples: https://www.google.com/search?q=Caf%C3% A9&oq=Caf%C3%A9&aqs=chrome.0.69i59l2j0l4.784j0j4&sourceid=chrome&ie=UTF-8**.** A necessidade de entregar conteúdo baseado em geolocalização é uma das formas de tornar o conteúdo relevante, assim, informações como essa se tornam fundamentais tanto para um motor de busca quanto para anunciantes.

A coleta mais expressiva de dados em um dispositivo móvel, como mostrado no exemplo anterior, faz necessário revisitarmos o modelo proposto por Altman sobre privacidade, já citado neste estudo. A ideia consiste em criar uma forma de manter sob controle constante a quantidade de informações divulgadas, empoderando o usuário e dando a ele a escolha de explicitar o que deseja. Tal modelo foi pensado para as redes sociais, mas em um cenário digital, podemos nos apropriar desse funcionamento para a comunicação móvel. Deixar claro para o usuário do dispositivo quais são as empresas que detém suas informações, qual a forma que os dados são utilizados, revogar o acesso à informação para determinadas empresas, são formas que permitem uma equidade de relação entre as partes.

A finalidade de tanta coleta de informação, segundo Lins (2000) se dá pelas grandes empresas para fins comerciais, oferecendo enorme vantagem competitiva sobre os seus concorrentes. No entanto, a prática não é somente dos anos recentes.

---

[61] *Vehicle traffic management*. Google Patents. Disponível em: https://patents.google.com/patent/KR101820575B1/en. Acesso em: 19 ago. 2019.

Cate (1997) lembra outras formas mais antigas de coleta e cruzamento de dados por atividades usuais, como cartórios, hospitais, bancos, empresas de telefonia, provedores de internet e operadores de cartão de crédito. O que muda para o cenário atual é, como já dito, a disseminação dos dispositivos e ferramentas de coletas, dos bancos de dados, do cruzamento entre eles e a construção de perfis que revelam características do usuário que nem ele mesmo possa saber.

O cruzamento desses bancos de dados torna-se um perigo à privacidade quando conceitos como *Big Data* chegam para trazer inteligência e visibilidade para toda a gama informacional armazenada. Com formas cada vez mais complexas de analisar os dados, é possível revelar uma série de informações que expõem os indivíduos nos mais diversos ambientes, provocando sérias consequências. Um dos casos evidentes é o da varejista norte-americana Target. Segundo Boni (2019), tal empresa identificou uma série de produtos que eram consumidos por mulheres que estavam grávidas. Dotados dessas informações, eles criaram uma estrutura de algoritmos capaz de prever possíveis indícios de gravidez e, assim, passaram a oferecer produtos para mulheres potencialmente grávidas. O código foi tão eficaz que causou constrangimento em uma família, ao ter um pai furioso presente em uma das lojas acusando a empresa de “incentivar sua filha a engravidar”. Pouco tempo depois, o pai da garota se desculpou porque, de fato, sua filha estava grávida.

Casos como esse não são isolados. As empresas que detém uma base considerável de dados, aplicada aos princípios da *Big Data*[62], obtém vantagem competitiva diante das empresas que não aplicam – e, principalmente, exercem controle sobre seus clientes. Boff, Fortes e Freitas (2018) trazem um estudo intitulado *“Unique in the shopping mal: On the reindentifiability of credit card metadata”*. No estudo, foi apresentado um algoritmo matemático que era capaz de identificar um indivíduo a partir de seus metadados anônimos, obtidos em decorrência de compras realizadas com cartão de crédito dentro de um *shopping* – não sendo necessário efetivar mais do que três compras para isso.

Esse estudo mostra o poder que a análise de dados tem para identificar indivíduos em um oceano informacional. Boni (2019), por sua vez, nos traz uma forma de tornar os dados identificáveis em não pessoais, a fim de tornar mais plausível uma sensação de privacidade diante deste cenário de bases de dados estruturadas. Para

[62] Os 4 V’s da *Big Data* são: volume, variedade, velocidade para transmitir e veracidade das informações.

ele, devemos identificar quais elementos podem ser modificados, suprimindo-os ou generalizando para que o grau de identificabilidade seja eliminado ou reduzido:

a) Não armazenar os cinco primeiros dígitos do CPF;

b) Generalizar os nomes completos. Manter apenas o prenome (para personalizar mensagens em e-mails, por exemplo);

c) Remover os três últimos dígitos de CEP, permitindo que haja uma noção de localização, mas não a mais próxima.

d) Categorização etária em vez de inserir a idade da pessoa, para evitar a sua individualização em meio a um universo de contatos.

As estratégias exemplificadas por Boff não garantem a total segurança do indivíduo, mas são formas de criar um equilíbrio entre a indústria da publicidade, que tanto depende dos dados para criar segmentações e anúncios relevantes, e os indivíduos, que são a parte mais frágil da relação. O autor ainda afirma que essa não é uma fórmula definitiva, mas que deve ser repensada e aplicada para cada contexto. O que ele garante é a irreversibilidade dos dados, uma vez que é mais difícil inserir dados que não podem ser inferidos – não há como adivinhar os cinco primeiros dígitos do CPF, por exemplo.

Dada esta discussão, podemos perceber que a privacidade, na sua função inicial, tinha como proteger o indivíduo das ferramentas de captura e reprodução de informação da época – como imagens, sons e discursos – que a imprensa detinha. Num segundo momento, passou a reger a relação entre as pessoas, criando círculos de confidencialidade no qual o indivíduo escolhia as pessoas que desejaria compartilhar determinada informação. Num terceiro momento, já com os dispositivos móveis, podemos ver que o controle pelas informações produzidas pelos aparelhos torna-se mais importante para governos, empresas e desenvolvedores, e também vemos que o usuário perdeu o controle sobre a coleta e utilização de seus dados. Isso abre precedentes para a exposição pública da intimidade, possibilidade de monitoramento, vigilância, controle e perda da autonomia.

4 MONITORAMENTO E VIGILÂNCIA

Discutir a definição das terminologias monitoramento e vigilância é fundamental para este estudo. Esses conceitos, ao serem diretamente contextualizados em uma sociedade da informação, tornam-se pertinentes, uma vez que ficam potencializados pelo uso massivo da tecnologia móvel. Lemos (2010) faz uma excelente referência a uma fala de Gow, ao afirmar que a principal qualidade de uma sociedade ubíqua e conectada é a capacidade de ser invisível e pervasiva. Portanto, no cenário que estamos inseridos – de um protocolo 4G migrando para um 5G "da internet das coisas" – torna-se cada vez mais importante questionarmos e debatermos esses termos.

4.1 MONITORAMENTO

André Lemos (2010) define monitoramento como uma forma de observação cuja função é acumular informações e criar projeções futuras ou cenários históricos (passado e futuro). Em resumo, trata-se de "uma ação de acompanhamento e avaliação de dados" (LEMOS, 2010, p. 623). Esse movimento, no entanto, não implica necessariamente em uma tomada de ação a fim de punir, remediar ou propiciar algo ao sujeito monitorado. Esse acúmulo é resultante das trocas comunicacionais entre indivíduos, ou entre indivíduos e máquinas, realizadas principalmente por meios digitais. As "pegadas na neve", cada vez mais presentes nos ambientes informacionais, permitem que os dados dos usuários sejam coletados diversas vezes e – o que torna mais perigoso – sem o consentimento ou conhecimento dele. Em virtude da ubiquidade e dos dispositivos móveis, esses espaços acabam por permitir a territorialização da informação, sendo essa um híbrido entre o que está armazenado nos bancos de dados e a sua relação com os espaços reais (LEMOS, 2010).

Lemos (2010) aborda a importância das mídias locativas como um dos motores para o monitoramento das massas. Para ele, a possibilidade das produções de conteúdo e das interações aliadas à geolocalização como *geotagging*, fotos, vídeos e GPS's, que utilizam a localização do dispositivo como insumo para o funcionamento, permitem que essas informações produzidas sejam armazenadas e, assim, utilizadas para monitorar o sujeito. Conforme Lemos (2010, p. 629) ainda aborda, "mais movimento significa também maior possibilidade de controle, vigilância e monitoramento de pessoas, informações e objetos". Com isso, há motivações claras

para que aplicações móveis desenvolvam métodos que permitam a coleta de dados e a ativação de *hardwares* de GPS mesmo com a tela desligada. O Waze, conforme abordamos anteriormente, registrou diversas patentes que explicam o funcionamento dessa coleta de dados “em segundo plano”[63]. Jogos locativos como Pokemon Go, o Ingresse, e até mesmo aplicativos que permitem publicações relacionadas à locais como Foursquare, Facebook e principalmente o Instagram, fazem com que seja essencial a habilitação do GPS durante sua utilização.

Seguindo na linha de monitoramento baseado apenas na localização, há diversos tipos de informação que se pode extrair após um volume considerado de dados: residência do indivíduo, local de trabalho, hábitos de consumo e de lazer, entre outras. Todas essas informações podem ser inferidas cruzando o padrão de deslocamento com o horário, o tempo de permanência e a frequência desses mesmos pontos durante o período observado. Esse movimento de análise dos metadados geográficos é muito semelhante ao estudo realizado pela universidade de Standford, trazido por Schneier (2015) e já mencionado neste projeto.

Como anteriormente também abordei, se antes as redes telefônicas conseguiam ter, com precisão considerável, a nossa posição em troca do sinal telefônico, agora o poder de saber a nossa localização está nas mãos das empresas presentes nos nossos dispositivos móveis. Sejam os desenvolvedores dos *smartphones*, como Google e Apple, ou através das principais empresas responsáveis pelos aplicativos instalados na maioria dos dispositivos, como Facebook, Amazon e o próprio Google.

As coletas de dados geográficos são realizadas, como já apresentado, majoritariamente, pela utilização do GPS, atuando com eficiência para ambientes externos. No entanto, para ambientes internos, são desenvolvidas as tecnologias de *Beacons*[64] que, por sua vez, possuem uma precisão de centímetros. A publicação realizada pelo The New York Times[65] intitulada *Em lojas, a vigilância escondida rastreia cada movimento seu*[66] relata as táticas que algumas lojas dos Estados Unidos

[63] Segundo plano significa executar um código em paralelo a outras aplicações principais do dispositivo, ou mesmo quando está com a tela desligada.
[64] Beacons são tecnologias que funcionam por *Bluetooth*, permitindo a localização de dispositivos celulares em espaços *indoor*.
[65] KWET, Michael. In Stores, Secret Surveillance Tracks Your Every Move. The New York Times. Disponível em: https://www.nytimes.com/interactive/2019/06/14/opinion/bluetooth-wireless-tracking-privacy.html. Acesso em: 05 out. 2019.
[66] In stores, secret surveillance tracks your every move (tradução nossa).

aplicam para rastrear os consumidores. Os Beacons instalados em diversos pontos da loja verificavam a intensidade do sinal *Bluetooth* de cada dispositivo e, ao identificarem a permanência de dois minutos em frente a um ponto específico, enviavam a informação para uma central que analisava os dados e oferecia, logo que o consumidor deixasse a loja, um cupom de desconto para compra daquele produto. Importante destacar que a loja em questão havia disponibilizado um aplicativo para ser instalado no *smartphone* que, além das funcionalidades de mostrar produtos e promoções, podia gerenciar o *hardware Bluetooth* e exibir as informações que a central de *marketing* enviava para o dispositivo.

A intensidade da coleta de dados geográficos, revelado por outro artigo do NYT intitulado *Seus aplicativos sabem onde você esteve na noite passada e não mantém isso em segredo*[67] é assustadora. A notícia conta a história da norte-americana Magrin que, por meio de um aplicativo instalado no celular, teve as coordenadas de latitude e longitude coletadas a cada dois segundos e cedidas para terceiros, sem a ciência dela. Mas ela não está sozinha, pois diversos aplicativos realizam tal prática. A matéria aponta que são mais de 75 empresas que recebem dados fornecidos por usuários que aceitaram disponibilizar para receber notícias sobre previsão do tempo e condições de trânsito. A investigação ainda revela que só em 2017 foram mais de 200 milhões de dispositivos móveis monitorados, mostrando detalhes de viagens, por exemplo, com precisões absurdas[68]. O que impressiona, além da enorme quantidade de dados coletados, é o tempo de armazenamento destes dados – considerando que a notícia foi publicada em outubro de 2018 e as empresas detinham informações das pessoas desde 2017 ou, pelo menos, é o prazo que admitem manter.

O caso apresentado pelo NYT mostra o enorme poder das empresas em armazenar os nossos dados e, com uma facilidade enorme, duplicar, distribuir, publicar e cruzar. Bruno (2008), ao trazer uma afirmação de Solove, revela que as empresas públicas e privadas, até o início da década de 70, realizavam coletas de dados de seus clientes de forma pontual e eventual. Seguindo o raciocínio, a autora nos fala que a capacidade de monitoramento cresceu de forma drástica nos últimos 40 anos. Para complementar e exemplificar as mudanças, trago o parecer de Schneier

[67] Your Apps Know Where You Were Last Night, and They're Not Keeping It Secret. *In:* The New York Times. Disponível em: https://www.nytimes.com/interactive/2018/12/10/business/location-data-privacy-apps.html. Acesso 05 out. 2019.
[68] "A sample of information gathered in 2017 and held by one company — reveals people's travels in startling detail, accurate to within a few yards".

(2015) sobre as formas que as empresas faziam e utilizavam a coleta de dados, evidenciando assim a natureza e as intenções em cada momento.

Inicialmente, os dados eram internos, utilizados para que a empresa tivesse o controle de saber quem eram seus clientes, o que eles estavam comprando, e um meio de contato, caso houvesse algum problema ou para agilizar uma próxima compra. Com armazenamento puramente analógico, em fichários e catálogos, os dados levavam mais tempo para serem recuperados e demandavam de um esforço considerável para serem cruzados, a fim de tomar decisões baseadas em dados. Um passo importante foi possível após a inserção de sistemas digitais. Esses sistemas permitiram que fossem inseridos os cartões de fidelidade que, com a promessa de descontos conforme a recorrência do uso, incentivaria o consumo utilizando o cartão e, assim, haveria insumos de dados suficientes para gerar um mapa de uso, perfil e preferência de consumo. Interessante observar que neste ponto surgiram os primeiros *softwares* responsáveis pelo gerenciamento dessas informações, os CRM's[69]. Esse *software* é capaz de tornar visível e acessível um relatório das interações de clientes com a empresa.

Houve um segundo momento, mais focado em *marketing* direto. A disponibilização de listas de e-mails à companhias que, por meio de breves cruzamentos demográficos, faziam com que as empresas, que antes emitiam *newsletters* impressas, passassem a enviar e-mails para os clientes que desejavam receber a mensagem eletrônica. Nesta prática, é importante observar que o endereço eletrônico não necessariamente pertencia à empresa que disparava o e-mail. Isso configuraria uma relação paralela entre duas empresas que trocavam ou vendiam dados dos usuários sem o consentimento ou ciência total da circulação das suas informações. O cruzamento realizado pelos dados demográficos, de certa forma, poderia ser comparado aos *cookies* que são analisados e trackeados por serviços especializados a fim de qualificar os destinatários.

O terceiro passo, ainda mais sofisticado, era feito pelas agências de crédito. Dotadas de uma série de informações, elas traçavam perfis de pessoas e vendiam aos bancos para que eles tivessem um panorama de quais clientes seriam

[69] CRM's são aplicativos de informação desenvolvidos com o objetivo de auxiliar na gestão do relacionamento com o cliente. CUSTOMER Relationship Manageent (CRM). *In:* Wikipedia: A enciclopédia Livre. Wikimedia. Disponível em: https://pt.wikipedia.org/wiki/Sistemas_de_CRM#Customer_Relationship_Management. Acesso em: 20 set. 2019.

possivelmente bons ou maus pagadores. Essas informações serviriam para liberar ou não o crédito, baseados no risco de calote. Nesse caso, que envolve veto ao acesso a bens de consumo, estava previsto na LGPD a revisão do resultado obtido pelo algoritmo por uma pessoa, no entanto, na versão sancionada pelo atual presidente Jair Bolsonaro, a revisão do algoritmo ainda existe, porém pode der realizada por outro algoritmo. Outro ponto a ser observado é a natureza deste algoritmo, uma vez que ele é programado baseado em critérios e esses, por sua vez, quase nunca são revelados, por motivos que serão abordados mais adiante. De qualquer forma, o ponto que desejo abordar é a fala da pesquisadora em Direito e Tecnologia do ITS-Rio, Priscilla Silva[70]. Ela enfatiza que "o programador, quando vai elaborar o algoritmo, passa para o código o seu ponto de vista, com vieses e preconceitos."

Por fim, há um quarto meio, que é feito pelos governos, ao registrar diversas informações sobre os cidadãos, tais como: data de nascimento, óbito, casamento, divórcio e licença para dirigir. Avançando para um cenário ubíquo e relacionando com o sujeito censor, Schneier (2015) aponta para um comportamento interessante do cidadão em relação ao governo. Segundo ele, se o governo criasse uma lei obrigando os cidadãos a carregarem consigo rastreadores, informassem quem são seus amigos ou pessoas com que mais convivem, ou outras informações desse tipo, ficaríamos em estado de alerta, ou de indignação. No entanto, realizamos ações desse tipo e tantas outras muito mais sensíveis à nossa privacidade para empresas – e algumas delas relacionadas ao governo – sem ao menos questionarmos ou nos darmos conta.

O censo, realizado pelo governo, já faz a coleta e armazenamento de dados da sociedade há anos. O próprio termo *censor* data da antiguidade romana, sendo este título dado ao responsável pela contabilização dos homens para fins militares, taxação e censura (ROSE, 1999 apud BRUNO, 2008). Posteriormente, a prática evoluiu e na Alemanha do século XVII surge a "estatística", resultante da coleta e tabulação sistemática de dados sobre cidadãos e fatos (HACKING, 1990 apud BRUNO, 2008).

Esse Estado não meramente burocrático mas agora informacional aperfeiçoa a forma de realizar o seu censo aproveitando-se da comunicação móvel. O *m-government* – referindo ao conjunto de estratégias de comunicações realizadas por governos públicos a partir de aplicações digitais (LEMOS; ARAUJO, 2018) – tem por finalidade ampliar os canais de informação entre cidadão e estado, ampliar o acesso

[70] Disponível em: https://epoca.globo.com/como-nova-lei-de-protecao-de-dados-fortalece-ditadura-dos-algoritmos-23802395. Acesso em: 20 set. 2019.

à informação e, como o próprio autor afirma, e já mencionado acima, “produzir mecanismos de extração de dados do cidadão, seja em suas ações cotidianas mais banais, como pegar um ônibus [...]” (LEMOS; ARAUJO, 2018, p. 2). Para um estado que necessita – e consegue – obter uma série de informações de comportamento dos cidadãos de forma automatizada e sem a necessidade de realizar ações de censo, trazem um dado que está relacionado a um hábito e a pessoa acaba por responder sem que haja uma pergunta propriamente feita. A informação é obtida pela simples portabilidade do dispositivo e pelos algoritmos que a compõem. Outra característica do estado informacional é, segundo (BOFF; FORTES; FREITAS, 2018), a interdependência com outros Estados. Essa relação faz com que fique em segundo plano o papel burocrático de controlar o desenvolvimento das instituições e passe a atuar na implementação e utilização de uma infraestrutura global que propicie o fluxo da informação para si. Exemplo disso foi a situação das telecomunicações durante a Primeira Guerra Mundial, em que as empresas de telefonia atuavam sem interação até que o governo às nacionalizaram com a finalidade de oferecer maior conexão e rapidez, beneficiando a sociedade (BRAMAN, 2009 apud BOFF; FORTES; FREITAS, 2018). As influências e consequências do Estado Informacional será melhor explicada no próximo subtítulo, Vigilância, a fim de explicar o estado *panspectron*.

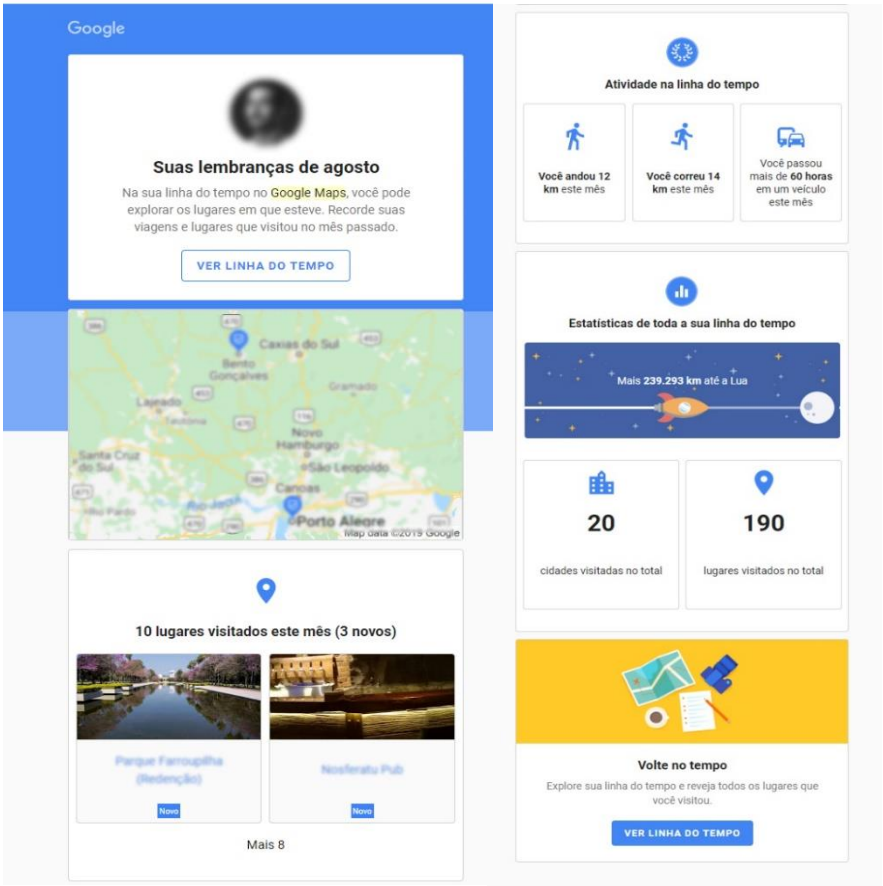
Voltando ao monitoramento, o que podemos perceber das quatro formas apresentadas é a notável fonte e ambiente de circulação dessas informações. Se em um primeiro momento, de forma analógica e posteriormente digital, havia uma circulação puramente interna dos dados a fim de fornecer o maior conhecimento da sua base de clientes, posteriormente, passamos para um cenário no qual a coleta de informações se torna mais sofisticada, necessitando cada vez de mais informações, mas também começa a circular entre outros meios e, de fato, acaba por afetar a vida do cidadão. Schneier (2015) lembra que companhias de *marketing* e de finanças foram as primeiras a realizarem trabalhos conjuntos a fim de fornecer a qualificação dos dados. O enriquecimento dos dados, nome da prática utilizada, dá a visão do comportamento do usuário baseado na interação com outras empresas. Se antes a empresa detinha os dados para registro ou conhecimento dos hábitos de seus consumidores em relação aos seus produtos ou serviços, agora elas conseguem

cruzar, a partir de uma chave primária[71], o que torna sua base de dados mais elaborada.

O Google, por exemplo, possui o Google Maps, presente em diversos sites e aplicativos e que, ao fornecerem acesso do mapa aos desenvolvedores de aplicativos, permite saber onde os utilizadores estão, sem necessariamente responderem à empresa. Mascarado de um serviço gratuito, o Google Maps utiliza o GPS do usuário para mostrar a sua localização em um mapa virtual e armazena todos esses dados. Uma evidência disso é o relatório mensal que o Google envia a alguns usuários sobre as movimentações realizadas durante o mês. Com isso, sabe-se a distância percorrida, a forma que o percurso foi realizado – a pé ou por veículo – e os pontos de interesse.

Um exemplo desse relatório pode ser visualizado na figura 4, a seguir.

Figura 4 – Relatório de movimentações



Fonte: Google Maps (2019).

[71] Chave primária é a denominação que se dá para um dado que permite identificar uma pessoa em outras bases de dados. As mais comuns são: e-mail, CPF e impressão digital.

A proliferação de tecnologias, tema também abordado por Lins, propiciou essa maior coleta de dados e, também, a sua estruturação e a variedade de informações provenientes de diversas fontes. Não somente a democratização do acesso aos dispositivos móveis, mas também o que influenciou diretamente foi a democratização do acesso à rede de dados, conforme afirmou Pellanda (2009), principalmente pela disponibilização da rede 3G, levando internet para áreas que eram economicamente inviáveis e desinteressantes para as grandes empresas. Com esses dois eventos, o mercado se tornou propício para que empresas apostassem no desenvolvimento de aplicações diversas, que utilizariam cada vez mais os recursos do dispositivo móvel, como GPS, câmera, microfone e acelerômetro.

Outro ponto interessante que favorece o monitoramento detalhado e constante da nossa vida é o declínio do preço de armazenamento para bancos de dados. Segundo Gandy (2002, apud BRUNO, 2008), os preços caíram drasticamente nos últimos 30 anos – coincidência ou não, quase o mesmo período do crescimento vertiginoso da coleta de dados[72], como já apontado pela autora – permitindo que toda essa gama de dados fosse armazenada. Assim, as empresas conseguem guardar, por um preço baixíssimo, detalhes minuciosos das nossas vidas, momentos que a nossa própria memória – falha – esqueceria (BRUNO, 2008).

Essa facilidade de armazenar e recuperar as informações propiciam a formação do *self estendido*. Como mencionado no início deste estudo, o conceito formulado por Belk em 1998 transformou a forma com que nos comunicamos, apresentamos e consumimos (MARTINS; OLIVEIRA; CORSO, 2018). E é nesse aspecto que a ubiquidade da conexão móvel, somada à convergência de diversas ações em um único dispositivo, o *smartphone*, torna tão fácil de criar um cenário de monitoramento em massa e revelador das nossas rotinas. Os locais que frequentamos, o tempo que permanecemos em cada um deles, entre outros dados metamapas desse nosso comportamento. Se em um primeiro momento o padrão das nossas ligações era possível de traçar perfis de comportamento ou inferir situações, hoje, com uma riqueza

[72] Um estudo realizado por Gantz e Reizel, em 2012, e trazido por Boff, Fortes e Freitas (2018) relata que, propiciado pelas tecnologias de informação e comunicação (TIC) a quantidade de dados passará de 130 hexabites para 40.000 hexabytes até 2020. Isso, segundo os autores, representará 5.200 gigabytes para cada indivíduo.

maior de dados, podemos prever comportamentos e traçar perfis com muito mais facilidade.

Na comunicação móvel, principalmente no *smartphone*, o *software* ganha um papel importante no monitoramento dos indivíduos pois é ele quem gerencia o *hardware* e executa as nossas ações. Seja o sistema operacional ou aplicativos instalados – sem mencionar os *malwares* e vírus que podem acompanhar alguns apps – temos alguns indícios de que o *software* coleta automaticamente dados sobre conversas que foram realizadas na presença do *smartphone,* mas não pelo seu uso, ou seja, as pessoas conversam, normalmente, mas o conteúdo desse diálogo é capturado pelo dispositivo e compartilhado com anunciantes.

Em 2018, uma reportagem da Vice[73] revelou, com auxílio do consultor sênior em *cyber*-segurança e pesquisador da Universidade Edith Cowan, Dr. Peter Hannay, que os dados produzidos no microfone dos dispositivos são acessados com frequência pelos sistemas operacionais em busca de “gatilhos” que ativem seus assistentes pessoais. Até aí, nenhuma novidade. Como mencionado anteriormente, os assistentes pessoais necessitam ser acionados e, em contra partida, devem estar atentos ao ambiente para perceberem quando são requisitados. O que torna revelador e preocupante é o acesso aos dados por aplicações instaladas no aparelho móvel. Não bastando acessar pontualmente os dados produzidos pelo microfone, aplicativos como Facebook e Instagram não tornam claros quais sãos os *triggers* que comandam isso. Esse fato explica o motivo de alguns anúncios aparecerem para os usuários tempo após eles mencionarem, em conversas com pessoas, sobre determinados assuntos.

Importante ressaltar que as empresas negam qualquer ação deste tipo, mas, conforme reforça Peter, não há razões para que isso não ocorra. Na mesma reportagem, o autor conta sobre a realização de um teste: por vários dias, ele repetiu pelo microfone do dispositivo frases que suspeita serem gatilhos para a ativação de buscas e, a partir disso, monitorou a mudança de anúncios recebidos. Ao final, ele percebeu um direcionamento de conteúdo relacionado às conversas que ele produziu intencionalmente para o estudo.

---

[73] *Your Phone Is Listening and it's Not Paranoia*. *In:* VICE. Disponível em: https://www.vice.com/en_au/article/wjbzzy/your-phone-is-listening-and-its-not-paranoia. Acesso em: 28 de set. 2019.

No livro *Data and Goliath*, Bruce Schneier (2015), já mencionado neste trabalho, fala de um aspecto interessante que visa tornar menos assustadora a prática de entrega de anúncios baseados no nosso monitoramento. Para isso, o autor faz um paralelo com a nossa ideia de sentirmo-nos mais confortáveis quando robôs parecem robôs ou totalmente humanos, mas, em paralelo, sentimo-nos assustados quando os robôs tentam se passar por humanos – pela aparência ou inteligência – e falham. Seguindo a linha de raciocínio, ele menciona o que a crítica Sara M. Watson sugere que há uma similaridade com os anúncios: se os anúncios são personalizados de maneira desleixada ou extremamente assertivas, as pessoas até aceitam, mas, se percebem que estão sendo manipuladas, acabam ficando desconfortáveis. Para remediar isso, a indústria da publicidade acaba por inserir esses anúncios extremamente reveladores, amenizando a forma de abordar.

Outro grande vilão e grande contribuinte para um monitoramento sistemático é o *Browser*. O *software* que permitiu navegar pela Web de forma amigável, no *Desktop*, construiu ao longo da sua história diversas ferramentas para catalogar as informações de cada usuário, sendo a mais conhecida delas o *cookie*[74]. Inicialmente desenvolvido para informar o usuário se ele já havia clicado em determinados *links*, reter algumas informações do último acesso – como formulários preenchidos, preferências de configuração em sites e produtos inseridos em carrinhos de compras – ele foi se aperfeiçoando e passou a *trackear*[75] os usuários em diversas páginas. Os *3rd party cookies*, diferente dos *cookies* primários, são tipos de arquivos instalados em diversos sites e pertencem às corporações. Com isso, as empresas conseguem perfilar os visitantes de seus clientes a fim de entregar, para outros clientes, usuários segmentados por comportamento e preferências.

Um estudo empírico realizado em cima desses *trackers* foi feito pela Universidade de Berkeley, da California, conforme conta Boni (2019). Foram identificadas formas mais eficazes, baseadas em *cookies*, para a identificação dos usuários pela sua navegação: *flash cookies, HTML5 Web Storages, evercookie* e *fingerprint,* são algumas das variantes da mesma aplicação. O último deles, *fingerprint*, chama a atenção pois combina uma série de informações a fim de

[74] Pequeno arquivo de computador ou pacote de dados enviados por um sítio de Internet para o navegador do usuário, quando o usuário visita o site. https://pt.wikipedia.org/wiki/Cookie_(inform%C3%A1tica)

[75] *Trackear* é rastrear por meio de algoritmos que coletam e armazenam a informação. Os *trackers* utilizam os cookies para tentar identificar cada usuário.

identificar os usuários individualmente sem que esses tenham permitido o acesso à totalidade de dados – os dados são, por exemplo, tipo de dispositivo, tipo de navegador e *plug-ins* instalados.

Vale ressaltar que os *cookies* gerados pelos navegadores não são totalmente compatíveis com os coletores de informações presentes nos aplicativos. No entanto, há outras formas, como explica a Interactive Advertising Bureau (IAB)[76], de tentar identificar os usuários. Há um componente para desenvolvimento de aplicações mobile chamado Webview. Esse, por sua vez, permite a exibição de conteúdo Web dentro das aplicações, como propagandas, vídeos ou sites que simulem aplicativos. Em paralelo, eles aproveitam o espaço para gerar dados aos *cookies*, uma vez que o Webview é um componente do navegador e permite a escrita dos *cookies* por meio dele.

Outra forma é o *login* universal. Muitas aplicações – com o intuito de facilitar o *login* dos usuários – disponibiliza a possibilidade de realizar o *login* por meio de redes sociais ou clientes de e-mail (Facebook e Gmail, por exemplo). Essas duas empresas são conhecidas por possuírem, na maioria dos websites e aplicativos, seus códigos para auxiliar na mensuração de campanhas de *marketing* e de interação dos usuários. Nessa lógica, ao realizar o *login* universal, ou *login* social, possibilita que um usuário seja identificado em mais de um ambiente – aplicativo e web.

Essas formas de trackeamento de cruzamento de *cookies* são mais presentes em usuários de Android. A Apple, desenvolvedora do IOS, possui questões de segurança mais rígidas, a fim de proteger seus usuários – mas isso não impede que esses também sejam trackeados. A IAB aborda que há outra forma de encontrar os usuários entre os ambientes: o Client ID. Esse se define por um código gerado e fornecido pelo próprio fabricante, e que algumas aplicações, por falha de segurança ou de forma lícita, obtêm durante a execução do código. Assim, por ser único para cada dispositivo, basta que o usuário realize demais operações, como fornecimento de e-mail, cartão de crédito e CPF, para que a estruturação do seu perfil seja montada.

Por fim, vale lembrar que o monitoramento é o movimento chave que possibilita a vigilância em potencial. De acordo com Bruno (2008), o monitoramento faz parte de uma série de processos que, junto ao algoritmo, torna-o sistemático e caracteriza, assim, a vigilância.

---

[76] UNDERSTANDING Mobile Cookies. *In:* IAB. Disponível em: https://www.iab.com/wp-content/uploads/2015/07/IABDigitalSimplifiedMobileCookies.pdf. Acesso em: 02 out. 2019.

4.2 VIGILÂNCIA

A vigilância, diferentemente do monitoramento, tem outro propósito: o de evitar algo. Em outras palavras, Lemos (2009), caracteriza esse ato como um olhar de prevenção, um comportamento atencioso, zeloso e cauteloso. O autor segue embasado na definição de Gow (2005 *apud* LEMOS, 2009), que coloca a vigilância nas dimensões de controle e de monitoramento.

Ao citarem a vigilância, Bruno (2009) e Lemos (2009) divergem sobre os conceitos. No artigo *De que vigilância estamos falando*, Lemos faz um relato crítico ao que Bruno considera ser vigilância a partir de seu texto *Mapas de crime. Vigilância distribuída e participação na cibercultura*. Para Lemos, as ações de vigilância só poderiam ser aquelas “ações nominais com vistas a evitar ou causar algo” (LEMOS, 2009, p. 2), exigindo assim dois elementos: a intencionalidade (o que deve ser evitado) e a identificação nominal do indivíduo ou do grupo que estaria sendo alvo de tal ação. O autor exemplifica com o fato de suas ligações telefônicas não serem consideradas vigiadas pela companhia telefônica, apesar de serem todas monitoradas e registradas, mas não há a intencionalidade explícita aí. No entanto, essas ligações podem ser requisitadas pela Polícia Federal, por exemplo, através de uma quebra de sigilo telefônico, e assim ser, de fato, monitorada com uma motivação – caracterizando então a vigilância.

Lemos não questiona o fato de não poder existir a possibilidade de vigilância. O que o pesquisador tenta desmistificar e deixar claro é que nem todas as ações e sistemas podem ser chamados de vigilantes:

> Não me parece que, ao usar o “Facebook” eu esteja sendo vigiado (as informações são protegidas e não há intencionalidade). Mas o “Facebook” pode ser usado para vigiar (se houver quebra da proteção dos meus dados pessoais e uma intenção com vistas a evitar ou causar algo) (LEMOS, 2010, p. 3).

Em relação à opinião de Lemos sobre a ausência da vigilância nas redes sociais, eu acredito que ele esteja sendo brando demais. A ferramenta, de fato, é uma vigilante em potencial, visto que a natureza das interações faz com que os usuários se expressem das mais variadas formas, o que enriquece o tipo de dado produzido na plataforma. Mesmo que haja as configurações de privacidade, dando ao usuário

um certo controle sobre quais informações são disponibilizadas aos demais integrantes da rede social, há uma série de metadados que são produzidos em toda interação com o conteúdo que, por sua vez, é coletado pela ferramenta. Assim, a possibilidade de não ser vigiado, que pode dar alguma razão para Lemos, é por outros usuários. No entanto, as informações que são compartilhadas aos anunciantes ainda são motivos para que se considere as redes como vigilantes, dada a forma que os algoritmos foram estruturados.

Para o pesquisador, por mais que as redes sociais tenham possibilidades de monitoramento e vigilância, essa prática é imanente a elas. É assim que elas podem personalizar e otimizar a oferta de serviços. Ele questiona se não seria um exagero inserir os três termos (controle, monitoramento e vigilância) como definições para qualquer captura de informação e considerar as plataformas sociais como vigilantes. No entanto, o autor reconhece que está apegado à forma mais canônica e jurídica do termo, e que os novos tempos podem implicar em uma mudança de significados, justamente pela variedade de coleta e a possibilidade de cruzamento de informações: “Ao meu ver, estes sistemas monitoram e controlam e isso é perigoso justamente por poder acarretar, *a posteriori*, forma de vigilância individual ou grupal” (LEMOS, 2009).

Dessa forma, arrisco afirmar que Lemos estaria negando a intencionalidade do algoritmo que, latente, aguarda o gatilho ser acionado. De fato, a maioria das análises que Lemos realizou e que tive contato remetiam à estruturas vigilantes tradicionais, com pessoas atrás de câmeras olhando atentamente ao que ocorria nos espaços públicos. O que acompanhamos neste estudo é a automação dessa prática vigilante, não sendo necessário um humano operar a máquina de vigiar. Já o controle, que Lemos também pensa em distinguir, é um efeito gerado pela automação da vigilância, mas de forma mais invisível – uma vez que não temos certeza de quando estamos sendo controlados ou não pelo algoritmo – fazendo-nos pensar que estamos tomando decisões por conta própria.

Já Bruno (2008, p. 11) conceitua vigilância digital como: “monitoramento sistemático, automatizado e à distância de ações e informações de indivíduos no ciberespaço, com o fim de conhecer e intervir nas suas condutas ou escolhas possíveis”. Ainda segundo a autora “estes dispositivos têm como principais elementos as tecnologias para monitorar as ações, informações e comunicações dos indivíduos no ciberespaço, a montagem de bancos de dados e a elaboração de perfis

computacionais". A autora ainda define o processo de vigilância digital, mesmo que não se aplique somente a isso, em quatro processos:

a) Os mecanismos de coleta, monitoramento e armazenamento de informações;
b) Os sistemas de classificação e conhecimento de dados;
c) Os procedimentos de individualização e produção de identidades;
d) As formas de controle sobre as ações e escolhas dos indivíduos.

Podemos perceber que Bruno (2008) traz uma visão mais contemporânea e digital da vigilância. Em vez de termos um vigilante de "carne e osso" atrás da tela recebendo imagens das câmeras, há uma série de códigos, os algoritmos, desenhados para registrar todo o comportamento, armazenar e recombinar para produzir conhecimento.

Schneier (2015), do meu ponto de vista, contribui com a visão de Bruno (2008), ao relatar a forma que o exército norte-americano define vigilância moderna e eletrônica. Para os militares, o ato de vigiar implica em uma observação sistemática que nos torna "livros abertos", tanto para o governo quanto para as empresas, e reforça que esse poder de conectar as nossas vidas é o maior da história[77]. Bruce ainda traz uma importante afirmação para reforçar o estado em que nos encontramos: "A vigilância em massa é impossível sem o uso da computação, rede e automação. Não é 'siga aquele carro', mas sim 'siga todos os carros'"[78].

Como Boni (2019) afirma, o próprio conceito de vigilância sofreu um desgaste conceitual. Não estamos mais sobre um olho de um Big Brother Orweliano. Assim, sinto-me mais propenso a concordar com Bruno e com Schneier ao considerar a visão moderna e automatizada sobre o ato de vigiar. A vigilância está distribuída, assim como define Bruno, não mais por uma única grande tela, mas por várias microtelas. Os *tiny brothers* passam a monitorar – de forma sistemática, caracterizando vigilância – todas as nossas ações. O poder de vigilância sobre o indivíduo é potencializado pelas tecnologias da informação e da comunicação (BOFF; FORTES; FREITAS, 2018), sendo essa forma de obter dados um reforço à definição de Bruno, ao discorrer

[77] A vigilância moderna é exatamente isso: todos nós somos livros abertos para o governo e as corporações. A habilidade de perscrutar nossas vidas pessoais é maior do que antes (tradução nossa).
[78] It's not "follow that car". It's "follow every car." (SCHNEIER, 2015, p. 32).

sobre uma vigilância distribuída. O controle dessa informação produz, de certa forma, poder para quem a detém.

Foucault define poder como “ação sobre a ação possível” (FOUCAULT, 1933 apud BRUNO, 2009). Essa linha reforça a possibilidade de atuação sobre os vigiados – não necessariamente em um ato que tente curá-lo, e sim de evitar que se ele torne doente. Como exposto por Bruno, não é reformar o criminoso, é evitar que o crime aconteça.

Diferentemente do que o romance de George Owrell relata, Bruno (2008) reforça que a vigilância não está mais centralizada no Estado, como era na década de 70. Hoje, com as tecnologias de interação e comunicação, a possibilidade de obter dados de forma sistemática e de vigiar está ao alcance de qualquer um que tenha interesse e tecnologia para isso. Essa descentralização do poder sobre os dados permite uma visão que Boff, Fortes e Freitas (2018) nos trazem em seu livro Proteção de dados e privacidade: saímos de um estado *panóptico* para o *panspectron*.

O cenário panóptico reflete sobre a origem do termo, remetendo à organização do chão das fábricas da Crimeia e, posteriormente, às instituições reguladoras, onde o observador possuía um local privilegiado em relação aos observados. Estando sob constante vigia, os observados não sabiam em que momento estavam ou não no campo de visão do vigilante. Este modelo, inicialmente apresentado por Bentham em 1791 e depois aperfeiçoado por Foucault em 1987, reflete na forma de exercer poder dos observadores diante dos observados, e revela que as próprias instituições panópticas não necessitavam de reforço nas suas estruturas físicas, pois o estado eminente de observação acabava por disciplinar os observados. Como Lemos (2010) aborda de forma esclarecedora, a nova vigilância difere-se dos espaços confinados, dos internatos, das instituições feitas por blocos de concreto. Agora ela se faz presente das mais diversas formas.

> [...] perfis da internet, nos bancos de dados em redes sociais interconectadas, nos deslocamentos com o telefone celular monitorando o “roaming” do usuário, na localização por GPS, nos rastros deixados pelo uso de cartões eletrônicos, nos smartcards dos transportes públicos, nos sinais emitidos e captados por redes bluetooth, nas etiquetas de radiofreqüência que acompanham produtos e compradores... (LEMOS, 2010, p. 610).

Um dos reflexos que Boff apresenta ao trazer a obra de Foucault intitulada *Microfísica do Poder* é relevante para a presente pesquisa, por abordar o controle

sobre o corpo em vigilância como algo não perceptível. Neste cenário ubíquo, portanto, chegamos ao *panspectron,* transformando todos os cidadãos em vigiados, independentemente momento ou local. Os objetos de coleta tornaram-se diversificados e eficientes, a ponto de extraírem toda essa informação com o mínimo de fricção. Além dos celulares e *smartphones* apresentados no estudo, vale destacar os demais dispositivos existentes que contribuem para a coleta de dados, como RFID e IoT; cartões das mais diversas finalidades, como transporte, fidelidade, crédito, débito; além de redes sociais, plataformas de comunicação e sites.

Bruno (2008) reflete sobre uma "bulimia de dados", atravessada pelos novos processos tecnológicos (TIC)[79]. Com o avanço e aperfeiçoamento dos algoritmos e dos *hardwares* presentes nos dispositivos, o sistema torna-se cada vez mais habilidoso na arte de coletar as informações e armazená-las. As finalidades para isso são diversas: montar perfis, construir cenários hipotéticos – frutos do capitalismo de vigilância.

Outro ponto interessante para observarmos é que os dados que servem para vigiar não necessariamente são resultantes de ações realizadas pelo usuário. Observando o que Casilli (2015) afirma utilizando a Internet das Coisas como exemplo, constatamos a mudança da Internet da publicação – em que o usuário posta conscientemente o conteúdo na rede – para a internet da emissão – tendo os dados e metadados transmitidos por esses dispositivos conectados. Lemos (2010) contribui com a afirmação de Casilli ao trazer os conceitos de *data* e *capta.* O que diferencia um do outro é que o primeiro é representado pelo dado que é fornecido, e o segundo é a informação digital extraída por meio dos TICs. Assim, concordamos com Lemos ao afirmar que não faz-se necessário confinar as pessoas em espaços, mas sim estimular o movimento delas, tornando eficaz tal modelo de vigilância e, parafraseando Deleuze, Lemos provoca o fato de todos esses aparatos tecnológicos serem invisíveis – novamente pela nossa não percepção psicológica – e pervasivos, sendo isso um fator crucial para o rastreamento dos nossos movimentos enquanto sujeitos móveis:

> Essas fronteiras são invisíveis e muitos usuários não percebem a real dimensão dessa faceta da sociedade de controle: uma vigilância sutil, difusa, deixando o usuário com a sensação de liberdade de produção de informação e de mobilidade (LEMOS, 2010, p. 638).

[79] Tecnologias de Informação e Comunicação (TIC).

Partindo disso, as microtelas que nos observam seriam compostas e dependentes de microdispositivos e de conjuntos de *softwares* que realizam a comunicação entre eles e os aparelhos de comunicação móvel. Para exemplificar, trago como exemplo o SmartWatch[80] da Xiaomi. O seu funcionamento pleno depende de uma conexão com um *smartphone*: as informações coletadas por ele são transmitidas para o dispositivo, que retorna ao usuário as métricas de sono, atividade física e quantidade de passos, relacionando aos demais usuários. Essa comparação só existe pois há uma comunidade fornecendo os dados, pelo mesmo tipo de dispositivo. Muito mais do que essas informações, há dados sobre posição, hábitos de consumo – onde essa pessoa mora, em que local trabalha, quanto tempo passa em cada local e qual período do dia está demonstrando maior atividade com o *smartphone*. Essas informações não são fornecidas pelo usuário, mas sim, coletadas pelo dispositivo e enviadas sem que o usuário tenha controle ou percepção.

Sobre a característica das informações que são obtidas, Bruno (2008) faz uma distinção entre elas, seguindo a mesma linha de raciocínio de Bioni (2019). A autora difere em dois tipos os dados: os relativamente estáveis e os que mudam constantemente. O primeiro se refere às informações geodemográficas, de gênero, biometria, entre outras. Já o segundo é aquele produzido e alterado com maior frequência, resultado de relações transacionais realizadas por meio de plataformas, softwares e dispositivos eletrônicos. Apresentando essa segunda tipologia, Bruno afirma que é nela que mora a nossa “vida digital”, onde os dados são coletados em tempo real, sem a necessidade de entrevistadores e questionários.

Após termos visto como funciona a coleta sistemática das informações, descaracterizando-a como monitoramento e configurando-a como vigilância, devemos atentar para o fato de que nada serve toda essa informação sem que haja, de fato, a produção de conhecimento. Assim, mais do que devorar uma massa de dados, a vigilância se constitui a partir da produção de um saber próprio da análise dos dados que foram coletados (BRUNO, 2008).

Como vimos no capítulo anterior sobre monitoramento, especificamente quando abordadas as formas que os aplicativos de redes sociais escutam as nossas conversas, posso considerar tal prática como um ato de vigiar. Utilizando a descrição

[80] Relógios inteligentes dotados de sistema operacional. Na atualidade, se conectam aos Smartphones para realizar a troca de informações diversas.

que o Google dá para o funcionamento do seu assistente pessoal – que está continuamente escutando o ambiente, a fim de identificar quando é acionado por voz – já consiste em uma vigilância pois há a intencionalidade necessária para isso. Em paralelo, o microfone está habilitado e coletando constantemente informações. Elas podem não acionar nenhuma ação para o usuário, mas isso não invalida a persistência em escutar o ambiente.

O GPS é outro dispositivo que envia informações para as empresas, podendo acionar medidas que impactam os usuários. Ações de *Push Notifications* são capazes de enviar notificações de *push* baseadas no comportamento geográfico dos usuários que possuem determinados aplicativos instalados nos seus *smartphones*. Além da coleta constante da localização das pessoas, a inteligência dessas empresas é capaz de traçar perfis de comportamento inferindo, inclusive, a residência e o local de trabalho dessas pessoas[81]. Em particular, os esforços da empresa *In Loco*, para ser eficiente na localização dos usuários utiliza, em conjunto com o GPS outros *hardwares* – como *Bluetooth*, acelerômetro e bússola – tornando a localização *indoor* mais precisa possível. Para se ter uma ideia, a forma de monetização deste tipo de ferramenta é Custo Por Visita (CPC), que considera o tempo de permanência de um usuário dentro dos estabelecimentos.

As câmeras de celulares também se tornam objetos vigilantes quando inserem Inteligência Artificial na sua forma de operar. Com a aplicação dessa tecnologia, as empresas prometem realizar reconhecimento facial, de imagens, padrões e composições, além de melhorar a qualidade das fotos tiradas. Para que a funcionalidade se torne eficiente é necessário o treinamento do algoritmo, que é realizado por meio da inserção de uma diversidade de imagens nos bancos de dados das empresas. Assim, ao abrir a câmera e mirar em uma organização de elementos, sejam eles objetos ou rostos, o algoritmo é capaz de identificar e retornar características e descrições do que é encontrado. De fato, a inteligência presente nessa câmera tem a intencionalidade de capturar o que está presente na composição fotográfica, o que nem sempre faz parte da intenção do fotógrafo.

Outro caso que pode ser exemplificado como vigilância foi a recente denúncia

[81] A ferramenta *Real World Audience*, da *In Loco Media*, foi uma das pioneiras nessa funcionalidade. IN LOCO RWA: Como uma tecnologia brasileira traz o mesmo poder analítico do online para o offline. *In:* Linkedin. Disponível em: https://www.linkedin.com/pulse/loco-rwa-como-uma-tecnologia-brasileira-traz-o-mesmo-poder-ferraz/. Acesso em 15 out. 2019.

que o New York Daily News[82] fez sobre as empresas Randstad e Google ao afirmar que a primeira, a serviço da segunda, estava abordando moradores de rua e pessoas negras para “operarem” o novo *Pixel4*[83]. Entre as diversas funcionalidades haviam aplicações que trabalhavam com selfies – com filtros parecidos com o Snapchat – e outras que, simplesmente, exigiam o uso do aparelho por 10 minutos em troca de 5 dólares. O que a reportagem trouxe à tona é que, durante o uso do aparelho, a câmera frontal estaria habilitada constantemente na tentativa de reconhecer o padrão de rosto das pessoas negras, a fim de suprir a carência de imagens para tornar melhor o desbloqueio facial.

Podemos perceber que o poder de inserir *softwares* cada vez mais inteligentes operando dispositivos cruciais, que trazem uma percepção do mundo tátil sem o consentimento e a ciência do operador, torna-se um perigo, afinal, temos os elementos necessários para que tal prática seja considerada vigilância: monitoramento e a intencionalidade.

O que torna mais perigoso, na minha opinião, é esses *hardwares* estarem tão próximos e continuamente presentes nas nossas vidas. Como se não bastasse, há o algoritmo que faz o gerenciamento deles, tornando a captura de informações constante e opaca, coletando e produzindo conhecimento sobre nosso comportamento como nunca vimos.

Diferentemente do conhecimento produzido pelos governos em seus censos, a potencialização da coleta de dados proveniente da popularização dos dispositivos coletores aumenta a capacidade de “classificar e conhecer”, dando sentido à essa enorme quantidade de dados adquiridos. Como define Bruno (2008, p. 12): “os bancos de dados e perfis computacionais envolvem um sistema particular de classificação e conhecimento de indivíduos e grupos”. O resultado do processo de produção de conhecimento a partir do cruzamento das bases de dados denomina-se *profiling*. Ele caracteriza-se por determinar características, padrões de comportamento e/ou consumo que são relacionados a certos dados” (BENNET, 1996 apud BRUNO, 2008). Com isso é possível individualizar ou agrupar pessoas em *clusters*[84] e, a partir de uma

[82] GOOGLE mirou negros e moradores de rua para melhorar reconhecimento facial. *In:* Olha digital. Disponível em: https://olhardigital.com.br/noticia/google-mirou-negros-e-moradores-de-rua-para-melhorar-reconhecimento-facial/91078. Acesso em: 17 out. 2019.
[83] Pixel4 é um modelo de *smartphone* desenvolvido pelo Google.
[84] Cluster é a forma de segmentar pessoas a partir de características e comportamentos em comum.

infinidade de combinações, encontrar uma sequência de informações que a torne totalmente única, identificável.

Um dos fatores que mais contribuem para que uma pessoa tenha a sua identidade rastreável, certamente, é a pessoalidade do dispositivo. O fato de o *smartphone* ser parte do seu portador o torna uma prótese rastreadora, indicando dados correlatos a um indivíduo específico. Assim, com o padrão de comportamento direcionado, chegamos a um outro aspecto da vigilância: a predição de algo – para evitar ou favorecer algo – a partir do algoritmo.

Como já abordamos anteriormente ao utilizarmos a definição de Foucault, o poder como a ação sobre a ação implica em inferir ativamente sobre alguém caracteriza uma das faces do algoritmo preditivo, principalmente quando este infere algo sobre uma pessoa ou um grupo privando de determinadas situações ou oportunidades. Com a evolução dos algoritmos, que são favorecidos pelas redes neurais, *machine learning* e Inteligências Artificiais – ou tomadas de decisão automatizadas[85] – é possível, de certa forma, produzir futuros. Segundo Bruno (2008, p. 14-15) a predição do futuro é "uma espécie de oráculo, na medida em que ele não implica uma acuidade na previsão de um futuro certo e necessário, mas a efetuação de uma realidade antecipada."

Uma das evidências da ação do algoritmo preditivo já foi apresentada anteriormente, no caso da empresa Target. Não sendo um caso isolado, o algoritmo preditivo e a sua capacidade de produzir futuros e atuar sobre eles torna-se um problema de privacidade quando vai ao encontro da premissa do direito de não sofrer inferências externas sobre as suas escolhas. (RORHMANN, 2000). Uma das formas de utilizar o *smartphone* para inferir sobre as escolhas é a possibilidade de segmentar anúncios publicitários baseados no tipo do dispositivo. A partir do fabricante, modelo e versão do sistema operacional, presume-se uma faixa salarial e, com isso, oferecem produtos diferentes ou versões diferentes de um mesmo produto para esse público.

Como visto em uma série de exemplos neste trabalho, o mercado de dados pessoais é amplamente direcionado para a publicidade, mas não são os únicos a utilizarem este bem. Seguradoras de bens, de saúde, entidades financeiras e até imobiliárias estão utilizando cada vez mais algoritmos para medirem riscos antes de

[85] Prefiro utilizar este conceito pois a ideia de uma Inteligência Artificial Geral – que tudo sabe – é utópica. Baseio-me em uma conversa, durante uma sessão de leitura sobre o livro *Trabajo, conocimiento y vigilância*, com o professor Rafael Grohman.

venderem algum serviço. Assim, para evitar possíveis fraudes – como um morador afirmar que mora em um bairro com baixa incidência de roubo de veículos a fim de baixar o valor do seguro automóvel quando, na verdade, reside em um local mais violento – os dados obtidos a partir do *profilling* podem ser utilizados para práticas conhecidas, como *geo pricing* e *geo blocking*[86]. Um caso já praticado no Brasil pela empresa Decolar.com[87] foi alvo de denúncia e punição. A empresa alterou preços do mesmo trecho de voos para clientes que estavam em locais diferentes.

Baseando-me nos exemplos apresentados, podemos ver que os dispositivos móveis, por terem diferentes *hardwares* acoplados e *softwares* que fazem a gestão deles, permitem que desenvolvedores dos mais diversos tipos se aproveitem dos potenciais dados gerados e não meçam esforços para coletá-los ou armazená-los, podendo cruzar e produzir conhecimento infinitas vezes. Assim, como potencial objeto vigilante, acredito que os dispositivos móveis são bem mais que objetos comunicantes resultantes da convergência midiática. Para encerrar, trago as palavras de John McAfee, criador do antivírus McAfee:

> Todos os *smartphones* são desenvolvidos para aplicações que sabem onde você está, para quem você está ligando, quanto tempo você usa o *smartphone*, quem são os seus contatos, aplicações que leem as suas mensagens e os seus emails. Quando você baixa um aplicativo, você precisa selecionar “Sim/Aceito” para aceitar todas essas condições. Mas ninguém realmente lê essas condições, ninguém presta atenção. […] Então, porque os smartphones são desenvolvidos exatamente para coletar informações, hackeá-los é algo trivial. (McAfee, 2016)[88]

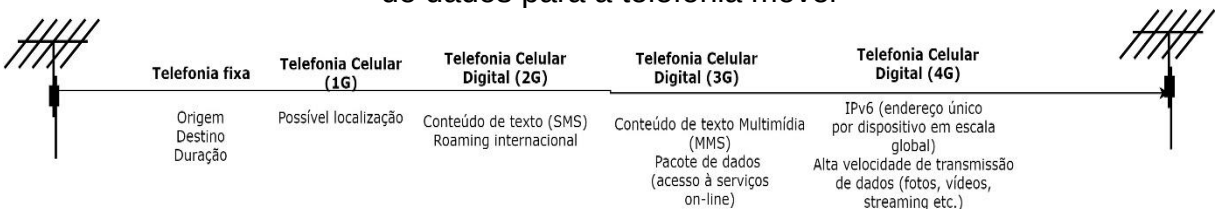
[86] *Geo pricing* e *geo blocking* são práticas de alterações de preços ou bloqueio de serviços, respectivamente, baseado no local de requisição.
[87] Decolar.com é multada por prática de *geo pricing* e *geo blocking*. Ministério da Justiça e Segurança Pública. Disponível em: https://www.justica.gov.br/news/collective-nitf-content-51. Acesso em 18 out. 2019.
[88] ‘JOGUE fora agora o seu *smartphone*', diz John McAfee ao TecMundo. *In:* Tecmundo. Disponível em: https://www.tecmundo.com.br/crime-virtual/109769-jogue-fora-smartphone-diz-john-mcafee-tecmundo.htm. Acesso em: 18 out. 2019.

5 CONSIDERAÇÕES FINAIS

Durante o desenvolvimento deste trabalho, percebi dois momentos distintos do percurso da comunicação móvel. O primeiro é marcado pela constante evolução das tecnologias de infraestrutura para a comunicação móvel, passando de um sistema totalmente analógico para o digital, tendo como consequência a possibilidade de transferir dados e mudando o foco em entregar maiores volumes de dados. Com isso, o usuário passava a ter segurança na comunicação, melhor qualidade do serviço oferecido e a possibilidade de trocar dados com a rede fora do ambiente doméstico.

Abaixo, me preocupei em resumir os principais dados que cada rede permitiu coletar, à sua época, e que implicavam diretamente sobre a nossa privacidade. O desenho, a cada nova geração da rede, exibe apenas o que foi incrementado a ela, sendo o que está no passo anterior herdado ou aperfeiçoado na nova versão.

Figura 5 – Linha do tempo das principais gerações das tecnologias de transmissão de dados para a telefonia móvel



Fonte: Elaborada pelo autor (2019).

O segundo movimento dá-se pelas mudanças nos dispositivos. Os principais upgrades se dão na capacidade de processamento de dados e na transferência e armazenamento de informações. Enquanto as redes não ofereciam troca de dados em velocidade considerável, os aparelhos não possuíam grandes inovações. Novos modelos surgiam, mas as diferenças entre eles eram em questão de formato – chamando grande atenção os modelos *flip* da Motorola – com jogos e funcionalidades como tela colorida e toques polifônicos. Quando as redes passaram a oferecer trocas de dados com velocidades cada vez maiores, a corrida pelo desenvolvimento de sistemas operacionais se tornou um ponto chave para as empresas do ramo telefônico. Investimentos em *hardwares* – como GPS, acelerômetro, câmera digital, entre outros sensores – além do forte desenvolvimento das aplicações que executariam diversas operações, fariam um movimento semelhante, na comunicação

móvel, como a que a Microsoft fez com o Windows: inserir tudo o que um escritório tinha dentro do seu sistema operacional.

Outro fato constatado foi a forte aderência da população à tecnologia móvel e o tipo de utilização que faziam do aparelho. Inicialmente servia apenas para efetuar e receber ligações. Ao passo que a convergência de funcionalidades migra para o dispositivo móvel, a dependência dele cresce e, com isso, o investimento em infraestrutura aumenta, significando um maior número de antenas que cobrem um mesmo espaço. Isso leva ao aumento da precisão da localização dos *smartphones* por meio da triangulação das torres celulares. Cada vez mais atividades são executadas e terceirizadas nesse tipo de dispositivo, como relacionamento interpessoal, funções administrativas, gerenciamento da vida cotidiana e até mesmo ligações as telefônicas são mediadas, tornando-se este um mercado atraente para os mais diversos tipos de mercado. Assim, a comunicação móvel inseriu novos fatores em toda essa forma de coleta e monitoramento, marcando a presença de fabricantes, desenvolvedor do SO. de aplicativos e dos provedores de serviço de comunicação.

Olhando para os aspectos sociais, o acesso à internet fora do ambiente residencial – principal característica da rede 3G – era possível e acessível para todos que portassem um aparelho celular com esta tecnologia. Assim, a democratização do acesso à rede contempla uma parcela da população que até então era desfavorecida economicamente ou geograficamente, chegando então às periferias e à zona rural (PELLANDA, 2009). O número de pessoas conectadas aumenta de forma drástica no Brasil e, com isso, as consequências foram várias: o celular passou a ter uma dinâmica diferente na vida das pessoas, passando a ser, anos depois, a principal fonte de acesso à internet. A massificação do acesso também permitiu que as empresas desenvolvessem mais aplicações, cada vez mais simples e específicas para facilitar ações rotineiras – como enviar mensagens, editar e postar fotos, relacionar com outras pessoas – tornando-nos dependentes dessas aplicações para executar diversas tarefas. A partir disso, a utilização dessas aplicações passou a produzir, como subproduto, a coleta de dados.

Com o *software* no comando de uma quantidade cada vez maior de *hardwares*, a versão *smart* do celular permitiu que a coleta dos nossos dados fosse cada vez mais precisa, contínua e diversificada. Esse *software*, ora sistema operacional, ora aplicativo, é operado por poucas empresas – duas principais para SO's de *smartphones* – e no caso das aplicações a situação não é tão diferente, já que a

maioria das aplicações amplamente utilizadas pertencem à empresas como Facebook e Google. Os aplicativos de redes sociais, mensageiros, acesso à Internet e de relacionamento tornaram-se populares e, com isso, encontramos outro ponto crucial: a monopolização. A grande presença de poucos *players* – visto que só é possível e viável a existência do serviço se houver quantidade considerável de pessoas ativas nele – leva a uma forte dependência da sua existência, favorecendo a sua adoção. Assim, além da tendência à monopolização de alguns aplicativos, os dados coletados pela sua utilização concentravam-se nestes poucos desenvolvedores.

Um ponto interessante observado é a constante busca de identificação dos usuários pelos mais diferentes espaços. Enquanto na telefonia móvel há um *hardware* que realiza este papel (NAM e cartão SIM), os aplicativos e sites Web trabalham com códigos capazes de coletar uma infinidade de dados que, uma vez enviados para bases de dados estruturadas, são capazes de analisar inúmeras vezes os dados, combinando-os até encontrar padrões únicos que identifiquem o usuário.

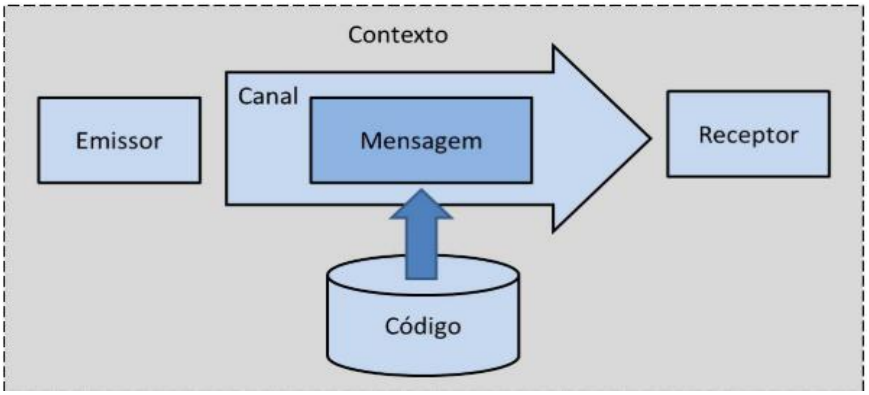
Nesta busca incessante pela identificação do usuário, entramos em alguns pontos de monitoramento e vigilância que afetam diretamente a privacidade do indivíduo. Assumindo que há um olhar atento sobre nós e que há ações baseadas em interesses dos mais diversos tipos (econômicos, políticos, entre outros), há diversas inferências na nossa vida cotidiana, caracterizando um grave ataque à nossa privacidade. Sem entrar em detalhes de vazamento de dados e interceptações de mensagens, o que também é grave, a falta de clareza e a desigualdade de relações entre os que coletam nossos dados e quem utiliza os serviços causa impactos relevantes no nosso livre arbítrio. O algoritmo – cada vez mais inteligente e eficiente – que gerencia a nossa comunicação realiza, a todo momento, escolhas que podem impactar em decisões importantes, por exemplo: o que o indivíduo verá e o que ele não verá, quais oportunidades serão apresentadas e quais serão negadas. Essa inferência direta na vida nos coloca em “bolhas” e fazem com que o nosso direito de sermos deixados em paz, de termos nossas decisões cientemente tomadas sem inferência externa não seja respeitado; fazem da nossa privacidade um objeto frágil perante os interesses das empresas que elaboram os códigos.

Os dados resultantes dos TIC’s que são compartilhados sem a nossa ciência ferem a premissa relatada por Lins (2000). Assim, se em um primeiro momento havia a central telefônica responsável por registrar nossas chamadas, origem, destino e duração, e o uso do telefone era apenas para ligação, hoje temos, no mínimo, quatro

intermediários com acesso a esse nível de interação, além de uma diversidade de aplicações específicas que necessitam da nossa atenção e utilização para funcionar. Essa mediação algorítmica torna nebulosa a percepção de quais informações são coletadas e de que forma são utilizadas pelos atuantes deste processo comunicacional.

O modelo de comunicação de Jakobson descrito por Villela (2016), é um dos diversos modelos encontrados na bibliografia sobre o tema que ilustra como seria o caminho da informação entre o emissor e receptor:

Figura 6 - Modelo de Comunicação de Jakobson



Fonte: Villela (2016, p. 15).

Após algumas reflexões que fiz durante este estudo, problematizo a quantidade de intermediários que estão entre o polo emissor e receptor. Compreendendo o papel que cada um desempenha, é importante refletir que apesar de ser um mesmo dado que percorre por todos eles, o metadado produzido durante o trajeto é extraído de acordo com os interesses de cada um:

Figura 7 - Representação das diferentes empresas que participam da transmissão de uma mensagem entre 2 atores

Fonte: Elaborada pelo autor (2019).

Cada elemento descrito na imagem acima possui importância na transmissão da mensagem. Há intenção de cada código, ou dos códigos, que estariam dentro de

canal, serem aos próprios interesses de cada empresa. A empresa telefônica, com seus protocolos que identificam cada usuário dentro da sua rede para fins de cobrança, os fabricantes que possuem os códigos básicos para operar à nível de *hardware*, os desenvolvedores do sistema operacional que, por sua vez, possuem um gerenciamento macro de todo o dispositivo – volta para o fabricante, novamente, com algumas aplicações proprietárias desenvolvidas para o sistema operacional – o provedor de acesso à internet se o dispositivo estiver em uma rede Wifi e, por fim, os desenvolvedores dos aplicativos. Todos esses pontos de passagem da mensagem possuem suas próprias regras de negócios, algoritmos e bases de dados individuais, permitindo que a mesma mensagem seja armazenada em diversos pontos simultaneamente, com dados e metadados.

As formas de trackeamento apresentadas, visando monitoramento e vigilância, tem como foco majoritariamente a entrega de anúncios segmentados e utilizam os dados para tentar entender o comportamento dos indivíduos. No entanto, a coleta de dados tem seu outro lado: controle. Alguns questionamentos ficaram pairando pela minha cabeça, mas, infelizmente, o tempo não foi hábil para seguir nesta linha. Perguntas como: as formas que estes dados coletados perfilam a ponto de propiciar algum benefício ou punição aos usuários; como se dá a percepção – ou se ao menos há uma percepção – desse controle sobre as nossas vidas; qual a forma – e se há uma forma – de mantermo-nos menos influenciados pelo poder do raciocínio algorítmico.

Alguns pontos interessantes em que este trabalho poderia progredir: realizar um estudo dos impactos físicos, na sociedade, resultantes das tomadas de decisões automatizadas que utilizam a massa de dados produzidas por cada indivíduo; entender os players que mais se beneficiam disso e como eles utilizam – ou poderiam utilizar – tal insumo; analisar, por uma ótica de um cenário positivo, que há, de fato, um ganho à população já que tratamos de mobilidade e com isso podemos pensar em cidades inteligentes, mas também há o cenário caótico que pode servir para potencializar a repressão de públicos indesejados em locais distantes, evitando que saiam dos seus espaços “predestinados”.

Por fim, entende-se que este trabalho contribuiu para resgatar e agrupar, através de um conjunto de referências, um apanhado importante sobre o atual estado das formas de coleta de dados distribuídos em redes de comunicação móvel. Buscou-se construir um movimento arqueológico que abrangesse as especificidades

tecnológicas e culturais das transformações pelas quais a comunicação móvel passa e que acabam por impactar na privacidade. Os apontamentos expostos não encerram as indagações inicialmente realizadas; potencialmente, sinalizam alguns caminhos a serem percorridos para possíveis soluções e, principalmente, indicam possibilidades para o aprofundamento das pesquisas em torno do tema.

REFERÊNCIAS

3G. *In:* Wikipedia: A enciclopédia livre. Wikimedia Foundation, 23 mar. 2019. Disponível em: https://pt.wikipedia.org/wiki/3G#Caracter%C3%ADsticas. Acesso em: 09 jun. 2019.

ALECRIM, Emerson. **Tecnologia bluetooth:** o que é e como funciona? *In:* Infotester [S. l.], 2018. Disponível em: https://www.infowester.com/bluetooth.php. Acesso em 25 maio 2019.

ALENCAR, Marcelo Sampaio De. **Telefonia celular Digital**. 1. ed. Érica: São Paulo, 2004.

ARAUJO, André. **Arqueologia das mídias pela literatura.** *In:* LTDA, Appris (Ed.). A(na)rqueologia das mídias. 1. ed. Curitiba. p. 311.

BATISTA, Marcela de Moraes; FARINIUK, Tharsila Maynardes Dallabona; MELLO, Sérgio Carvalho Benício de. **Smartsurveillance em aplicações recentes no Brasil: um estudo de caso nas cidades de Recife e Curitiba**. [s. l.], p. 34, 2016.

BEIGUELMAN, Giselle; LA FERLA, Jorge. **Nomadismos tecnológicos**. São Paulo.

BINE, Jamilson; KUK, Josiel Neumann. **Estudo de segurança em dispositivos móveis**. [s. l.], p. 1–30, 2013.

BIONI, Bruno Ricardo. **Proteção de dados pessoais**. São Paulo: Saraivajur, 2018.

BOAS razões para fazer mobile. *In: Think with google*. [*S. l*], jun 2015. Disponível em https://www.thinkwithgoogle.com/intl/pt-br/marketing-resources/metricas/por-que-mobile/. Acesso em: 26 jun. 2019.

BOFF, Salete Oro; FORTES, Vinícius Borges; FREITAS, Cinthia Obladen de Almendra. **Proteção de dados e privacidade**. Rio de Janeiro: Lumen Juris, 2018.

BRASIL tem 230 milhões de smartphones em uso. *In:* Época Negócios [*S. l*]*,* 2019. Disponível em https://epocanegocios.globo.com/Tecnologia/noticia/2019/04/brasil-tem-230-milhoes-de-smartphgones-em-uso.html. Acesso em 19 jun. 2019.

BRUNO, Fernanda. **Dispositivos de vigilância no ciberespaço:** duplos digitais e identidades simuladas. Revista Fronteiras, [s. l.], v. 2, n. 2, p. 152–159, 2009. Disponível em: http://revcom2.portcom.intercom.org.br/index.php/fronteiras/article/view/3147/2957. Acesso em: 10 mai. 2019.

_____. **Monitoramento, classificação e controle nos dispositivos de vigilância digital.** Revista Famecos, [s. l.], v. 15, n. 36, p. 10, 2008.

CALHEIROS, Tânia da Costa. TAKADA, Thalles Alexandre. **Reflexões sobre privacidade na sociedade da informação.** Informação@Profissões. v. 4, n. 1, p. 251, 2005. Disponível em: http://www.uel.br/revistas//uel/index.php/infoprof/article/view/22564. Acesso em: 20 jun. 2019.

CAMARA, Marlon; Bluetooth: **O que é e como funciona.** *In:* Techtudo [S. l.], 2012. Disponível em https://www.techtudo.com.br/artigos/noticia/2012/01/bluetooth-o-que-e-e-como-funciona.html. Acesso em 24 maio 2019.

CARVALHO, Victor. **Novo Bluetooth 5.1 será tão exato que poderá medir seu posicionamento com centímetros de precisão.** *In:* Tudocelular [S. l], 2019. Disponível em https://www.tudocelular.com/tech/noticias/n137129/bluetooth-5-1-tera-localizacao-de-grande-precisao.html. Acesso em: 25 maio 2019.

CÓDIGO QR. *In:* Wikipedia: a enciclopédia livre. Wikimedia Foundation, 22 abril 2019. Disponível em https://pt.wikipedia.org/wiki/C%C3%B3digo_QR. Acesso em: 25 jun. 2019.

DEFLEUR, Melvin L. (1966) **Teorias da Comunicação de Massa.** Jorge Zahar Editor. Rio de Janeiro, 1976.

ESTAÇÃO de rádio Base. Wikipedia: a enciclopédia livre. Wikimedia. 2017. Disponível em: https://pt.wikipedia.org/wiki/Esta%C3%A7%C3%A3o_Radio_Base. Acesso em: 02 mai. 2019.

FARBER, Dan. **Jobs:** *Today Apple is going to reinvent the phone*. *In:* Zdnet [S. l], c2007. Disponível em: http://www.zdnet.com/article/jobs-today-apple-is-going-to-reinvent-the-phone/. Acesso em: 18 jun. 2019.

GODDARD, Michael. Arqueologia das mídias, “anarqueologia” e ecologia das mídias. *In:* LTDA, Appris (Ed.). **A(na)rqueologia das mídias.** 1. ed. Curitiba. p. 311.

GOOGLE. **Gerenciar Atividade de voz e áudio do Google**. 2019. Disponível em: <https://support.google.com/websearch/answer/6030020>. Acesso em: 23 jun. 2019.

GREGORI, Isabel Christine De; HUNDERTMARCH, Bruna. **A fragilidade da proteção do direito à privacidade perante as facilidades da internet**. [s. l.], p. 749–764, 2013.

HENRIQUES, Sandra. ***The journalistic portrait***. [s. l.], v. 3, p. 81–96, 2016.

HISTÓRIA do telefone celular. *In:* Portal São Francisco. [S. l.], 2019. Disponível em: https://www.portalsaofrancisco.com.br/historia-geral/historia-do-telefone-celular. Acesso em: 02 maio 2019.

INATEL. **Uma breve história do mundo conectado:** do código morse às *smart cities*. 2019. Disponível em: https://rdstation-static.s3.amazonaws.com/cms%2Ffiles%2F15904%2F1553607519ebook_TIC_2019.pdf. Acesso em: 15 jun. 2019.

JESZENSKY, Paul Jean Etienne. **Sistemas telefônicos**. 1. ed. Barueri: Manole, 2007.
JOBS, Steve. **Steve Jobs *announcing the first iPhone in 2007***. 2011. Disponível em: https://www.youtube.com/watch?v=wGoM_wVrwng. Acesso em: 18 jun. 2019.

KAHL, Marcelo et al. **Computação Ubíqua**: Tecnologia Sem Limites. [s. l.], p. 11, 2011.

KLEINA, Nilton. **A história da BlackBerry:** do passado glorioso ao presente discreto [vídeo] *In:* Tecmundo. [S. l], 23 maio 2017. Disponível em: https://www.tecmundo.com.br/blackberry/116811-historia-blackberry-passado-glorioso-presente-discreto-video.htm. Acesso em 22 jun. 2019.

KONDER, Carlos. **Privacidade e corpo:** convergências possíveis. Pensar - Revista de Ciências Jurídicas, [s. l.], v. 18, n. 2, p. 354–400, 2014.

LEMOS, A. **Mídias locativas e vigilância:** sujeito inseguro, bolhas digitais, paredes virtuais e territórios informacionais. Porto Alegre, p. 621–648, 2010. Disponível em: http://scholar.google.com/scholar?hl=en&btnG=Search&q=intitle:MÍDIAS+LOCATIVAS+E+VIGILÂNCIA+:+sujeito+inseguro+,+bolhas+digitais+,+paredes+virtuais+e+territórios+informacionais#0. Acesso em: 10 mai. 2019.

LEMOS, André Luiz Martins; ARAUJO, Nayra Veras de. **Cidadão Sensor e Cidade Inteligente:** Análise dos Aplicativos Móveis da Bahia. Revista Famecos, [s. l.], v. 25, n. 3, p. 28708, 2018.

LEMOS, André. **Cibercultura e Mobilidade:** A Era da Conexão. [s. l.], p. 1–17, 2005. Disponível em: http://www.intercom.org.br/papers/nacionais/2005/resumos/r1465-1.pdf. Acesso em: 10 mai. 2019.

_____. **Cultura da mobilidade**. *In:* Nomadismos tecnológicos. [s. l.], p. 278.

_____. **De que vigilância estamos falando?** [s. l.], 2009. Disponível em: http://www.compos.org.br/data/biblioteca_1176.pdf. Acesso em: 10 mai. 2019.

LINS, Bernardo F. E. **Privacidade e internet**. 2000. Disponível em: <https://www2.camara.leg.br/atividade-legislativa/estudos-e-notas-tecnicas/publicacoes-da-consultoria-legislativa/arquivos-pdf/pdf/001854.pdf>. Acesso em: 10 mar. 2019.

MACHADO, Irene. **O que há de novo no século XX?** Sobre o curso Arqueologia das mídias. 2001.

MANTOVANI, Camila Maciel Campolina Alves; MOURA, Maria Aparecida. **Informação, interação e mobilidade.** Informação & Informação. v. 17, n. 2, p. 55–76, 2012.

MARTIN, Chuck. **Mobile marketing:** a terceira tela - como estar em contato com seus clientes através de Smartphones, Tablets e outros dispositivos. 2013. Disponível em: http://search.ebscohost.com/login.aspx?direct=true&db=cat06772a&AN=uni.410383&site=eds-live. Acesso em: 10 mai. 2019.

MARTINS, Valquíria Marchezan Colatto; OLIVEIRA, Marta Olivia Rovedder de; CORSO, Kathiane Benedetti. **Sou o que eu consumo?** Smartphones e o Self Estendido a Luz de Paradoxos Tecnológicos. Revista Brasileira de Marketing. v. 17, n. 03, p. 329–343, 2018.

MELANINHO, Guilherme; THEREZA, Wesley Barbosa. Uma Rede Social para o Compartilhamento de Ajuda. [s. l.], p. 106–120, 2018.

MONT'ALVERNE, ADELINO. **Jogos Móveis Locativos:** Estudo de casos Brasileiros. [s. l.], 2010.

MORIMOTO, Carlos E. **IrDA**. 2005. Disponível em: <https://www.hardware.com.br/termos/irda>. Acesso em: 19 maio. 2019.

_____. **Smartphones:** guia prático. 1. ed. Porto Alegre.

PARIKKA, Jussi. **Arqueologia da Mídia:** interrogando o novo na artemídia / Media *Archaeology: Questioning the New in Media Arts*. Intexto, [s. l.], n. 39, p. 201, 2017.

PELLANDA, Eduardo Campos. Comunicação móvel no contexto brasileiro. *In:* **Comunicação e Mobilidade**. Bahia, editora da universidade federal. 1. ed. Salvador. p. 11–18.

PNAD Contínua TIC 2016: 94,2% das pessoas que utilizaram a Internet o fizeram para trocar mensagens. *In:* Agência de notícias IBGE. Rio de Janeiro, 2018. Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-sala-de-imprensa/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens. Acesso em 27 mai. 2019.

ROBERTO Landell de Moura. *In:* Wikipedia: A enciclopédia livre. Wikimedia. 18 de maio 2019. Disponível em: https://pt.wikipedia.org/wiki/Roberto_Landell_de_Moura. Acesso em: 27 mai. 2019.

RODRIGUES, Guilherme Rodrigues E. **Smartphones e suas tecnologias**. São Carlos, 2009.

ROHRMANN, Carlos Alberto. **Notas acerca do Direito à Privacidade na Internet:** A Perspectiva Comparativa. 2000. Disponível em: https://www.direito.ufmg.br/revista/index.php/revista/article/view/1165/1098. Acesso em 10 jul. 2019.

SANTAELLA, Lucia. **A estética política das mídias locativas**. Nómadas. n. 28, p. 128–137, 2008. Disponível em: http://nomadas.ucentral.edu.co/nomadas/pdf/nomadas_28/28_12S_Aesteticapoliticadasmidias.pdf. Acesso em 10 jul. 2019.

_____. **Comunicação ubíqua:** repercussões na cultura e na educação. Paulus: São Paulo, 2014.

SANTOS, José Rodrigues. **O que é comunicação**. Lisboa: Difusão Cultural, 1992.

SCHNEIER, Bruce. **Data and Goliath**. 1. ed. New York: W.W. Norton & Company, 2015.

SILVEIRA, Sergio Amadeu da. **Tudo sobre tod@s**. 1. ed. São Paulo: Edições Sesc SP, 2017.

_____. **Revolução tecnológica, automação e vigilância 7**. 2018. Disponível em: <http://www.comciencia.br/revolucao-tecnologica-automacao-e-vigilancia/>. Acesso em: 15 mar. 2019.

SMAAL, Beatriz. **No flagra:** agora você pode rastrear amigos pelo SMS. 2011. Disponível em: https://www.tecmundo.com.br/telefonia/10152-no-flagra-agora-voce-pode-rastrear-amigos-pelo-sms.htm. Acesso em: 19 mai. 2019.

STEUERNAGEL, Robert. ***The cellular connection***. 4th. ed. New York: Sons, John Wiley &, 2000.

TECNOLOGIA E GAMES. **69% dos brasileiros já têm acesso à internet pelo celular, afirma IBGE.** [S. l.], 2019. Disponível em: https://tecnologia.ig.com.br/2018-04-27/acesso-a-internet.html. Acesso em: 03 mai. 2019.

VIERA, Angel Freddy Godoy; FORESTI, Fabricio. **A ubiquidade proporcionada pelos dispositivos móveis e o fluxo da informação.** DataGramaZero - Revista de Informação, [s. l.], v. 16, n. 4, 2015. Disponível em: http://dgz.org.br/abr15/Art_01.htm. Acesso em 10 jun. 2019.

VILLELA, Maria Lúcia. **Um modelo de design de privacidade para o compartilhamento de informações pessoais em redes sociais online.** Tese de doutorado, Departamento de Ciência da Computação, UFMG, Minas Gerais. p. 156, 2016.

WALKIE-TALKIE. *In:* Wikipedia: a enciclopédia livre: Wikimedia Foundation, 12 mai. 2019. Disponível em: https://pt.wikipedia.org/wiki/Walkie-talkie. Acesso em: 03 mai. 2019.

WINDOWS phone deve contar com apenas 0,1% do mercado em 2020, segundo IDC. *In:* Canaltech. 2016. Disponível em: https://canaltech.com.br/produtos/windows-phone-deve-contar-com-apenas-01-do-mercado-em-2020-segundo-idc-79379/. Acesso em: 19 jun. 2019.

YEREGUI, Mariela. **Móveis em movimento**: corpo e território na cena pós-midiática. *In:* Nomadismos tecnológicos. [s.l]: s.n.]. p. 278.

ZUBOFF, Shoshana. *Big Other*: capitalismo de vigilância e perspectivas para uma civilização da informação. *In*: BRUNO, Fernanda et al. (Orgs.). **Tecnopolíticas da vigilância:** perspectivas da margem. São Paulo: Boitempo, 2018.