UNIVERSIDADE DE SÃO PAULO
ESCOLA DE COMUNICAÇÕES E ARTES

MAURÍCIO BARBOSA DA CRUZ FELÍCIO

Privacidade e e-vasão

**Uma visão propositiva sobre a privacidade em meio à aceleração
comunicacional**

São Paulo

2020

MAURÍCIO BARBOSA DA CRUZ FELÍCIO

Privacidade e e-vasão

**Uma visão propositiva sobre a privacidade em meio à aceleração
comunicacional**

Versão Corrigida

Tese apresentada à Escola de Comunicação e Artes da
Universidade de São Paulo para obtenção do título de Doutor
em Ciências da Comunicação.

Área de Concentração: Interfaces Sociais da Comunicação
Orientação: Professora Doutora Lucilene Cury

São Paulo

2020

Nome: FELÍCIO, Maurício Barbosa da Cruz

Título: Privacidade e e-vasão: Uma visão propositiva sobre a privacidade em meio à aceleração comunicacional

Tese apresentada à Escola de Comunicações e Artes da Universidade de São Paulo para obtenção do título de Doutor em Ciências da Comunicação.

Aprovado em:

Banca Examinadora

Prof(a). Dr(a).: _____

Instituição: _____

Julgamento: _____

Prof(a). Dr(a).: _____

Instituição: _____

Julgamento: _____

Prof(a). Dr(a).: _____

Instituição: _____

Julgamento: _____

Prof(a). Dr(a).: _____

Instituição: _____

Julgamento: _____

A Deus, com toda a humildade e gratidão. À Júlia, amor e alegria inabalável, semente da fé, fonte da esperança dentro de mim, vida que exala o perfume raro do jardim do Senhor. Ao fruto da Graça, Clara, na esperança de poder construir um mundo mais amável para sua vida e ser seu pai e amigo por todos os dias de sua vida. Aos meus pais, Mário da Cruz Felício Júnior e Marília Barbosa da Cruz Felício, fortaleza da minha infância, paciência na minha juventude e saudade nos meus dias, para que sigam vivos, iluminados pelos passos que demos e daremos juntos. Aos meus irmãos, Mário da Cruz Felício Neto e Mariza Barbosa da Cruz Felício, que aceitaram uma jornada longa com alguém que já nasceu velho, e são na vida a companhia, o esteio e a amizade. Aos meus padrinhos José Luiz Romão Batista e Antônio Carlos, para que possam dizer do que fizemos juntos durante todos estes anos, na certeza de que seguimos esta jornada unidos até os últimos instantes, inseparáveis no amor e na tormenta. Ao Marquinhos, felicidade e paz, doçura e arte. A toda tropa que me protegeu e me conduziu em cada momento de temor, fraqueza e dúvida. Vocês foram e seguem sendo bons anjos da guarda. Os melhores que alguém poderia ter. A Deus, uma vez mais, que nutriu sonhos no coração pobre de um menino. E que o fez acordar e ver que na vida há amor. Que nada se perde.

Fé, Luz e Paz.

AGRADECIMENTOS

À minha orientadora, por sua humanidade ímpar e por aceitar que eu pudesse seguir seus passos em um caminho de aprendizado e eterna busca.

À Universidade de São Paulo, que foi capaz de mudar a minha história, e a de tantas pessoas. Por ser esperança e conhecimento em meio a tantos desafios.

À sociedade, com meus sinceros agradecimentos, na certeza de recebi o privilégio que faltou a tantas outras pessoas capazes, competentes e merecedoras.

Àqueles que me ajudaram nesta caminhada, amigos de perto e de longe.

RESUMO

FELÍCIO, Maurício Barbosa da Cruz. **Privacidade e e-vasão: Uma visão propositiva sobre a privacidade em meio à aceleração comunicacional**. 2020. 214 f. Tese (Doutorado em Ciências da Comunicação). Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2020.

Análise crítica sobre os contornos da privacidade nos tempos atuais e os modos como a dromocracia, a transestética e o infopoder se coadunam na construção de um imperativo de exposição, interferência e condicionamento da vida em sociedade, sendo infraestrutural para o que se debaterá nas próximas páginas. Para tanto, será feita uma breve análise comparativa sobre itens relevantes na LGPD e em algumas outras legislações ao redor do mundo, a fim de apresentar com clareza o pano de fundo formal no qual se debate tal assunto. Tais questionamentos darão origem à proposta de um termo que possa carregar em seu significado os interesses diversos na invasão da privacidade, além das formas de sedução e internalização do desejo de estar exposto. Estudo localizado na comunicação por entender que este é o terreno de manifestação do eu e de suas articulações. Há também a concomitância do olhar sobre a tecnologia que gera condições distintas sobre a dromoaptidão contemporânea, participando de modo profundo na e-vasão transestética.

Palavras-chave: Privacidade. Comunicação. Dromocracia. Infopoder. E-vasão.

ABSTRACT

FELÍCIO, Maurício Barbosa da Cruz. **Privacy and e-vasion: A propositional view on privacy amid of communication acceleration.** 2020. 214 f. Tese (Doutorado em Ciências da Comunicação). Escola de Comunicações e Artes, Universidade de São Paulo, São Paulo, 2020.

Critical analysis on the contours of privacy in the present times and the ways in which dromocracy, transesthetics and infopower are combined in the construction of an imperative of exposure, interference and conditioning of life in society, being infrastructural for what will be discussed in the next pages. To this end, a brief comparative analysis will be made on relevant items about LGPD and in some other legislations around the world, in order to clearly present the formal background in which this issue is debated. Such questions will give rise to the proposal of a term that could carry in its meaning the diverse interests in the invasion of privacy, in addition to the forms of seduction and internalization of the desire to be exposed. This study is located in communication because this is the field of manifestation of the self and its social articulations. There is also the concomitance of looking at technology that generates different conditions on contemporary dromoaptitude, participating in a profound way in transaesthetic e-vasion.

Keywords: Privacy. Communication. Dromocracy. Infopower. E-vasion.

SUMÁRIO

INTRODUÇÃO	9
SUJEITO E TECNOLOGIA	23
PRIVACIDADE	73
DIREITO E PRIVACIDADE	119
INFOPODER E SUAS ARTICULAÇÕES	150
E-VASÃO – UMA PROPOSTA CONCEITUAL.....	176
CONCLUSÃO.....	198
REFERÊNCIAS.....	203

INTRODUÇÃO

As reflexões que se apresentarão neste trabalho são fruto de muitas observações ao longo dos anos de estudo, principalmente durante a realização do mestrado pela mesma instituição que agora recebe esta tese para análise.

À época, refletindo sobre o direito ao esquecimento e as estruturas de memória, em seus aspectos comunicacionais, foi possível perceber que o esquecimento buscado estava vinculado a uma visão de si, ou a uma necessidade de imagem diferente daquela apresentada não apenas pelos buscadores da internet, mas também pela mídia e pela sociedade.

Um processo angustiante de ressignificação da imagem de si apresentada por outros actantes que muitas vezes estavam preocupados com a defesa da verdade, como grande instituição balizada pela retórica factual, e que se esqueciam ou se permitiam ignorar os impactos na vida específica, na realidade cotidiana do indivíduo que era suporte da verdade, suporte da notícia, pretexto da comunicação.

Esta invasão descompromissada da vida alheia com o pretexto do atendimento do interesse público aguçou o incômodo ao passo que as tecnologias da informação e comunicação (TICs) estavam subvertendo parcialmente seu potencial emancipatório para se tornar fator coercitivo em casos específicos.

Com o aprofundamento da pesquisa, foi possível compreender que as tecnologias de comunicação não estavam sendo distorcidas, pura e simplesmente, mas estavam concretizando parte do seu destino manifesto da cibernética (WEINER, 1954) na medida em que se conectavam, constituíam redes de dispositivos inteligentes, ampliando sua função de comunicação para a função de vigilante e de observador, tendo em consideração que a cibernética tem sua origem nas estruturas de comunicação e controle com fins militares, e como tal, já veio ao mundo sustentada por uma rede de dados e de marcadores que evoluíram ao longo do tempo para construir as derivações comerciais e mercadológicas de usos variados que se dão através de computação embarcada em dispositivos comuns e na conectividade cruzada entre tais aparelhos e também com a internet.

Quanto mais inteligente as tecnologias de comunicação foram se tornando, ainda mais aumentavam seu potencial de interferir sutilmente na vida das comunidades.

Esta interferência é indicada como sutil justamente por ter seu uso e função normalizadas ao longo do tempo, de modo acelerado que nem sempre é percebido por estar envolto em camadas de sedução e estética que camuflam os movimentos infraestruturais.

A percepção de que o grande vigilante havia sido dissipado em pequenos dispositivos de captura de dados (Grande Irmão vs Pequeno Irmão) foi se tornando nítida de tempos em tempos com a proliferação dos dispositivos vestíveis sendo alardeada majoritariamente como algo obviamente benéfico nos noticiários e rodas de conversa; aumento da capacidade de processamento dos aparelhos celulares, fazendo os computadores de décadas atrás parecerem reles calculadoras com apelo estético e placa gráfica; configurações pré-definidas de compartilhamento de dados a partir dos sistemas operacionais, sem que isso estivesse em pauta nas grandes redes de notícias ou mesmo nos círculos políticos que deveriam zelar pela sociedade de modo geral; escândalos de vazamento de dados pessoais em massa que apareceram na mídia e rapidamente se dissiparam sem grandes impactos na agenda pública.

A cada momento, uma nova informação se unia à inquietude sobre o caminho que a sociedade estava trilhando através da tecnologia de modo tão estupefado e encantado sem que se discutisse aprofundadamente sequer o caminho desejado, quem dirá seu fim, seu marco de chegada.

Compreender que mais do que serem contempladas, as novas telas estavam observando e reagindo a cada comportamento foi o gatilho necessário para dar início à segunda fase da pesquisa, com o objetivo de compreender como alguns dos fatores contemporâneos se somam para criar um sentimento epocal em que a tecnologia segue encantadora, sentimento este que pode ser apenas o resultado de séculos de desenvolvimento e que não necessariamente será transitório, sendo que alguns fatores cruciais para a manutenção dialógica da sociedade se mantêm em segundo plano, ao menos no modo aparente no período em que esta pesquisa teve seus primeiros traços dados.

Na busca por um denominador comum que abarcasse a tecnologia, o maravilhamento tecnofílico, a morosidade legislativa e a complexidade midiática, encontrou-se mais ao centro do estudo anterior a questão da privacidade, fazendo perceber que o direito ao esquecimento era uma parte gravitante de um complexo

maior, com potencial de construir ou desconstruir mais do que um campo da vida específico, mas a sociedade de modo em suas estruturas democráticas.

Enquanto o estudo anterior tinha características muito específicas, e de certa forma inovadoras pela oportunidade temporal, este novo estudo oportuniza o debate em meio a aplicação da Lei Geral de Proteção de Dados (LGPD) no Brasil, que no momento de confecção desta tese encontrava ainda atos protelatórios do poder Legislativo, demonstrando a pertinência do tema dentro de um lapso temporal relevante, mas também não estará restrito a isto, uma vez que se buscará trazer à luz uma percepção ainda macroscópica dos movimentos resultantes e que resultam neste fio condutor contemporâneo que sutilha a coleta de dados e a exposição da privacidade a ponto de reconfigurar o discurso sobre o que vem a ser este campo do privado, quais suas funções e valor na sociedade.

Após a banca de qualificação, foi possível perceber que entre tantos caminhos expostos e propostos, aquele que carregava o maior potencial de contribuição provocativa para a comunidade acadêmica e para a sociedade estava intimamente ligado ao presente-futuro da privacidade e as diversas formas contemporâneas de assediá-la.

Diversos exemplos foram apresentados para e pela banca que estavam em consonância com este tema e com a visão de que seu potencial e importância seriam únicos entre as opções.

Muitos motivos poderiam ser narrados neste momento, mas espera-se que o próprio trabalho seja capaz de falar por si na consolidação da relevância do tema na vida e futuro da sociedade cibercultural.

Contudo, grande parte do desafio desta tese foi manter sua relevância ao longo do tempo, com discussões que pudessem representar a realidade do tempo da entrega, e não de dois ou três anos pregressos, o que já significaria tempo suficiente para envelhecer muitos exemplos e aumentar ainda mais a obsolescência inevitável destas palavras que seguirão.

Então cada página teve que ser produzida na busca de um olhar no presente-futuro e, principalmente, com um caráter provocativo, prestando um papel de instigar mais questionamentos do que oferecer respostas propriamente ditas.

Isso fez também com que as referências bibliográficas fossem revisadas constantemente para garantir ao máximo que os pensadores aplicados no corpo do trabalho estivessem com suas contribuições ao máximo atualizadas, novamente, na mesma busca necessária pela proximidade das referências ao tempo de leitura e questionamento do aparato tecno-social.

Houve um esforço em manter no texto as referências mais recentes para que a provocação mantivesse o frescor dos debates contemporâneos, ainda mais ao se considerar o período de transição de eras tecnológicas e que na dromocracia cibernética (TRIVINHO, 2007) tal aceleração tanto não cessará quanto seguirá na base das transformações vindouras que já estão, desde muito antes de compreendermos, sendo fermentadas na vida em sociedade, e que culminará em novas derivações do que hoje está a se debater sobre privacidade e demais temas correlatos, assim como todos os outros aspectos da cibercultura.

Muitos autores fizeram parte da construção do pensamento majoritário, e com a evolução do trabalho, suas citações foram suprimidas, e tomaram seus lugares as referências mais recentes.

De toda forma, os principais autores estarão indicados nas referências finais, mesmo que tenham sido extraídos do texto, uma vez que colaboraram sobremaneira para a construção do pensamento aplicado a cada página.

Todavia, aqueles que tiveram uma relevância menor ou pouca inovação no processo de levantamento e pesquisa frente aos autores mais impactantes na construção da tese foram retirados inclusive das referências, uma vez que parte do esforço da academia também é auxiliar no processo de curadoria do conhecimento e do pensamento.

Desta forma, evita-se dispersão daqueles que porventura pretenderem utilizar esta tese seja como ponto de partida para a pesquisa, seja como complemento ou referência para algo que esteja em andamento.

Claro que há, sabidamente, um viés da curadoria feita durante a produção desta tese, como ocorre em todos os trabalhos, e que incessantemente todo pesquisador busca dirimir. Todavia, é relevante tais declarações para alertar e relembrar a todos que o trabalho em tela não está livre de representar apenas uma fração do tema, e com certo viés.

Dá-se tal lembrete para que, mais do que saber do possível viés, sejam os colegas pesquisadores e leitores novos avaliadores que venham a apontar tais falhas em busca do aprimoramento científico da falseabilidade, primorosa e necessária tanto na ciência quanto em tempo de fanatismos ideológicos.

Isso toca outra inquietação que deu forma à tese que é a avaliação do quanto é infrutífero prolongar alguns debates ao invés de tocar mais constantemente nas feridas necessárias para a transformação da sociedade.

Assim, em lugar de exercícios retóricos longitudinais que poderiam demonstrar o preciosismo ou a verborragia, em cada capítulo decidiu-se ser mais incisivo e focado no cerne das questões, a fim de não dispersar a atenção sobre as batalhas vinculadas à privacidade no tempo atual.

Esta característica incisiva e provocativa deverá permear a tese de modo constante, fato que possivelmente dê contornos grosseiros em muitos momentos, parecendo certa aversão tecnológica.

Faz-se então cabível declarar que, para o autor, a tecnologia não é em si um bem ou um mal, mas um fato. Seus usos e aplicações trazem impactos distintos que podem sempre serem vistos em espectros amplos de favorabilidade ou desfavorabilidade, de acordo com os interesses e ponto de vista daqueles que os analisa.

Tal provocação e traços grossos sobre os impactos da tecnologia nos tempos atuais vai ocupar parte das linhas justamente por compreender que o papel de destacar os benefícios já está sendo feito tanto pelas empresas, quanto em muitos discursos positivistas, embalado pelo progressismo, carecendo então de maiores alertas sobre o seu contraponto.

Buscou-se também, ainda sobre a escrita, suprimir ao máximo as miudezas dos exemplos, na tentativa de garantir que tais exemplos sigam como facilitadores da compreensão e evitando que desloquem o debate para especificidades e peculiaridades que pouco se conectem com o tema geral.

Pouco sentido teria seguir constantemente avaliando a tecnologia em exemplos práticos de momentos em que a Internet das Coisas ainda estava nos seus primeiros dias ou os aparelhos celulares ainda tinham décimos da capacidade de processamento atual.

Há de se perceber que poucos são os casos de exemplos práticos na medida em que foi necessário fugir dos especificismos que podem ser suplantados por exemplos mais relevantes, mas ao mesmo tempo, casos de alta relevância foram mencionados em momentos oportunos.

Ao leitor é estendido o convite para que consiga aplicar o debate que se oportuniza aqui em diversos outros exemplos práticos, sejam de ordem nacional ou global, sejam de foro íntimo.

Seguindo também a expectativa que emana de toda tese de doutoramento, foi preciso romper as amarras da replicação, no sentido de que houve o empenho e grande esforço em busca do rompimento das esferas narrativas de cada pensador de forma a integrar ao máximo as suas falas a um fio que pudesse, não forçosamente, auxiliar no entendimento do que ocorre nos dias atuais.

Desta forma, as páginas vindouras apresentam certa ousadia heterodoxa de combinar, muitas vezes, autores que jamais estiveram frente a frente para um debate, mas cujas ideias precisam entrar em diálogo, seja consonante, seja dissonante, para construir uma visão ampla da contemporaneidade e de sua aplicação ao tema proposto.

Tal esforço se mostra arriscado uma vez que muitos conceitos precisaram ser provocados em sua essência para que dialogassem com estruturas mais complexas do discurso sobre a contemporaneidade, ainda mais ao perceber que o tempo presente segue seu inexorável fluxo de aceleração sem se importar com as caixas nas quais tentamos aprisioná-lo.

O caminho mais simples seria seguir com capítulos extremamente estruturados com um longo rol de citações.

Mas se buscou nas citações e referências a robustez da academia, e ao mesmo tempo, permitiu-se ir além da leitura, obrigação formal de todo processo de doutoramento.

Foi necessário fazer colidirem pensamentos que, separados, já são relevantemente críticos, como a dromocracia cibercultural de Trivinho (2007), o capitalismo transestético de Lipovestky e Serroy (2015), o infopoder de Masur (2017), a infovigilância dos dispositivos de comunicação de Bruno (2013).

Juntos, estes autores seminais darão o pano de fundo combinado, extremamente necessário para compreender os encaminhamentos propostos, uma vez que buscam esclarecer qual o fio condutor que está a guiar a conduta social de modo amplo em conjunto com a tecnologia, sua infraestrutura, usos e aplicações por diversos actantes.

São de relevância ímpar, apoiando a visão sobre a aceleração como infraestrutura de origem longínqua, que move todos os processos e que, na cibercultura, através da camada social vinculada às tecnologias em rede, se tornam ainda mais aceleradas, exigindo a dromoaptidão de todos no manejo, na atuação comunicacional e performática, demandando um entendimento sobre o imperativo transestético apresentado por Lipovestky e Serroy (2015) que vai fortalecer ainda mais o campo da visualidade, da visibilidade, mas não apenas este.

A dromoaptidão, habilidade de seguir o ritmo acelerado da dromocracia, e aplicá-la nos processos comunicacionais diversos, seja no trabalho, em casa, com os amigos, em todas as etapas da vida, participará de forma importante da construção do pensamento que se apresenta nesta tese.

É através da internalização das regras, da dromoaptidão, aplicada à efemeridade estética e aos movimentos do infopoder através dos meios de comunicação, entretenimento e vigilância que será possível atingir o cerne do debate que impacta a privacidade e seu estatuto de valor, seja para a análise presente, seja para um exercício de intelecção sobre como poderá se tornar esta questão a médio prazo.

Enquanto o primeiro autor tratará a aceleração aplicada a todas as camadas da vida em sociedade, o segundo indicará como tal aceleração se aplica no panóptico hiperestético a ponto de internalizar a demanda estética e transformar a arte em ápice contemporâneo do poder simbólico.

Tal panóptico foulcaultiano, porém, aqui se verá de modo distinto, não sendo um governante ou uma estrutura de repressão militar ou governamental, psiquiátrica, mas sim o fluxo mercadológico e imagético que trará forma para as atuações na esfera social.

Será através da visualidade que todos os outros sentidos seguirão estetizados para que sirvam ao capitalismo transestético, como uma força performática que exigirá

um comportamento de exposição, de inflação estética constante e alta efemeridade visual.

Tal estetização se mostrará como imperativa e ao mesmo tempo sutil para aclarar quem está sendo premiado, reconhecido como dromoapto no campo de negociações, e ao mesmo tempo deixará evidente quem está sendo relegado à margem do sistema.

O discurso identitário passará tanto pela efemeridade transestética quanto pelo uso dos meios de comunicação, entretenimento e vigilância com maestria dentro do escopismo panórgico, melhor explicado ao longo da tese.

Somado a tudo, virá o infopoder como forma maior do poder, não como segmento específico, para trazer à tona os impactos da datificação da vida contemporânea, resultante dos dois diagnósticos precedentes, dromocracia cibercultural e capitalismo transestético.

Tal infopoder se aplicará como troféu compartilhado daqueles que foram dromoaptos o suficiente para apresentarem suas identidades articuladas e construídas com a matéria-prima da hiperestética e expostas nos meios de comunicação como espaço de validação e premiação.

Mas o infopoder também agirá na conversão dos meios de comunicação e entretenimento em meios de vigilância e evasão da privacidade.

É através dele que os meios de comunicação, como dito rapidamente em linhas anteriores, se converterão em estruturas de vigilância (BRUNO, 2013), seguindo o destino manifesto da cibernética, que está na base estruturante da comunicação tecnológica deste novo século.

Lembrando que tal controle não precisou ser forçosamente inserido nos meios de comunicação tecnológicos, mas sim aclarados e bem utilizados para que emergisse da base as formas de monitoramento do uso e do usuário de cada dispositivo.

A conexão em rede permitiu que tal controle se tornasse parte de um sistema maior de coleta, armazenamento e tratamento de dados (FLORIDI, 2014) que também será oportunamente trabalhado.

Assim, não é uma deturpação da estrutura que faz com que os dispositivos tecnológicos se tornem vigilantes.

É apenas a sua utilização em máxima capacidade que extrairá da tecnologia mais do que o processo comunicacional do indivíduo para seus interesses específicos, fazendo com que cada momento de uso, cada dado capturado possa servir também a um sistema econômico que, por sua vez, se utiliza do sistema político e da utilização das violências para se legitimar e se expandir.

Usando-se da estetização da comunicação, o infopoder será capaz de sutilar sua força e conduzir os agentes a um desejo de exposição em busca de maior visibilidade e reconhecimento.

A infoesfera estetizada será alimentada pelas informações fornecidas pelas próprias pessoas, desejantes de reconhecimento em um campo que demanda apelo estético e exposição, mas ao mesmo tempo efemeriza todas as manifestações, tornando necessário um fluxo de exposição que se torna compulsório, permeando a vida comum e espetacularizando até as tarefas mais básicas como os momentos de almoço ou jantar, quantos copos de água se toma num dia.

Assim, cada indivíduo se torna desejante de que sua intimidade seja exposta de modo interessado e articulado para conquistar a aprovação social na nova ágora que vai combinar o online e o offline.

Neste ponto, Floridi (2014) será trazido para auxiliar principalmente na percepção de que a vida contemporânea não mais se divide nas categorias conectada (*online*) e desconectada (*offline*) mas que os processos comunicacionais alteram nossa dinâmica social e individual fundando o *onlife*.

Não é mais a internet conectada a um dispositivo que define se as pessoas estão ou não conectadas entre si.

Isso por dois motivos relevantes. O primeiro se dá pela incorporação da plasticidade dos meios de comunicação na mentalidade e conduta, que condicionam os atos praticados.

Significa que mesmo sem sinal no celular, a mente do indivíduo segue articulando sua forma de agir no mundo levando em conta sua conectividade passada, presente e futura.

Ou seja, a cibercultura transtética não se resumirá aos momentos específicos de exposição pública, mas antes disso precisará ser internalizada e produzir um modo de pensar que articule os valores deste campo de modo coerente e prepare a próxima exposição de modo que seja condizente com a estética transitória prevalente em cada momento.

O segundo ponto que impede a desconexão é justamente a vigilância compulsória dos meios de comunicação em rede, principalmente nas grandes cidades, e que estão a todo momento impactando, através dos dados e dos gatilhos da tecnologia, a vida das pessoas, ponto este que aparece de outra forma em Floridi (2014), mas que pode ser derivado do que se verá ao longo desta tese e fará corpo para conduzir à proposta do conceito que abará os movimentos de dados que ocorrem a partir do que foi e será exposto aqui.

Da mesma forma, o *onlife* que se vê nestes dois itens acima se combinam ainda para criar duas outras entidades de alteridade.

A comunidade dos actantes, amigos, família e todos os interlocutores que seguem *onlife* (FLORIDI, 2014) e que, como tal, impactam diretamente com sua mentalidade cibercultural até mesmo a vida do mais desconectado dos cidadãos.

E a segunda entidade é a percepção do observador oculto, o grande irmão algorítmico que será, em dado momento deste trabalho, ressignificado através das estratégias transtéticas de entretenimento e camuflagem do infopoder, que Balick (2014) vai chamar de *online social third* justamente em alusão à percepção da observância que interfere no *self*.

Mas é relevante notar que, para esta tese, em muitos momentos em que os autores mencionam o online, o que se aplicará é, sim, o conceito de *onlife* (FLORIDI, 2014).

No exemplo acima, de Balick (2014), o *social third* não está / é apenas o online, mas todos se tornam nós.

Todos os actantes farão parte de uma rede que perpetuará o imperativo transtético dromocrático, em busca do reconhecimento na infosfera, que por sua vez, também não se resume ao digital, mas sim a todas as camadas humanas nas quais é possível criar, observar, capturar, armazenar e tratar dados que farão parte do infopoder.

Solove (2011) e Mayer-Schönberger (2009) ajudarão a dar o aporte contemporâneo da privacidade e das tecnologias de memória.

De toda forma, requer-se aqui que, caso o leitor tenha interesse mais aprofundado em compreender os processos de memória não apenas em Solove e Mayer-Schönberger, que recorra à monografia de mestrado apresentada por Felício (2015), de modo que parte deste contexto já está desenvolvido e pouco sentido faz tornar redundantes os trabalhos.

Através destes autores será possível dar corpo ao debate com foco no papel da tecnologia, no discurso sobre a tecnologia e nas formas de suavização da atuação do infopoder em busca da distribuição compulsória da vida íntima a fim de aumentar as bases de dados que sustentam a infosfera.

E não apenas a vida íntima em si estará exposta, mas também as bases da privacidade, como poderá ser percebido logo adiante.

Outro ponto que será discutido é a relação do eu discursivo, da imagem de si apresentada por cada indivíduo nas mídias que dispõe.

Será relevante para esta discussão a questão da imagem arquitetada justamente por ser produto e produtora do que se percebe acima com a inflação estética e a aceleração como base da conduta social.

É na relação decisória do eu com a sua privacidade, com a escolha de tornar acessível, visível parte da sua vida privada, da sua intimidade e da sua individualidade que está centrado este exercício de compreensão.

Espera-se apresentar de modo mais claro que a construção da privacidade depende de um processo decisional do indivíduo.

Motivo pelo qual, muitas vezes, ao invés de apresentar brechas na privacidade, o termo usado será intimidade, que é uma das manifestações que dão origem à privacidade.

Nos casos de exposição do corpo, da casa, da alimentação, são formas de construir um discurso estético na infosfera com base na intimidade, mas que através da recorrência e dos metadados atrelados, irão tornar possíveis as brechas na privacidade.

Só será possível, tal vulnerabilidade da privacidade, na medida em que a autonomia na tomada de decisão também for afetada, e isso será um ponto precioso para a tese que se apresenta.

Chegará o momento em que se debaterá a infraestrutura de publicidade como exemplo mais comum de interferência na capacidade decisional das pessoas.

Mas, novamente, aqui não se fará um juízo de valor contra ou a favor da publicidade, em si, mas sobre os usos dados a ela.

Da mesma forma, será preciso também aplicar certo esforço em apresentar um quadro jurídico que torna possível tais condutas dos actantes vinculados à questão da intimidade e da privacidade.

Destaque-se, desde já, que também não serão detalhados em minúcias todos os itens da LGPD ou de demais legislações, pois tal análise poderia se perder em novas especificidades ou críticas pouco pertinentes ao quadro geral.

O que se fará é uma curadoria sobre quais itens podem ser relevantes para compreender como se chega à LGPD e os pontos controversos mais relevantes para esta tese.

Abre-se, então, mais um convite para que os colegas pesquisadores e leitores sigam o mesmo exercício, analisando a LGPD de modo mais aprofundado nos outros impactos que ela traz para a sociedade de modo normativo.

Além da legislação brasileira, serão apresentadas partes dos textos legais de outros países como forma de compreender como a questão da privacidade está sendo conduzida na esfera jurídica ao redor do mundo.

Novamente, apenas alguns países se mostraram relevantes para seguirem como referência neste trabalho.

Se mostrará relevante também a questão da tutela da defesa da privacidade, na medida em que esta será apresentada de forma que não se produza e tenha valor apenas para direito individual.

Na medida em que a privacidade será tratada como necessária para o desenvolvimento da democracia como é constituída nos dias atuais, se questionará a quem deverá caber a tutela e o dever de zelar pelo estabelecimento de garantias para a proteção da privacidade.

Na mesma seara estará a questão do direito a alienação da privacidade, lembrando que neste caso não há o limite do termo ao campo da intimidade física, mas algo maior, que significa questionar se cada indivíduo tem o direito de entregar a outro parte do seu processo decisional através da exposição de sua privacidade de modo amplo.

Finalmente, para os limites deste trabalho, será proposta a compreensão de todos os itens acima, de modo conjunto, como estrutura consolidadora do que se chamará de e-vasão.

Conceito realmente propositivo, provocativo, que busca consolidar os movimentos invasivos e evasivos da privacidade através da compreensão de que ambos os movimentos são, em si, um só, na lógica contemporânea que foi historicamente estimulada para gerar em cada indivíduo um desejo de exposição performática.

Em outras palavras, a e-vasão servirá para evocar, no momento de cada debate, tanto o movimento do dado, considerando seu vetor de fora para dentro ou de dentro para fora, e também o acultramento para a internalização da datificação como fluxo discursivo identitário.

De tal modo, movimento de dado e ideologia epocal estarão conectados para significar mais do que a entrega ou invasão de dados, mas sim um modo de estar no mundo que condiciona a mentalidade da vigilância com contornos específicos e desejados para a conformação do campo de negociações transestéticas do e para o infopoder.

Conceito de movimento de dados, como proposto neste trabalho, é o artefato material, coletável, da conduta humana, que é por sua essência intencional, ainda que tal intencionalidade seja reconhecível na arquitetura da estrutura de coleta. Assim, não necessariamente é o tratamento à posteriori da coleta de dados que construiria a intencionalidade do dado, mas a própria intenção de captura do dado já carrega em si o gérmen dos usos que lhe serão aplicados.

Tal movimento de dados ganha também os contornos posteriores à coleta, reformando e conformando as manifestações informacionais aos estados compreensíveis e depurados da consciência sobre a conduta humana.

Assim, o movimento de dados aqui indicado se dá de formas distintas de acordo com o seu suporte.

O movimento de dados mais facilmente observável está no campo da vida comum, na realidade cotidiana das ações, constituída a partir dos diversos sistemas imanentes à vida em sociedade. A segunda forma de compreender informação sendo movida, vibrada e transformada está nas condutas dos aparatos técnicos de vigilância, que a partir de sua engenharia e arquitetura aplicam uma ideologia específica e reflexiva ao movimento de dados primários que se pretende observar e armazenar. Assim, os aparatos técnicos nesta instância se aplicam na coleta e armazenagem específica das informações, além de, em alguns casos, praticar tratamentos básicos dos dados a partir do ponto de processamento próprio, ou seja, segundo suas capacidades de processamento local. Já ao conectar os artefatos de coleta de dados e vigilância à internet ou qualquer outra rede local, com capacidade de processamento escalável, chegamos à terceira forma de compreender os movimentos dos dados, de modo mais aprofundado na violência sutilizada da e-vasão da vida cotidiana, das manifestações do eu e da sua individualidade sócio-criadora.

Ao atingir este patamar, o dado individual coletado já não precisa mais de chaves, de vínculos únicos para invadir a personalidade e pessoalidade. Mais adiante traremos à luz deste trabalho a discussão do impacto comunicacional do tratamento de dados em larga escala, e neste momento se tornará ainda mais evidente como o nome ou o CPF de um indivíduo se torna desnecessário frente a um arsenal de informação e de técnicas capazes de entender e influenciar comportamentos mesmo sem sequer saber qualquer opinião manifesta de alguém.

Com isso, tem-se visibilidade de que o indivíduo em si não é o alvo das estruturas comerciais e governamentais dos dias atuais, mas sim uma célula necessária para atingir o todo. A vigilância pervasiva de todos os indivíduos na sociedade não se dá pelo interesse específico, mas sim pelo interesse indistinto em todos.

SUJEITO E TECNOLOGIA

Antes de falar diretamente da privacidade, é preciso entender como está posto no cenário o indivíduo que vai ser o lastro de tal direito, de tal prática discursiva e decisiva.

Sem compreender, ainda que rapidamente, o indivíduo, sua forma de articular seu discurso identitário através das TICs, a análise da privacidade se torna ineficiente e leviana.

De modo breve, vale a consideração do que vem a ser o sujeito que interage através das estruturas comunicacionais e de vigilância, a fim de compreender como que a relação entre sujeito e tecnologia se torna possível para a produção do infopoder e-vasivo, conceito este que está melhor explicado ao longo do trabalho em momento oportuno, mas que a princípio deve ser considerado como o ato de evadir, interessadamente, a própria privacidade.

O indivíduo, que nos dias atuais se conecta com as redes sociais digitais, conversa com amigos através de chamadas de vídeo através do Whatsapp ou Skype, o faz com base na percepção da comunicação, do aspecto conectivo da mídia, que amplia suas habilidades e permite se relacionar à distância com incontáveis pessoas e demais actantes¹.

Gradativamente estas estruturas comunicacionais foram se convertendo em estruturas panópticas e em seguida se converteram em um escopismo panórgico através da e-vasão, do interesse em se ver exposto.

Cada indivíduo passa a ser um nó expositor de sua intimidade mediada, reinventada e construída com a percepção de que um código de conduta está a validar a atuação social em meio ao online e offline, mas de forma muito mais abrangente do que os limites da conectividade tecnológica imediata.

Informational conceptions of the self may tend to privilege a dualista view of the relationship between mind and body, more or less along the line of the distinction between hardware and software. Our culture, so imbued with ICT ideas, finds sci-fi scenarios in which you swap your old body for a new one, or the suggestion that the self may be a cross-platform structure, like an app, perfectly conceivable. (FLORIDI, 2014, p. 69)

¹ Por actante entende-se qualquer agente, humano ou tecnológico, que atue sobre um dado ou sobre uma realidade, de modo intencional ou programado.

Através do conceito de *onlife* (FLORIDI, 2014), da permeabilidade e hibridização da vida entre plataformas e o ambiente físico, o indivíduo precisa lutar para construir um eu mediado, um discurso sobre si que beire a naturalidade mas jamais prescindia da articulação discursiva com foco em resultados específicos no espaço da visualidade, da estética.

Centrar o discurso das redes sociais digitais no eu, fato que se torna cada dia mais comum, é ocupar o indivíduo com estratégias de articulação e-vasiva de sua intimidade e de seus dados que condicionam sua aceitação em cada grupo social, no campo simbólico que pretende adentrar, do qual pretende fazer parte, e tal e-vasão de dados e da intimidade passa a ser condição mínima.

Sem a oferta de dados, da privacidade de modo performático, o indivíduo enfrentará barreiras para ser recebido e compreendido como um igual entre os membros dos grupos de interesse.

Importante considerar que a conduta e-vasiva não é um exercício simples ou apenas um ato repetitivo sendo protagonizado pelo indivíduo com suporte das tecnologias, mas uma relação dual, dupla, através da qual indivíduo sustenta seu discurso nas plataformas e tais plataformas se constroem sobre os pilares das e-vasões discursivas.

Não é um exercício, na medida em que não é algo claramente proposto, algo com princípio e fim, mas sim um empenho de energia vital convertida em transformações do tempo e do espaço em estratégias gradativamente mais elaboradas sobre a efemeridade das publicações que precisam deixar transparecer um resquício de unidade discursiva através das diversas estéticas emergentes para que o saldo dos processos de exposição sejam constitutivos de um discurso identitário aceitável e reconhecível como tal.

Excessive narcissistic investment in the self, expressed as an increased concern with the self, is what gives individuals a measure of transitory security in a world in which social networks are fragmenting and traditional value systems are being undermined. (BEHRENDT, 2015, p. 380)

Do ponto de vista do indivíduo, estar centrado em si é ter um lastro em meio a tanta transitoriedade.

Mas ao mesmo tempo em que o eu faz gravitar ao redor de si os discursos produzidos cotidianamente, em um grande fluxo, gravita também as efemeridades e modismos das redes.

O que o autor vai trazer de forma relevante para esta discussão é justamente o sentimento transitório de segurança que há na exposição do seu discurso identitário como forma de estar em contato com a sua comunidade, com as formas de caracterizar a existência e relevância de si.

Comunicação é fator primordial para a criação dos vínculos, e a cada momento se verão muitos pretextos para reafirmação da identidade que se busca arquitetar para ter como recompensa tanto o reconhecimento quanto tal prazer transitório da segurança, do sentimento de pertencimento.

As transience of social relationships became a pervasive feature of modern Western society, personal identity ceased to be embedded firmly in the local community and culture. [...] With social relationships having become temporary and unstable, the need became paramount to have an attractive, likable, and competent self, a self that serves as a means of gaining access to groups, attracting partners, and retaining relationships (BEHRENDT, 2015, p. 381)

Isso pode significar que para ser socialmente atraente e aceitável, um indivíduo pode ser conduzido a entregar parte de sua intimidade e individualidade para que o sistema sedutor de vigilância (BRUNO, 2013) possa ter uma narrativa aceitável sobre si para oferecer aos demais actantes da rede.

As comunidades locais acabam por não ser mais fatores tão decisivos no discurso da identidade.

Espacialidade, copresencialidade já podem ser prescindíveis através dos processos de globalização, que são, em suma, processos comunicacionais mediados pela tecnologia, com impacto econômico de modo amplo, seja na economia financeira, seja na economia inflacionária da estética nas comunidades humanas.

As formas de construir o discurso identitário ganham novos artefatos e caminhos, conectando pessoas em diferentes lugares e tempos.

Assim como as cartas de antigamente eram um processo comunicacional com uma temporalidade própria, o mesmo ocorre com a comunicação em tempos de conectividade global. A diferença é que a potencialidade de exposição e conexão de muitos para muitos, aliada à atemporalidade e sem a necessidade do espaço físico,

faz com que cada indivíduo seja uma miríade de possibilidades complexas de comunicação e discurso.

Porém, mesmo com tantas possibilidades, cada indivíduo só será conhecido e encontrado na medida em que libera seus dados, em que produz rastros de informação, e também considerando a qualidade transestéticas que aplica em suas manifestações.

Desta forma, sem ter ao menos um volume consistente de informações disponível na rede e entre as plataformas de busca e redes sociais, uma pessoa pode acabar enfrentando dificuldades de se relacionar socialmente.

Today, there is nothing unusual about Googling a potential date, an employer or employee, a partner's ex-partner, or even one's potential psychotherapist. As each person has little control about what is collated, the Google search provides only a fragmented view of someone through the elements of his or her life that happen to have gone online, whether it is winning the custard contest at the village fete or having been accused of paedophilia. In this sense, online identities are pre-packaged and ready for quick consumption, creating an automatic, externally "cobbled-together" identity an identity that can hang like a ghost between individuals, affecting their interpersonal relations to varying degrees. This passive cobbled-together online identity operates both intrapsychically and intersubjectively, becoming a part of how we view ourselves, our concerns about how we are viewed by others, and the way others actually view us (BALICK, 2014, p. 29)

Assim, ter conteúdo disponível é ter um álibi social, uma validação.

Este resumo breve e altamente amputado da realidade pode ser o fator de validação para a entrada em algumas redes, em alguns grupos sociais.

Tanto faculdades e empresas podem estar observando diversos movimentos de dados, quanto governos e entidades de interesses diversos.

Estar invisível já não é uma opção. Da mesma forma, estar pouco visível é também recriminável quando todos estão expostos em nome da diversão, alegria, conforto, conexão, segurança, confiança e muitos outros jargões que tomam a frente de utilização das estruturas de vigilância.

[...] as Facebook expands its ecosystem, it becomes more than a forum of self-expression through words on a status update or fotos uploaded from last weekend's party; it becomes a presentation of self based on the music one listens to, the newspapers one reads, and a whole variety of other activities that become public through these social applications. (BALICK, 2014, p. 77)

Desta forma, Balick (2014) vai lembrar que as pessoas expõem suas vidas nas redes sociais de modo que construam formas de conexão com seus amigos e conhecidos.

Tais exposições são intencionais, e já existiam mesmo antes das redes sociais digitais.

Seu impacto contemporâneo se dá tanto pela capacidade de proliferação e disseminação que tais redes têm quanto pela forma como elas, e toda a cibercultura, ressignificam os processos comunicacionais.

Mas comunicar não é apenas publicar informações, consumir informações de outras pessoas e interagir momentaneamente.

A conduta através de movimentos de dados intencionais sob a vigilância e conformação de sistemas como as redes sociais é também um consumo-construção de uma identidade oferecida ao mundo de modo articulado e interessado, com vistas para a conquista de troféus específicos que passam a ser articulados através da máscara social constituída sobre as regras de cada comunidade e sobre a lógica de cada ferramenta.

Cada tecnologia favorecerá um tipo de artefato comunicacional específico, que por sua vez, dará cores distintas ao que se comunica.

The heroic moment becomes choosing a self, a ready-made identity, rather than the, by contrast, apparently mundane task of choice-making in the course of everyday existence. This choice of a new self is really best thought of as the purchase of a new social mask. The self goes to the supermarket, as it were, or Amazon, and takes a new self off the metaphorical shelf: a new social mask behind which to hide and which defines the self from then on. The self then seeks acceptance and recognition for this self from others: which, if not forthcoming, prompts an often furious and intolerant reaction. An understandable enough reaction given the self is in the process of trying to give meaning to and reason for its very existence. (FUREDI, 2019, p. 203)

As formas de manifestação estão sempre em acelerada transformação, fazendo emergir modos diferentes de comunicar o eu a cada período.

Furedi (2019) vai falar de um dos modos contemporâneos que é a selfie, fotografia batida pela própria pessoa sobre si mesma, podendo ter um cenário ou mais pessoas ao fundo, e que ganhou espaço com redes como Instagram nos anos mais recentes.

O ponto interessante é a compreensão de que a selfie atualiza a máscara social, mas não de modo permanente.

Sua transitoriedade exige que mais e mais selfies sejam tiradas para que a máscara social esteja em constante adequação com a estética prevalente, que por sua vez também é transitória.

Não que seja tremendamente simples abdicar de sua identidade de modo descartável, tão pouco se pretende confrontar o que o senso comum chamaria de realidade e o que este indivíduo em questão exemplificado por Furedi (2019) venha a chamar de eu.

Para os objetivos deste estudo é preciso ter em mente que na medida que as redes permitem um discurso articulado com técnicas próprias, também permite a conformação de redes comunicacionais distintas. E como tal, exige artefatos e troféus próprios para que haja identificação entre seus membros.

A fluidez compulsória da atualização da máscara social se torna possível, em um primeiro momento, por conta da melhora da câmera dos aparelhos celulares e da capacidade de armazenamento das redes sociais digitais, mas a partir do momento que é possível, passa a ser necessário.

Os indivíduos que se apropriarem desta linguagem discursiva da melhor forma e como mais agilidade usufruirão da disputa por um lugar de destaque.

Uma das preocupações de Freitas (2017) é justamente que esta versão excessivamente midiaticizada da intimidade e do indivíduo, que busca a qualquer custo ser percebido como um interlocutor de sucesso e de confiança, que manifesta constante e inabalável felicidade como algo tão normalizado que tenha impactos psicológicos.

Para a pesquisadora, a relação que está sendo construída e fortalecida ainda resulta em formas ditatoriais do uso das redes sociais e dos aparelhos de comunicação.

É como se cada indivíduo fosse obrigado a manifestar felicidade constante nas redes sociais mesmo que esta não seja sua realidade.

Complementa-se aqui que tal modo imutavelmente feliz através de uma ditadura tecnocrática da vida cotidiana se dá de modo e-vasivo.

We need a dramatic change in our relationship to social media and its delivery devices. We need to shift our culture so that we have a healthy relationship to new technologies. I think both the home and the college campus are ideal

testing grounds for such a shift, and that there are simple things that can help us begin to change our relationship to social media and smartphones, and the way they affect our sense of self and our social lives. (FREITAS, 2017, p. 271)

A autora está alertando para a necessidade de se estabelecer uma relação com os meios de comunicação, aqui fazendo uma expansão de suas palavras, que não seja baseada em simulações de uma vida inexistente.

Entre seus pontos de alerta está a questão axiomática sobre a felicidade manifesta nas redes que se torna uma pressão sobre os indivíduos que, mesmo postando fotos com a estética da felicidade e do sucesso enquanto estão de fato tristes ou desenganados, estas mesmas pessoas não obrigatoriamente compreendem ou sentem que seus pares estejam na mesma situação.

Sabe-se que a própria foto é um fingimento de alegria para fazer parte da estética sempre feliz das redes sociais digitais nos dias atuais, mas não se sente que há simulação da parte do outro.

Logo, as comparações se tornam injustas e angustiantes. A nossa mentira e fingimento contra a alegria aparentemente real de todas as outras pessoas conectas nas redes.

Em certa medida, enquanto esta voz tenta trazer à consciência as pessoas que estão sendo assediadas por este tipo de sistema, do outro lado a sedução da contrapartida parece suficiente para cooptar tantos outros agentes para seguir postando e influenciando mais e mais pessoas.

Mas agir sobre a tecnologia não é algo simples.

[...] good reminder of how influential ICTs are becoming in shaping our personal identities. They are the most powerful Technologies of the self to which we have ever been exposed. Clearly, we should handle them carefully, as they are significantly modifying the contexts and the practices through which we shape ourselves. (FLORIDI, 2014, p. 59)

As formas de sedução e de convencimento para que as pessoas continuem liberando parte de si e conformando suas identidades e a um fluxo normativo das grandes redes é considerável.

Importante, desde pronto, destacar que ainda que haja interesses comerciais nas grandes empresas de comunicação e tecnologia, elas em si não são suficientes para **determinar**, para garantir um resultado específico, mas são detentoras de modos

que oferecem **condições** mais favoráveis a tipos específicos de manifestação da identidade coletiva.

Desta forma, mesmo que uma grande empresa de tecnologia decida limitar as formas de e-vasão de privacidade ou combater a estetização excessiva das pessoas através de suas plataformas, esta não seria capaz de desconstruir sozinha um mercado estético inflacionário.

Mais do que isso, seria suplantada por diversas outras empresas e redes sociais que ocupariam o espaço deixado para trás, já que não é qualquer uma das empresas majoritárias que dita o mercado transestético, mas sim acompanha e responde a tais movimentos.

Em suma, o que se propõe é refletir sobre os impactos perceptíveis da conduta comunicacional de e-vasão da privacidade de modo que seja possível estabelecer uma visão mais longa e complexa sobre o tema.

Sem isso, as normatizações apenas cobrirão as pequenas lacunas, mas não serão capazes de desenvolver o conhecimento humano e humanístico necessários para a edificação de uma sociedade em que os valores superficiais não estejam obturando os debates morais.

Para tanto, é preciso compreender que o indivíduo em rede não está olhando apenas para si, mas também está encarando os seus nós relacionais e comunicacionais.

Além disso, encara uma entidade amorfa, mas que ao mesmo tempo exige atitudes e condutas específicas, que é o terceiro, o outro, o observador, o algoritmo.

Algo que opera por trás do sistema, de modo sutil, e que faz incutir nas mentes a necessidade de produzir compulsoriamente discursos, estéticas, e-vasão de formas específicas que sirvam ao campo das representações.

As online social media is contained within this broader social milieu, we can begin to conceive this matrix as its own kind of holding environment, or container, alongside what we might call an online social third. (BALICK, 2014, p. 50)

Estar em rede é ser e se saber vigiado, mas nem todos os nós desta rede estão declarados.

Tal questão pode se apresentar de modo axiomático uma vez que o eu em transformação e construção deverá lidar com o resultante de interesses comerciais

travestidos de engenharia social para oferecer a melhor experiência de consumo, seja de bens físicos, serviços, ideias, versões de si.

E isso não pode ser, uma vez mais, encarado como substrato de uma ou de outra empresa, mas como resumo do que massivamente foi possível construir até o presente momento.

Em outras palavras, para que o resultado fosse distinto, cada célula precisaria buscar novo alimento. Cada pessoa que se constitui em um nó com movimentos de dados precisa objetivar a conduta em sociedade de modo diferente do que se faz atualmente.

O terceiro observador, mesmo que desconhecido em sua totalidade, é percebido em sua essência e pelas articulações que causa oscilações na malha comunicacional das redes.

Este terceiro pode ser rotulado como algoritmo, inteligência artificial, segmentação de conteúdo. Muitos serão os nomes, mas todos são exemplos do que é o terceiro observador, a entidade que não tem patente nem propriedade que responde ao processo dromocrático transestético contemporâneo que se articula dentro da cibercultura.

A cibercultura equivale a um processo social-histórico bem mais vasto e complexo do que supõe o imaginário da pesquisa especializada. Ela está já pressuposta no contexto *a priori* de relação com os próprios *media* interativos e com o capital cognitivo a eles necessário. É assim que, como categoria de época, ela se confunde imanentemente, com o cenário material, simbólico e imaginário contemporâneo. (TRIVINHO, 2017, p. 67, itálicos do autor)

A dromocracia cibercultural também faz parte deste processo discursivo identitário, condicionando as formas de manifestação, na mesma medida em que acelera os desdobramentos tecnológicos, fazendo frutificar cada ramo que um dia brotou na semente antiga da tecnologia e da sociedade.

Importante ter em mente que atacar apenas o suporte da comunicação e do discurso identitário contemporâneo, mais do que errar o alvo, pode significar aumentar a fumaça em torno do que é relevante.

Sem colocar as pessoas no centro e suas condutas como resultantes de um processo formativo só tardará a resolução da vida em consonância com a nova realidade infotécnica.

O indivíduo então está trafegando em uma infovia complexa que demanda habilidades variadas conectadas ao campo da visibilidade infotécnica, sendo exigido que demonstre dromoaptidão (TRIVINHO, 2007) para responder como produtor de discursos e-vasivos de modo constante, hábil e sedutor.

A violência da velocidade se autojustifica pela transformação compulsória da *dromoaptidão* em imperativo categórico de época, válido para todos os setores sociais. A dromoaptidão pode ser encarada por vários ângulos: individual, grupal, institucional, empresarial, não-governamental, nacional, global, sem prejuízo de outros níveis intermediários. [...] A questão, com efeito, é, antes: ser veloz ou não ser. Tal é a redutora fórmula antropológica do momento. Depois disso é que se afirma a interatividade, epifenômeno procedimental do *imperativo dromológico vigente*. (TRIVINHO, 2017, p. 97, itálicos do autor)

Não bastará, para ser considerado dromoapto no cenário contemporâneo, produzir discursos mediados pelas redes e pela estética inflacionária. É necessário mais do que replicar. É preciso seduzir.

É preciso ser fator de convencimento que fortalece o discurso majoritário do qual cada indivíduo é apenas uma parte.

O indivíduo dromoapto, nos moldes do que se apresenta como sucesso, deve ser capaz de produzir comunicações e-vasivas que envolvam as pessoas e as façam desejarem ser parte do espetáculo transestético em busca do infopoder e da catequização e-vasiva.

Receber um posto de destaque e glamour na sociedade infotécnica contemporânea demanda não apenas representar o sistema, mas incorporar a dromocracia de modo constante, reprodutivo, envolvente. É ser nó de disseminação tanto das mensagens como da estética, do resultado e do resultante. É ser propagador da e-vasão como modo de estar no mundo.

Just as the professionalization of social media has exacerbated the dissonance between the real and online selves, the trend toward taking selfies and the pressure to constantly prove what one is doing and with whom (remember: "pics or it didn't happen!") interrupt the real lives and experiences of students with ever greater frequency. Young people feel anxiety and stress around what they perceive as fakery in how they and others present themselves online. Yet with the pressure to post photos to prove that their lives are great comes a further intrusion into time spent alone, with friends, and participating in the activities they enjoy. Whatever else selfies are, they are a particularly immediate and egregious cause of the (FREITAS, 2017, p. 102)

A considerar, para se tornar dromoapto é preciso ter, possuir os meios de produção da comunicação.

É preciso ser detentor das tecnologias para a prática cotidiana da hiperexposição imagética, de e-vasão em testes contínuos da aceitação dos actantes sobre as articulações discursivas.

O processo de produção de discurso mediado não permite, dada sua atual aceleração, que alguém se manifeste publicamente apenas uma vez por semana, por exemplo.

Se antes o consumo de notícia tinha horários coletivos condicionados pelos meios de comunicação de massa, como o telejornal transmitido para toda nação ao mesmo tempo, ainda que uma parte das pessoas consumisse informações e notícias ao longo do dia com jornais e revistas, por exemplo, hoje o processo de consumo de informação segue jornadas múltiplas, não tendo momentos definidos, reservados.

O consumo de informação é compulsório e constante.

Da mesma forma, a produção de informação, de fatos publicáveis também acaba seguindo o ritmo frenético das mídias.

E para produzir conteúdo de modo tão acelerado, não é possível fazê-lo sem ter a posse dos meios de articulação do discurso comunicacional.

[...] a pressão empírica e publicitária do contexto é sutilmente implacável em suas recomendações de praxe ao prever, no núcleo do capital social conforme, no que concerne ao domínio privado *pleno* padrão, a necessidade deste outro elemento basilar: acompanhamento satisfatório (em geral, não-sequencial, em sentido estrito) *da lógica da reciclagem estrutural da mais-potência das senhas infotécnicas de acesso*. [...] Em suma, a dromoaptidão condecorada pelo *mainstream* digital é a que equivale àquele domínio (posse) das senhas infotécnicas próxima ou precisamente situado no ponto extremo da *esteira agonístico-restaurativa da mais-potência*. (TRIVINHO, 2007, p. 193, itálicos do autor)

Estas senhas infotécnicas de acesso precisam estar consubstanciadas na prática cotidiana derivada da velocidade. Ser veloz é mandatório, condição basal. Em seguida, tal velocidade precisa se aplicar sobre o aparato infotécnico para, a partir dele, articular formas de acesso que dependem da dromoaptidão praticada diuturnamente.

Assim, ter um celular com boa capacidade de gravação e processamento de dados é parte da condição de ser actante na esfera comunicacional, além de possuir conexão com a internet.

Possuir um celular é uma das condições básicas da articulação dos discursos mediados necessários para a participação na esfera transestética (LIPOVETSKY; SERROY, 2015).

Quanto mais a tecnociência governa o mundo, mais a oferta comercial é artealizada, mais a demanda é marcada pelos desejos de experimentar as alegrias das 'impressões inúteis' que caracterizam a experiência estética. Com a era emocional do consumo aumenta inevitavelmente uma busca incessante de experiências hedonistas e sensíveis, renovadas e 'surpreendentes'; em outras palavras, estáticas. (LIPOVETSKY; SERROY, 2015, p. 334)

Esta busca hedonista encontra na instantaneidade estética das conexões dos celulares e das redes sociais digitais um terreno fértil para sua disseminação.

Esta questão se antecipa aqui justamente para que se esclareça que o processo produtivo impacta diretamente o discurso identitário.

Sem a infraestrutura disponível e a dromoaptidão, não é possível estabelecer um diálogo com a infosfera e o infopoder.

Mas também não basta apenas produzir diversos conteúdos. É preciso ser reconhecido como um produtor legítimo, de destaque, consistente através das flutuações estéticas.

But the answer of the selfie is that, from now on, it is the user who decides how to write the relationship to notoriety. Celebrity has changed: Rather than being called to passively attend a show, as in the time of the Sun King, the audience slips within the frame and affirms its interest by playing as actors, then shares these images via its own social media. Today, which event would have the least interest if it wasn't accompanied by these testimonies of public approval? (GUNTHER, 2018, p. 43)

As produções de artefatos comunicacionais são provas de valor, são parte das trocas simbólicas necessárias para a manutenção das relações comunicacionais permeadas pela e-vasão da intimidade e da privacidade.

O status de celebridade não pode mais ser mantido de modo passivo, de modo reativo.

Pelo contrário, é construído e estruturado diária e ativamente.

As máscaras sociais no discurso do eu precisam de atualizações cotidianas e, por vezes, múltiplas.

Ao mesmo tempo, a constante produção de conteúdo não pode apresentar as mazelas cotidianas como se fossem fracassos, em detrimento do espetáculo comunicacional sedutor da e-vasão da privacidade.

Already by talking about the self, individuals engage in a sort of self-assessment that helps to reduce ambiguity and inconsistency in their own thinking. The overall purpose is consequently the avoidance of self-criticism and potential criticism from others (MASUR, 2017, p. 77).

O esforço apresentado pelas pessoas é para terem uma imagem produzida e apresentada de si mesmo que reduza ao máximo a ambiguidade e que possa construir um senso próprio, assim como anteriormente foi possível compreender com Behrendt (2015), na medida em que o eu acaba sendo parte do que resta de lastro, de visão de mundo .

Neste sentido, Masur (2017) vai indicar que do outro lado desta régua estará o julgamento do outro, da conduta praticada pelos pares.

Indicará ainda que “disseminas informações pessoais para uma audiência ampla aumenta a oportunidade de receber feedback social” (MASUR, 2017, p. 78, tradução nossa) compreendendo que as pessoas possam estar em busca de uma forma de se constituírem de modo evolutivo e que o excesso de exposição pode ter também uma característica de busca por um caminho.

É como se a máscara social, o discurso identitário, precisasse estar sempre em teste para conferir qual a melhor forma de apresentá-lo com resultados mais favoráveis para o indivíduo.

Mas sobre a estética da felicidade sempre presente, e a impossibilidade de apresentar dificuldades próprias dentro as manifestações do eu, aparentemente o que resta é a regra de que os problemas intransponíveis são os das outras pessoas. O indivíduo que está em busca de reconhecimento traça discursos estéticos que possam legitimá-lo como detentor e merecedor do infopoder.

Não descendo na crítica sobre os interesses individuais, para o propósito aqui discutido, basta compreender que na medida em que a auto-exposição aumenta, as formas de ser tutorado pelo sistema também se avolumam.

O feedback social que Masur (2017) menciona também emana da estrutura transestética. É resultado dela.

Cada actante que segue em contato com esta pessoa se torna um provedor de *feedback* que pode ajudar a moldar um sujeito mediatizado para a performance estética e e-vasiva, conceito que será melhor trabalhado ao longo das páginas futuras

e que é crucial para o entendimento dos impactos sofridos pela privacidade nos dias atuais.

Estar em rede é estar visível, é fazer parte do espaço de visibilidade que traz regras específicas para o *self*.

E por *self* não se busca traduzir como algo apenas leviano como as selfies, fotografias feitas da e pela própria pessoa. Mas algo mais profundo na medida que se mostra como discurso estruturado e interessado em produzir um impacto determinado em sociedade.

Social media sites exploit the 'social' as they enable us to transact and interact through a profile culture and an architecture of interactivity where the self is visualised through its engagements and movements. [...] These platforms then function as 'technologies of the self' premising on modes of identity creation and self-objectification. Social networking sites as facilities for self-presentation and identity negotiation enmesh public and private spaces with multiple audiences, enabling a networked self to emerge. (IBRAHIM, 2018, p. 5)

Na medida em que as pessoas encontram um espelho plástico, o algoritmo das redes sociais digitais, o processo mimético sofre alterações que podem ser impactantes para a percepção do *self*, de si e para a construção da máscara que será apresentada socialmente.

Aparece a questão da negociação do *self* que será apresentado, mas para Ibrahim (2018) já está claro que este *self* segue fragmentado. Mas enquanto anteriormente o espaço físico poderia ser crucial para a característica fragmentária do *self*, hoje estes fragmentos convivem nos diversos filtros de grupos das redes sociais digitais.

Today, an integral aspect of the curation of the self is also bound up with the notion of desire for oneself and equally how we may be commodified for others. Mimetic desires in society underscore the deeply social and cultural character of desire, where consumer desire can be an affirmation of belonging in a globalising consumer culture and equally niche communities offline and online. (IBRAHIM, 2018, p. 52)

Ser infodesejado, ser midiaticamente desejado é parte da dromoaptidão, através da e-vasão seletiva e articulada. É a prática objetivada da e-vasão transestética.

Mas ser dromoapto (TRIVINHO, 2007) não necessariamente está na mesma seara da literacia, quando esta pressupõe certo aprofundamento consciente do indivíduo a alterar suas condições de atuação em sociedade e através das tecnologias

comunicacionais, enquanto a dromoaptidão apresenta indivíduos governados, conduzidos pela aceleração. Ser dromoapto não significa, então, ser literato.

Com efeito, como a velocidade não é um acontecimento, a violência que lhe é própria não se põe como fato concreto aqui e acolá, a exemplo das modalidades empíricas, situacionais, visíveis e documentáveis de violência, sejam elas esporádicas ou recorrentes, cotidianas ou atípicas. A violência da velocidade comparece alçada à categoria de 'fato social total'. (TRIVINHO, 2007, p. 93)

Acelerar é parte da violência infraestrutural que exige velocidade antes de mais nada.

Ter o domínio técnico da exposição do *self* de modo que um grupo específico reconheça valor e ofereça troféus simbólicos não significa necessariamente ser capaz de olhar para o sistema de modo consciente e crítico e ser capaz de transformá-lo intencionalmente.

Neste caso, o indivíduo é compelido a desenvolver as habilidades imprescindíveis dentro da dromocracia como condição de pertencimento mas não é ofertado a ele as formas de tomada de consciência sobre os impactos de seus atos sobre si e sobre os outros.

E não se trata de uma mediatização do eu apartada, por mais que diversos *selves* sejam apresentados no dia a dia, o online e o offline não passam de classificações racionais, mas através do *onlife* (FLORIDI, 2014) as fronteiras do digital e do analógico se tornam pouco operantes.

The wonderful thing about the self is that it is always in the process of changing, mutating, and developing new dimensions of itself. In many respects how we view the self, the things that we attribute to it, and above all the way we experience ourselves, is always changing because, whether we like it or not, we are always in the business of remaking ourselves, refashioning, and reimagining ourselves. (FUREDI, 2019, p. 14)

Não é apenas atualmente que o *self*, que a manifestação do eu está em transformação, mas sim algo que acompanha as pessoas em sociedade desde os primórdios.

A diferença, quando os atos contemporâneos são colocados frente a frente com Trivinho (2007) é que, assim como sempre houve, os processos de reconfiguração do *self* estão mais acelerados do que antes, e seguirão acelerando dia a dia.

Estar em sociedade sempre foi articular os próprios discursos com objetivos sociais, em muitos momentos, com aspectos econômicos.

O que se torna galopante é o processo de criação de novos discursos dentro das esferas comunicacionais de cada indivíduo, além da transição de estéticas em um fluxo também acelerado.

A exemplo das redes sociais digitais, tal fluxo ávido se torna insaciável.

Social network sites like Facebook, Twitter, and Instagram offer a steady opportunity for sharing content, uploading, and posting; their interfaces encourage a never-ending update of one's online representation. Users are invited by the structure of the user interface as well as by the feedback of the community to post again and again, to like, to comment on pictures, and to comment on comments. Consequently, the single image is not separate; it is rather part of a profile, a collection, a stream, or a feed—all structures that are asking for more pictures (WIRTH, 2018, p. 229)

Por mais que a estética seja transitória, de certa forma, a macro-estética, o que Lipovestky e Serroy (2015) vai chamar de capitalismo transestético seguirá.

Ou seja, as fotos postadas em redes sociais, em grupos de conversas do Whatsapp seguem um fio condutor que está vinculado ao discurso identitário, ao imperativo transestético, à dromoaptidão necessária, ao infopoder e a e-vasão da privacidade.

Self-representation in commercial spaces may be mediated in ways which are less obvious but as important as the mediation evidenced in public service settings online. Moreover, in addition to considering publicly funded and commercial spaces, we also need to pay attention both to 'alternative' and to mainstream practices, wherever they appear. An analysis of how processes of institutional mediation shape self-representation in commercial settings must ask what the purposes of the self-representation in question are – that is to say, why it is taking place in a given setting. Moreover we should also consider how the political economic structures might actually shape the kinds of self-representation that take place in any given example. (THUMIM, 2012, p. 140)

Também através das estruturas econômicas, o espaço da manifestação da identidade é moldado.

Não á toa em muitos casos não apenas a privacidade por si só é defendida ou buscada, mas sim uma privacidade construída desde o rascunho das soluções comunicacionais.

Ainda que algumas empresas não se preocuparem com as manifestações identitárias dentro de suas plataformas, espaços e afins, suas decisões comerciais certamente impactarão à revelia a forma como as pessoas se expressarão através dos artefatos disponíveis.

Em questão aqui não está a ideia de que há caminhos determinantes, categóricos, nem que as empresas possam se tornar detentoras dos discursos identitários, mas sim que suas decisões estão dentro dos fatores que criam condições específicas e privilegiam formas mais interessantes, no nível econômico, de manifestação do eu e e-vasão de informações.

The publication of images formerly considered as private, or even intimate, is not only becoming more accepted but also increasingly demanded. There is an economic rationale behind this development: Facebook profits from increased data divulgence; its algorithmic software codes are designed to support and symbolically reward the publication of such materials. (WELLGRAF, 2018, p. 359)

Os aspectos econômicos, ao interferirem no desenho das soluções, criam caminhos para as apresentações específicas da comunicação sobre o *self* na medida em que as imagens, os textos que mais se adequam à linguagem e-vasiva seguirão sinalizados positivamente, recompensados para que tal comportamento se torne recorrente, desejado, aprendido.

As curtidas, os compartilhamentos, os comentários são formas de gerar um reforço positivo, como o *feedback* mencionado por Masur (2017), em todas as manifestações que respondem ao tipo de e-vasão desejada feitas dentro de cada plataforma.

The self is seen as a complex informational system, made of consciousness activities, memories, or narratives. From such a perspective, you are your own information. And since ICTs can deeply affect such informational patterns, they are indeed powerful technologies of the self, as the following examples about embodiment, space, time, memory and interactions, perception, health, and finally education illustrate. (FLORIDI, 2014, p. 69)

Falar então do *self* é buscar um caminho que o compreenda não como algo dado, constante, sólido, mas como um exercício fluído de perpétua reinvenção dialógica e ecossistêmica, em busca de conexões e contatos com os demais actantes.

As Tecnologias da Informação e Comunicação (TIC), que em Bruno (2013) são em algum momento também tecnologias de vigilância, fazem parte da complexa gama de actantes do infopoder que moldam gradativamente as formas e-vasivas de manifestação identitária.

É, de certa forma, necessário ressaltar que o que se busca aqui não é tornar pejorativas as manifestações identitárias através das mídias, principalmente por compreender que é justamente também através das mídias que o campo de

construção da imagem se dá, mas colocar mais destaque sobre os pontos axiomáticos de como este processo ocorre nos dias atuais.

Não existe construção de imagem e identidade sem compreensão da comunicação e, como tal, de seus meios.

E também não significa que este processo seja sempre mediado de modo negativo, apesar deste trabalho estar mais voltado aos impactos de risco, uma vez que a academia precisa se manter vinculada à construção do conhecimento com vistas últimas à edificação social.

[...] the experience of the digital gaze may start from a healthy and wilful exposure/exploration by the self of itself through a medium, but social pressure may force it on selves that are then negatively affected by it, leading them to modify themselves in a way that could impose some external and alien rules on the process of construction of one's own identity. (FLORIDI, 2014, p. 74)

Em casos diversos, a manifestação midiática não se molda de pronto a todas as pressões sociais e infotécnicas.

É preciso, primeiramente, compreender a linguagem sociotécnica praticada em cada meio de comunicação para que, com o tempo, a pressão ideológica possa ser internalizada para conduzir a conduta de modo mais sutil.

Dito de um modo diferente, cada usuário em uma rede social digital precisa primeiramente passar pelo processo de construção de sua dromoaptidão com habilidades especificamente reconhecidas tanto pelo grupo ao qual deseja se unir quanto as technicalidades inerentes à plataforma pela qual a comunicação é estabelecida.

Produzir um discurso do eu em diversas plataformas ao mesmo tempo é crítico na medida em que cada uma oferece não só artefatos distintos, mas também um campo de valores e significados próprios que certamente contaminará, seja positiva seja negativamente, o discurso do *self*.

Indeed the use of new media technologies, as well as the idea of interactive new media technologies, is not innocent here. The very same technological properties that facilitate spaces for selfrepresentation may also be responsible for the tip of the balance towards the therapeutic rather than the deliberative/democratic. This is so insofar as the properties of new media technologies – namely friendliness, immediacy and accessibility – facilitate visibility and exposure but do not by themselves catalyse/enable the coordination of more elaborate projects of deliberation, collaboration and change. (THUMIM, 2012, p. 128)

Esta plasticidade da manifestação identitária está posta a partir da compreensão de que os indivíduos podem, e irão, compreender os códigos simbólicos de reconhecimento que cada tipo de rede e grupo carrega e, ao longo do tempo, passarão a articular sua comunicação de modo a buscar maior aceitação social, reforços positivos e afins.

O que se convencionou chamar de amigabilidade, ou *user-friendly*, não está de fato focado na amizade para com o usuário, se não na redução de fricção entre o usuário e uma plataforma ou site, um sentimento de maior conforto.

Informational friction refers to the forces that oppose the flow of information within a region of the infosphere. It is connected with the amount of effort required for some agent to obtain, filter, or block information about other agents in a given environment, by decreasing, shaping, or increasing informational friction. To see how, consider the following scenario. (FLORIDI, 2014, p. 103)

Tal amigabilidade servirá para manter entretido o usuário de um serviço, produto, para que na medida de tal conforto, o processo de exposição, de e-vasão se dê com menor resistência.

Quanto mais as redes sociais digitais desenvolverem formas mais fluidas de manifestação da individualidade, das peculiaridades performáticas do eu, reduzindo barreiras e acelerando a oferta de *feedbacks*, mais dados serão e-vadidos e mais cada um dos indivíduos dentro das redes e sites servirão de propagadores da cultura e-vasiva.

Não à toa a palavra selecionada por Thumim (2012) foi inocente. Não há inocência no desenho das plataformas que pretendem facilitar o processo de e-vasão da privacidade.

Selfies permit the study of what people want to look like in a photograph because people are shown in control of the exposure. Selfies lend themselves to various readings of self-reflexivity: They may be viewed as self-reflections of individuals, they can be seen to reflect certain aspects of the medium of photography and its practice, and, finally, these two reflections can be combined and the agent of the selfie scene be understood as composed of human and technological components. RUCHATZ, 2018, p. 68)

No caso das *selfies*, quando combinada com seu uso contemporâneo, valendo um destaque para tal uso dentro do Instagram, se torna mais do que uma imagem, mas sim um metadado que precisa ser construído, antes de mais nada, na mente do usuário.

Além da técnica mais óbvia dos ângulos de fotografia, o usuário precisa compreender a função que a selfie terá na construção de sua identidade narrada e de atualização de sua máscara social em cada grupo.

Raro encontrar fotos no estilo frontal, como *selfies*, sem que estejam acompanhadas de textos explicativos, provocativos, *hashtags* e afins; sem contar que o próprio ângulo torna possível que a pessoa se exiba em um local determinado, o que constantemente leva os indivíduos a não apenas escreverem sobre o momento da fotografia, como também convida de modo fluído a marcarem o local onde a fotografia foi tirada, muitas vezes como forma de agregar valor e glamour à manifestação identitária.

The incorporation of reality television and the re-fashioning of the public gaze to view the ordinary and intimate details of people's everyday lives became a precursor in enabling the perfunctory and the everyday to become part of media content. The unscripted watching of people and leveraging on people performing for the camera or 'acting up' constituted a new era of watching others but equally envisioned the screen as part of the exposure. Equally it re-inscribed the banal and domestic routines of people's uneventful lives and the ordinariness of existence to become viable subjects. (IBRAHIM, 2018, p. 29)

Some-se então à glamurização da e-vasão a aceleração dos processos mediados e transestéticos nos meios de comunicação de massa, não apenas nas plataformas de comunicação digitais, e tem-se um reforço positivo ainda maior sendo praticado cotidianamente.

A cultura dos *reality shows*, ressalte-se uma vez mais, não é uma criação contemporânea, no sentido de algo surgido do nada, mas condição acelerada e extremada da curiosidade, do interesse escópico.

Performance e-vasiva, que facilmente se exemplifica através de tais *reality show*, que só se torna possível da forma como se dá através dos meios de comunicação contemporâneos, se mostra filha do voyerismo, que por sua vez se dissemina através do escopismo fotográfico que permite olhar sem ser visto, mirar o detalhe sem ser mirado de volta.

Ainda pensando sobre o eu que se torna projetado, espelhado nas redes sociais digitais e nas formas contemporâneas de manifestações da identidade, é necessário compreender que mais do que uma réplica, ocorre um processo de análise sobre a própria linguagem dentro do campo das negociações simbólicas permeadas pelas TICs.

The autoscopic encounters of the self through digital technologies that coalesce with our everyday lives mean that the self is performed with and through the screen. These autoscopic encounters collapse space and place and equally the temporal and spatial offering the autoscopic self as both a performative commodity without relinquishing the immediacy or banality of the everyday as a scope for new forms of narratives and performances. (IBRAHIM, 2018, p. 20)

A autora chama à luz a questão da autoscopia a partir dos meios de comunicação.

Caso a definição seja buscada na medicina ou na psicologia, facilmente se percebe que se trata de um quadro psíquico no qual o indivíduo crê estar vendo a si mesmo, seu próprio corpo, como se fosse uma outra pessoa, um observador de fora do corpo.

Na psicologia, especificamente, existe a técnica de autoscopia que consiste em gravar um indivíduo para que depois ele possa avaliar seus atos, gestos, reações de modo externo, de modo um pouco mais afastado.

Já no caso citado por Ibrahim (2018), a questão não é um si um uso consciente desta técnica para que o indivíduo conheça melhor a si próprio, mas um processo normalizado nos dias atuais de avaliação do eu através das próprias manifestações de sua identidade nas redes sociais digitais, por exemplo.

Alguns pontos da fala da autora merecem ainda mais destaque.

O primeiro, que vai de encontro ao pensamento de Floridi (2017) que é uma ideia de que há um *self* performado em dissonância com uma vida cotidiana, ou seja, fora do *onlife*.

Novamente é possível notar o quão controversa a questão do eu ainda é nos dias atuais. A cibercultura ainda não é vista como cultura. O ciberespaço ainda não é visto como espaço. Ainda se constroem narrativas que separam o online do offline como se isso fosse possível na vida, e não apenas como caráter metodológico e científico que, ainda assim, merece severas ressalvas.

Ciberespaço é o novo espaço. Cibercultura é a nova cultura. Dromocracia é o imperativo que torna possível compreender que o ciber não é uma criação idiopática, mas a evolução germinada.

O Ciber não é uma classificação de um pedaço exclusivo e apartado da realidade, mas a forma de mostrar que o potencial germinal já brotou e constituiu nova vida, reconfigura as forças internas das estruturas sociotécnicas.

Assim, para efeito deste estudo, este trecho da autora acaba por ser cuidadosamente pinçado para que seja percebida a distinção.

O segundo trecho que merece mais atenção e tempo dedicado é a questão do colapso entre espaço e lugar através da autoscopia.

Interessante que a autora tenha se recordado de mencionar e caracterizar o espaço como algo distinto do lugar, uma vez que o primeiro é físico, duro, e o segundo é social, constituído, construído.

Mas como a autoscopia pode colapsar ambos, se não através de uma maior exposição da distinção entre eles, resumindo a fisicalidade dos espaços como menos relevante do que a reunião de artefatos identitários que possam constituir um lugar, um lugar de fala, lugar de escuta, lugar de estratégia e de articulação, lugar de manifestação identitária, assim como já se percebe há anos no pensamento de Augé.

O lugar como campo das articulações identitárias que não se restringe à espacialidade material, mas pode e a cabo utilizará destas como suporte das narrativas identitárias.

Há ainda mais um ponto relevante, que vem a ser a questão performativa, que na manifestação da autora, segue presente tanto no cotidiano quanto nas articulações vindouras.

O tempo e espaço estão, dentro da autoscopia do eu, vinculados para a criação do lugar da performance, que para este estudo pode ser entendido, em certa medida, também como suporte para os movimentos dos dados, para a construção das virtualidades do eu multiplicadas pelas formas de coleta e tratamento de dados que estão disponíveis e em atuação.

The selfie as an autoscopic experience is about moving beyond the visualisation of the self through technologies and about casting the self into new modes of circulation, sharing, aestheticization as well as new forms of anxieties afforded through the networked economy of image and content sharing, tagging and voyeurism. Here the gaze can be visualised through the interactivity of the platforms and the ability to track the metrics of the digital platform. (IBRAHIM, 2018, p. 95)

É necessário compreender que as manifestações identitárias do eu não se dão nas tecnologias, pura e simplesmente, mas através e com as tecnologias.

Tal experiência autoscópica não é uma pura observação externalizada de si como quem mira uma fotografia antiga num álbum fotográfico, mas um ato performativo constante de busca estética e forma de compartilhamento e disseminação de uma imagem de si que possa ser aceita pelas pessoas constitutivas do grupo de interesse no qual se espera obter troféus e reconhecimentos e que demanda articulação ativa.

Entre as questões importantes que estão relacionadas a esta economia da estética, que no caso de Lipovetsky e Serroy (2015) se tornará o capitalismo transestético, está o fato de que tal performance e movimento de dados que se mostram fio condutor das interações não pode estar lastreado apenas nas fotos, apenas nos artefatos miméticos das mídias tradicionais, mas está lastreado também nas interações do eu com outros avatares e entes.

O capitalismo artista é esse sistema que produz em grande escala bens e serviços com fins comerciais, mas impregnados de um componente estético-emocional que utiliza a criatividade artística tendo em vista a estimulação do consumo mercantil e do divertimento de massa. (LIPOVETSKY; SERROY, 2015, p. 67)

Este divertimento em massa, ao compreender em TRIVINHO (2007) que os meios de massa e os meios ciberculturais diferem, será levado a outra escala quando fomenta e se alimenta das diversas manifestações estéticas do eu nas mídias digitais de modo perversivo.

A interação, em si, é um artefato relevante na construção da persona, da manifestação identitária e das multiplicidades virtuais dos perfis gerados por tais movimentos.

Desta forma, parte do rastro deixado por cada interação infotécnica se transforma em um rizoma dentro da cibercultura.

E tais interações são relevantes para o terceiro observador, para que os algoritmos sejam capazes de interagir e interferir nas manifestações identitárias realizadas em cada rede.

Tanto por isso que cabe uma nova provocação, vinculada a esta interferência com base nos dados coletados de modo compulsório sobre cada pessoa, que vem a ser a chamada Internet das Coisas (IoT), que em realidade pouco se importa com as

coisas em si, mas se constitui através da possibilidade de mensuração disseminada em muitos artefatos físicos com o foco em compreender e conduzir os movimentos do actantes para que estes estejam sempre visíveis, acessíveis e em diálogo com a infosfera para que esta possa não apenas compreender mas também articular as mobilidades dos discursos e da estética.

Nesta provocação preliminar, mas que não terá uma resposta direta, quando muito será respondida de modo variado através das reflexões futuras nestas páginas, é que a chamada IoT é, em si, uma estrutura infotécnica que busca objetificar as relações dos actantes sociais e econômicos a fim de cooptar suas condutas através da conveniência e conforto para que a dromocracia cibercultural (TRIVINHO, 2007) infopolítica transestética siga seu processo de aceleração e datificação, e como tal, acabam por interferir não só na dinâmica de consumo dos discursos identitários, mas também no modo como tais discursos são construídos.

Assim, também se tornam parte produtora e produto da mentalidade epocal da cibercultura.

Discutir a identidade de alguém *onlife*, para usar um termo de Floridi (2014), significa passar pela estrutura infotécnica que permite a edificação de um discurso em plataformas digitais distópicas.

In advancing our understanding of the relationship between social networking (and other online activities) and the performance of identity within contemporary cultural norms, structures, and frameworks, it is importante to bear in mind that social networking uses, activities, changes, updates, and account management are not only conscious representations and choices made for access, but simultaneously activities or performances which construct identity and selfhood. (COVER, 2016, p. 27)

Existir com um discurso identitário nas redes sociais digitais é mais do que apenas publicar algo. É preciso performar diuturnamente uma vida consonante para que tal identidade seja compreendida de modo constante pelos interlocutores nodulares.

Por isso que Cover (2016) vai se antecipar para indicar que há uma ligação ainda maior e mais profunda com a memória dos suportes técnicos do que apenas *hashtags* e etiquetas digitais.

Não basta apenas olhar para a apresentação inicial em uma rede digital em um tempo de escrutínio acelerado das identidades que competem pelo espaço

espetacular da visibilidade panórgica. O processo de representação é muito mais complexo e aprofundado.

From the perspective of the user who has utilized Facebook's profile function and wall in the construction of a performance of coherent identity which has, by necessity, involved disavowing past experiences, the undoing of identity is initiated by an encounter with the past. Not a memorialized past – rewritten in one's memory or narrative through the framework of an identity present, but an archaeological artifact that might grate against the currency of one's identity performance, both online and offline. In other words, tagging not only takes identity out of the myth that it is represented, articulated, commanded, and controlled by the subject through profiles and performances, but acts as a reminder that the network framework commandeers and potentially thwarts the performativity of an intelligible selfhood. (COVER, 2016, p. 27)

A narrativa necessária para sustentar uma percepção de identidade, seja para si, seja para o outro, vai além da superficialidade muitas vezes reportada e reputada aos usuários das redes sociais digitais.

O que é transitório, neste caso, são os artefatos de manifestação identitária, mas isso não significa que haja exclusivamente superficialidade neste processo de criação e manifestação das máscaras sociais, uma vez que demanda vertiginosamente tal dromoaptidão que seguirá excluindo diversas pessoas do centro das gratificações, todas aquelas que não conseguirem produzir suas manifestações aceitavelmente consonantes com a estética acelerada e efêmera em cada um dos momentos de diálogo mediado.

É preciso um conhecimento infotécnico aplicado cotidianamente em cada manifestação comunicacional para que o fio que alinhava a identidade pública seja consistente e sustente o discurso de modo que o sujeito ocupe seu espaço dentro da ominiágora, a ágora redefinida entre a quadra levýtica (LEVY, 1999) real, virtual, digital e atual.

É o *onlife* (FLORIDI, 2015) aplicado em uma matriz fractal do que vem a ser a identidade em um mundo de virtualidades.

The information flow needs some friction in order to keep firm the distinction between the macro multi-agent system (the society) and the identity of the micro multi-agent systems (the individuals) constituting it. Any society (even a utopian one) in which no informational privacy is possible is one in which no self-constituting process can take place, no personal identity can be developed and maintained, and hence no welfare can be achieved, social welfare being only the sum of the individuals' involved. (FLORIDI, 2014, p. 119)

Esta fricção é o resultado do contato das identidades e das estruturas que lhe oferecem suporte, caminhos de manifestação e condições de influência, que de certo modo já fora alertado por Floridi (2014).

Não se age no mundo sem ser preenchido por ele durante o processo constitutivo. Da mesma forma, não se evade dados sem que eles voltem oportunamente como um tipo de pressão ou de demanda de forma dialógica e dinâmica.

A sutileza desta pressão, desta fricção, se dá em maior escala na medida em que o indivíduo segue o vetor das informações que liberou de modo coerente e constante.

Ou seja, na medida em que os dados oferecidos ou roubados se mostram suficientes para construir uma persona midiática próxima da realidade cotidiana do indivíduo, os conteúdos recebidos em resposta, por sua vez, se mostrarão cada vez mais suficientes para seu entretenimento mercadológico e político. É como se envolver em uma bolha criada pelos próprios gostos e hábitos.

Neste exemplo, tal indivíduo seguirá respondendo afirmativamente a cada fragmento da comunicação, produzindo ainda mais dados, e a cada dia mais conectado com o tecnoalterego, reforçando e ensinando ainda mais para o terceiro observador quais são suas preferências e preterências tanto no nível consciente quanto no subconsciente.

Contudo, quando a estrutura técnica entra em dissonância com a conduta cotidiana, ou o oposto, quando o indivíduo decide rumar com caminhos distintos daqueles que sempre manifestou para uma estrutura infotécnica de memória (FELICIO, 2015), as manifestações dissonantes serão cada vez mais evidentes e o sistema fará pressão para tentar entender, com a maior agilidade possível, qual é a forma de consolidar um perfil mais certo sobre cada pessoa.

A infosfera não tolera sua autoignorância sobre a existência e conduta das pessoas, e já possui formas consolidadas de compreender os discursos identitários e lidar mercadologicamente com eles.

Nesta dificuldade da infosfera se manter alheia às individualidades, um dos exemplos cabíveis sobre o esforço de reinserir as pessoas no sistema são os descontos em farmácias que param de ocorrer de acordo com a conveniência

econômica, mas esta questão se torna muito mais profunda do que alguns reais a mais ou a menos na fatura do mês.

Plataformas de conteúdo começam a buscar este novo eu que está se conectando para oferecer outro caminho consonante de vídeos, artigos, piadas, memes, que possam cooptar a atenção, o tempo e a energia destes entes, travestindo todas as capturas pelo dinheiro.

Não se trata dos lucros de uma ou outra empresa, mas de como o mercado global está se desenhando em torno na pervasividade dos dados que, como tal, invadem e evadem o eu e, quando possível, interferem na percepção de valor para que a e-vasão se torne parte intrínseca da conduta individual e, coletivamente, seja um dos aspectos da cibercultura contemporânea.

There are three aspects necessary to cover here in order to make sense of the ways in which digital, networked activity and identity, subjectivity, and selfhood are intertwined in a contemporary era. First, it is necessary to delve deeper into the relationship between the media itself since it is that which “makes available” the very discourses through which identities are made intelligible and cited in performative articulations of selfhood. Second, we then need to question this media–identity couplet further by asking how access and the audience operate to produce particular readings of those identity categories – in other words, to interrogate how subjects read from identity positions when identities are only understood from highly subjective interpretations of what is given in a media context. Third, we must put this complex circularity to task by asking how the self is fashioned through broader cultural frameworks of subjectivity. (COVER, 2016, p. 28)

Mesmo que não se compreenda em nível profundo as diversas formas de constituição da identidade, e nem é este o objetivo deste trabalho, é perceptível que há uma relação dos artefatos de suporte da comunicação e a construção e apresentação desta identidade para apreciação e avaliação dos pares que se pretende impactar.

Assim, as tecnologias de comunicação (entretenimento e vigilância) são, por seu papel, tecnologias identitárias. E como tais, as decisões de coleta, tratamento e uso de dados são, mais cedo ou mais tarde, decisões de impactos cultural, sociológico e antropológico.

The body as a site for embedding smart communication technologies produced the self as constantly mediated through both its physical space and the virtual one enabled through the screen. If the screen acquired social resonance and dominance in the age of broadcasting, it acquired a bodily intimacy in the age of the digital media, becoming an extension of the body where it was possible to ubiquitously consume the world as well as our selves online while simultaneously offering ourselves to others for consumption. (IBRAHIM, 2018, p. 28)

O espaço físico do corpo já não é mais a superfície obrigatória e prevalente da identidade, mas uma parte constitutiva dela, em concomitância com meios de comunicação que agora invadem o pensamento, assim como já anteciparam McLuhan (1964) e seu discípulo Kerckhove (1997).

As telas que estão cada dia mais próximas do corpo desconstroem a espacialidade física do corpo e o colocam dentro da esfera de digitalização e virtualização, conferindo potência e dinamismo a este corpo-suporte.

Dinamismo este que é necessário para tornar evidente a dromoaptidão de cada indivíduo dentro da omniágora.

[...] digital media serve the dual function of gathering data about the subject for the subject and, in doing so in ways which help produce intelligible subjectivities, also gather data for others. In several ways, then digital identity is very much about being given over not only to the discourses of identity that precede us, but to the process of social and economic flow that relate to and are beyond us. (COVER, 2016, p. 249)

O corpo, tanto quanto o espaço físico como um todo, se virtualizam para participar dos movimentos de dados e para serem artefatos necessários em sua transitoriedade, não em suas predefinições.

The freedom to construct our personal identities online is no longer the freedom of anonymity advertised by Peter Steiner's famous cartoon, in which a dog, typing an email on a computer, confesses to another dog that 'On the Internet, nobody knows you're a dog'. Those were the nineties.¹⁰ Today, if one is or behaves like a dog, Facebook, Google, or at least some security agency probably knows about it. Rather, it is the freedom associated with self-determination and autonomy. You may no longer lie so easily about who you are, when hundreds of millions of people are watching. But you may certainly try your best to show them who you may reasonably be, or wish to become, and that will tell a different story about you that, in the long run, will affect who you are, both online and offline. So the onlife experience is a bit like Proust's account-book, but with us as coauthors. (FLORIDI, 2014, p. 64)

Construir uma identidade, seja considerando ambientes distintos, seja considerando o conceito *onlife*, é tarefa mais complexa do que apenas a permissão ou concessão.

Neste sentido, a infraestrutura técnica precisa estar consonante com a multiplicidade das identidades na mesma medida que a sociedade precisa estar preparada para receber a personalidade impressa nestas redes de modo autoral sem que o critério seja necessariamente a fisicalidade da identidade.

Ao mesmo tempo, proteger o espaço de criação identitária é mais do que propor apenas contexto ou sigilo.

É preciso fomentar um espaço social que permita florescer formas distintas de compreender as relações comunicacionais e identitárias entre indivíduos de modo amplo.

A privacidade, como se verá em momento oportuno, também está na capacidade e direito de articular as estruturas para que seja possível uma criação de uma identidade motivada, desejada, construída com base nos interesses e desejos do indivíduo.

A contextualização proposta por Nissenbaum (2009) parte de um pressuposto importante de garantias de que o cenário em torno de onde se coleta uma informação deve estar disponível para entregar contornos inteligíveis ao dado observado, mas ainda que os contextos estejam preservados, é mister lembrar que os interesses e os filtros aplicados para compreensão de tais dados são transitórios e efêmeros.

Considera-se então a necessidade de estruturas muito mais robustas de fomento e proteção ao indivíduo em meio à miríade de agressões e violências possíveis que este enfrentará na construção da sua identidade.

Desenvolver a sua identidade é mais do que constituir um espaço privado, no sentido econômico, ou sigiloso. É permitir que os indivíduos em transformação sejam a crítica constante à sociedade que a fará evoluir a um estado de humanidade mais elevado ao longo do tempo.

Assim, em um paralelo possível entre o que Nissenbaum (2009) diz sobre privacidade e liberdade de expressão, a identidade de cada indivíduo não é antagônica a constituição da sociedade, muito pelo contrário.

Da mesma forma que Liberdade de expressão e direito à personalidade e privacidade não se colocam realmente em antagonismo, a visão de uma sociedade fortalecida também se deitará sobre os ombros de diversas identidades ascendentes que se formarão nas zonas intersticiais das relações humanas.

Mais adiante será perceptível que este tema se unirá à questão da coleta e consolidação dos movimentos de dados de cada indivíduo que tem o potencial de infringir violências em diversos espectros temporais sobre a vida de cada indivíduo na medida que, em um nível básico, não considere a contextualização, que neste caso serve ao olhar jurídico de Solove (2011) e Nissenbaum (2009) mas também de um desenvolvimento humano que vá além dos artefatos de registro do passado.

Após passar pelas etapas apresentadas, principalmente com o objetivo de problematizar o campo vasto da coleta tratamento e uso de dados, chega-se à chamada quarta revolução industrial que tem na IoT um de seus expoentes e que pode ter impacto significativo na exposição da privacidade.

Internet of Things (IoT) is a digital environment wherein different manufacturing resources and objects are embedded with actuators, digital devices and sensors. The embedded objects are then connected together and therefore data is collected and exchanged between them (Xia et al. 2012). Thus, the IoT framework aids in object-to-object communication and sharing of data through the enhanced connectivity between physical objects, services and systems. IoT environment has aided various industries in achieving automation for various purposes such as machining, heating, space lighting and remote monitoring. One of the key characteristics of IoT framework is to create smart objects through automatic identification technology. (KUMAR; ZINDANI; DAVIM, 2019, p. 10)

A IoT se torna relevante para este estudo justamente por trazer à luz o fato de que os actantes produtores de dados não são estritamente e exclusivamente humanos, mas gravitam e observam as condutas humanas.

Semáforos, cadeiras, carros, o piso de uma calçada os marcadores nas estradas, presilhas de cabelo podem se tornar coletores de dados.

Com isso, cada momento em sociedade ou na intimidade do lar pode se tornar um artefato observável e, aos olhos do mercado, comercializável.

What [she] means is that it's the data generated and transmitted across this network which should interest us, rather than the network itself. Many if not all of the nodes on the internet of things are constantly generating data, often about individuals, or groups of people. Sometimes that's with that person's knowledge and consent, but not always. (SUMNER, 2016, p. 167)

Torna-se importante refletir sobre a questão da comunicabilidade dos atos humanos como forma de vigilância de modo além do panóptico, pois não há um ponto central que tudo observa, mas sim múltiplos olhos que captam uma massa de dado enorme que será usada a favor e contra os indivíduos de acordo com os interesses dos seus detentores.

Dentro desta questão, há um aspecto de extrema necessidade da atenção social.

Na medida que muitos sensores captam tantos dados, ainda que tais sensores não sejam capazes de abarcar toda a realidade, podem trazer uma ideia de imensidão e pervasividade tal que, impregnada a ela, haja um sentimento de verdade ao invés de verossimilhança.

Ou seja, os dados captados em uma sociedade permeada pela IoT podem ser tomados como uma fotografia multifacetada da verdade. Aquilo que ela mostra pode se tornar tão forte que se torna a realidade jurídica e social. E aquilo que a IoT não mostra, se torna inexistente.

Mas não é simples pedir a cidadãos que atuem, ajam em sociedade considerando que a cada dia comum, ao invés de apenas receber milhares de estímulos, eles possam estar sendo observados por também milhares de sensores.

The internet of things on this scale, both macro (in terms of pervading an entire city) and micro (in terms of tracking every tiny movement of an individual), raises interesting questions of how we consider privacy. How much of our lives now are not online? When there are objects out there passively recording every trivial detail of our day, without our consent, which is then analyzed, brokered and sold on in ways of which we're not even aware, where. (SUMNER, 2016, p. 168)

Destaque-se, então, que Sumner (2016) coloca a questão das pessoas estarem cientes de que suas cidades são coletoras de dados. Mas tal afirmação dentro do panorama da IoT é similar aos contratos de adesão *opt-in* da internet atual.

É necessário colocar esta afirmação dentro da vida comum das pessoas.

Alguém que more em um estado da federação que proíba a coleta indiscriminada de dados e que, durante sua vida profissional, receba uma proposta de trabalho, mas que para aceitá-la seja necessário mudar-se com sua família, e que o novo posto deva ser ocupado em uma Cidade Inteligente levanta a questão. Neste momento fica mais evidente que apenas informar as pessoas não é suficiente.

A permissão de tais coletas indiscriminadas significa cercear a liberdade social e econômica de muitas pessoas que decidem manter sua vida privada longe dos olhos das empresas de dados.

Em outras palavras, é necessário um novo passo técnico, que permita às pessoas se tornarem inacessíveis às coletas de dados generalizada ou que permita a vigilância do vigilante.

When we look at IoT devices they are horrendously insecure, criminally insecure. One of the things everyone involved in Industrie 4.0 and the 4th industrial revolution and in respect of smart and future cities and societies need to understand is that we are trying to create well governed spaces that are both in the physical world and increasingly now in the virtual world too. (SKILTON; HOVSEPIAN, 2018, p. 208)

Como mostra Skilton e Hovsepien (2018), a visão mais afável sobre a IoT está vinculada à eficiência dos espaços *onlife* (FLORIDI, 2014), que de fato tem seus benefícios. Alguns que merecem destaque são fáceis de se identificar.

Nas cidades inteligentes espera-se que ambulâncias sejam acionadas e direcionadas, com os paramédicos, para atender a pessoas com princípio de infarto antes mesmo que elas mesmas sintam o avançar dos sintomas. Semáforos podem conduzir o fluxo do trânsito para abrir caminho para policiais, ambulâncias ou bombeiros em casos de emergência. Celulares podem reportar, de acordo com a posição e o movimento, de modo coletivo e automático, aonde estão os buracos nas vias públicas ou se seus detentores estão dirigindo embriagados. Em um extremo tecnofílico, pessoas poderão ser convocadas para salvar vidas de acordo com seus registros fisiológicos através de implantes de monitoramento de saúde, doenças serão estudadas não apenas de acordo com suas características fisiológicas, mas com grandes bases de dados sociológicas de condutas individualizadas.

Turing displaced us from our privileged and unique position in the realm of logical reasoning, information processing, and smart behaviour. We are no longer the undisputed masters of the infosphere. Our digital devices carry out more and more tasks that would require some thinking from us if we were in charge. We have been forced to abandon once again a position that we thought was 'unique'. The history of the word 'computer' is indicative. Between the seventeenth and the nineteenth century, it was synonymous with 'a person who performs calculations' simply because there was nothing else in the universe that could compute autonomously. (FLORIDI, 2014, p. 93)

Por outro lado, é preciso considerar que nesta condição de sujeito profundamente monitorado e vigiado, passa-se a evadir as atitudes de modo amplo e com pouco conhecimento sobre os encaminhamentos que serão dados às informações coletadas.

So our privacy is now under threat from dustbins, street cameras, and our very cities. And whilst the internet fridge may still be a myth, the internet of things is already penetrating our homes in several guises, including the smart meter. (SUMNER, 2016, p. 172)

Qualquer objeto pode se tornar um marcador de conduta. Até mesmo aqueles que nunca foram vistos como dispositivos eletrônicos.

Na fala de Sumner (2016) é possível buscar a menção da intimidade sendo vigiada e coletada por latas de lixo, ou seja, objetos que antes recebiam apenas a ação física, agora também podem ter uma contra-ação de vigilância, coleta e tratamento de dados sobre os indivíduos.

Ainda que algumas pessoas possam alegar que parte desta vigilância já era possível antigamente, tomando o exemplo das latas de lixo como icônico, através do roubo de lixo de alguma residência específica, vale destacar ao menos dois pontos.

O primeiro é a escalabilidade da vigilância, que agora pode operar em um nível massivo com um custo decrescente ao longo do tempo. Já o segundo ponto, que vai além da questão da vigilância sobre uma população, e que age em uma camada mais profunda, é a transformação da vigilância em um modo de pensar que ativa a autocensura nas pessoas ou as faz ter que escolher como agir em sociedade de modo preventivo à vigilância ou ao modo como imaginam que o sistema vigilante irá interpretar seus atos e seu consumo.

Se torna papel do cidadão médio intuir como o sistema espera que ele se comporte no agora, com vistas na repressão ou na recompensa imediata, e no amanhã, com vistas às recompensas e riscos futuros.

Porém isso é o mesmo que tornar a conduta na sociedade uma atividade repleta de atitudes especulativas como a bolsa de valores. Quantos comportamentos serão cerceados por pessoas mais precavidas pela simples ideia de que um governo autoritário (seja de direita, seja de esquerda) venha a assumir o poder dentro de um determinado país.

A simples ideia de repressão futura pode ser suficiente para bloquear inúmeras pessoas, fazendo com que gerem um auto-impedimento de conduta com base em suposições a cerca da perpetuidade da vigilância.

Disciplinary regimes that activate nation state legal systems and rely on new forms of digital surveillance are productive in the inculcation of these new identities that are complexified by being at once both performative within local and global spaces. This is not to suggest, of course, that these particular coordinates of identity are meaningful to subjects, nor that the kinds of positioning of subjects in the context of differential regimes of time and space necessarily undo the powerful newness of encounters with otherness. (COVER, 2016, p. 179)

De um modo mais prático, isso não significa que a identidade em si do sujeito está determinada pelo sistema de vigilância, mas segue condicionada, no sentido de oferecer condições específicas para que uma dada forma de conduta no mundo se manifeste.

Assim como a espiral do silêncio não muda estruturalmente a opinião do indivíduo, mas sim a manifestação do que viria a ser sua opinião, através do que se

convencionou chamar de viés do observado, na medida em que o observado se sabe em estudo e intui um caminho de melhor aprovação social e menor violência, o mesmo poderá ser impactado na forma de agir em sociedade enquanto se tem consciência da vigilância pervasiva.

O problema se dá na medida em que, enquanto na espiral do silêncio o entrevistado sabe que em breve se verá livre do entrevistador, e dificilmente será rastreado e reprimido no futuro pela opinião emitida, o vigiado numa sociedade da IoT pode não conseguir se desvencilhar facilmente do seu vigilante.

Cover (2016) chegará a questionar se não estamos rumando na academia para um certo pânico tecnofóbico. Porém, há de se fazer a ressalva que responde parcialmente ao apontamento do autor que trata justamente do cenário em que se realiza a observação da sociedade.

Na medida em que o mercado está disposto e empregando energia para convencer as pessoas sobre as maravilhas da tecnologia, torna-se desequilibrada a balança no que tange aos riscos iminentes de sua adoção indiscriminada.

Entre os que ainda emitem os alertas estão alguns jornalistas, que ao observar os movimentos da sociedade, buscam apresentá-los de modo palatável ao público em geral de modo que este possa tomar consciência do máximo de fatores que influem sobre suas vidas, e a comunidade acadêmica que, ao operar o máximo possível livre das amarras do lucro e do mercado, e estando incumbida de pensar sobre qual sociedade existe e existirá, apresenta como resposta os achados de cada pesquisa.

Ao colocar na balança a sedução mercadológica acelerada e descompromissada com a longevidade das relações humanas em nível de equilíbrio, e o tempo da pesquisa, que exige a responsabilidade de trazer a fotografia de recortada e o máximo precisa possível sobre uma realidade, há claramente uma dissonância tanto de objeto, quanto de narrativa e de forças.

Ter isso em mente pode aumentar a percepção do motivo que leva tantos pesquisadores a apresentarem textos alarmistas ao invés de conformadores.

Entretanto, mesmo tendo clareza do que leva a esta posição mais acentuada, não significa que um modelo ajustado de contrapesos tenha sido implementado ou sequer que alguma proposta de conduta social esteja ganhando maiores contornos e

apoios da comunidade acadêmica para confrontar e absorver de modo socialmente favorável as transformações no campo da memória digital e da privacidade.

Information privacy experts may argue that perfect contextualization is creating a devilish infrastructure of surveillance. But as Oscar Gandy has reminded us, surveillance is about the asymmetric power to watch, a power that necessarily benefits the surveyor over the surveilled.⁵³ In a world where all information is transparent, Brin suggests, surveillance loses that power. And if the infrastructure of digital remembering could be organized in a decentralized fashion, much like the instruments Gordon Bell uses, perhaps no single entity, no matter how powerful, could ever hope to control all of it. (MAYER-SCHÖNBERGER, 2009, p. 97)

O que se vê Mayer-Schönberger (2009) é que em dado momento o autor vai reunir diversas visões sobre a vigilância e propor algo que fortalece ainda mais o sistema vigilante.

Quando a proposta de descentralização aparece, ela não está a combater a vigilância, mas a aceitá-la como um fato consumado que deve ser combatido com a liberação transparente da vida comum para que a realidade seja auditada por diversas fontes de dados.

Este posicionamento parte de três pressupostos dúbios.

O primeiro é que as pessoas agem de modo plenamente consciente, e por isso é plausível observar seu comportamento como reflexo de suas manifestações de interesse motivado pela identidade, unindo emoção e pensamento de modo consonante e intencional.

O segundo é que ainda que fossem plenamente conscientes de todos os reflexos e interpretações possíveis sobre seus atos, que é desejável ter cada conduta mapeada e salva para estar eternamente disponível.

E o terceiro é que há transparência, e que ela é plenamente possível, ignorando qualquer tipo de fricção entre ato e registro.

Há de se entender, porém, que sobre esta questão implicam os esforços mercadológicos para a educação de um desejo pela observação, por ser observado e observar.

Assim, trata-se de uma educação midiática, ou seja, que através da técnica e dos suportes, consolidam uma forma de aprovação da conduta social que depende da exposição e da participação no processo de vigilância e reforço do capital

simbólico, sendo que por capital simbólico é necessário recorrer a Bourdieu (1987) para ter o sentido estrito oferecido pelo autor ao cunhar o termo.

[...] a ideia de que as lutas pelo reconhecimento são uma dimensão, fundamental da vida social e de que nelas está em jogo a acumulação de uma forma particular de capital, a honra no sentido de reputação, de prestígio, havendo, portanto, uma lógica específica da acumulação do capital simbólico, como capital fundado no conhecimento e no reconhecimento; a ideia de estratégia como orientação da prática, que não é nem consciente e calculada, nem mecanicamente determinada, mas que é produto do senso de honra enquanto senso desse jogo particular que é o jogo da honra; a ideia de que existe uma lógica da prática, cuja especificidade reside sobretudo em sua estrutura temporal. (BOURDIEU, 1987, p. 35 - 36)

Desta forma, não há como se pensar neste capital simbólico sem compreender que ele é histórico, construído ao longo do tempo e com os balizadores disponíveis e validados socialmente.

Na medida que o mercado consegue agir sobre uma camada cultural e inclui nos fatores de legitimação da identidade e do lugar de fala na sociedade a questão da auto-exposição midiática e da evasão da privacidade, o capital simbólico se avoluma com uma nova forma instrumental de legitimação.

Neste cenário, e considerando a pervasividade técnica e mercadológica das formas de vigilância contemporâneas, altamente simbióticas com os dispositivos de comunicação, Bruno (2013) irá indicar que não se trata mais de um panóptico benthaniano que, apropriado por Foucault (2013) deixa de ser uma estrutura física e passa a ser uma estrutura social e de controle das populações observadas a partir de um ponto específico.

Nem panóptico nem sinóptico, mas um modelo reticular e distribuído onde muitos vigiam muitos ou onde muitos veem e são vistos de variadas formas. Algo como um palinóptico, para brincar com o radical grego palin, que designa processos de dupla via. Ver e ser visto ganham aqui sentidos atrelados à reputação, pertencimento, admiração, desejo, conferindo à visibilidade uma conotação prioritariamente positiva, desejável, que ressoa nos sentidos sociais que a vigilância assume hoje. Ser visto e ser vigiado, assim como ver e vigiar, são progressivamente incorporados no repertório perceptivo, afetivo, atencional, social, e associados a processos de prazer, diversão, sociabilidade. A escopofilia e o voyeurismo saem dos quadros nosológicos da sexualidade e incorporam-se ao cotidiano dos meios de comunicação. (BRUNO, 2013, p. 47)

Quando menciona o palinóptico, pressupõe-se sutilmente a equivalência de forças da vigilância, mas o panóptico anterior, aquele que já traz consigo o peso do poder concentrado no vigilante e a vulnerabilidade do vigiado, segue aplicável no sentido que indica esta disparidade do infopoder.

É neste momento que Bruno (2013) se une aos autores referenciados por Mayer-Schönberger (2009) para coadunar com o sistema dentro do mesmo passo que dão para criticá-lo.

Tanto não há equivalência de poderes quanto não há de se pensar na IoT como apenas uma forma de descentralizar a vigilância de modo transparente.

Cada uma das proposições pode se tornar corrosiva da visão de forças dispostas no cenário atual.

Não à toa Marx (2016) irá mirar no objetivo do mercado midiático quando cria e comercializa programas de entretenimento que se baseiam na exploração da invasão da intimidade das pessoas.

The mass media in pursuit of selling advertising offers personal information as entertainment, and often the more personal, private, intimate, sensitive, or embarrassing the entertainment, the better from the standpoint of garnering a large audience. The worldwide popularity of Big Brother kinds of TV programs is noteworthy. However, the initial and driving goal of the personal information gathering and revelation regarding the TV shows' participants in these cases is profit, or persuasion using surveillance as free entertainment to reach those of interest. (MARX, 2016, p. 80)

Desta forma, a corrosão se dá na medida em que a vigilância, esticada ao extremo em programas popularescos de TV como Big Brother, coloca-se como aliada do entretenimento, e como tal, acaba por gerar uma chancela cultural espelhada na comunicação nacional ou regional.

Com o ideal midiático da fama, muitos são tutorados a desejar a exposição como forma de sentir parte do sabor que a fama tem.

A exposição de si passa a ser uma forma de status e de caminho para a conquista de um dos troféus simbólicos (BOURDIEU, 1987) estabelecidos através do suporte da mídia panórgica e perversa.

O prazer de se expor aparece na satisfação das curtidas que um sujeito recebe em suas publicações nas redes sociais.

[...] outra característica do universo do Facebook [e não apenas dele, mas das redes sociais digitais com um todo] reside na importância que tem a lógica afetiva, levada a cabo em particular pelo botão 'curtir'. O importante não é mais o ideológico ou a posição na escala social, mas o reativo, o apreciativo e a estética, que aparecem como polos privilegiados da expressão da identidade hiperindividualista. Assim, diante de uma mensagem, uma opinião, uma foto, uma música, o usuário do Facebook [idem acima] clica no botão 'curtir'. (LIPOVETSKY; SERROY, 2015, p. 374)

A validação social passa a ser ranqueada pelo número de seguidores, compartilhamentos etc. Mas isso não se dá apenas no campo sociológico e psicológico, mas traz respostas fisiológicas também, com descargas hormonais que geram o reforço positivo na medida em que as curtidas aumentam, os compartilhamentos se avolumam.

Tais espetáculos de realidade ganharam ainda mais espaço com a popularização de novos formatos, como o Big Brother e os chamados reality shows de intervenção ou de transformação, em que os participantes sofrem mudanças ao longo do programa, as quais incluem desde renovações no vestuário a cirurgias plásticas. Este ingresso do indivíduo comum no reino televisivo não anuncia o fim do espetáculo das celebridades e sua substituição pelo espetáculo dos anônimos. Sabe-se que estes dois formatos convivem e se alimentam reciprocamente, ainda que constituam dois modos distintos de relação com o espectador. (BRUNO, 2013, p. 67)

Pode-se dizer o mesmo quando o olhar se volta para as redes sociais digitais e o convite sedutor da exposição da própria imagem, oferecendo displicentemente a chance mágica de alçar desconhecidos ao posto de celebridades.

O estrelato oportuno está na próxima foto, no próximo vídeo, na próxima exposição do corpo, da vida.

Os espaços construídos para a vida privada podem facilmente ser erodidos e minados pela permeabilidade técnica justamente dos meios de comunicação.

Another problem with looking at expectations of privacy is that technology will gradually erode what people expect to be private. As this process occurs, the government will be able to engage in ever more invasive searches and seizures. And then there's the circularity problem - expectations of privacy depend in part on the law, so a judicial decision about reasonable expectations of privacy can become a self-fulfilling prophecy. (SOLOVE, 2011, p. 117)

Cada indivíduo é convidado a experimentar os benefícios da tecnologia para facilitar suas tarefas diárias, e ao mesmo tempo é ensinado, clique a clique, como se consome conteúdo identitário na internet, nas ruas, nas assinaturas de clubes de livros, em cada caixa eletrônico ou guichê de farmácia.

Os meios de comunicação convertidos em tecnologias de vigilância passam a largo de um grande déspota autoritário lançando mão de inúmeras agressões pesadas e visíveis.

A tecnologia é o líder sedutor que conduz seu povo com micro-violências sutilizadas no campo da vida comum e que paulatinamente tutoram a conduta desejada em sociedade retribuindo com prazeres efêmeros.

Estar em constante fluxo comunicacional, por si só, não basta. O processo comunicação, para se dar de modo atraente precisa ser imagético.

O eu-imagem deve ser reativo ao olhar do outro. Sua autenticidade não mais se esconde por trás de signos a interpretar, mas se constitui no ato mesmo de se fazer ver pelo outro. Esta íntima relação entre existir, ver e ser visto é explicitada, por exemplo, nas votações que decidem o futuro dos participantes de reality shows, nas conversações e “curtidas” em redes sociais, ou nas ferramentas de comentários de blogs e de plataformas de compartilhamento de fotografias ou vídeos, por meio das quais os leitores e espectadores participam ativamente da escritura e da composição da imagem que o autor constitui para si e para os outros. (BRUNO, 2013, p. 69)

Neste caso, apresenta-se o olhar do outro como o campo de conquista do estrelato.

O agir em sociedade de modo exposto vincula-se ao ato de produzir uma imagem desejada no outro, na audiência ampla, ou convencer um algoritmo que se é mais influente, relevante, importante do que outra pessoa na rede em questão.

A conduta compartilhável das pessoas nas redes sociais, principalmente as digitais, através de um fluxo constante de e-vasão de imagens cria uma topografia especial que encobre a topografia clássica dos espaços e reconstrói cada viela com o verniz performático das curtidas.

Estar disponível, estar na ágora para ser consumido é tornar acessível o cotidiano espetacular. É e-vadir cada instante em potencial.

Isso não significa que a câmera precisa estar ligada 24 horas por dia para que a intimidade esteja exposta.

Mais do que isso, o simples fato de poder, de ser capaz e desejar a qualquer momento e-vadir a intimidade faz com que tal intimidade seja ainda mais performática, esteja sempre cercada dos artefatos performáticos.

Ou seja, no íntimo, quando este já está cooptado pelo saber técnico da e-vasão, além do desejo de se e-vadir há também a coletânea dos artefatos que tornam possível tal e-vasão.

Assim, as e-vasões cotidianas não estão dispostas ao acaso, mas estão postas como resultado de uma articulação íntima para expor o eu desejado, arquitetado e construído.

Breve enxerto é necessário neste momento para um questionamento que pode ser recorrente ao trazer à luz este eu-mídia, um conceito derivado por Terra (2010) de

Latour, que é um eu pretensamente real contraposto ao eu articuladamente apresentado através das redes sociais digitais, à sombra do que se apresenta nos debates esvaziados da privacidade contraposta à segurança, assim o farão aqueles que observarem apenas rapidamente o eu-infotécnico contemporâneo como contraponto de um eu-real.

O que se apresenta até este momento é a visão de que cada indivíduo pode articular as formas de tornar visíveis suas facetas sociais, e que tal habilidade de composição imagética está em curso de aceleração, assim como todas as outras técnicas em sociedade seguem sua jornada ecossistêmica.

Cada técnica aplicada pelas pessoas está em sua jornada memética pela sobrevivência e aprimoramento. Assim, não são as redes sociais virtuais como contorno que definem a conduta humana, mas em simbiose, os actantes se moldam, ou seja, moldam a si, e remoldam, ou seja, reconfiguram seus moldes, para obter ao final deste processo uma sobrevida e, quiçá um prazer.

The majority of wearable Technologies synchronize with personal computers and smartphones, in which dedicated applications store and analyze data, as well as share them with friends and the community. Sharing data with friends on the social media, or at least within a given wearable social network ecosystem, is usually a default option because without the possibility of praising oneself for the accomplishment ("I ran 5 miles today!") and comparisons with others the functionalities of such applications would greatly diminish. It is the collaborative, interaction-enabling component that mostly constitutes their usability. (PRZEGALINSKA, 2019, p. 48)

Em casos como os expostos acima se torna mais evidente que a e-vasão da privacidade, através da midiatização das identidades, está construído também no desenho das tecnologias de comunicação e de vigilância.

Quando empresas como a Nike criam dispositivos vestíveis e conectáveis, o projeto é maior do que apenas manter seus clientes engajados na prática esportiva.

A propagação da cultura do esporte praticado com e para as redes sociais digitais faz com que cada cliente se torne um propagador da marca e da cultura exibicionista da prática esportiva através dos dispositivos pela praticidade do uso e facilidade do compartilhamento que se torna parte da construção discursiva do eu, da máscara social.

A estética do compartilhamento da corrida do final do dia, do treino na academia, do mapa com o percurso percorrido de bicicleta traz um senso de conduta coletiva, expectativa generalizada.

Ao entrar nas redes sociais digitais e ver que muitos amigos estão, ao mesmo tempo, postando o trajeto da última corrida do dia, faz com que as pessoas se perguntem se deveriam estar inseridas nessas mesmas práticas. Mas aqui vale a ressalva de que a prática em questão não é apenas a corrida ou o esporte, mas sim o esporte como suporte da comunicação e exposição do eu.

Claro que há o benefício para a saúde quando se fala em assumir práticas esportivas recorrentes, mas para este trabalho o que se faz necessário é compreender que o esporte aqui não necessariamente ocupe o centro da prática, mas seja uma condição necessária para a midiatização do eu dentro de um grupo específico.

Assim como os troféus simbólicos dentro de um campo de disputas apresentado por Bourdieu (1987), correr não tem o mesmo significado social do que correr enquanto se publica stories ou vídeos ao vivo no parque. Pedalar não significa a mesma coisa do que monitorar o trajeto usando dispositivos vestíveis com coleta e tratamento de dados que, ao final, permitirão o compartilhamento de um infográfico com o desempenho obtido durante os minutos de empenho.

Os dispositivos vestíveis não cobrem os corpos de tecidos e silício, simplesmente, mas recobrem a mente de uma camada comunicacional e-vasiva e reforçam o caráter memético de suporte do corpo para a propagação informacional.

Neste caso, a IoT não fundou a auto-mensuração ou a auto-documentação (*self-tracking*), mas exponenciou seus efeitos em uma aceleração intensa.

Exemplos como diários ou até mesmo as pinturas rupestres são formas de consolidar parte da história de uma ou de várias pessoas.

Mas nos termos atuais, o *self-tracking* assume um caráter fugaz e transitório, sendo produzido para o compartilhamento instantâneo e válido para aquele momento.

A corrida do dia anterior não pode ser ostentada hoje. E ao mesmo tempo, a exigência dromocrática (TRIVINHO, 2007) vai exigir tamanha produção de conteúdo, e não é um conteúdo simples senão performático e transtético (LIPOVETSKY; SERROY, 2015), que mesmo os mais engajados ainda precisarão de uma forma de reciclar suas narrativas e seus artefatos comunicacionais para apresentar versões transitórias de si na mídia e nos contextos sociais.

No Instagram esta reciclagem, que funciona como uma reativação das narrativas performáticas, e ao mesmo tempo um respiro para o e-vasor na saga de produzir mais e mais artefatos, materializa-se no chamado #TBT, do inglês *Thuesday Back in Time*, ou algo que se traduziria como “uma quinta-feira tempos atrás”, que abre uma licença midiática para trazer artefatos antigos para o campo performático.

Uma viagem rara, um encontro glamuroso, ou mesmo a estética da valorização das pequenas coisas como forma de demonstrar valores pretensamente mais elevados do que os #TBT internacionais, que serve ao mesmo exibicionismo e-vasivo, faz com que o passado seja estetizado e sirva para dar mais alimento para a performance hiperestética.

Tais aparelhamentos servem a um movimento que e-vade muitas formas do corpo e da mente e tutoram tal e-vasão, novamente, para que sejam desejadas e buscadas.

Mais do que aplicar energia para tirar informações, o sistema tecnocrático convence as pessoas a usarem seus próprios recursos para e-vadirem seus dados, o que torna a relação mais profunda e a produção de capital infotécnico mais suave, com menor fricção e maior rentabilidade.

Simultaneously to the formation of self-tracking communities, the users were able to experience the evolution of tracking hardware and software. We observe the progression from simple assisting devices to the rise of increasingly sophisticated trackers, including those that measure brain activity like the aforementioned Muse, the brain sensing headband for training relaxation and meditation, and similar brain-trackers, such as Melon or Emotiv. These trackers ascend to a different level of interaction with users and engender profound changes in how we understand the role of a tracker. They are more personalized, unobtrusive, and usable anytime and anywhere. Although these devices measure very complex activities like affects or emotions and provide feedback about them, they retain a high degree of portability. Thus, people may use them in various spaces, for instance at group meetings or workplaces; such collaborative relaxation sessions is what Muse users are encouraged to do. Moreover, the rise of big data analytics enables more insightful analyses of all users' digital footprints. (PRZEGALINSKA, 2019, p. 59)

Entende-se então que se deixa de falar de um registro apenas externo, ou de traços simples da conduta cotidiana, para descer em aspectos emocionais e psicológicos.

Uma provocação, que não se pretende encerrar por aqui, mas entregar para a comunidade científica e civil, é o prazo em que análises com estruturas e-vasivas

serão gradativamente inseridas nos processos seletivos empresariais, nas análises de visto para viagens e assim por diante.

Hoje em dia é comum empresas aplicarem testes psicológicos para aqueles que se aplicaram a uma vaga.

Muitas vezes o que se percebe é um esforço profundo em compreender estas pessoas antes que elas ganhem acesso ao corpo funcional da empresa, ou seja, apenas no período de contratação, mas poucas formas de acompanhamento psicológico são aplicadas para os atuais funcionários.

Parte disso pode se justificar pelo custo que isso traz, seja em tempo, seja em profissionais alocados.

Mas na medida em que a IoT é suavizada em seus aspectos e-vasivos, pode se tornar comum nas empresas de anos adiante a obrigatoriedade de uso de tecnologias vestíveis que podem gerar alertas automáticos e individualizados quando o funcionário estiver com algum problema de saúde ou mal súbito, e esta é a forma positiva de apresentar os entregáveis deste tipo de prática, e ainda gerar sinais constantes sobre o nível de tensão ou desafeto entre as pessoas no trabalho, condicionando parte dos profissionais a serem excluídos do convívio laboral antes que tenham tempo de lidar com suas emoções e desenvolver habilidades necessárias para a vida comum.

Ou seja, pergunta-se quais seriam os impactos quando o sistema econômico conseguir, de forma mais barata e prática, expurgar os dromoinaptos (TRIVINHO, 2007) e observar as manifestações sociais do eu.

Ainda que pareça forte usar a palavra expurgo para tanto, é necessário considerar o conceito de infopoder que está por trás da aptidão e inaptidão acelerada recorrentemente no processo e-vasivo.

Infopower is exercised in concern with a “data episteme.” By this I mean to suggest that information itself is today a formidable mode of rationality by which entire domains of knowledge are made possible. The data episteme is an epistemology in which the need for more and more data is the spawn of data itself. Consider how frequently information is presented as a suficiente premise for other information. (KOOPMAN, 2019, p. 160)

E-vadir a privacidade é parte do processo de conquista do infopoder, mas que não é suficiente.

Como mencionado, é preciso querer estar exposto, visível.

A busca por motivos pelos quais contar, narrar o cotidiano, a cada detalhe oportunista, é parte da busca por uma linguagem específica que permita ao indivíduo se destacar entre todos os actantes acelerados em busca de um reconhecimento distintivo dentro do campo de negociação simbólica dos poderes informacionais.

A estrutura e-vasiva da privacidade e do *self* depende não apenas de uma lógica, de uma mentalidade, um pensamento prevalente em seu tempo, mas também de infraestrutura tecnológica para que os movimentos dos dados sejam possíveis.

A catalogação analógica de dados depende de muito esforço e especialização, motivo pelo qual sua ocorrência é mais prevalente em sistemas governamentais altamente centralizados como, por exemplo, os regimes ditatoriais.

Para sua ocorrência com maior pervasividade, ubiquidade, é preciso uma infraestrutura que, da mesma forma, esteja disseminada em diversas camadas sociais.

O uso indiscriminado das tecnologias de comunicação, convertidas em estruturas de entretenimento e vigilância, é condição necessária para a disseminação da e-vasão.

At the core of Industry 4.0 there are two key enabling technologies: Internet of Things and Cyber-Physical Systems. Learning and understanding of these new technologies aids in realizing an interconnected world wherein customer needs are responded dynamically and efficiently by the developed smart factories. I4.0 results in the virtual replication of the physical processes and systems which ultimately supports in intelligent analysis of the large volume of generated data. (KUMAR; ZINDANI; DAVIM, 2019, p. 43)

É através da coleta compulsória de dados, em grande volume, em diversos pontos de observação que se torna possível ensinar as inteligências artificiais a processarem, a tratarem os dados com diversos exemplos de comportamento, de modo a abranger grande parte dos espaços de convívio.

Para desenvolver uma engenharia algorítmica que toque, intencionalmente, a vida cotidiana, diversas etapas são necessárias. Etapas estas que só foram possíveis através do barateamento das tecnologias e da disseminação de seu uso por indivíduos consumidores e por projetos estatais.

A quick overview of this list reveals the well-known methodology of the Level of Abstraction at work, including all aspects from the very concrete to the formal, from the isolated act of computation to its complex environment: the formal structures underlying data and their algorithmic treatment; their implementation in language and use for program design; the design and construction of (networks of) hardware to manipulate, visualize and process

data; data analytics and its use to lead automatic processes; the relation between machine and the user; the study of autonomous agents; the mechanical engineering of living systems. (PRIMIERO, 2016, p. 91)

Nas grandes cidades, as tecnologias de automação do trânsito, como faróis inteligentes, radares com reconhecimento de placas, câmeras com reconhecimento facial são parte desta infraestrutura. Da mesma forma que os dispositivos móveis, os aparelhos celulares.

Do ponto de vista das cidades, não apenas estes sensores fazem parte da infosfera.

Há de se considerar sensores de estacionamento, monitores de fluxo de pessoas nas ruas e nos transportes públicos, geolocalizadores da malha de transporte público, câmeras de ônibus, coletores de áudio que buscam sinais de disparos de arma de fogo. São diversos tipos de sensores aplicadas com o objetivo, ou pretexto, da segurança e da comodidade, da eficiência dos serviços públicos.

Da mesma forma que as cidades vêm se vestindo e revestindo de tecnologias de comunicação e vigilância, os indivíduos já começam a se utilizar de tecnologias vestíveis que proporcionam conforto, praticidade e infoentretenimento e para auxiliar na construção do discurso do eu-midiático.

O movimento de anos atrás que permeou os espaços públicos agora se torna mais próximo e sutil, através das tecnologias de uso individual construídas com base do imperativo e-vasivo de uso necessário para demonstrar o pertencimento à comunidade transestética e a dromoaptidão na linguagem tecnológica.

Wearable technology then extends the sensory functions of the body, blurring the boundaries between the corporeal body and technology. This mobile body embedded with technology extends the ability to freeze frame images in real time, and to disseminate, archive and retrieve these on digital platforms. The ubiquity of the mobile phone well as the rise of smartphones has enabled image capture and storage on a large scale, unleashing a wider digital visual culture where images are shared, exchanged and commodified on video/image sharing sites and apps. (IBRAHIM, 2018, p. 38-39)

Quando compreende-se que as tecnologias vestíveis estão a estender os sentidos biofísicos do corpo, retoma-se automaticamente o pensamento de McLuhan (1964) e Kerckhove (1997).

Ao cobrir o corpo, cobre a mente, redimensionando as habilidades de tocar o mundo e de ser tocado por ele.

Desta forma, não pode ser vista como algo apenas externo, mas intersticial.

A tecnologia se infiltra, vai além da epiderme e dá frutos na simbiose.

Tanto corpo como mente se tornam plasticamente transformados em algo além, distinto à materialidade original, e através dos processos simbólicos reconstroem a percepção do mundo e de si.

Quando Ibrahim (2018) indica o congelamento da imagem, em si o que está a colocar em questão através das tecnologias vestíveis e internalizadas é a suspensão do tempo cronológico para a criação de um campo de significações além da fisicalidade e que faz parte da narrativa do eu nas mídias e nas redes.

Importante compreender que da mesma forma que as tecnologias vestíveis tornaram o corpo expandido, transformado, o mesmo ocorre com a infraestrutura acoplada nos prédios e ruas das cidades.

O espaço urbano já vem se vestindo de tecnologia há muito tempo. Ocorre que, com a internet permeando os objetos e conectando as bases de dados, o que se processa agora é a globalização microestrutural das cidades, que como corpos, ressignificam seus sentidos alterando parte do seu estar-no-mundo.

Os transeuntes se convertem em células de um corpo urbano expandido que vigia perto e longe ao mesmo tempo, sobrevoando os entes orgânicos e invadindo suas mentes no mesmo movimento duplo.

O exercício do vigilante está dentro e fora. A IoT se torna manifestação do mesmo fio dromocrático que vai converter qualquer ponto de coleta de informações em um sensor, um formador de autocensura, uma vigilância que com o tempo normaliza a e-vasão da privacidade e do *self*.

What is currently happening with wearable wellness devices provides a sense of the complexity of the privacy issue. An increasing number of insurance companies are considering making this offer to their policyholders: If you wear a device that monitors your wellness – how much you sleep and exercise, the number of steps you take each day, the number and type of calories you eat, etc. – and if you agree that this information can be sent to your health insurance provider, we will offer you a discount on your premium. (SCHWAB, 2016, p. 97)

Neste caso, os dispositivos vestíveis, através do apelo financeiro, oferecem um tipo de assédio em busca da e-vasão.

A oferta de desconto, como em muitas vezes neste trabalho seguirá evidente, não é uma diminuição do custo para quem permite a e-vasão, mas uma forma punitiva e de pressão para aqueles que decidem manter seus dados e sua privacidade o mais

longe possível das corporações e governos, dificultando a construção do seu perfil nos bancos de dados para manter um discurso do eu mais centrado na autodeterminação.

Não é o e-vasor que paga menos, mas o privativo que paga mais para ter certo / leve domínio sobre sua privacidade.

E se o processo de Lobby e de normalização da e-vasão seguir a passos largos, em muitos casos os países poderão aprovar leis que autorizem o tratamento diferenciado nos preços e condições de acordo com o que cada cliente se permite e-vadir.

Compreendendo, como se conferirá no capítulo legal, que parte do direito à privacidade na realidade segue protegido, muitas vezes, pelos códigos de consumo de modo mais afiado do que pelos direitos propriamente civis, a permissão para a distinção entre e-vasores e os que preferem manter sua privacidade se torna um passo significativo para que a conduta da opressão e da violência contra a privacidade se torne prevalente.

Algoritmos são tendenciosos pois a função deles é ser. Cada algoritmo recorta e molda os dados à maneira que foi pensado e para aquilo que foi programado.

O mesmo vale para o que se convencionou chamar de inteligência artificial (IA), que se trata de uma programação orientada ao aprendizado, porém não a um aprendizado aberto, mas sim dentro dos limites de recorte inseridos em seu código por seus programadores.

Um bom exemplo é o Watson, da IBM. Esta IA foi programada para varrer a internet e outros bancos de dados extensos e a partir disso oferecer respostas probabilísticas às perguntas feitas por seus usuários. Ou seja, Watson não cria respostas, ele trata dados com análises probabilísticas e expõe o resultado.

Mas estes vieses de pesquisa estruturados a partir da programação podem gerar fatores críticos distintos de acordo com o objeto que estamos observando.

As search engines not only provide textual documents, but also images, videos etc., they need to treat these different kinds of information objects differently, if only for their different properties. For instance, it is not possible to treat images to be found in the same way by the same algorithm as textual documents. Therefore, it is misleading to speak of the index of a search engine, as search engines have multiple indexes for each type of content. (LEWANDOWSKI, 2017, p. 67)

Da mesma forma que imagens ainda não conseguem ser bem indexadas pela lógicas dos buscadores, emoções, sentimentos, angústias estão sendo analisadas, e muitas vezes, algumas IA trazem tecnonarrativas sobre os dados das pessoas, traçando perfis psicológicos.

Uma interface homem-máquina que utiliza algoritmos para interpretar parte do cérebro humano para produzir uma ação, e que foi muito festejada, é o exoesqueleto desenvolvido por Nicoletti (2011) que através de um eletroencefalograma capta de pulsos eletromagnéticos intracranianos, interpreta os estímulos com base no algoritmo desenvolvido pelo pesquisador e sua equipe e converte tais estímulos de áreas específicas do cérebro em comandos motores.

Há interesse do pesquisador em encontrar um caminho paralelo ao natural para que portadores de paraplegia e tetraplegia consigam se locomover com autonomia.

Mas uma forma de compreender de modo simples e breve o que é o viés do algoritmo, é possível formular um exemplo com base nos desafios enfrentados e perseguidos por Nicoletti (2011) e sua equipe.

Ao avançar em seus estudos e aplicações, a equipe de pesquisadores reabilita os pacientes para caminhadas e para realizarem movimentos com mãos e braços para conseguir pegar objetos.

Parece óbvio que a pesquisa que busca devolver movimentos a portadores de paraplegia e tetraplegia comece por coisas muito simples, mas o alvo dos pesquisadores poderia ser reabilitar tais pessoas para a natação, para atividades circenses, para práticas de yoga.

Pode parecer um extremo, mas é justamente aí que está o viés. Quanto mais comum é para cada pessoa acreditar que está no caminho certo, maiores as chances de todos olharem pelo mesmo ponto de vista.

E por mais que a prática circense demande movimentos complexos que estão embasados nos movimentos que hoje são foco da reabilitação acima, percebemos o viés na medida em que rapidamente nos afastamos com espanto da provocação de atuar para que paraplégicos tenham autonomia a ponto de praticarem rapel ou escalada, yoga ou malabarismo.

Tal exercício de raciocínio é relevante pois quando voltamos ao campo de estudo proposto neste trabalho encontramos outras formas de viés que nos conduzem a uma conduta padronizada e a opiniões consonantes.

É confortável fazer perguntas aos buscadores, na internet, e receber respostas rapidamente, sem ter que questionar se são verdadeiras, relevantes, significativas. Sem questionar quais interesses podem estar levando aquele resultado a ser apresentado com maior frequência.

Search engine bias is the tendency of a search engine to prefer certain results through the assumptions inherent in its algorithms. This means that every search engine is biased, as it is impossible to design algorithms without human assumptions. Therefore, search engine bias does not mean that search results are deliberately manipulated by the search engine vendor but simply that results are ordered in a certain way that is determined by assumptions of what constitutes a good or relevant result in response to queries. It is even at the core of every idea of ranking, based on certain technically mediated assumptions, that certain items are preferred over others. (LEWANDOWSKI, 2017, p. 67)

Abre-se, ainda que não seja o objeto deste estudo, margem para a pesquisa sobre o consumo coletivo de notícias com base nos resultados dos buscadores.

O ponto crítico é receber resultados com base em tratamentos de dados e ter pouca margem para influir sobre eles.

A exemplo, não é permitido às pessoas alterar de modo intencional e específico a forma como o buscador da internet oferece respostas a ela. Se um aluno de administração quiser encontrar conteúdo no buscador do Google, mas gostaria que o resultado mostrasse páginas que apenas aquela camada pequena de altos executivos acessa, ele terá que agir por semanas como um alto executivo, enganando o algoritmo. Mas por onde começar?

Esta questão dos indexadores e algoritmos traz o enclausuramento do indivíduo na bolha infotécnica simbioticamente gerada pelo indivíduo, tecnologia e algoritmos.

Śledziwska e Włoch (2017) se concentrarão nos benefícios da vida em uma sociedade onde o chamado *big data* se torna prevalente.

Big data is poised to reshape the way we live, work, and think. A worldview built on the importance of causation is being challenged by a preponderance of correlations. The possession of knowledge, which once meant an understanding of the past, is coming to mean an ability to predict the future. The challenges posed by Big Data will not be easy to resolve. Big Data can change economic and social research relied on methods such as surveys, experiments, and ethnographies. (ŚLEDZIEWSKA; WŁOCH, 2017, p. 269)

Neste sentido, *big data* se refere, então, à naturalização da conduta de coleta e tratamento de dados em larga escala para tomada de decisão, seja no nível governamental, seja no nível mercadológico.

De toda sorte, Śledziwska e Włoch (2017) indicarão benefícios como a celeridade na consolidação de pesquisa, contrapondo a velocidade de tratamento das técnicas contemporâneas com os 3 anos que a Polônia teria demorado para divulgar seu senso de 2011. Indicarão ainda a transparência prometida por autores como Mayer-Schönberger (2009), mas sem entrar no mérito sobre que tipo de transparência e a qual sociedade isso nos leva. Há também a propagação de um dos argumentos mais recorrentes no campo político para a validação da pervasividade informacional.

O *big data* aumentaria a eficiência policial na manutenção da segurança pública. Reforçando a cultura do medo como validadora instantânea de práticas invasivas e cerceadoras da liberdade coletiva.

PRIVACIDADE

Esta tese busca provocar reflexões contemporâneas sobre a conduta em sociedade que, através disso, fomentar uma mudança na forma como a academia segue tratando o tema da privacidade e dos suportes comunicacionais para a prática e ressignificação do centro e entorno do tema, tendo nas redes sociais digitais um dos maiores expoentes axiomáticos para tanto, mas não estando de modo algum limitado a ela, é tarefa complexa.

Ainda que a linguagem siga um caminho acadêmico, é objetivo também buscar conectar universos paralelos nos debates para que tal conexão seja forma de provocação ainda mais profunda.

Antes de apresentar os conceitos e definições, reservou-se um espaço inicial para trazer o cenário, o contexto atual.

Este foi um desafio adicional, pois como se trata de tema altamente contemporâneo, pouco sentido faria lastrear as análises em exemplos antigos, obsoletos.

De pronto vale buscar o Contrato para a Web, cunhado por Berners-Lee (2019), ninguém menos do que o próprio inventor do que viria a ser a web atual, que com o apoio de mais de 80 instituições, redigiu nove compromissos tripartidos para que governos, empresas e cidadãos apliquem. Haverá um momento deste trabalho, inclusive, apenas para descer nestes itens dentro do aparato propositivo que permeia os debates infraestruturais das nações e do direito.

§ 3.6 The distinction between public and private has often been grasped in spatial and oppositional terms: the home versus the agora, the private company versus the public institution, the private collection vs. the public library, and so forth. The deployment of ICTs has escalated the blurring of the distinction when expressed in spatial and dualistic terms. The Internet is an important extension of the public space, even when operated and owned by private actors. The notions of fragmented publics, of third spaces, and of commons, and the increased focus on use at the expense of ownership all challenge our current understanding of the public-private distinction.

§ 3.7 Nevertheless, we consider this distinction between private and public to be more relevant than ever. Today, the private is associated with intimacy, autonomy, and shelter from the public gaze, while the public is seen as the realm of exposure, transparency and accountability. This may suggest that duty and control are on the side of the public, and freedom is on the side of the private. This view blinds us to the shortcomings of the private and to the affordances of the public, where the latter are also constituents of a good life.

§ 3.8 We believe that everybody needs both shelter from the public gaze and exposure. The public sphere should foster a range of interactions and

engagements that incorporate an empowering opacity of the self, the need for self-expression, the performance of identity, the chance to reinvent oneself, as well as the generosity of deliberate forgetfulness. (FLORIDI, 2015, p. 10-11)

Este trecho do “The Onlife Manifesto”, um texto que já no título busca trazer uma provocação transformadora a partir na produção de um manifesto que se proponha a ser *onlife*, inscrito completamente na vida, naquela vida cotidiana das tarefas comuns que se repetem culturalmente de lar em lar e que são ubíquas, não respondem a uma categoria offline e a outra online.

Entre as mais de 500 instituições signatárias já estão World Wide Web Foundation, Amazon, Google, Facebook, Microsoft, Twitter.

Para este estudo, de pronto se mostra relevante o terceiro princípio governamental proposto, que convida as instituições a “respeitar e proteger a privacidade online fundamental das pessoas e seus direitos sobre dados” (BERNERS-LEE, 2019).

Quando se vê o próprio criador buscando formas de influenciar os caminhos da internet de modo ainda muito paliativo, percebe-se o tamanho do esforço necessário, além de compreender, uma vez que a privacidade toma corpo dentro de um manifesto de importância considerável, que este tema precisa de cuidado e atenção.

Retomando, tal início precisará se dar com a definição de privacidade, epicentro, que como tal, pode provocar abalos muito distantes de sua fricção.

Privacy is a complex concept that has proved to be difficult to define. Often privacy is considered a human right integral to society's moral value system. Lack of privacy can lead to self-censorship, as individuals restrict their expressions and actions. free expression can be considered a fundamental right in a free democracy, and therefore, it can be stated that privacy is crucial for society. (POIKELA, 2019, p. 2)

A privacidade não pode ser vista de modo simplista.

Ser privativo está muito além de ser oculto ou escondido.

A função do espaço privado se relaciona tanto com a questão da intimidade quanto com a questão da segurança, na maioria dos casos óbvios, mas será possível perceber que seus desdobramentos são mais profundos do que isso.

Os problemas narrados acima decorrentes da falta de privacidade ajudam a compreender rapidamente os impactos da ausência de privacidade. Importante, a

ausência de algo que é sentido como sendo necessário, ou seja, a privacidade sendo expurgada ao mesmo tempo que o indivíduo já conviveu com ela.

Um dos pontos mais duros de Poikela (2019) é justamente a auto-censura, que em outros momentos apareceu de modo sutil neste trabalho quando se tratou, anteriormente, do terceiro observador e da internalização de um modo de conduta na sociedade que levasse em conta a vigilância e os processos estéticos necessários para ser reconhecido como ente interlocutor na omniágora.

De pronto, tal sensibilidade está justamente na questão de se saber observado, e de temer os resultados desta vigilância, seja governamental, seja corporativa, seja comunitária, principalmente por compreender que tal percepção gera no indivíduo uma conduta conformada ou reformada mesmo que o vigilante não esteja por perto, ou em busca de algo que lhe seja próprio.

Relevante com isso notar que no momento em que o indivíduo percebe-se desprovido de privacidade, ele passa a ser o seu censor, mesmo que não haja outro vigilante, na medida em que imagina estar sendo seguido, rastreado, ou que no futuro os seus atos presentes possam ser repreensíveis ou puníveis.

Já neste momento aparece rapidamente a questão da liberdade de expressão que é ponto fundamental da democracia ocidental contemporânea, que é muitas vezes desconhecida em sua integralidade, mas que no caso deste trabalho não se trata de ponto central.

Bastará, por ora, dizer que a liberdade de expressão e o direito à privacidade, muitas vezes colocados em polos opostos, não são de fato antagônicos, mas condição intrínseca de existência simbiótica. Para tanto, recomenda-se a leitura da monografia precedente a esta tese (FELÍCIO, 2015).

A liberdade de expressão só pode ser construída e exercida na medida em que haja um espaço de criação apartado da pressão sócio-política, oferecendo condições para os pequenos testes da manifestação das opiniões e das estratégias de transformação social antes mesmo de ter a completude das decisões e com o fim de construir gradativamente a própria consciência social.

De modo mais vertical, Masur (2017) vai caracterizar demoradamente a privacidade em 6 tópicos complementares.

1. Privacy is inherently subjective. When an individual needs privacy, how he or she perceives situations as involving privacy, what he or she perceives as privacy violations, and what he or she does in order to achieve, maintain, or optimize the level of privacy depends on the individual's personality, skills and knowledge, developmental stage, prior experiences, cultural background, and the situations in which the individual finds him or herself.
2. Privacy involves withdrawal from social interaction to a certain degree. The desired extent of withdrawal depends on the individual and the situation. An imbalance between desired and achieved levels of privacy fosters privacy regulation or optimization (if the necessary options for the respective behaviors are available)
3. Privacy thus constitutes a form of limited access to the self—either physically or psychologically—that is deliberately chosen and achieved by privacy regulation. Privacy can only be experienced if an individual simultaneously has the ability to abandon this privacy if he or she wishes to do so. Forced seclusion (i.e. isolation) is hence not a form of privacy.
4. Privacy is not an end itself. People temporarily try to achieve certain levels of privacy in order to satisfy more fundamental needs (e.g., autonomy, selfevaluation, protected social interaction). Individuals may also employ long-term strategies that aim at securing a future level of privacy in anticipated situations.
5. Privacy does not only refer to information about the self. Although the exact dimensionality deserves further investigation, it is important to acknowledge that privacy also refers to the physical (body, home, territories...), the social (interactions with other persons), and psychological (input control, setting constraints on external influences).
6. Finally, it is important to note that privacy regulation behaviors can meaningfully be distinguished into preventive and corrective privacy strategies. (MASUR, 2017, p. 67-68)

Já no primeiro item, o autor vai destacar o caráter peculiar da percepção da privacidade de acordo com as idiossincrasias pessoais, o que deixa mais clara a construção social, e como tal simbólica, que é a privacidade, além de indicar que o sujeito pode estar em busca de níveis distintos de privacidade a cada momento, e que para tal aplicará estratégias diferenciadas nestes casos.

Em muitos casos, diversos autores chamarão este tipo de interpretação sobre a privacidade de situacional, justamente para apresentar o caráter dinâmico da busca pela privacidade em níveis distintos que se adapta a diversos fatores de modo complexo.

De certa forma há uma relativização da privacidade na medida necessária de aportá-la na vida cotidiana e prática de cada pessoa.

No segundo item há a indicação de que a privacidade é também um fator constitutivo das relações sociais, de acordo com o controle exercido pelo indivíduo sobre quais informações podem ser compartilhadas com cada grupo de indivíduos de acordo com seu grau de intimidade e proximidade.

Neste ponto já é possível compreender de modo breve que privacidade também tem um vínculo com intimidade, e como as pessoas constroem os seus círculos de amizade e afetividade.

Destaque-se que é esta característica da privacidade que tornará ela mimética a sua parte, ou seja, é aqui que a privacidade recorrentemente será confundida com apenas a intimidade.

Seguindo os pontos do autor, sem a privacidade, a vida compulsoriamente exposta se torna comum a todos, reduzindo os artefatos comunicacionais que indicam proximidade e distinção.

Ao colocar a privacidade desejada e a privacidade atingida, localiza-se o embate contemporâneo sobre quais os contornos a lei deve dar nestes casos.

Mas não apenas a lei, mas a cibercultura de modo geral.

Cada comunidade vai aportar limites na conduta a fim de promover o espaço privado e a correta interação entre as esferas de interesse público e a vida pessoal e íntima, além da articulação privada das transformações sociais, dando destaque aqui para o fato de privado não ser sinônimo exclusivo de intimidade, sendo afirmativamente também o espaço de fermentação da transformação coletiva necessária para a manutenção do modelo democrático contemporâneo.

Em seguida, haverá a questão da experiencição da privacidade a partir do ato de escolher liberar informações privadas ou não, de acordo com o contexto.

Aqui Masur (2017) vai constituir a privacidade como um ato, não apenas como um conceito.

Isso quer dizer que a existência da privacidade se materializa no ato decisório de expor ou não suas ideias, pensamentos, corpo, entre outras instâncias.

Este ponto norteará todo o entendimento de privacidade utilizado neste trabalho.

Interessante notar que o substantivo é verbo conjugado.

Sem a deliberação, a privacidade não pode ser constituída. Logo, o ocultamento compulsório não é um ato privativo. Tudo que obrigatoriamente precisa

ser ocultado não está sob proteção da privacidade. Ao invés disso, está coagido a manter-se oculto.

Da mesma forma, tudo que é compulsoriamente revelado não é resultado da escolha sobre a redução da privacidade.

Este é um ponto nevrálgico que vai ganhar corpo ao longo deste trabalho na medida em que for discutida a e-vasão de dados e a sedução para que o escopismo panórgico seja cada vez mais prevalente como desejo orgasmático por ser exposto e ser visto, avaliado e reconhecido na esfera da dromoaptidão transestética da cibercultura.

No quarto tópico, o que se coloca à luz é a transitoriedade e contextualidade dos níveis de privacidade que cada indivíduo buscará ao longo do tempo.

Desta forma, pode-se compreender que não há um único nível de proteção da privacidade que pode responder a todas as demandas sociais, mas sim um espectro de possibilidades que dialogam com as necessidades individuais.

A privacidade não é idiopática, mas sim contextual e objetivada.

Qualquer esforço para fazê-la compulsória se torna tão violento quanto a invasão da privacidade, sendo facilmente convertido em forma específica e sutilizada de censura.

Em outras palavras, o ocultamento forçoso não pode ser praticado com a alcinha da defesa da privacidade, incorrendo em censura camuflada e violência estrutural.

Há ainda que se considerar, além de tudo, que a privacidade não está substanciada no corpo e na materialidade direta da vida, sendo restrita aos corpos ou espaços de convívio, mas também se aplica na capacidade de pensar em interferências e de formular visões de mundo distintas.

Isso significa que a privacidade tem lastros polivalentes, na conduta decisional cotidiana, sobre o corpo, a mente e as emoções.

O assédio às emoções, então, pode ser compreendido também como uma violência contra a privacidade.

A pressão para o ocultamento de sentimentos não é um ato privativo, se não a censura recém comentada e, como tal, torna-se um modo de discriminação.

Por último, Masur (2017) vai indicar a obviedade do sistema jurídico, que caracteriza as leis em torno da privacidade como preventivas e corretivas.

O teor preventivo estará declarado nas proibições e nas estruturas de auditoria e fiscalização das condutas. Mas justamente a peculiaridade deste tema exige que o Estado não seja o super-vigilante que tudo olha, a ponto de ser capaz de interromper quase que instantaneamente todo ato contra a privacidade, pois para tal, o próprio Estado precisaria estar a par de cada movimento das pessoas.

Para tanto, existirão as medidas corretivas, ou os chamados remédios jurídicos, que se converterão em penas específicas em cada caso de violação, como forma de reeducar os infratores e compensar o dano aos vitimizados.

Todas as formas expostas até agora por Masur (2017) caracterizam a privacidade de um modo amplo, mas não a tipificam propriamente.

É preciso compreender que em muitos momentos, várias formas de exercer a privacidade podem coexistir.

Assim como o autor mencionou a questão da decisão sobre o corpo e a mente, Floridi (2014) vai gerar uma classificação ainda mais funcional para o entendimento dos contornos possíveis para a privacidade, não apenas os contornos legalistas.

It is common to distinguish four kinds of privacy. They can all be formulated in terms of 'freedoms from'. Let me quickly introduce them in no particular order of importance. First, there is [someone]'s physical privacy. This is her freedom from sensory interference or intrusion, achieved thanks to a restriction on others' ability to have bodily interactions with her or invade her personal space. Second, there is [someone]'s mental privacy. This refers to her freedom from psychological interference or intrusion, achieved thanks to a restriction on others' ability to access and manipulate her mental life. Third, there is [someone]'s decisional privacy. This is her freedom from procedural interference or intrusion, achieved thanks to the exclusion of others from decisions— especially but not only those concerning education, health care, career, work, marriage, and faith—taken by her and her group of intimates. And finally, there is [someone]'s informational privacy. This is her freedom from informational interference or intrusion, achieved thanks to a restriction on facts about her that are unknown or unknowable. (FLORIDI, 2014, p. 102 - 103)

Importante descer em cada tipo de privacidade pois, muitas vezes os aspectos debatidos pela agenda pública se limitam a questões da espacialidade e temporalidade da privacidade corpórea, que no campo performático da mídia tem

parte de sua visibilidade conquistada pelos paparazzis de celebridades, invadindo à distância os espaços físicos das residências, festas, piscinas, carros de estrelas do mundo midiático.

Esta privacidade, do tipo mais basal, é há muito debatida nos grandes centros urbanos, gravitando a discussão sobre câmeras de segurança e vigilância, assim como será apresentado neste trabalho quando da discussão sobre a lei que regulamentaria as limitações sobre uso de imagens de circuitos internos de vigilância como exemplo de desserviço no campo do debate sobre privacidade.

A privacidade espacial está conectada ao corpo físico, apresentado invariavelmente no cotidiano das pessoas e capturado de modo telemétrico. Sistemas de reconhecimento facial já estão há tempos ultrapassados.

A exemplo do que é apresentado por Zahari e Zaaba (2017), novas formas de acompanhar o comportamento das pessoas no espaço físico estão sendo colocadas em prática cotidianamente.

Com o pressuposto da segurança, novamente, ligada à espacialidade, é feita uma proposta a seguir.

[...] a crime prevention tool that overcomes shoplifting in small shops by utilising the surveillance camera using security image processing techniques and the biometrics approach on suspicious human behaviours to identify potential intruders or shoplifters before the incident happens. (ZAHARI; ZAABA, 2017, p. 264)

Ou seja, não apenas os rostos estão sendo escaneados compulsoriamente nos ambientes, mas também as condutas, os corpos de modo integral, os gestos, os passos.

Em uma lógica temporal, em uma sociedade futurística onde todas estas imagens possam compor um banco de dados acessível aos grandes vigilantes, a história de uma pessoa estará narrada pelos espaços por onde transitou, com um diferencial sensível que vem a ser o contexto no momento da consulta, não no momento da execução das ações.

Assim, se uma pessoa teve algum comportamento em 2020 que se torna recriminável no ano de 2034, lá à frente o comportamento do passado poderá ser revisto, escrutinado em busca de sinais de desvios.

A perpetuidade da informação transforma o presente em um jogo de adivinhação dos movimentos econômicos e políticos, com riscos sensíveis à condição social presente e futura das pessoas.

O escrutínio da topografia, ao menos o mais basal, que busca compreender em que espaços cada indivíduo transita, já está em curso constante e aproximado do corpo.

Os aparelhos celulares mais recentes já contam com formas de monitoramento de localização construídas desde o desenho tanto do hardware quanto do software para que este dado seja compartilhado de modo compulsório em muitos momentos, sem que o usuário sequer seja notificado de tais condições de modo claro.

The difference between Bluetooth-tracking beacons and Wi-Fi tracking systems is that the modern smartphone leaves Wi-Fi on, even when manually switched off for data connectivity, as a way of pinpointing its location. It is part of the location services with GPS and cellular network triangulation, which speeds up positioning for mapping and other location-dependent services. (GIBBS, 2016)

Em diversos casos, mesmo as pessoas desligando o Wi-fi para busca de rede de dados, os aparelhos celulares estão coletando e compartilhando informações sobre geolocalização com base em metadados das redes de Wi-fi, bluetooth e outros dispositivos próximos.

Isso significa dizer que, por padrão, os aparelhos celulares já estão criando um mapa espaço-temporal da vida cotidiana de seus proprietários desde seu desenho, convertendo-se em um dispositivo de dupla função, servir ao usuário e evadir seus dados em multiníveis.

Mas aqui, apenas como caráter provocativo, questiona-se quem é o real proprietário do aparelho celular, uma vez que o comprador não é autônomo para decidir se estes aparelhos irão monitorá-lo ou não.

Assim, proprietário pode ser considerado tanto a empresa que construiu o hardware e decide como, através das atualizações, fará com que se torne obsoleto, ou mesmo as empresas produtoras dos sistemas operacionais que decidem por forçar um modelo de vigilância à revelia do comprador.

There is a trade-off in the need to know why you want to centralize this type of information and to give this level of personal data access. What are the benefits that outweigh the risks of doing it. So you could have a central control system for all your systems in your house but if these could be used for nefarious reasons. For example my smart lights could be switched remotely

on or off or the heating energy system could be overloaded as a gateway to some other system, for example, triggering the home security doors to open in a false heating or fire alert that then might enable someone to gain entry to something that might be of value to steal. It is an equation of cost, risk and value and does it really matter at the end of the day. Machine learning and algorithms are starting to be used in cyber-attacks. (SKILTON; HOVSEPIAN, 2018, p. 220)

Quando todas as casas utilizam o mesmo sistema de segurança, ou quando grande parte da mesma comunidade está a usar as mesmas plataformas de comunicação, com aplicativos instalados em seus aparelhos celulares, isso pode significar que a comunidade como um todo está e-vadindo os dados coletivos de modo constante.

Um único celular invadido pode ajudar a mapear dezenas de quilômetros com imagens, redes de wi-fi, dispositivos bluetooth e assim por diante, classificando a localização de cada um destes dispositivos.

Mas mais do que isso, um único aparelho que conceda permissão para este tipo de tarefa pode fazer o mesmo, com a diferença de que o aplicativo coletor de dados não será combatido pelas lojas, pelos usuários de modo tenaz, uma vez que terá recebido o consentimento de seu usuário.

Além destes casos, estão as empresas detentoras de aplicativos de celulares, que seguindo os exemplos acima também, por sua vez, coletam dados muitas vezes incoerentes com o propósito de seus aplicativos, a fim de comercializarem esses dados para diversos fins, sendo o mais comum deles a venda de dados para a publicidade, mas não apenas isso. Sistemas de classificação de crédito, de vigilância e tantos outros se aplicam neste caso.

Retorna-se então aos contratos de adesão com cláusulas leoninas uma vez que os Estados não se manifestam quanto à invasão da privacidade dos indivíduos.

Deixado à própria sorte para decidir se adere ou não aos contratos leoninos, o neoliberalismo informacional colocou cada cidadão para negociar com conglomerados inteiros de comunicação e tecnologia.

Em uma análise mais ácida, seria possível considerar parte dessas empresas não mais como empresas de tecnologia ou de comunicação, mas sim empresas de vigilância com produtos comunicacionais e tecnológicos de entretenimento informacional.

Destaque-se que ainda estamos a tratar da privacidade física, espacial, que gravita os corpos e sua posição no espaço-tempo.

As formas comuns de vigilância e invasão da privacidade espacial passaram então da observância das câmeras nos estabelecimentos comerciais, prédios residenciais e públicos para caminharem dentro dos bolsos e observarem cada trajeto feito.

Ainda que alguns aleguem que a troca é justa e necessária, trazendo incrementos na segurança pública e individual com base nas análises de grandes volumes de dados, ainda são desconhecidos movimentos mais robustos para tornar os dados do governo estadual e federal realmente disponíveis para o escrutínio do cidadão versado em tratamento de dados e modelagem estatística.

Isso significa que a segurança pública com base em dados ainda não é uma realidade tal qual a promessa que camufla os interesses econômicos na captura de tantos dados, com o aval do Estado.

Ousado mas possível indicar que a partir das cartas da NSA, os EUA são mais capazes de exercer uma vigilância cirúrgica sobre um cidadão brasileiro do que o próprio Brasil, tanto por uma realidade jurídica distinta quanto por fatores econômicos sobre a constituição da internet e dos protocolos globais de transferência de dados, além da infraestrutura física dos servidores, que cedo ou tarde territorializam qualquer informação em servidores ou cabos nos EUA, tornando o governo estadunidense apto a agir sobre tais dados em território próprio sem sequer violar o que hoje se entende por soberania.

Seguindo nas formas de vigilância física, a IoT já começa a ter maior penetração em certos espectros econômicos da população.

Nos ônibus municipais de São Paulo as catracas já fotografam os rostos de cada pessoas que passa seu bilhete de transporte, carros de alto padrão já estão sendo vendidos com sistemas de vigilância embarcados e oferecidos como um concierge digital, como o OnStar da Chevrolet, disponível no Brasil já há alguns anos, que promete acompanhar viagens para casos de acidente ou imprevistos, oferece indicações de lugares para jantar. A camada sedutora segue atuante.

Ainda que a empresa ofereça o OnStar como um serviço de facilitação e segurança, o que de fato pode ser executado no dia a dia, a mesma realidade que

expõe o Google às cartas da NSA deixa a Chevrolet e qualquer outra montadora vulnerável a ter que apresentar os dados de qualquer pessoa ao governo estadunidense em caso de solicitação sem que a empresa possa avisar seus clientes de que algum governo o está vigiando.

Ao avaliar o que viria a ser o segundo tipo de privacidade, referente à privacidade mental, localiza-se a percepção de que uma pessoa tem direito do livre-pensamento, mas isso vai além de uma visão rasa sobre o pensamento.

Pensar, de modo livre, em uma sociedade com tantas formas de vigilância, pode ser sentir que seus pensamentos não estão sendo conduzidos de modo sistemático a uma linha única ou a interesses específicos alheios ao sujeito.

Assim, considerando a chamada mídia programática e os algoritmos de classificação e categorização da comunicação, quando uma pessoa acessa um portal de notícias dificilmente receberá as mesmas notícias que algum de seus amigos, na mesma origem, da mesma forma.

Isso significa que mesmo o jornalismo, que apresenta o mundo de acordo com uma narrativa coletiva, está permeado de maneiras de segmentar o conteúdo com o objetivo de aumentar o consumo de notícias, e como tal, deixa de se preocupar com uma pauta social coletiva em essência e passa a entregar conteúdos mais interessantes, mesmo que eles sejam menos relevantes para a sociedade ou opinião pública.

Assim, o pensamento livre pode ser conduzido de acordo com classificações de matérias, artigos que são mais interessantes para um público similar ao de uma pessoa em questão.

Consumir notícias é ser exposto a matérias que agradaram a pessoas iguais a si, mais do que consumir um editorial que pode contrariar as preferências de um consumidor-leitor.

Cidadão passa a ser, neste caso, consumidor. Consumidor de notícias, de um plano comunicacional voltado a interesses específicos.

O desagravo não importa tanto, e quanto mais entretido, mais vale o consumidor nas redes digitais, na medida que passará mais tempo exposto à mídia,

abrindo maiores chances de impactos adicionais de publicidade no intervalo entre uma matéria e outra.

Desta forma, como dizer que um indivíduo tem liberdade de pensamento sendo que o seu entorno se condiciona à melhor forma de mantê-lo anestesiado durante o processo informacional.

Não se trata, nestes casos, de comunicação ou de diálogo, mas sim de um fluxo sedutor de entretenimento informacional que está travestido de imparcialidade, mas que em verdade busca contê-lo na postura de consumidor.

Considere-se também que ao consumir conteúdos frequentemente similares e perceber que a mídia começa a impactar e segmentar conteúdos de modo parecido, cada indivíduo pode intuir que está sob uma vigilância que no primeiro momento é amável e coerente. Quanto mais consome conteúdo, mais o conteúdo novo que lhe surge é agradável.

Ao mesmo tempo, em dado momento, cada indivíduo pode se sentir vigiado e condicionado a consumir sempre os mesmos conteúdos e pode sentir que não deva clicar em matérias diferentes para não sujar seu algoritmo dentro da egocracia contemporânea.

Intuir que o celular coleta o áudio das conversas que são mantidas ao redor é intuir também que o pensamento e a manifestação do pensamento podem estar sob vigilância.

Quando as notícias sobre o caso Cambridge Analytica se tornaram normalizadas na mídia do dia a dia, o consumidor médio de conteúdo compreende de modo leviano que sua forma de pensar pode estar sob vigilância em um nível ainda mais profundo e, como tal, também normalizar a afasia sobre o tema.

Mais do que um assunto de governos, é a possibilidade de mapear condutas e comportamentos que torna o caso Cambridge Analytica tão emblemático.

Muitas coisas estão em jogo, mas para o presente trabalho, o objeto principal que se extrai daqui é a autocensura que pode ser praticada no cotidiano a fim de evitar confrontos presentes e futuros, o que desconstrói a privacidade na medida que interfere na liberdade tanto de pensamento, em um exercício constante e intelectual,

quando nos atos decisoriais sem a interferência de padrões de comportamentos classificados através de outras pessoas ou de um interesse corporativo.

E desta forma, o campo do pensamento passa a ser permeado pelo autovigilante que foge de um ente indeterminado e difuso, capturado por uma vaga percepção de autoridade ou de conduta comum desejada.

Se antigamente se discutia a mão invisível, hoje a percepção do invisível agrega a camada de dados e de vigilância que pretende invadir o campo do pensamento e, como consequência, domesticá-lo.

Por outro lado, acreditar que o pensamento próprio pode ser previsto não necessariamente é algo sentido com repulsa pelas pessoas.

Da mesma forma que a vigilância física é utilizada pela promessa da segurança e inviolabilidade do corpo ante a morte violenta possível, a vigilância do pensamento é utilizada e transformada em promessa sedutora da praticidade, do serviço, da diminuição do atrito.

Transfere-se para os algoritmos e para as tecnologias a função de trazer a satisfação e a alegria, o conforto de modo constante.

A tristeza, a hiância primordial se torna entretida, obturada de modo muito fugaz por artefatos comunicacionais pueris que se alternam em um fluxo imagético performático.

Ter a mente escrutinizada pode significar aumentar as chances de alegrias instantâneas e o afastamento do tédio.

É neste ponto que a privacidade do pensamento toca a privacidade decisória, na medida em que o escrutínio da mente pode conduzir a uma automação das decisões cotidianas.

De modo similar, há formas de utilizar a terceirização da tomada de decisão, tornando-a desejada na medida em que o indivíduo já não precisa mais revisar seus critérios, basta ser alegrado pela tecnologia.

Um exemplo contemporâneo da sedução exercida pela terceirização da tomada de decisão para que esta ocorra através das estruturas tecnológicas citado anteriormente pode ser mencionado através do Netflix e da classificação de conteúdo que pode mais agradar a cada pessoa com um perfil específico na plataforma.

Ser visto pela infraestrutura comunicacional, e como tal, de vigilância, é permitir-se ser alegrado de modo instantâneo.

Mas a privacidade decisional está além das miudezas de plataformas de entretenimento.

Quando o aparelho celular decide religar o wi-fi, como mencionado há pouco, não apenas a vigilância física está em curso, mas a interferência sobre as escolhas de cada indivíduo está se instaurando e se normalizando.

Da mesma forma, compartilhar compulsoriamente as informações econômicas de alguém, informações médicas, provas e resultados de exames são formas de interferir na privacidade decisional de alguém.

Um dos itens que se coloca em debate é a pressão exercida pelas redes de farmácias para que uma pessoa ofereça seu CPF em troca de descontos, que na prática significa o oposto, já que ao se recusar a entregar o CPF, um cliente comum será punido economicamente e terá que pagar uma multa para ter acesso ao medicamento.

A forma sutil de dizer isso é que o CPF habilita desconto em programas de fidelidade, mas a realidade é que os clientes que prezam pela privacidade são diariamente multados. Isso interfere, de modo econômico, na liberdade decisional de modo claro.

Assim como a autovigilância e a impressão de que um governo pode estar interessado nas condutas de um indivíduo faz com que esta pessoa em questão tome atitudes distintas da que gostaria, da mesma forma suas ações são intencionadas a provocar um resultado não apenas na própria vida, em seu entorno, mas também se age com o objetivo de causar um impacto e resultado específico sobre o algoritmo de vigilância, interferindo, novamente, na decisão e na forma de agir no mundo.

Destaque-se a questão decisional como âmbito da privacidade, quando combinados Masur (2017) e Floridi (2014).

Se na definição do primeiro autor a privacidade só pode existir como ato, como decisão autônoma, no segundo autor, ainda que apareça classificada como um tipo, pode ser compreendida então como linha-mestra da privacidade a ação de decidir sobre a manifestação e a exposição dos artefatos privados.

Sem esta compreensão, muito do que se debaterá ao longo de todas as páginas pode ter seu valor reduzido.

É preciso dar atenção e mérito à percepção de que a privacidade só pode existir como ato, como decisão interessada, consciente e livre sobre si.

Ainda há também a privacidade condicional da auto-determinação informacional, pela qual cada pessoa tem meios para construir as informações que tratam sobre si em diversas camadas tecno-sociais.

É neste campo que atua o direito ao esquecimento contemporâneo (FELÍCIO, 2015), que em outros momentos deste trabalho está já foi mencionado.

Aqui, ao compreender que a identidade dos cidadãos passa ao largo do registro oficial do governo ou apenas das narrativas afetuosas dos entes queridos, compreende-se também que há muitas camadas informacionais que podem assediar um indivíduo e sua conduta no mundo.

Quando a narrativa sobre uma identidade se torna extremamente desproporcional, dando força a outras entidades para definir que tipo de conteúdo é mais relevante sobre a personalidade de alguém, pratica-se aqui um tipo de violência que condena as pessoas a uma narrativa usualmente econômica.

A exemplo do direito ao esquecimento, quando o algoritmo do Google tem mais relevância para rotular a vida de uma pessoa do que ela própria, entende-se que as formas que condicionam o interesse corporativo pode trazer um peso social adicional, e uma nova camada de preocupação para a formação da auto-narrativa social, que precisa ter em conta como que as condutas podem ser elencadas e se tornarem eternas nas mídias sociais digitais, nos sites de busca, nos indexadores de conteúdo, nos inúmeros bancos de dados.

O princípio da privacidade como fator de auto-determinação informacional é o que vai levar muitos legisladores a inserirem artigos legais relacionados à retificação de dados, principalmente os dados inferidos nos bancos de dados das entidades coletoras e manipuladores de dados.

Mas como não seria de se esperar de modo distinto, aqui há um ponto de inflexão do debate público na medida em que a auto-determinação informacional

muitas vezes é colocada em contraponto e em confronto com o que se considera interesse público e o conceito de verdade.

Até mesmo o jornalismo nos dias atuais se permite ajustar e atualizar matérias antigas, mas ainda muito se discute em que medida uma informação indexada por buscadores como o Google e o Yahoo! devam ser modificadas ao longo do tempo a fim de permitir a multiplicidade do desenvolvimento da vida humana sem o condicionamento e o determinismo histórico e documental, que em diversos casos pode ser uma barreira e um peso limitante.

No direito, mais adiante, se perceberá que estes fatores se chocam em muitos momentos e será, então, necessário sopesar os valores em questão. Se é preferível a uma sociedade ter a visão completa de seu passado, através da qual condicionará as condutas presentes, ou aplicar energia em compreender o presente e aumentar as possibilidades plásticas do seu próprio futuro.

O passado, em conformidade com a privacidade autodeterminante, não está dado como fator presente, mas como forma de compreender uma jornada, uma trajetória, mas que pode ser reescrita não com o objetivo de se apagar uma realidade documental, mas sim dando mais valor ao que se pode construir a partir da reforma da realidade humana específica.

É claro que o que se entende neste ponto não é a completa exclusão dos registros, mas sim a possibilidade de retificá-los de modo a permitir a mobilidade social necessária para que cada pessoa desenvolva seu maior potencial para si e para a coletividade.

Personal privacy is important, and risks of 'scape-goating' are real. But a denial of transparency can result in responsibility for organisational failure being attributed to those at the operational 'front line'. Binary divisions between transparency and secrecy, as with public and private, are too simplistic. (SHEAFF, 2019, p. 133)

Se esta visão simplista e reducionista já não faz sentido quando apresentada de modo dual entre transparência e segredo, ou entre público e privado, mais ainda se percebe a incompletude deste tipo de classificação quando se empilha os quatro tipos de privacidade e se busca encaixá-los em uma vida comum.

The problem, however, is that utilitarian balancing between individual rights and the common good rarely favors individual rights—unless the interest advanced on the side of the common good is trivial. Society will generally

win when its interests are balanced against those of the individual. (SOLOVE, 2011, p. 49)

Sobrepostas as privacidades, a lembrar, física, mental, decisional e autoinfodeterminante, estruturam um caminho para compreender diversas formas de agir no mundo e, também, em seu oposto, diversas formas de praticar violências contra cada indivíduo.

Na mesma medida, também se compreende as formas de sedução que convencem cada indivíduo a ceder sua força em prol das formas de vigilância, travestidas, pela ordem, de segurança, conforto, praticidade e veracidade.

Espera-se até este ponto que já esteja mais claro que nenhum dos extremos é realidade aplicável, se não um tipo de conduta média weberiana.

Nem é factível uma vida onde todas as privacidades estejam postas de modo rígido e intocável.

E na queda de braços apresentada inicialmente por Solove (2011), os direitos individuais, quando colocados em confronto com o discurso coletivista, reduz as proteções dos indivíduos e expõe a sociedade a uma dicotomia pouco vantajosa para o futuro democrático e muito vantajosa para o presente econômico.

[...] privacy is not merely a set of restraints on society's rules and norms. Instead, privacy constitutes a society's attempt to promote civility.⁹ Society protects privacy as a means of enforcing order in the community. Privacy isn't the trumpeting of the individual against society's interests but the protection of the individual based on society's own norms and values. (SOLOVE, 2011, p. 50)

Com base no autor, é possível intuir que a privacidade não se trata de um conjunto de direitos individuais que formam um direito social, mas o oposto, em certa medida, como sendo uma necessidade social e coletiva que se cristaliza em direitos individualizados.

Importante destacar novamente, direito individualizado em sua aplicação, mas não individual em seu valor. Esta diferença reforça a distinção entre a ideia acima e os argumentos coletivistas.

Ao compreender os diversos tipos de privacidade apresentados por Floridi (2014), e ao descer nos exemplos práticos de sua aplicação, compreende-se também que o aspecto infotécnico é parte do axioma sobre privacidade e conduta social.

It is hence not just the technology that affects how privacy is perceived, defined, or affected; the ways in which people use these new media and the

social practices that shape the design of these technologies also influence how privacy is perceived or conceptualized. More often than not, it is the corresponding socio-technical dynamics that cause new tensions and threats to individuals' privacy. (MASUR, 2017, p. 13)

Masur (2017) vai destacar a necessidade de compreender este debate de modo integrado às tensões técnicas e infraestruturais da comunicação contemporânea.

Em alguns momentos o autor chegará a comentar a crise da intimidade gerada e fortalecida pelo modo como as pessoas estão utilizando as redes sociais e como seguem expondo seus corpos.

Note-se que a crise comentada foi referenciada como crise da intimidade, trazendo um espectro ainda maior sobre a privacidade no que toca o campo emocional, e não restritivo à uma visão localizacionista ou intimista da privacidade.

Não que as tipificações de Floridi (2014) já não toquem a questão emocional, ainda mais quando se leva em conta a concepção de Damasio (1994) sobre como nosso corpo pensa junto com a mente, e não apenas a obedece, conseguimos compreender que a privacidade física e de pensamento estão conectadas em um corpo sensorial.

Expor a intimidade é uma das formas de romper com o conceito e conduta anteriores sobre privacidade e sedimentar paulatinamente uma nova forma de agir no mundo que tem sua narrativa muitas vezes sustentada nos acontecimentos oportunizados na vida cotidiana, espetacularizada para os fins comunicacionais, e que, em certa medida, perceberemos ser também fins vigilantes, censores também.

Urban environments fostered a type of privacy based on anonymity. Anonymity may be understood as the unavailability of personal information, due to the difficulty of collecting or correlating different bits of information about someone. (FLORIDI, 2014, p. 105)

Esta questão abrirá caminho para a compreensão do impacto das tecnologias vestíveis sobre a privacidade, assim como também a hiper-vigilância nas cidades através da IoT.

Na medida que o campo da intimidade, note que não se disse campo da privacidade, se torna matéria-prima para os processos transestéticos contemporâneos para a conquista do infopoder, que será melhor explicado adiante, o que se constitui aí não é um nível de exposição da privacidade, mas o colapso da privacidade como estrutura.

Isso ocorre através da sedução para a e-vasão da intimidade de modo compulsório e frequente de forma pouco reflexiva, com actantes desconhecidos, pelo escopismo panórgico.

Floridi (2014), porém, apresenta um resumo dos veios que fervem em análises e questionamentos sobre privacidade e seu impacto.

Em dado momento trará apenas à baila os reducionistas que atuam nas consequências do vazamento de informações pessoais, por exemplo, e aqueles que interpretam as informações como parte de uma propriedade e ser protegida, como podemos ver abaixo.

Two theories about the value of our privacy are particularly popular: the reductionist interpretation and the ownership-based interpretation. The reductionist interpretation argues that the value of privacy rests on a variety of undesirable consequences that may be caused by its breach, either personally, such as distress, or socially, such as unfairness. Privacy is a utility, also in the sense of providing an essential condition of possibility of good human interactions, by preserving human dignity or by guaranteeing political checks and balances, for example. The ownership-based interpretation argues that informational privacy needs to be respected because of each person's rights to bodily security and property, where 'property of x' is classically understood as the right to exclusive use of x. A person is said to own his or her information (information about him- or herself)—recall Virginia Woolf's 'infinitely the dearest of our possessions'—and therefore to be entitled to control its whole life cycle, from generation to erasure through usage. (FLORIDI, 2014, p. 116)

A medida da limitação do quadro apresentado permite que Floridi aponte falhas aos dois polos, mas faltou-lhe uma busca mais vasta que lhe proporcionasse uma matriz menos dual e mais integral na medida que de um lado coloca os benefícios e malefícios da prática da privacidade, e do outro da prática da privacidade como um bem sobre as informações e sobre o *self*.

O que se destaca neste caso é que o segundo grupo apresentado pelo autor tem um apelo claramente comercial e trata o dado como mercadoria, como posse não como ato, decisão, conduta.

Ainda que haja um valor comercial para a privacidade, motivo pelo qual há tanta dificuldade em estabelecer limites frente a tanto interesse mercadológico e pressão de sedução para a entrega de dados, é de se estranhar que de pronto a defesa do valor da privacidade esteja tão fortemente recalcada no direito patrimonial.

Por argumentos como estes, que focam no texto ao invés do valor a ser protegido, que a privacidade em muitos momentos será posta em contraponto com a

liberdade de expressão e ao direito à informação de interesse público, como se o exercício da privacidade fosse uma forma material de bloqueio de ambos, na medida em que a privacidade vai limitar jornais e revistas de falarem abertamente sobre o foro privado de figuras públicas, reduzindo o material disponível ao escrutínio dos jornalistas e curiosos (FELÍCIO, 2015).

Em um exemplo mais prático, a privacidade vai ser colocada na mesma seara que publicidade, descendo o nível do debate de princípios constitutivos da democracia para ser barganhada por comodidade e conforto.

Contudo, mesmo parecendo trivial, a publicidade tem em si o potencial de oferecer tanto a sedução como a violência do processo democrático.

A privacidade decisional, por exemplo, pode ter no caso Cambridge Analytica um dos seus principais ofensores quando o assunto é eleições ou a base da democracia.

Beyond the potential power of micro-targeted advertising, there is another level of concern about Cambridge Analytica related to privacy. But again, the problem is less the breach that allowed Facebook's data to be accessed by a third party like Cambridge Analytica, than how anyone was allowed to gather so much data in the first place. (BALDWIN, 2018, p. 248)

E é este dado, consolidado e estruturado, que pode vir a ser base para as violências e ressignificações em torno do campo da privacidade.

Se um indivíduo não consegue, de modo prático e claro, compreender que está sendo alvo de uma campanha de conteúdo que busca aumentar sua exposição de forma desequilibrada a uma única visão de mundo, como poderá exercer livremente a escolha sobre seus dados e sua privacidade, seja ela decisional, seja ela sobre a sua autodeterminação informacional?

E de um modo geral, o impacto dos algoritmos na privacidade se dá não apenas em casos explícitos como o da Cambridge Analytica, mas também com a verticalização dos resultados de buscadores de acordo com um *egocasting*, ou seja, com resultados tão segmentados e relevantes para cada indivíduo que acaba por reduzir a serendipidade, reforçando cresças estabelecidas e diminuindo a exposição aleatória a pontos de vista divergentes.

O mesmo se dá quando a Netflix não oculta resultados, mas cria um ranking por probabilidade de relevância e, como poucas plataformas o fazem, mostra este

índice para o seu usuário, sutilizando a interferência, mas ao menos dando certa visibilidade ao indivíduo.

O mesmo não acontece com as redes sociais digitais no momento de tornar claro quais critérios fazem com que pessoas específicas apareçam muito mais na linha do tempo de alguém do que muitos outros.

Os critérios mais lógicos poderiam ser interações, tempo despendido olhando fotos e textos daquelas pessoas, mas os itens menos óbvios podem conter as listas de similaridade que impactam na espontaneidade da vida em sociedade.

Chamados de *Look-alike Clusters*, estes grupos de similaridade fazem com que uma pessoa “A” veja mais conteúdos específicos sobre um amigo “B” do que sobre outras pessoas pois seu comportamento online pode aparentar similaridade com o comportamento de algum outro ente “C” na rede, e é justamente este ente “C” que gosta muito e acompanha fervorosamente todas as postagens do indivíduo “B”.

Ou seja, o gosto de alguém que age como nosso personagem em questão é que pode ajudar a definir o que ele verá.

Isso significa que parte do que alguém verá nas redes sociais digitais não está plenamente condicionado à linha do tempo, sequer ao acaso ou às pessoas adicionadas como amigos na rede social digital, mas sim ao tipo de resposta que outras pessoas estão dando às publicações dos entes constitutivos da rede.

Assim, a privacidade está posta, no campo decisional, sob os cuidados de algoritmos cuja finalidade mercadológica última é gerar lucro através do entretenimento informacional.

How do surveillance and privacy relate? In popular and academic dialogue surveillance is oft en wrongly seen to be only the opposite of privacy— the former is seen as bad and the latter good. [...] Surveillance is not necessarily the dark side of the social dimension of privacy. Surveillance implies an agent who accesses personal data (whether through discovery tools, rules, or physical and logistical settings). Privacy, in contrast, involves a subject who can restrict access to personal data through related means. (MARX, 2016, p. 23)

O antagonismo, comum em uma análise rápida, acaba gerando uma visão apenas de negação do oposto. Neste caso, tanto a vigilância não é colocada como diametralmente oposta à privacidade, ainda mais se considerarmos que apesar de pervasiva, até mesmo a vigilância nos dias atuais tem seus limites, o que ainda abre brechas para o secreto, que por sua vez não é o resumo da privacidade, quanto não

são opostos os conceitos de direito ao esquecimento (FELÍCIO, 2015) e de privacidade (NISSENBAUM, 2009).

Há espaços que podem ser vigiados para propósitos restritos, com garantias e proteções, e ainda assim não inviabilizar a constituição do campo privativo, mas para tanto as garantias precisam ser estabelecidas não apenas no nível dos remédios jurídicos, mas nas ações ativas de fiscalização para a manutenção do direito à privacidade social, em detrimento da atual defesa mais robusta à privacidade comercial.

Desta forma, a restrição de acesso a informações, como uma ação pensada e decidida, forma os contornos da privacidade.

A vigilância entra em questão como exercício constante de acesso a dados em busca de um padrão de comportamento específico.

No caso Estatal, a vigilância serve para observar condutas subversivas ao sistema, desvios da ordem pública e afins.

Já para as empresas, há um aspecto econômico vinculado à produtividade e proteção das propriedades intelectuais desenvolvidas através do financiamento corporativo.

Ainda que o argumento da segurança pública se torne prevalente, é preciso que certos limites sejam respeitados pelo bem da operacionalidade da democracia nos patamares contemporâneos, e tendo em vista sua própria evolução com base nos pesos e contrapesos institucionais para a constituição e manutenção da privacidade como ato.

Para tanto, a invasão da privacidade, seja através do Estado, seja através das organizações, carece de maior observância e, certamente, de limites claramente determinados.

[...] personal information is protected when, what is at issue is not wrongdoing, or corruption, but mistake, misunderstanding, inattention to detail, or the like. Seen as potentially damaging to reputation and thus an unjustified intrusion into privacy, such information gains protection. (SHEAFF, 2019, p. 122)

A proteção da privacidade é parte da existência democrática pela razoabilidade da conduta dos indivíduos de modo afastado dos olhares vigilantes para criticar a própria sociedade e democracia a fim de torná-la ainda mais elaborada e favorável aos propósitos a ela designados.

Importante destacar novamente que o direito à privacidade não é, em si, um direito individualista, mas sim uma forma de, coletivamente, garantir que cada indivíduo possa manter um espaço de articulação de si e para as pessoas de seu interesse onde se torna possível articular também testes de conduta e pensamento que não estão necessariamente estabelecidos como normativos na sociedade antes de apresentá-los de modo público.

Sem deixar espaço para a leviandade, é claro que haverá o contra-argumento paranoico da segurança e da vigilância que indicará que no espaço privado, oculto, é que se dão os desvios de conduta, de caráter e o crime.

Tal forma de caracterizar a privacidade responde à conquista da pauta pública através da pauta governamental. Em outras palavras, ensinado a temer, o cidadão médio pedirá a vigilância como forma de minimizar seus riscos da morte violenta, mas entregará de si a possibilidade de construção de uma identidade mais próxima ao seu eu e parte do que lhe conferiria a estrutura para transformar a própria sociedade ao longo do tempo.

Commentators often attempt to refute the nothing-to-hide argument by pointing to things people want to hide. But the problem with the nothing-to-hide argument is the underlying assumption that privacy is about hiding bad things. By accepting this assumption we concede far too much ground and invite an unproductive discussion of information people would likely want to hide. (SOLOVE, 2011, p. 26-27)

Este discurso vinculado ao poder que ensinou os benefícios da vigilância do Estado em troca da segurança está na base do discurso potencializado pelos interesses do capital que, cooptado pelo mercado, se transforma na oferta de benefícios sutis em troca da privacidade revelada.

A evasão dos dados em uma sociedade *onlife* (FLORIDI, 2014) se torna ainda mais arriscada do que nas sociedades anteriores.

Currently, when privacy is balanced against security, the scale is rigged so that security will win out nearly every time. When we are balancing rights and liberties against government interests, it is imperative that the balancing be done appropriately. Security and privacy often clash, but there need not be a zero-sum tradeoff. There is a way to reconcile privacy and security: by placing security programs under oversight, limiting future uses of personal data, and ensuring that the programs are carried out in a balanced and controlled manner. (SOLOVE, 2011, p. 207)

Esta é uma das formas pela qual a privacidade vem sendo traduzida e levada ao campo belicoso da comparação entre privacidade e segurança ao invés de ser

desenvolvido um trabalho coletivo, social de definição dos limites do interesse público sobre a vida privada.

Of course, normative expectations of privacy and publicity do not Always correspond to how the adjectives public and private are applied to empirical facts. Th us, the cell phone conversations of politicians and celebrities that have privacy protections may become public. Information subjected to publicity requirements, such as government and corporate reports and disclosure statements, may be withheld, destroyed, or falsifi ed. Information not entitled to privacy protections, such as child or spouse abuse, may be unknown because of the inaccessibility of the home to broader visibility. Th e distinction here calls for empirical analysis of the variation in the fit between the rules about information and what actually happens to it. (MARX, 2016, p. 24)

Assim, os termos privado e público não resumem a base do que é privativo.

Esta análise precisa ser feita de acordo com o interesse público protegido nas democracias, e o interesse privado, que neste caso também é o próprio interesse coletivo.

De certa forma, aqui já começará a aparecer um dos principais problemas que contamina e corrói o debate sobre privacidade, mas que serve ao infopoder, como poderá ser visto mais a diante.

Tal forma é a desinformação, propositadamente aplicada ao tema, oferecida de modo sistêmico pelo mercado, governo e muitas vezes mal identificada pelos meios de comunicação.

Alarmista no tom, a afirmação acima se consolida na medida que se percebe que o interesse de elucidar a dimensão da privacidade não está posto com energia sob qualquer dos entes citados.

Caso estivesse, certamente a agenda pública apresentaria iniciativas mais robustas para alavancar o debate e conscientização sobre o tema.

Ao falar em interesse público e interesse privado, toca-se no campo das opiniões sobre o que é interessante, não sobre o que é interesse.

Em outras palavras, a vida privada de uma celebridade pode ser interessante, no campo do entretenimento, mas não é de interesse público quando tomado pelo conceito e impacto do que entendemos por Esfera Pública (HABERMAS, 1999).

Apesar de não entrar no detalhe, neste trabalho, sobre o conceito habermasiano, é relevante que se tenha em mente que estar em público não é, por si só, ser de interesse público.

Nesta medida, estar escondido não significa ser privado.

O enxerto acima traz no texto de Marx (2016) um caso simples que já indica a inversão, ou seja, algo de interesse público mas que é mantido em sigilo. Um caso clássico. Fatos da gestão pública que são mantidos em sigilo por tratar de desvios de conduta ou de dinheiro e que são, por excelência, de profundo interesse público.

Com estes dois exemplos postos lado a lado, ou seja, a corrupção do sistema político podendo e devendo ser apresentada ao público para as providências necessárias, e a vida privada das celebridades que, apesar de serem invadidas constantemente e tal ato ter sido normalizado pela mídia e pela sociedade, ainda carece de proteção e remédios de modo mais ativo, ambos dão uma das dimensões sobre a desinformação corrosiva ao redor do tema.

Na medida em que os meios de comunicação seguem oferecendo espaço para as investidas contra a privacidade das celebridades, age de modo constante para normalizar a mesma conduta em outras esferas, ainda mais quando isso se dá em meios de comunicação de massa, que trazem a percepção de condutas culturalmente validadas.

Do ponto de vista econômico, tal invasão gera receita para as emissoras de televisão e rádio, revistas, sites, youtubers e afins. E ao ir para o outro lado da mesa, da perspectiva de quem teve sua privacidade invadida, muitas vezes o remédio jurídico se limita também a fatores econômicos. Em outras palavras, a privacidade está dirimida em acordos e contrapesos financeiros, mas não oferece garantias ou maior auditoria sobre os vários aspectos da privacidade, principalmente a privacidade decisional.

Os impactos sociais da invasão da privacidade e sua exposição indevida não está, no campo prático, sendo protegida ativamente, e sim, reativamente.

Quando, no direito, a invasão da privacidade está sendo tutelada apenas pela pessoa que requer reparação, mas não é acompanhada pela promotoria pública, por si só tal ato já traz uma percepção de que o campo da privacidade não é visto no direito como algo de interesse público pela sua manutenção, mas como especificismos particulares.

Caso a justiça entendesse o direito à privacidade como um bem tal para a constituição da vida em sociedade e do fazer democrático, parte de sua tutela deveria

ser transferida para a promotoria pública, principalmente quando o invasor se utiliza de recursos públicos (dos poderes constitutivos da república, a lembrar o executivo, legislativo e judiciário) para realizar tal ato.

Desta forma, ignorar que há distinções entre o direito na proteção da sociedade e dos indivíduos e a legislação que protege as empresas é algo mimético à ignorância sobre a distinção entre o que deve ser protegido.

By convention, the term secrecy often refers to organizational data, while privacy refers to the data of individuals. Since organizations do not generally have “rights” in the same sense that individuals do, secrecy is a better term here than privacy. This may involve legitimate organizational secrets, as with patent details and strategic plans, or illegitimate organizational secrets, as with false reporting and cover-ups. The rules around organizational information, as with those around personal information, vary from mandatory disclosures to closures with a large discretionary middle area. (MARX, 2016, p. 27)

O autor ainda indica o termo sigilo como mais apropriado para dirimir questões relacionadas a empresas, deixando claro que privacidade não é algo referente ao direito de manter algo afastado do escrutínio dentro do campo economicamente privado, mas sim a privacidade como conceito e direito emanado e derivado da conduta humana em sociedade e que precisa, para tal, do lastro particularmente humano para existir.

Assim, direito à privacidade só se torna uma realidade possível na medida que está aplicado e refletido em uma população de indivíduos.

Espelhar tais direitos às organizações pode ser parte do mesmo viés que, de modo inverso, aplica aspectos econômicos dos remédios jurídicos para as violências praticadas contra a privacidade, ou seja, contra um ou mais indivíduos.

Concerne trazer ao foco que a estrutura comunicacional, de modo muito similar ao que anuncia Bruno (2013), suavizada pelos interesses e fluxos mercadológicos, preparou e treinou as estruturas de vigilância através do financiamento publicitário para a e-vasão.

Silenciosamente, os algoritmos de controle social seguem sendo desenvolvidos com o pretexto de oferecer uma experiência de consumo de informação na internet mais prazerosa e precisa.

Individualized (targeted or segmented) marketing communication often occurs as a result of some form of surveillance. Calls to an 800 number, visits to a web page, or consumption behavior can lead to spam or targeted solicitations via telephone and mail. Law enforcement also uses mass communications

such as advertisements and mailed solicitations to identify potential off enders (those who respond), who may then become subjects of stings and other forms of surveillance. Contemporary television and webcam transmissions also combine or blur the line between surveillance and communication. (MARX, 2016, p. 32)

Vê-se que um dos pontos sobre a vigilância e quebra da privacidade é justamente que ela se dá através de estratégias diversificadas.

O ponto de Bruno (2013) que residia fortemente, mas não de modo exclusivo, nos dispositivos de comunicação como câmeras e celulares, agora ganha escalabilidade e diversidade na medida que esta vigilância cresce através do avanço do *hardware*, e se aproveita do potencial de coleta de dados dos *hardwares* para, através da capacidade de processamento dos dispositivos e da própria nuvem, assumir aspectos múltiplos de tratamento de dados de modo acelerado.

Cada dispositivo de comunicação pode conter em si centenas de protocolos de tratamento de dados que podem interferir na privacidade do usuário de modo muito variado a fim de atender a interesses múltiplos de inúmeras empresas.

Então, para tocar a privacidade como um conceito, de praxe já se esbarra em sua alegada e incorreta antagonista, a insegurança.

Privacy is often misunderstood and undervalued when balanced against security. It is possible to have potent security measures and to protect privacy too, since protecting privacy doesn't entail scrapping security measures but demands only that they be subjected to oversight and regulation. (SOLOVE, 2011, p. 14)

Segurança e insegurança são conceitos que muitas vezes aparecem de modo mal aplicado e que, com isso, geram desinformação sobre a aplicabilidade da privacidade nos dias atuais sem que a individualidade de uma pessoa possa causar medo e ameaça à vida de diversas outras pessoas ao seu redor.

Da mesma forma, a desinformação faz com que alguns possam pensar que a privacidade esteja sempre ou majoritariamente vinculada a atos ilícitos ou que mereçam, por algum motivo escuso, estarem afastados da vista social.

Manifestações como esta servem mais ao sistema que busca invadir as intimidades e fazê-las ao longo do tempo serem constantemente e-vadidas do que necessariamente à segurança que declara buscar, uma vez que quanto mais as pessoas acreditam que o campo do privado, do íntimo alheio, do pensamento e da articulação comum à democracia possa estar ocultando seus próprios medos, cada indivíduo temerário se torna reforçador da vigilância panescópica.

Este escopismo temerário disseminado e encorajado alimenta a orquestração sistêmica dos olhares em sociedade e tutora os cidadãos médios a se tornarem replicadores censitários, sem antes apresentar claramente qual o papel que a privacidade desempenha no sistema de pesos e contrapesos da democracia contemporânea.

Importante dizer que as observações, alguns dirão até a bisbilhotice, já existiam em modelos sociais anteriores aos dias atuais.

Da mesma forma, em cidades menores, muitos vizinhos conheciam os horários e o cotidiano de diversas famílias, o gerente do banco conhecia os hábitos de consumo de diversas pessoas da cidade. Isso é um fato.

Entretanto, o que muda nos dias atuais é tanto a pervasividade de tal escopismo, a multiplicidade dos actantes que são coletores, a memória dos sistemas que conserva estas informações por muito tempo e o grau de aceleração como tais formas de captura das informações cotidianas seguem infringindo às pessoas uma exigência de aptidão para dar conta tanto das transformações técnicas quanto do agir social, coletivo, relacional, além do potencial que tal vigilância tem de sutilar as violências e pressões e conduzir um processo decisional enviesado a partir da limitação sistêmica da visão de mundo.

O termo privacidade vem muito à baila quando algo vexatório ocorre, trazendo a impressão de que apenas aquilo que é vergonhoso precisa estar no campo oculto, na zona intermediária onde a sociedade está presente mas não vigia e o indivíduo pode construir transformações leves ou profundas em si e arquitetar a transformação do meio onde vive.

Exemplo disso é considerar o corpo nu como algo que deva ser protegido pelo direito à privacidade. Ao mesmo tempo, artistas expõe o corpo muitas vezes como forma de chamar à atenção as violências cotidianamente praticadas.

O nu tem seu espaço de realização, nos banheiros, nos quartos, mas também está expulso de outros espaços como a praça pública, com o pretexto do privado, mas aplicado compulsoriamente e legalmente, como um ato de censura do viver o próprio corpo.

Desta forma, por privado claramente não se quer dizer aquilo que não deva ser exposto, tanto num sentido legal quanto no sentido moral de uma dada sociedade.

Os motivos pelos quais a sociedade expulsa o nu são divergentes dos motivos pelos quais a sociedade protege ao mesmo tempo que invade a privacidade.

Aspectos pulsionais da libido não são o epicentro nem características básicas da privacidade social.

A questão dos afetos, das permissões e dos limites são parte da constituição da privacidade nos dias atuais, mas ao mesmo tempo estão sendo ressignificados constantemente pelos atos compulsórios de e-vasão.

Sem o processo decisional, que cria valor para cada dado compartilhado, a privacidade se torna campo esvaziado.

The disclosure and dissemination of personal information about individuals within a community has traditionally been regulated by a nuanced system of social norms. Social norms regulate prying and gossip and also the "inappropriate" disclosure of certain kinds of personal information in certain contexts. (STRANDBURG, 2006, p. 32)

Desta forma, avaliar o impacto da evasão ou invasão da privacidade não pode ser algo estudado de modo isolado das formas de interação sociais e de suas nuances mais sutis.

Em termos mais diretos, não é possível determinar de modo único os resultados de tal invasão e evasão.

Cada realidade objetiva sofrerá os impactos de tal exposição de modo distinto, demandando muita energia no espectro social, de todos os actantes, para compreender a melhor forma de lidar e responder a tal disseminação de dados ou da intimidade de certo indivíduo.

Tais nuances servem para compreender que os casos objetivos não são, em si, base direta para a normalização dos atos. Ou seja, ainda que haja convivência de algumas pessoas para a e-vasão de seus dados, intimidade e liberdade decisional, isso não significa que o aparato legal se afaste deste âmbito ou apenas o abandone à sorte de visões restritas ou antigas sobre o tema.

Now, US and EU negotiators are not the only important actors. They face pushback from different actors - NGOs, privacy advocates, and data privacy authorities - with different goals and different access to the international arena. European privacy activists not only have no direct access to transatlantic negotiations but are primarily organized at the national level. (FARRELL; NEWMAN, 2019, p. 158)

Não se trata exclusivamente de colocar este debate nas mãos ou nos ombros de algumas entidades.

Ao invés disso, é preciso incrementar o nível dos debates sobre a e-vasão da intimidade de modo que a sociedade possa amplamente compreender e agir sobre seu próprio código de conduta.

Agindo assim, o texto jurídico irá refletir o que emana das necessidades e interesses do povo não como um reflexo distante interpretado por algum legislador, mas sim por um texto que seja costurado a custas de muito debate, pensamento aprofundado e contrapontos.

Mais adiante serão apresentados os conceitos de e-vasão de modo mais claro, e as estruturas jurídicas que ajudam a compreender o contexto no qual a sociedade está imersa, através da dromocracia cibercultural transestética.

Mas para tanto, é de suma importância ter em vista as definições de privacidade como parte constitutiva não apenas do indivíduo, de sua percepção de si, mas também da relação social que estabelece com os outros e com a sociedade de modo geral.

Sem o espaço de tomada de decisão e testes sociais que a privacidade acarreta, o espaço democrático se esvazia gradativamente, tornando-se um espaço ditatorial com aparência democrática.

Sem a privacidade, a democracia deixa de ser uma emanção da vontade articulada do povo e passa a ser um simulacro, uma representação em segunda instância, um símbolo que representa apenas a si próprio como ideia consolidada, mas sem grandes lastros na vida comum.

A provocação, que infraestrutura a democracia através da privacidade e da sua polivalência, está posta aqui também como aspecto constitutivo basal da comunicação.

Sem o espaço de construção que não esteja vigiado e pressionado pela vigilância do Estado ou das instituições e pelo julgamento dos pares a comunicação não pode germinar.

De certa forma, a transparência extrema é um processo de aniquilamento da comunicação na medida que se torna um ato estéril, troca de dados e informações, ao invés de construção dialógica sócio-política intencionada e direcionada de acordo com as necessidades de cada indivíduo.

Para que a comunicação se estabeleça, o ato decisional de eleger quais informações serão trocadas e como este processo se dará é de extrema relevância, assim como é este o pressuposto básico da privacidade.

Entende-se aqui, então, a distinção da transparência, imperativa para as coisas públicas (república), para as coisas do povo, para os governos e instituições, e a privacidade para o campo dos indivíduos e da sociedade.

Ocorre que nos patamares do infopoder como está sendo praticado nos dias atuais aparenta-se uma inversão na qual a vida comum está a ser escrutinizada pela tecnologia enquanto o governo segue auto-protegido e as instituições seguem seguras pelas leis de contrato e patentes que impedem sua exposição à auditoria popular.

É como se as empresas e os governos tivessem constituído espaços de articulação que impactam os interesses públicos e a vida das comunidades enquanto se tornaram permissivos e muitas vezes agiram favoravelmente à criação de um comércio baseado na invasão, evasão e e-vasão dos dados de populações inteiras sem pudor.

Fruto de um mercado sedutor, a privacidade propalada não passa de uma escolha pífia entre aceitar contratos de adesão de redes sociais digitais ou ser expulso de uma parte relevante da ágora contemporânea.

Desta forma, questiona-se e provoca-se, como deve ser o papel de toda tese, mais um enfrentamento do *status quo*. Coloca-se à mesa a pergunta se os espaços de comunicação e socialização da internet, assim como as emissoras de rádio e de televisão, não deveriam ser uma concessão, na medida em que são constitutivas da sociedade?

Mas mais do que uma concessão de um Estado, quem deveria tutelar esta concessão sendo que não há instância que consiga reunir a humanidade?

Esta quase-privacidade mencionada acima está sendo trocada por descontos em balcões de farmácias e em caixas de supermercado.

Os chamados programas de fidelidade permitem, nos dias de hoje, um trocadilho de muito mal gosto que questiona a quem tais programas são fieis, na medida em que cada consumidor que oferece seus dados a estes programas de

milhagens acaba por oferecer ainda mais dados para um sistema mercadológico infotécnico que condicionará parte de seu consumo no presente-futuro.

Por outro lado, é relevante avaliar visões tão ufanistas como a de Schwab (2016) trazem o lado belo da promessa tecnológica, mas trabalham pouco com os impactos reais na sociedade. A conexão técnica não significa conexão humana, constituição de comunidade.

Não há aqui uma busca da negação dos benefícios da tecnologia, mas sim uma visão mais clara dos entregáveis sociais.

Há contribuições humanas na conectividade de povos que antes mal se conheciam, tanto quanto na disponibilidade de informação a partir de pesquisas em linguagem familiar à própria cultura a partir do refinamento do algoritmo dos buscadores na internet, mas a informação também não é suficiente para abrir as portas da transformação social e econômica de modo coletivo.

New forms of digital media, which form a core component of the fourth industrial revolution, are increasingly driving our individual and collective framing of society and community. Digital media is connecting people one-to-one and one-to-many in entirely new ways, enabling users to maintain friendships across time and distance, creating new interest groups and enabling those who are socially or physically isolated to connect with likeminded people. The high availability, low costs and geographically neutral aspects of digital media also enable greater interaction across social, economic, cultural, political, religious and ideological boundaries. (SCHWAB, 2016, p. 88 – 89)

Os benefícios estão apresentados ao longo da obra sem que houvesse ocorrido de modo equivalente o sopeso dos riscos e atuais dilemas vividos com a ubiquidade e pervasividade das redes de comunicação e, como tal, de vigilância.

Tal conceito se encontra mais substancialmente definido na obra de Bruno (2013) que busca compreender não apenas as estruturas objetivas, mas também subjetivas da simbiose contemporânea das plataformas e dispositivos comunicacionais e as plataformas e dispositivos de vigilância.

Quanto à vigilância contemporânea, a sua função estratégica se exerce em três principais circuitos, que buscam legitimar suas práticas: os circuitos de segurança e controle; os circuitos de visibilidade midiática; os circuitos de eficácia informacional. Tais circuitos, que serão descritos adiante, alimentam-se reciprocamente, conferindo à vigilância um caráter multifacetado, com registros de legitimação superpostos e com uma significação social e subjetiva plural, que reúne segurança, cuidado, temor, suspeição, prazer, entretenimento, pertencimento, conforto, performatividade, entre outros. (BRUNO, 2013, p. 21)

Quando segurança, cuidado e temor dividem o mesmo parágrafo que prazer, entretenimento, pertencimento e conforto, vemos que apesar de usualmente restarem classificados como antagônicos no sentimento do homúnculo, na sociedade atual eles são faces da mesma estrutura. Comunicação e vigilância se imiscuem tanto quanto prazer e segurança.

O processo contemporâneo de vigilância passa por uma camada de interiorização de tecnologias e técnicas de evasão da privacidade, através da valorização aprofundada da exposição e composição imagética de um sujeito transformado em mídia, como a dialogia do ator-rede (LATOUR, 1993), mas que para esta análise serve de inspiração para a dualidade da comunicação-vigilância, que em certa medida este duplo é único, é a comunicação vigilante.

Curiosamente, as mesmas tecnologias que ampliam as possibilidades de emissão, acesso e distribuição da informação tornam-se instrumentos potenciais de vigilância e controle; as mesmas tecnologias que possibilitam o anonimato nas relações sociais e comunicacionais mostram-se eficientes instrumentos de identificação. Paralelamente, o ciberespaço é marcado pela expansão das margens de visibilidade do que costumávamos entender por intimidade [...]. (BRUNO, 125)

Foi preciso que a União Europeia começasse um movimento jurídico mais radical para que o mercado se movesse de modo menos obscuro sobre as políticas de compartilhamento de dados.

Mas ainda assim, nem mesmo por lá é fácil imaginar nações inteiras compreendendo o potencial crítico, seja positivo, seja negativo, da coleta irrestrita de dados, tratamento e compartilhamento de acordo com interesses meramente comerciais e como isso pode impactar a privacidade como um todo.

How many members of the public are aware that detailed information on what they purchase with their credit and debit cards is available to anyone who wants to pay for it? Where is the opt-out button? The answer of course is that there simply isn't one, how could there be when most people are totally unaware that this is going on? Or at least there isn't an opt out button that anyone concerned over retail data snooping is likely to find. Some credit card companies do offer an opt out from this sort of activity, if you're prepared to look hard enough. Mastercard offers a 'Data Analytics Opt-Out' under the global privacy notice on its website. (SUMNER, 2016, p. 51)

Atualmente parte dos dados que muitos acreditam ser segredo está sendo comercializado de modo amplo por diversas plataformas disponíveis no mercado por alguns centavos incrementais no custo de publicidade para cada pessoa impactada.

Apenas alguns centavos pode ser o custo de saber em que nível de renda uma pessoa se encontra atualmente, em qual bairro reside, se tem empresa, se gosta de esportes radicais. Centavos são suficientes.

These are useful measures, which, if employed, would result in firms being at least a little less gung-ho with consumer data. But until the law catches up (and even then we're supposing that the law will actually improve the situation, rather than further muddy the waters which not an uncommon outcome), there will always be problems. Partly this is because without the right regulations in place, companies are caught between the expectation that they should treat data reasonably, and the demand from their shareholders that they do everything possible to maximize value. (SUMNER, 2016, p. 79)

O que Sumner (2016) está apontando é que mesmo o mercado precisa de certo modo de limites para que possa se desenvolver em alguns aspectos.

Caso a regulamentação não seja proposta e aplicada pelos Estados, a autorregulação do mercado fará com que os dados canibalizem as experiências e as pessoas comecem a se sentir encurraladas pelos próprios atos praticados e mensurados, pela quebra da privacidade e seus resultados.

Should we trust cloud providers with our precious data? The only logical answer is that each cloud provider must be assessed on a case by case basis, it would make no sense to automatically distrust them all because the whole idea of the cloud is in some way untrustworthy, just as it would be irrational to decide that every cloud provider is a safe bet. Firms and individuals consuming cloud services (which increasingly means all firms and most individuals) can draw some comfort from the fact that any cloud vendor who develops a bad reputation for security and privacy will quickly go out of business. (SUMNER, 2016, p. 166)

Em outras palavras, entregam-se muitos dados sem compreender quem terá acesso a estas informações além das empresas de face, das empresas com quem estão sendo trocadas as informações.

Casos recentes de compartilhamento de áudio gravados por assistentes digitais tomaram proporção considerável na mídia, porém pouco disso é realmente ilegal, uma vez que muitos destes serviços estão protegidos pelo opt-in.

Ou seja, a legalidade e a moralidade seguem ainda caminhos muito distintos neste campo que ainda está em desenvolvimento.

É de se esperar que enquanto os Estados e as Nações não se posicionarem contundentemente, a prática mercadológica continuará a seguir se desenvolvendo neste abismo ético.

Para Baldwin (2018) este assunto é ainda mais visceral. O autor aponta seu foco totalmente para os riscos de termos uma sociedade privatizada, ao invés de uma sociedade que em certa medida seja privativa.

Governments have allowed private firms to extract information—the oil of the digital economy—worth hundreds of billions of pounds. This time, it has not been have pumped out of the ground but out of citizens. Worse still, this vast transfer of wealth and power has happened without touching the sides of democratic debate, until it is perhaps too late to stop it. (BALDWIN, 2018, p. 235)

Enquanto Baldwin (2018) traz contornos pesados para o processo, muitos podem acabar ignorando seus alertas por considerá-los em demasia pesados, mas ele não é dissonante de tantos outros estudiosos da relação dos dados e os riscos sociais em curso juntamente com os benefícios.

Sob o fluxo visível das trocas e conversações sociais, constitui-se um imenso, distribuído e polivalente sistema de rastreamento e categorização de dados pessoais que, por sua vez, alimenta estratégias de publicidade, segurança, desenvolvimento de serviços e aplicativos, dentro e fora destas plataformas. Cruzando este processo, empresas e governos especializam-se em monitorar e coletar rastros, gerados pela navegação de usuários na Internet, construindo bancos de dados e técnicas de composição de perfis que orientam ações comerciais, políticas, securitárias, administrativas. (BRUNO, 2013, p. 9)

É através da sutil camada comunicacional que se estrutura as formas de vigilância e estas ganham corpo, e minam a estrutura básica da privacidade, que no caso de Bruno (2013) aparecem com contornos estatais, e que em Sumner (2016) e em Baldwin (2018) recebem coloração mais mercadológica.

Seja na vertente de análise que considera o risco da vigilância extrema vir do Estado, seja para o lado em que o mercado é o grande consumidor de dados, parte da questão é que a ponta vulnerável é a sociedade, através do indivíduo, o ente humano na sua particularidade que perde, mesmo que sem ter consciência disso, a capacidade de transitar com maior liberdade entre os sistemas político-econômicos pelo enfraquecimento de sua privacidade. Liberdade esta conferida pelo anonimato, pela serendipidade, pela possibilidade de revolucionar sua própria história e reinventar sua vida cotidiana.

Ao adentrar as questões da privacidade, do esquecimento e da possibilidade de reinvenção de si numa sociedade altamente vigiada e vigilante, na qual cada indivíduo que possui um aparelho smartphone se torna um vetor comunicacional vigilante, se faz necessário retomar o poder e o valor de se saber mutável.

Neste sentido que Mayer-Schönberger (2009) se faz necessário quando estuda o custo da memória décadas e séculos atrás quando comparado ao preço do esquecimento nos dias de hoje.

Em termos mais simples e diretos, a história narrada pelos vencedores é também repassada através dos artefatos de memória. Livros, pinturas, fotografias. Tudo sempre teve seu preço. Um preço muito maior do que um plebeu ou um operário médio conseguiria dispor para contar sua própria história, ou até mesmo sua versão sobre a narrativa oficial.

Ser lembrado pela história foi algo para poucas pessoas.

Entretanto, nos dias de hoje, ser esquecido é algo difícil, raro, quase proibido em termos práticos.

This overabundance of available storage capacity makes it easy for us to shift our behavioral default regarding external memory from forgetting to remembering. We save different versions of the documents we are working on to our hard disks. And store images and music files, on the assumption that perhaps some day we might need them. Storing information has become fantastically convenient, but it's more than convenience that induces us to preserve. The truth is that the economics of storage have made forgetting brutally expensive. (MAYER-SCHÖNBERGER, 2009, p. 46)

Com o barateamento dos dispositivos de coleta e armazenamento de dados, lembrar se tornou mais barato do que esquecer.

Da mesma forma, o preço de se ter privacidade nos dias atuais é alto e os descontos, os benefícios de ceder à pressão do infopoder transestético são sedutores e afáveis.

O exemplo oferecido por Mayer-Schönberger (2009) refere-se à agilidade para tirar diversas fotos contraposto com o tempo necessário para olhar para cada foto e decidir se deve ou não a manter, sendo que o custo para continuar com cada imagem salva nos celulares ou na nuvem segue reduzindo a cada dia.

Ao pensar na aceleração cotidiana, compreende-se como factível que as pessoas prefiram guardar tudo a perder tempo realizando qualquer tipo de curadoria.

Assim, custo dos suportes técnicos interfere no custo de tempo, possibilitando e fortalecendo a inversão do que se teve até então como padrão das sociedades humanas. Lembrar era dispendioso, em tempo e em recursos materiais (como o dinheiro). Esquecer sempre foi o padrão.

Agora se torna cada vez mais difícil e suspeito não ser visível para o sistema panóptico de vigilância.

E tal visibilidade não está emanando, nascendo da microconduta em sociedade, mas é fruto de um sistema complexo.

[...] the posited causal relationship runs from the ways in which international trade shapes the preferences of different sectoral groups or collective actors, through institutionalized preference aggregation mechanisms at the national level, to shifts in national bargaining positions (and hence in the likely final forms of international agreements). The international shock affects domestic politics through its consequences for primitive group preferences, while national-level institutions remain constant. These assumptions lead the literature to emphasize traditional, formal interstate agreements, where the institutional mechanisms aggregating preferences are straightforward and easy to capture using formal or informal models. (FARRELL; NEWMAN, 2019, p. 21)

Da mesma forma que os autores estão destacando a permeabilidade da agenda global sobre os governos, há aqui uma derivação da atuação e da agenda governamental e estatal sobre seu povo e tal atuação sistêmica não é simples nem simplória.

One of the regulations that does exist in Europe is the ‘right to be forgotten’, which allows users to request that embarrassing data about them is erased from search results. But even this has generally been adjudicated upon by Google itself in what seems to be an implicit acknowledgment by the European courts that they are not competent to decide such matters.¹¹⁴ Similarly, a German law threatening huge fines against social media failing to remove ‘hate speech’ has also effectively been implemented by the tech firms, with Facebook hiring more than 1,200 new staff—a sixth of its global ‘community operations team’—to monitor posts in the country. (BALDWIN, 2018, p. 253)

O direito de ser esquecido não é em si uma novidade sequer para o direito brasileiro, como conceito. Mas como prática da forma como é conhecido hoje ainda está a largo de ser compreendido.

Ele está, de certa forma, ligado à privacidade na medida que permite que uma pessoa não seja mais assediada por seu passado nos momentos de atuação em sociedade. A privacidade decisional se faz respeitada a partir do momento que uma dívida já tenha sido paga, seja para o mercado, seja para a sociedade.

Explicando com um pouco mais de detalhes, um cidadão que tenha cometido um crime e que, ao final de um dado período, já tenha pago todas as penas impostas pela justiça, tem o direito de ter seu crime esquecido, para que sua vida possa ser reconstruída, a partir de um ponto neutro, no mínimo.

Assim, independentemente do crime cometido, todas as pessoas têm igualmente o direito de reiniciar suas vidas após estes incidentes.

Esta premissa básica é o que torna todos os crimes passíveis de ajustes e correções. Isso significa que o sistema judiciário e penal está em busca da ressocialização e reintegração do indivíduo pós-cumprimento da pena para que este volte a ser econômica e socialmente ativo.

Já quando se fala do direito ao esquecimento na internet, este se presta a algo mais complexo justamente pela questão da replicabilidade barata da informação e pela pressão e barreira que isso cria para a manutenção da privacidade, de modo geral, e principalmente da sua característica de autodeterminação informacional e decisional.

The German constitutional court, for example, created an important line of precedent developing the concept of informational self-determination. First elucidated in the 1980s in response to an overly detailed census questionnaire, the same logic was applied more recently by the court to European telecommunications surveillance rules. While the court's impact is ambiguous in some respects, it casts a shadow of authority over national and even European decisions that attempt to restrict personal privacy. (FARRELL; NEWMAN, 2019, p. 52)

Tornado simples, este direito trata da capacidade e possibilidade que qualquer pessoa deve ter de construir a si mesmo, através dos dados que consome ou emite, de modo livre.

Não é o objetivo deste trabalho entrar nos pormenores de tal liberdade nas sociedades, mas claramente este campo é um desdobramento possível desta jornada também no que tange a privacidade.

Ainda assim, poder se autodeterminar é ter direito às informações sobre como seus dados estão sendo tratados e, principalmente, conhecer e poder atuar sobre as inferências que foram construídas a partir dos seus dados e de dados de terceiros que possam interferir em sua vida.

Entre as grandes preocupações está a capacidade de inferência de informações que podem ser danosas, ainda que sejam verdadeiras, ou que sejam manipuladas de tal modo que forcem um conjunto de dados a declarar um conhecimento fantasioso sobre a realidade.

Some worried whether the use of analytics in baseball was discovering misleading and coincidental correlations, such as that the rise in the incidence of autism almost exactly matches increased organic baby food sales. And, as

data flooded into sport and coaches' offices, the very success of teams like the Red Sox bred imitation. Once everyone started using Sabermetrics there was no competitive advantage; it was no longer a wizard's wand but simply another tool, the use of which should be determined by skill and judgement. (BALDWIN, 2018, p. 179)

Esta questão é de extrema importância na medida em que as pessoas oferecem dados para empresas no mundo todo com apenas alguns cliques, mas sequer conseguem imaginar como estes dados estão sendo transformados em inferências indevidas sobre suas personalidades, interesses, inclinações e desejos.

Tanto a inferência correta é arriscada, na medida que desnuda mais o ser para as empresas do que para si próprio, quanto a inferência drasticamente incorreta.

Ou seja, as empresas se tornam por vezes mais capazes de compreender movimentos de consumo (e políticos, por exemplo, no caso Cambridge Analytica) do que o sabe o próprio sujeito, quando o tratamento de dados consegue compreender de forma ajustada as ações e interesses das pessoas.

Mas o oposto traz também seu risco, na medida em que o dado pode conduzir a uma classificação polar e oposta.

2

Acima vemos um gráfico construído justamente para lembrar que nem toda correlação em cálculos é, em si, um exercício de fazer caber realidades específicas em dados inteligíveis.

² SPURIOUS Correlations. Disponível em: <https://www.tylervigen.com/spurious-correlations>. Acesso em: 2 out. 2019.

Ou seja, toda metodologia de tratamento de dados traz consigo um viés que conforma a realidade à capacidade de observação e tradução desta realidade em dados específicos.

Isso significa que as metodologias de inferência são uma lente pela qual se vê o mundo, mas precisam ser usadas com a consciência plena e ativa de que há distorções produzidas por elas.

As melhores metodologias são aquelas que podem representar a realidade com a menor distorção possível, mas é inexistente qualquer técnica que se exima de colorir de modo distinto a realidade que observa e resume.

In years to come, a combination of data analytics and psychometric social media advertising is likely to mean individual voters are targeted with obscure or even contradictory adverts that tap into their deepest fears or desires. Self-learning algorithms that fine-tune messages with millions of variations could put much of this even beyond the control of the campaigns themselves let alone an external regulator. (BALDWIN, 2018, p. 282)

Quando se encontra este tipo de posicionamento, mas do que encarar como fatalismo, é necessário compreender tanto as ressalvas quanto os alertas. Neste caso, Baldwin (2018) busca chamar à atenção os fatores que podem se tornar muito críticos com relação aos algoritmos, à vigilância e à privacidade ao longo de anos muito próximos.

Ao se buscar os termos “Cambridge Analytica” no buscador do Google, recebe-se como resposta cerca de 11,1 milhões de páginas.

Isso é mais do que a população de Portugal (10,29 milhões de habitantes). É o mesmo que dizer que se todo cidadão português escrevesse um artigo sobre o caso, ainda faltaria gente para cumprir este volume de matérias.

Outro ponto importante é que esta empresa foi fundada oficialmente em 2013, ou seja, menos de 7 anos atrás.

Seus primeiros escândalos globais, que envolvem a candidatura do atual presidente estadunidense e a campanha de desligamento do Reino Unido como membro da União Europeia datam do início de 2018, porém a realização de tais trabalhos com dados pessoais ocorreu em 2016.

Apenas 3 anos após sua fundação, uma empresa com poucas dezenas de funcionários foi capaz de causar impacto na forma como se age em campanhas de influência da opinião pública.

The speed with which technology changes and the murkiness of the world of political strategy and communications makes the task of those with oversight very difficult. Even if it is a stretch to blame Cambridge Analytica for the victories of Brexit and Trump, the potential for highly sophisticated analytics and targeted adverts determining the result of future elections will grow. Any campaign would be crazy not to use them but the advantage will usually be with the deepest pockets and lowest morals. (BALDWIN, 2018, p. 281 - 282)

O chamado à consciência se faz mais evidente quando se é capaz de compreender que Cambridge Analytica é apenas um dos primeiros exemplos em escala global sobre o uso imoral de dados pessoais em larga escala em um campo tão sensível capaz de enviesar as estruturas democráticas.

Mas não significa que o caminho seja culpabilizar as grandes empresas como Facebook, Google e esquecer que todas fazem parte de um mercado ainda maior, orquestrado por interesses em diversas frentes.

A facilidade de duplicação e compartilhamento de dados, tanto no aspecto técnico, como no aspecto econômico, assim como destacou Mayer-Schönberger (2009), torna qualquer empresa pequena capaz de usar dados reais com objetivos justos ou escusos.

Facebook e Google, por exemplo, se tornaram grandes alvos por seu poderio de coleta e tratamento de dados, mas até o presente momento, o maior escândalo foi gerado não pelas grandes empresas, mas sim através das grandes empresas, assim como ocorreu através das brechas jurídicas dos países.

Ao invés de assumir a falha estatal, auxiliamos a geração de mais desinformação quando focamos nos alvos preferidos e ignoramos a infraestrutura do sistema mercadológico vigente que se reveste de dados para conduzir uma classe média consumidora dentro dos parâmetros econômicos de interesse do mercado global.

Por fim, ainda sobre a privacidade e sua caracterização, Masur (2017) vai cunhar uma teoria própria indicando que a privacidade tem cunho situacional e que o próprio indivíduo busca certos modos de ampliar a severidade das proteções e barreiras para o acesso aos seus dados e sua intimidade em momentos oportunos, e da mesma forma o oposto quando percebe benefícios na sua exposição.

A e-vasão aqui então seria parte de um ato mais consciente, de interagir com a persona que cria constantemente através do infopoder e-vasivo.

É preciso compreender, para o processo e-vasivo, que a privacidade possui mais do que a camada física, e por tanto não se trata exclusivamente de trabalhar os aspectos topográficos e corpóreos da privacidade, e também vai além dos limites sociais.

Enquanto focados nos limites espaciais, a privacidade pode dizer respeito dos lugares de convívio, da casa, do escritório. Espaços que já estão sendo escrutinizados pelas tecnologias vestíveis e pelos dispositivos inteligentes, novamente, com o pretexto de ampliar a segurança e a comodidade das pessoas.

Já no aspecto social, a privacidade toca mais do que as conexões, mas também a percepção de que uma pessoa possa optar por uma vida paralela da qual seus colegas de trabalho ou família jamais fiquem cientes. É a condição de ser capaz da recriação da identidade e do eu livre das pressões constantes da vida comum de antigamente, determinada pelo bairro, pela família mais próxima.

A desterritorialização das relações permite então um estilo de vida que se mostra mais abrangente.

Mas os algoritmos de coleta de tratamento de dados na internet, e que muitas vezes se cruzam com bases de dados de plataformas digitais com acesso a dispositivos vestíveis, podem ser os grandes reveladores desta realidade paralela através, por exemplo, de oferta de produtos relacionados a estes momentos íntimos.

Não é de muito espanto imaginar que grande parte das pessoas que tem acesso à internet já compreenderam que após pouco tempo de uso das redes sociais digitais a publicidade se torna mais verticalizada e foca nos gostos específicos de cada pessoa.

Assim, ver um anúncio no celular de uma namorada ou de um marido é um indício forte do tipo de conteúdo que eles consomem.

Esta forma de e-vasão está sustentada pela praticidade e pelos descontos financeiros sobre produtos de interesse.

Já um outro pilar importante da e-vasão, e que neste caso se torna ainda mais profundo, é a e-vasão da privacidade de modo a constituir um actante que interfira na capacidade decisional das pessoas.

Um exemplo prático de algoritmo que pode impactar na capacidade decisional de públicos altamente qualificados é o Watson da IBM. Esta inteligência artificial foi criada e treinada para que oferecesse a resposta mais provável, no campo da probabilidade estatística mesmo, para uma dada pergunta, como visto anteriormente.

Entre suas aplicações, está o ensino de crianças sobre matérias escolares ou curiosidades do mundo, embarcando esta tecnologia em brinquedos lúdicos.

Outra forma de utilizar o Watson, que já está em andamento, é para que ele avalie resultados de exames e diagnósticos e, com base em seus achados, possa ajudar médicos a definirem qual conduta aplicar.

Em outras palavras, uma inteligência artificial está prestes a ajudar na redefinição de protocolos com base em dados reais de sobrevida, qualidade de resposta e grupos étnicos diferentes.

Por um lado, este resultado se torna incrível para ajudar a aumentar ainda mais a taxa de resposta positiva dos tratamentos. Por outro, qual médico dentro de uma década irá contradizer o Watson e aplicar um procedimento distinto do que a inteligência artificial indicar?

Isso significa que já um processo de interferência na tomada de decisão por parte de um algoritmo que pode ter em seu desenho falhas estruturas com as quais a sociedade ainda não decidiu como lidar, da mesma forma que não se tem um consenso sobre quem deveria ser processado ou preso nos casos em que um carro autônomo atropelar alguém. Deveria se punir o proprietário do carro, ou o presidente da empresa que o criou? Ou ainda os profissionais que ensinaram a inteligência artificial a tomar decisões em caso de risco?

Compreendendo que em alguns anos o Watson, ou sistemas similares a ele possam se tornar prevalentes em muitos hospitais, em quanto tempo os médicos deixam de ser suportados para se tornarem dependentes?

Sem inocência, o mesmo hoje em dia se dá com relação a tomografias, exames de sangue e afins. A diferença é que todos estes exames são apresentados como material de análise. O parecer do Watson é uma indicação direta de procedimento.

O motivo, então, que traz esta discussão para este trabalho é a e-vasão por parte dos profissionais sobre sua capacidade decisional privada, mas que tem impacto direto na vida das pessoas.

Não apenas os médicos estão passando por este dilema, mas também juristas e advogados. A França proibiu o uso de algoritmos e inteligência artificial para análise de grupos de sentenças proferidas por cada juiz.

Isso por compreender que na medida em que uma empresa de advocacia com alto poder econômico pode lançar mão da tecnologia e compreender padrões de julgamento sobre um juiz, esta pode ter mais consciência dos modos de conduta e pensamento dele do que o próprio magistrado.

Assim, mesmo sem ter autorizado, mas ao mesmo tempo por se tratar de julgamentos públicos, a forma de tomar decisão de um juiz pode ser influenciada de modo muito mais preciso e vertiginoso.

Outra forma sensível que tal procedimento traz para o debate é que enquanto advogados independentes que defendam clientes menores contra grandes corporações seguirão com seus métodos tradicionais, seus contestadores terão poder econômico para fazer análises estratificadas sobre quais juristas um juiz mais cita, qual tipo de postura ele assume em casos similares. A disputa se torna ainda mais discrepante.

Relevante esta questão da e-vasão decisional pois na medida em que não há consenso, parte da mentalidade já está inserida na contenda.

Há de se perguntar se em um futuro médio ou longínquo haverá inteligências artificiais classificando e antecipando pareceres para que os juízes possam ter maior celeridade nos julgamentos.

Se na medida em que o Watson traz recomendações para os médicos, haverá uma inteligência artificial que traga perguntas mais recomendadas a serem feitas em casos específicos de acareação?

E se os dados que forem oferecidos para a inteligência artificial estiverem maculados pelo racismo e machismo estrutural, tal algoritmo será capaz de expurgar este fator antes de começar a dar suporte para os juristas?

De certa forma, quando Masur (2017) apresenta sua proposta teórica de privacidade situacional, está a relativizar os momentos de percepção de cada indivíduo, que através de cada situação perceberá e agirá de forma distinta.

No caso dos algoritmos, é preciso um debate maior do que apenas a percepção do indivíduo para não incorrer na falácia do opt-in.

Um cidadão comum, que posta mensagens subversivas em sua rede social digital pode ser considerado pela justiça como um transgressor mais provável do que uma pessoa de mesma idade e classe social que more no mesmo bairro mas que mantenha suas redes alimentadas por mensagens motivacionais ou religiosas?

Ao compreender o *self* arquitetado através do imperativo transestético em busca do infopoder cibercultural, a resposta que se dá diretamente ao longo deste trabalho é que não.

Porém os dados e-vadidos podem conter este tipo de viés que agirá sobre a vida prática e cotidiana das pessoas sem que se avalie exclusivamente os atos, mas majoritariamente os movimentos de dados, as manifestações identitárias, os artefatos classificados e processados pelos algoritmos.

Em uma análise pregressa, não se espera que haja ética no tratamento de dados dos governos ditatoriais, tendo no nazismo um dos exemplos mais extremos para o ocidente, mas não o maior, nem o mais cruel.

Isso serve para compreender que nos dias atuais nada garante que o processo de tratamento dos dados e-vadidos seja feito com ética. A bandeira do bem comum pode ocupar o mesmo espaço da discriminação, do preconceito, ou da falácia da segurança para cooptar os dados e-vadidos de modo que cada indivíduo na sociedade possa exercer o papel de censor do outro que se recusa a se e-vadir.

DIREITO E PRIVACIDADE

Na medida em que se estuda a questão da privacidade e da coleta de dados a partir de dispositivos tecnológicos, se faz necessário tocar, ainda que de modo breve, a questão legal da conduta humana, uma vez que esta também é produto e produtora da conduta, em uma dupla dinâmica.

Relevante dizer que o propósito deste trabalho não é, em si, consolidar-se na positivação de um texto específico, mas sim provocar a visão de juristas e operadores do direito sobre a perspectiva infotécnica da comunicação na medida que seus dispositivos se convertem gradativamente em actantes vigilantes e condicionadores de condutas específicas validadas jurídica e socialmente, ou formas de agir sob o risco daquilo que é vedado.

Interessante ter em mente que ao olhar para o aparato legal observa-se também o entendimento que uma sociedade tem sobre privacidade, e isso é crucial para compreender as articulações legais e infraestruturais que regem o pensamento sobre qual valor deve ser preservado em uma sociedade.

Nearly every law or policy involving privacy depends upon a particular understanding of what privacy is. The way problems are conceived has a tremendous impact on the legal and policy solutions used to solve them. (SOLOVE, 2011, p. 24)

E é nesta seara que se busca compreender como este trabalho pode ser fermento para debates relevantes sobre o que é a privacidade alardeada como proteção e como, partindo da sociedade, a estrutura privativa se consolida como um valor coletivo com esteio individual.

Destaca-se mais uma vez que este é um dos pontos principais desta tese, que é ressaltar o valor coletivo e social da privacidade que tem, em sua materialização, condutas individuais.

Por mais que o trabalho anterior tenha se convertido em uma referência doutrinária (SUPREMO TRIBUNAL FEDERAL, 2017), sendo recomendado pelo Supremo Tribunal Federal para os operadores do direito que buscam compreender melhor o que vem a ser o direito ao esquecimento nos seus aspectos contemporâneos, novamente a proposta é provocativa para que seja considerada dentro das bases de problematização sobre os impactos sociais e jurídicos dos

aparatos técnicos de coleta, tratamento e memória de dados (FELÍCIO, 2015) na conduta *onlife* (FLORIDI, 2014).

Assim, apresentaremos algumas questões referentes a legislações concernentes à privacidade em alguns países para referência, de modo que possam ajudar a formar uma visão mais holística sobre como a privacidade está sendo tratada pouco a pouco em vários lugares do mundo.

O modo mais abrangente de tratar o tema da privacidade é partindo para o que se torna mais genérico, mais aplicável.

Neste caso se tem a Declaração Universal dos Direitos Humanos publicada pelas Nações Unidas, que em seu 12º artigo onde é indicado que “Ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques” (NAÇÕES UNIDAS).

De pronto as questões culturais e linguísticas já começam a impactar este debate mesmo quando o agente que está em busca de definir as proteções e os sistemas de pesos e contrapesos se trata da própria Organização das Nações Unidas (ONU).

Diz-se isso neste momento pois o texto acima, na tradução oficial da ONU para o português, indica que as intromissões não devem ocorrer na “vida privada”, enquanto o texto original, em inglês, indicará que “No one shall be subjected to arbitrary **interference with his privacy**, family, home or correspondence, nor to attacks upon his honour and reputation.” (NAÇÕES UNIDAS, *negrito nosso*).

Ou seja, enquanto a tradução oficial fala em vida privada, o texto original fala em privacidade.

São correlatos, mas não similares.

Este ponto será crítico na medida em que privacidade e vida privada podem se confundir com a percepção do que vem a ser público e interesse público.

O espaço de ocorrência da privacidade pode, inclusive, ser os ambientes públicos.

Garantir que a privacidade de alguém não será violada é mais do que tratar de características domiciliares. É tratar da interferência sobre sua conduta e

intelectualidade. Estar no espaço coletivo e ainda assim manter os limites da privacidade é relevante.

A princípio pode parecer uma discussão irrelevante, mas a cada momento que este trabalho evoluir, pretende-se tornar mais explícito que a espacialidade não é ponto de definição categórica e exclusiva para o que vem a ser privado ou público.

Compreender a privacidade é compreender o seu papel na sociedade.

E uma das formas de se lançar nesta jornada é através das legislações, que de modo mais técnico, buscam resumir e ordenar a vida em sociedade de acordo com o entendimento de como a própria sociedade compreende que deva ser.

Mais do que trazer os debates históricos, para o fim que se propõe este estudo, ganha muito relevo o atentado terrorista de 11 de setembro de 2001 orquestrado pela al-Qaeda, contra os Estados Unidos da América.

Com impacto global, este ato marca a intensificação do fortalecimento da vigilância técnica do Estado.

Como forma de proteger sua nação, os EUA agem para aparelhar ainda mais o Estado para que este seja apto a vigiar de modo mais pervasivo e ainda mais silencioso cada ponto suspeito de sua grande malha de dados.

E é neste enredo que a Agência Nacional de Segurança dos EUA (NSA) passa a ter um papel ainda mais central no debate sobre a vigilância, ainda que sua fundação não seja recente, como trazem Farrell e Newman (2019), “the NSA established secretly in 1949 as the Armed Forces Security Agency, added to the mix, providing valuable communications intelligence on both US adversaries and allies (FARRELL; NEWMAN, 2019, p. 55)

Em outubro de 2001, os EUA aprovam o que ficou conhecido como Ato Patriota, um conjunto de alterações legais que visavam a segurança nacional.

Entre os itens mais controversos de tal Ato está a ampliação, mais tarde, dos impactos das cartas de segurança, emitidas pela NSA, a fim de acessar dados de qualquer pessoa que estivesse em posse de empresas americanas ou que operam em solo nacional, como pode ser visto no trecho a seguir.

Another controversial aspect of the PATRIOT Act concerns broad data collection powers contained in the so-called library records provision and the expansion of National Security Letters. Both allow for investigators to seize a

wide range of business records. The library records provision covers both content and transmission information but requires a court order. National Security Letters, by contrast, have a narrower scope, focusing on transmission data, but do not require investigators to have a warrant. Both provisions come with gag orders so that businesses that provide information are not allowed to disclose the request. (FARRELL; NEWMAN, 2019, p. 61)

Faz-se necessário notar que a ampliar o escopo e o poder da NSA, o Ato Patriota acabou por proibir que qualquer ente notifique os envolvidos em pedidos de dados sigilosos sobre si.

Assim, qualquer empresa que tenha se consolidado com a promessa de manter a privacidade e os dados dos seus clientes e usuários a salvo está, desde o ponto de partida, nos dias atuais, limitada a tal garantia, sendo que tal aparato de vigilância acaba por recair não apenas sobre a nação estadunidense, mas sobre qualquer pessoa que utilize serviços de empresas de tal país.

Para começar, o primeiro país a ser considerado é a Suíça nesta análise jurídica.

Sua Constituição Federal traz já no artigo 13 o direito à privacidade. Ou seja, uma constituição com quase 200 artigos traz já no início o direito à privacidade de modo extremamente genérico, mas ao mesmo tempo oferecendo no texto base a relevância do tema.

Art. 13 Right to privacy

1 Every person has the right to privacy in their private and family life and in their home, and in relation to their mail and telecommunications.

2 Every person has the right to be protected against the misuse of their personal data. (SUÍÇA, 1999)

Destaque-se o fato de que a Constituição suíça traz a privacidade atrelada à vida de modo amplo, mas dá foco para a vida em família, dentro da residência e nos processos comunicacionais.

Aqui a comunicação recebe a dimensão de espaço, de ágora e de rizoma. Não está aclarado o direito à privacidade nos espaços públicos e também não há desdobramentos que indiquem se a internet, como um todo, é considerada um meio de telecomunicação ou apenas um espaço de consumo de informação.

Mesmo o Federal Act on Data Protection (1992) não indica qualquer questão sobre os meios de comunicação de modo a caracterizá-los e distingui-los.

Desta forma, a internet de modo geral está apenas subentendida, mas não tipificada. O mesmo pode se dizer dos aplicativos e IoT.

Ainda há discussões incrementais em torno da Constituição, mas principalmente ao redor do Ato de Proteção de dados (1992), mas já em 1992 o país contava com parte do que hoje serve de inspiração para o que veio a ser apresentado como proposta britânica que, por sua vez, é fonte de inspiração para o modelo brasileiro.

Ou seja, a origem do que se discute no Brasil é, em suma, os debates suíços que foram iniciados há quase 3 décadas.

Outro país que serve de subsídio para este trabalho, que além de atender à legislação da União Europeia apresenta sua visão legal sobre a coleta e processamento de dados pessoais há mais de uma década, é a Romênia.

Sua relevância está em justamente reservar um espaço, ainda que diminuto, para tratar das comunicações eletrônicas.

Article 4: (1) The confidentiality of communications and the related traffic data by means of public electronic communications networks and publicly available electronic communications services is guaranteed. (2) Listening, tapping, storage or other kinds of interception or surveillance of communications and the related traffic data are prohibited, except for the following cases: a) these operations are carried out by the users who participate in that communication; b) the users who participate in that communication have previously given their written consent; c) these operations are carried out by the competent authorities, under the conditions set out by the legal provisions in force. (ROMÊNIA, 2004)

Esta forma de tipificação reduz conflitos como muitas vezes se viu nos tribunais brasileiros sobre a inviolabilidade da correspondência, garantida pelo artigo 5º, XII, da Constituição Federal, que chega a indicar a inviolabilidade da comunicação telegráfica (e de dados nos dias atuais), mas que em muitos momentos teve sua aplicabilidade questionada quando a comunicação se dava de servidor para servidor, ou seja, uma comunicação não humana e que, portanto, poderia tornar dúbia a aplicação do artigo referido.

Ocorre que, no caso romeno, um dos fatores que limitam os efeitos da legislação é o nível máximo de penalidade monetária, que sequer chega a EU\$50 mil, o que para grandes empresas pode ser considerado como irrelevante dependendo da receita que se pode produzir com base nestes dados indevidamente coletados e comercializados.

Aqui é possível compreender um aspecto necessário do direito que pode impactar o resultado social da lei, que é a proporcionalidade do remédio.

Em outros termos, pode ser inócua a lei que pretende onerar as empresas de acordo com as violações, mas que não oferece risco econômico real. Assim, agir contra a lei, ao menos no aspecto econômico, pode ser mais lucrativo do que respeitá-la.

Um exemplo, por outro lado, é a sanção que no Brasil chega a ser consideravelmente mais robusta, podendo atingir o teto de R\$50 milhões, o que já coloca em atenção empresas medianas. Os grandes operadores, por sua vez, levam em consideração não apenas o impacto financeiro direto das multas, mas a possibilidade de restrições e crises de imagem em outros países dependendo do tipo de sanção aplicada por aqui.

Isso significa que as empresas globais consideram o fator da escalabilidade das ofensivas estatais de acordo com precedentes dentro dos blocos políticos, jurídicos e econômicos.

É um caso de expatriação da lei não por determinação da tipificação, mas por uma questão de risco e oscilação de valor de marca, além de crises futuras.

Vale citar que a legislação brasileira tenta mimetizar parte desta ação através do Art. 4, IV da LGPD, exigindo que ao exportar dados, o país recebedor deverá prover o mesmo grau de proteção oferecida pela LGPD brasileira.

Dentro deste item, deve-se considerar que o que a legislação brasileira fala é sobre o grau de proteção legal, mas não fala da qualidade investigativa ou de precedentes de penalizações que possam garantir que mesmo havendo uma tipificação jurídica, que ela seja de fato acionável e renda frutos protetivos e corretivos para os entes envolvidos.

Há, porém, a legislação britânica que, de modo mais austero, expatriou sua aplicação, na medida em que aplica as sanções dentro de seu território mesmo que a violação ocorra em outros países, desde que o objeto da violação sejam informações a respeito de seu povo.

Isso é, enquanto o Brasil ainda se delonga nas definições sobre a legislação, com um código ainda cheio de brechas mercadológicas, o brasileiro médio acaba se

beneficiando da lei britânica que amplia suas sanções além do seu território, mesmo tendo o foco exclusivamente o seu povo, fez com que diversas empresas empregassem um padrão mundial com base nas restrições da União Europeia (UE).

Desta forma, a UE traz itens importantes que inspiraram a legislação brasileira de modo mais direto, como a portabilidade dos dados, o direito ao apagamento e retificação de dados, mas um dos itens de maior impacto da legislação europeia foi certamente o capítulo V que trata da transferência de dados pessoais para países terceiros ou organizações internacionais, fazendo valer a legislação de forma extraterritorial.

É importante também considerar o direito de oposição, que significa

Artigo 21

1. O titular dos dados tem o direito de se opor a qualquer momento, por motivos relacionados com a sua situação particular, ao tratamento dos dados pessoais que lhe digam respeito com base no artigo 6.o, n.o 1, alínea e) ou f), ou no artigo 6.o, n.o 4, incluindo a definição de perfis com base nessas disposições. O responsável pelo tratamento cessa o tratamento dos dados pessoais, a não ser que apresente razões imperiosas e legítimas para esse tratamento que prevaleçam sobre os interesses, direitos e liberdades do titular dos dados, ou para efeitos de declaração, exercício ou defesa de um direito num processo judicial.
2. Quando os dados pessoais forem tratados para efeitos de comercialização direta, o titular dos dados tem o direito de se opor a qualquer momento ao tratamento dos dados pessoais que lhe digam respeito para os efeitos da referida comercialização, o que abrange a definição de perfis na medida em que esteja relacionada com a comercialização direta.
3. Caso o titular dos dados se oponha ao tratamento para efeitos de comercialização direta, os dados pessoais deixam de ser tratados para esse fim. (UNIÃO EUROPEIA, 2016)

Note-se que apesar de indicar o direito de oposição ao tratamento dos dados, não se indica os meios pelos quais tais direitos serão exercidos, nem se indica que as empresas e entidades terão que criar tais meios de acordo com alguma característica, como facilidade de acesso e comunicação, inteligibilidade, familiaridade com o conteúdo, estilo vernacular.

Da mesma forma, prazos e condições não são determinadas, o que faz com que o cidadão médio precise de maior energia para conseguir fazer seus direitos serem respeitados.

Tal lacuna na legislação Europeia tem um reflexo também na legislação brasileira que ainda não conseguiu resultar em estruturas funcionais de manutenção da aplicação legal.

Ainda assim, vale destacar que mesmo com limitações, a legislação da UE ainda se destaca frente inúmeros outros textos constitucionais ou aditivos. Quando comparado à legislação nacional estadunidense, ainda há muito a ser feito nesta última, que reforma sua constituição através de emendas ou nas atualizações estaduais da legislação.

European privacy regulations limited the types of searches and the extent of data mining. Moreover, many European intelligence agencies did not have the capacity to conduct analysis at the same level as their US counterparts. (FARRELL; NEWMAN, 2019, p. 115)

Mas há um código jurídico mais preciso, altamente detalhado nas condições permissivas e impeditivas. Conhecido como California Consumer Privacy Act (CCPA), aprovado em junho de 2018, e com início de vigência em janeiro de 2020.

Antes de abrir qualquer peculiaridade do CCPA, é relevante dar destaque ao fato que tal lei restritiva sobre coleta de dados está aninhada dentro do campo comercial. Ou seja, a lei californiana que pode servir como exemplo de profundidade e detalhamento está objetivando proteger não a identidade atual, pretérita e/ou futura, mas sim as dinâmicas comerciais e de consumo.

É no campo do consumo, e não da dinâmica social e psicológica que estão se desenvolvendo algumas garantias humanas.

Isso posto, é necessário dar destaque a alguns trechos importantes do CCPA. Dentro da lei 1798.125, constituinte do Ato, está a proibição de discriminação dos consumidores quando estes exercem o direito de manter sigilosos os seus dados.

1798.125 (a) (1) A business shall not discriminate against a consumer because the consumer exercised any of the consumer's rights under this title, including, but not limited to, by:

(A) Denying goods or services to the consumer.

(B) Charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties.

(C) Providing a different level or quality of goods or services to the consumer, if the consumer exercises the consumer's rights under this title.

(D) Suggesting that the consumer will receive a different price or rate for goods or services or a different level or quality of goods or services. (CALIFORNIA, 2018)

O modo como as proibições de condutas discriminatórias estão dadas destaca práticas comuns que influem no processo decisório, como a oferta de desconto para aqueles que entregam os dados pessoais, indicado na lei acima, item B. Mas a realidade é que não é o consumidor que ganha um desconto ao aceitar a entrega do

CPF. É o consumidor que nega apresentar estes dados que se sente punido com um custo adicional.

Note-se que o item C reforça a proibição de desqualificação do serviço para aqueles que exercem o direito à privacidade comercial.

The GDPR attempts to minimize unwanted or unnecessary data collection and processing through privacy-by-design initiatives, opt-in requirements, and a right to data erasure (often referred to as the right to be forgotten). At the same time, it explicitly recognizes the transnational nature of data sharing, extending the legislation's scope to data concerning individuals based in the European Union regardless of whether or not data collection or processing occurs within the European Union. In other words, individuals based in the European Union enjoy extraterritorial protection of their rights. (FARRELL; NEWMAN, 2019, p. 168)

Destaque-se o trecho em que os autores Farrel e Newman (2019) trazem a declaração de que o GDPR além de buscar a privacidade desde o momento de concepção das iniciativas diversas, sejam elas digitais ou analógicas, diga-se de passagem, também reconhece a natureza transacional do compartilhamento de informação, extirpando da proposta de adendo constitucional a inocência sobre o caráter econômico também em debate dentro da questão dos dados.

Esta ressalva é extremamente relevante pois localiza o interesse econômico na região central do debate, uma vez que este é ente altamente articulador.

Quando os olhos se voltam novamente ao CCPA, mostra-se importante observar que tal código não impede a coleta de dados pessoais, mas busca garantir que o consumidor poderá pedir a exclusão ou reclassificação de seus dados.

Ou seja, a coleta, em si, não é o objeto da apreciação e legislação, mas sim os usos comerciais que são dados às informações coletadas.

Relevante também perceber que a CCPA se inicia com uma sessão que declara o cenário / contexto no qual tal Ato se apresenta de modo incremental.

E ao fazê-lo, indica que

SEC 2 The Legislature finds and declares that: (a) In 1972, California voters amended the California Constitution to include the right of privacy among the "inalienable" rights of all people. The amendment established a legal and enforceable right of privacy for every Californian. Fundamental to this right of privacy is the ability of individuals to control the use, including the sale, of their personal information. (CALIFORNIA, 2018)

Dotar a privacidade como bem inalienável é algo superior ao CCPA e reflete sua importância. Em termos leigos, é dizer que mesmo que o consumidor queira,

ele não pode ceder todos os seus dados. A totalidade dos dados gerados por uma pessoa ao longo do seu dia, da sua vida, estão indisponíveis para serem negociados, ofertados, doados ou vendidos.

É dizer que a tutela da privacidade de alguém não está na própria pessoa, mas foi transferida para o Estado, e é por ele protegida de forma direta e inegociável.

O Estado deveria então se tornar a entidade que age contra qualquer um que atente contra a privacidade de outrem através da promotoria pública, uma vez que compreende este a importância da privacidade como meio basal da constituição das condutas na sociedade contemporânea.

(i) Therefore, it is the intent of the Legislature to further Californians' right to privacy by giving consumers an effective way to control their personal information, by ensuring the following rights:

(1) The right of Californians to know what personal information is being collected about them.

(2) The right of Californians to know whether their personal information is sold or disclosed and to whom.

(3) The right of Californians to say no to the sale of personal information.

(4) The right of Californians to access their personal information.

(5) The right of Californians to equal service and price, even if they exercise their privacy rights. (CALIFORNIA, 2018)

Fica mais evidente, a partir dos pontos expostos, que realmente o CCPA não é um Ato que visa impedir a coleta de dados, de modo abrangente, mas sim consolidar os limites do uso destes dados de modo comercial.

Novamente, não há qualquer menção ao impedimento de coleta de dados. Há a declaração do direito de requerer e realizar o apagamento das informações coletadas, impedir o compartilhamento sem conhecimento do ente humano gerador de tais dados.

California, the world's ninth largest economy and home to Silicon Valley, enshrines and protects privacy in its Constitution. Also, it is home to the California Online Privacy Protection Act, which enables users of commercial websites to both review and request changes to their personal data. (SUMNER, 2016, p. 39)

Legislações como esta de revisão de dados salvos por empresas servem ainda mais para disseminar a cultura de coleta e uso de dados de modo profundo.

Ao invés de ser um gatilho de correção e respeito à vida das pessoas, serve muito mais ao ensino e calibração dos algoritmos para a classificação massiva das pessoas com base em seus comportamentos, gerando ainda no indivíduo que teve

seus dados coletados o falso poder de ser visto como único e de forma similar a sua imagem intencional na rede.

Então o que temos é, uma vez mais, um direito à privacidade comercial, ainda que seja uma das mais detalhadas e avançadas legislações aplicadas nos dias de hoje.

Ocorre que as grandes empresas de tecnologia, coleta e tratamento de dados podem até oferecer formas de retificação dos dados gerais sobre cada indivíduo, mas isso não significa que os tratamentos de dados pretéritos serão ressignificados a partir de uma contestação de um usuário, ou seja, não haverá revisão e ajustes nos critérios que podem influenciar a vida desta pessoa de forma retroativa.

Também não há garantias de que estes dados estão seguros e jamais foram copiados em outro servidor. Isso significa que por mais que uma empresa permita que seus dados sejam reclassificados, isso não garante que todas as bases de dados que usaram informações oriundas desta empresa serão atualizadas também.

Ou seja, quando uma empresa de coleta e tratamento de dados vende as informações (com base no opt-in do usuário), não há qualquer comprometimento em manter estes dados atualizados naquilo que pode definir um sujeito.

Sem contar no passivo histórico das redes sociais e da internet como um todo que coletaram dados indiscriminadamente sem se darem conta do nível de criticidade que tal conduta teria.

Em um dos momentos mais emblemáticos sobre o tema de privacidade, Edward Snowden revelou um esquema de vigilância estruturado pelo governo estadunidense que desanuviou não apenas a questão governamental, mas também a relação que empresas mantinham com o Estado para a troca de informações e, ainda mais além, como que os indivíduos seguiam, e seguem, vulneráveis à vigilância infotécnica.

The Snowden documents created a situation of rule overlap between security and commercial data regulations. Social media and internet service providers found themselves trapped between the legal requirements of commercial data sharing, which limited the onward transfer of data to outside organizations, and the intelligence community, which increasingly demanded access to massive amounts of data. (FARRELL; NEWMAN, 2019, p. 126)

Empresas e Estados seguiram no impasse regulatórios com implicações comerciais, macro e micro econômicas e, além disso, políticas.

Outro ponto ainda mais crítico são os casos de roubo de dados ou mineração de dados com base em arquivos tornados públicos.

Isso significa que ao consolidar muitos dados sobre uma pessoa em um único lugar, em uma empresa, em uma base de dados, aumentam-se as chances de estes dados serem cada vez mais sensíveis, e ao serem roubados, abrem uma brecha muito grande sobre como interferir na vida íntima das pessoas, assediando sua mente com artifícios focados em seu modo de tomada de decisão não mais de um modo genérico, mas de modo peculiar e altamente focado indivíduo a indivíduo.

A privacidade, nestes casos, pode ser violada de muitas formas distintas, em todos os outros espectros, tanto nos níveis físicos quanto, e mais importante ainda, nos níveis do pensamento, da autodeterminação e decisional.

Este tipo de direito tutelado pelo Estado também aparece na Lei Geral de Proteção de Dados brasileira, em seu artigo 18, inciso III, trazendo a garantia de que o titular do dado tem o direito de proceder com a correção de dado indevido, incompleto ou desatualizado nas bases do controlador, estando em foco a veracidade ou plausibilidade do dado.

Mas para que apenas este direito seja exercido de modo eficiente, ou seja, com celeridade, sem questionar neste momento se ele é efetivo, eficaz, já é possível esbarrar na questão da literacia não apenas digital, mas social em nível complexo da cibercultura.

Presumir que o brasileiro médio saberá compreender os relatórios de empresas de tratamento de dados e, além de tudo, ter visão holística que lhe permita compreender como tais informações duvidosas poderiam comprometer imediata e mediamente sua vida, sendo que grande parte dos algoritmos segue protegida por segredos de patente, é exigir de um cidadão comum que seja capaz de agir de modo consciente para se apresentar de modo intencional e legítimo a um algoritmo de crédito, de engenharia social com as chamadas redes sociais digitais e possa interferir contundentemente em seus resultados.

[...] we face the possibility of becoming an even more stratified society based on unequal access to information, with the result that individuals involuntarily live in glass houses while the external walls of large organizations are one-way mirrors. In short, there almost always seems to be a gap between the capabilities of the new surveillance technologies and cultural, legal, and technical responses. (MARX, 2016, p. 321)

Sem uma literacia básica sobre como as plataformas de crédito funcionam, como confrontá-la de modo apropriado e efetivo? Sem compreender o impacto que cada algoritmo de plataformas socio-digitais oferece, como apresentar contestação?

Tal relação de forças está desbalanceada tanto pela capacidade escópica das organizações e governos contra uma população quanto na capacidade de articulação dos entes econômicos quando comparados com o nível de literacia digital dos povos observados, e este desnível segue sustentado também pelas brechas e inobservâncias jurídicas.

A dificuldade de mensurar a capacidade que cada plataforma digital tem de interferir na vida de cada pessoa é substrato para a indefinição dos limites e dos freios e contrapesos não apenas legais, no sentido positivo do texto jurídico, mas também os limites morais, ao passo que não é possível apenas sedimentar sobre um texto jurídico algo tão crucial sem que isso precise estar arraigado na cultura de um povo. Assim, apenas leis não são suficientes como medidas protetivas, ainda mais em uma relação de forças desiguais pela qual cede com o tempo o indivíduo.

Cria-se o pretexto de oferecer ao usuário uma forma de retificar seu dado e, com isso, sustenta-se a falsa impressão de transparência dos coletores e tratadores de dados frente aos seus objetos.

Este pressuposto de que os dados poderão de fato ser consultados para, em seguida, passarem pelo crivo da veracidade do indivíduo é ponto axiomático, permitindo ver ou o caráter espetacular da legislação, ou sua ingenuidade.

Além disso, partindo do opt-in do usuário, muito pode ser feito. Mas pouco se considera sobre esta opção. Contratos de adesão, ou seja, os tipos de cláusulas que exigem aceitação plena e irrestrita do que uma parte propõe sem a capacidade de ajustes, fazem com que a opção seja categórica. Ou o indivíduo aceita tal contrato, ou o rejeita.

Mas como rejeitar todos os contratos de serviços digitais baseados em termos inalteráveis por parte do indivíduo?

Tais contratos, uma vez que estão autorizados pela infraestrutura legal, permitem que as organizações coletem os dados e tratem para, em seguida, simular uma proteção jurídica através da capacidade de retificação da informação e do seu tratamento.

Uma vez que parte do que cada algoritmo produz está sob a proteção do direito à propriedade intelectual e de patentes, mesmo que algumas características, classificações genéricas e dados brutos sejam apresentados, os resultados mais complexos e aprofundados dos actantes algorítmicos, mercadológicos e políticos seguirão em sigilo, tornando pouco relevante ou praticamente inefetivo o direito à retificação do dado pessoal.

De forma ainda indireta, apenas a CCPA, dentre as legislações avaliadas, possui mais clara defesa contra os assédios e discriminações que o mercado pratica para forçar o cidadão médio a liberar seus dados. Porém, uma vez mais, é muito importante destacar que a CCPA está protegendo o consumidor, não o indivíduo social.

Ou seja, aplica-se em casos de transações comerciais, como clubes de descontos que dependem do fornecimento de dados pessoais, mudança de preços dos seguros de acordo com o perfil de compras de cada pessoa, criação de score para empréstimos de acordo com fatores extraeconômicos, como etnia, religião, peso, local de residência etc.

Faz-se necessário destacar que, mesmo objetivando proteger o consumidor, como efeito colateral, há uma proteção parcial do sujeito, extremamente necessária tendo em vista a dinâmica mercadológica atual.

Ao proibir o assédio econômico em troca da privacidade dos clientes, protege-se o sujeito através do direito do consumidor.

Por outro lado, uma vez que a proteção é comercial, as sanções se tornam majoritariamente econômicas, dificilmente invadindo a área civil e criminal.

Um caso emblemático em teste prático se dá com o Sistema de Créditos Sociais Chinês, que busca fazer o que o governo local chamou de coerção positiva, que seria premiar e valorizar as pessoas que tivessem condutas tidas como positivas, favoráveis e aceitáveis.

Mas isso posto lado a lado com o CCPA, fica claro que um benefício a um grupo em detrimento de outro é, em si, punição ao mesmo tempo.

Assim como no Brasil tem se tornado comum oferecer descontos em medicamentos nos caixas de farmácias em troca do CPF do comprador, o mesmo se

dá com o pretexto positivo da premiação na China e que, claro, possui seu aspecto negativo. Apenas para referenciar o que está em andamento, tem-se que:

The Chinese program offers continuous data through networked CCTV cameras, remote monitoring of computers, digital voice recognition technology that identifies phone callers, and a Great Firewall capable of tracking and blocking Internet use. The system uses a photo ID card for identifying location and movement. Facial image and other biometric data, along with information such as residence and work history, are included in scannable electronic chips. When fully implemented, Golden Shield is expected to have data on each of the 1.3 billion people in China. (MARX, 2016, p. 3)

Ocorre que as farmácias podem se abastecer da vigilância da chamada Nota Fiscal Paulista para alimentar seus bancos de dados. Em outras palavras, a legislação brasileira ainda não está olhando para alguns pontos importantes relacionados ao direito ao esquecimento e à privacidade, na medida em que deixa para a promotoria pública a função de provocar a justiça em busca de impedimentos para práticas tidas como abusivas.

Caso a CCPA fosse aplicada no exemplo acima, os descontos deveriam ser ofertados a todos indiscriminadamente.

Imagine uma pessoa com poucas condições financeiras e com uma doença sexualmente transmissível que gostaria de manter sigilo sobre sua condição, não apenas mas justamente por saber dos estigmas que carrega em uma sociedade preconceituosa.

Caso ela decida comprar alguns medicamentos na farmácia, usando a receita, sabe que seu nome estará em algum momento em um banco de dados médico, mas imagina que este é o limite da informação.

Ao chegar no caixa, quando o atendente diz que verificará se tem desconto vinculado ao seu CPF, passa a ficar claro que ao invés de um desconto de R\$30 ou R\$40 por fazer parte de uma lista de pessoas selecionadas para o benefício, o que está se fazendo é cobrar R\$40 pelo anonimato, indicando exatamente quanto as empresa estão dispostas a pagar para saber da condição clínica de alguém.

Mas R\$40, neste exemplo, não é o valor que este dado tem. Apenas o que se aceita pagar.

O valor é muito maior. O lucro esperado com esta informação é muito maior. Mas ele vem de fontes múltiplas, descentralizadas, na venda de informação a diversas plataformas, empresas, seguradoras.

Se lembrarmos que a CCPA também está condicionada à inalienabilidade da privacidade, compreendemos que mesmo que deseje, o indivíduo pode ter barreiras intencionalmente construídas pelo Estado para entregar seus dados pela barganha de R\$40 em uma boca de caixa, caso a CCPA gere desdobramentos funcionais para a proteção da privacidade.

A legislação mundial, em grande medida, oferece proibições e remédios jurídicos, mas em poucos casos indica com tamanho peso o valor que a privacidade tem na formação e constituição das sociedades.

No caso da LGPD brasileira, a questão de tomada de vantagem econômica está nos casos de remedeio, indicados no Art. 11, II, § 3. Ainda assim, não está especificado o que vem a ser tal objetivo de obter vantagem econômica.

Também não está descrito na LGPD qual nível poderá ser atingido pelo poder público no escrutínio da execução legítima das práticas comerciais quando os casos se mostram suspeitos.

Há, assim, limite da atuação legal que segue tutelado pela proteção não mais do consumidor, neste caso, mas do segredo comercial e industrial.

Em outras palavras, novamente o direito à privacidade se mostra um direito com contornos econômicos ao invés de contornos sociais.

Da mesma forma, grande parte das penalidades, seja na legislação brasileira, seja na legislação mundial, está vinculada a remédios financeiros com multa, reforçando uma visão monetarista, enquanto as violências nos níveis sociais são de modo muito breve tocadas e sem uma resposta social à altura, como a reclusão e a prestação de serviços sociais.

O resumo, então, é que se estabelece entre a privacidade e o direito uma linguagem econômica em sua conclusão, no sentido de que os encaminhamentos se voltam para prejuízos na ordem financeira tanto para quem teve sua privacidade violada quanto para as empresas que incorrem nos crimes.

As prisões por vazamento de dados ocorrem no mercado financeiro, sobre segredos de Estado e na seara militar. O vazamento de dados em massa é tratado não apenas pela justiça, mas muitas vezes pela mídia, como um problema de imagem das empresas, de confiança e de qualidade tecnológica.

De um modo muito rápido, as diversas informações sobre compartilhamento indevido de dados e vazamento, após ataques de *hackers*, por exemplo, foram sendo normalizadas na medida em que os escândalos midiáticos não foram refletidos em penas mais incisivas e processos profícuos.

Parte da corrosão do debate sobre privacidade em espaços públicos se dá por encaminhamentos enganosos da opinião pública, não apenas na esfera global ou com multinacionais, mas também em escalas menores.

Um exemplo a ser citado da desinformação sistêmica que gravita o tema da privacidade é a lei municipal paulistana 13.541, de 24 de março de 2003, que obriga os estabelecimentos com sistemas de gravação de imagens afixarem placas com os dizeres "O ambiente está sendo filmado. As imagens gravadas são confidenciais e protegidas, nos termos da lei".

Ocorre que a lei 13.541 dispõe apenas, e exclusivamente, sobre a obrigação de fixar a placa. Já a lei que protege e torna confidenciais as imagens gravadas não existe.

Ou seja, a própria municipalidade cria condições para que a privacidade seja tratada de modo leviano.

É possível, então, para as pessoas que tiverem suas imagens gravadas por estes sistemas, e vazadas, ou utilizadas de modo danoso, entrar com processo judicial pedindo reparação por danos de imagem. Novamente, remédio jurídico.

Não há um dispositivo que fiscalize de modo ativo a forma como a privacidade e a imagem das pessoas estão sendo tratadas.

Retomando o caso da Lei Geral de Proteção de Dados (LGPD) brasileira, Lei nº 13.709 de 2018, sua fiscalização se dará através do órgão chamado de Autoridade Nacional de Proteção de Dados, ou ANPD. Tendo sua criação originalmente sendo prevista na própria LGPD como sendo parte do poder legislativo, sua real criação se deu com a medida provisória nº 869, de 27 de dezembro de 2018, do então presidente

Michel Temer, alocando sua existência no poder executivo, tendo sido sancionada pelo atual presidente, através da Lei nº 13.853, de 8 julho de 2019.

A confusão no aninhamento da ANPD dentro do legislativo, com vício de função, e não no executivo, como deveria ser mostra que mesmo entre o legislativo a questão sobre qual papel uma Autoridade vinculada à privacidade deva ter.

Além disso, destaca-se o fato de que sua criação oficial ser extremamente recente e em seu escopo haver uma diversidade de formas de agir na sociedade.

Ocorre que um assunto de tal envergadura que trata tanto da fiscalização quanto da auditoria e processos formativos e educativos da sociedade com relação à privacidade e o uso de dados de modo amplo ainda está sendo tratado com tema pequeno.

O princípio da eficiência do Estado está sendo aplicado de modo indevido, na medida que a ANPD está sendo constituída, estruturalmente, sem um orçamento específico e autônomo.

Um dos exemplos mais relevantes sobre a precariedade da infraestrutura do executivo para cuidar dos crimes vinculados a privacidade no âmbito digital é que no país ainda há menos de 20 delegacias especializadas em crimes cibernéticos.

Em tese, qualquer delegacia pode receber denúncias e queixas-crime sobre crimes virtuais, mas apenas nas capitais há infraestrutura dedicada a compreender o crime cibernético de forma aprofundada.

Ao mesmo tempo, não se tem notícia de uma entidade que centralize ou preste suporte às delegacias comuns na investigação de crimes cibernéticos.

De certo modo, quando a estrutura coercitiva do Estado não apresenta formas estruturadas para a busca de remédios legais, parte da mensagem que se passa é também de leniência e de letargia na aplicabilidade da lei.

Poucas são as notícias na mídia que narram crimes cibernéticos, e raras são as manifestações de busca de direito por crime contra a privacidade e intimidade.

Este silêncio midiático acaba por ocultar os crimes, além da dificuldade de denúncia e apuração reduzirem o número de registros.

Caso a população não perceba que é possível recorrer à justiça e à polícia em casos assim, a lei seguirá para casos extremos, normalizando casos intermediários.

Novamente, a lei comercial, a proteção do consumidor pode ser mais forte do que a proteção do indivíduo em si.

A ANPD ainda está em formação, mesmo já tendo meses de sua criação legal, não conseguindo ainda sequer produzir conteúdos educativos antes de ter uma estrutura de fiscalização e propositura de contendas jurídicas.

Sob a gestão da Serpro, empresa pública de processamento de dados, a ANPD ainda apresenta conteúdos muito básicos no site que pouco orientam sobre a aplicação futura e, principalmente, carece de material que sirva de base para que o cidadão comum compreenda a importância da LGPD, sua aplicabilidade no cotidiano e suas formas de agir desde já para evitar que seus dados sejam coletados de modo indevido.

Como mencionado anteriormente, a Serpro ratifica que a legislação brasileira tem sua inspiração no modelo europeu e indica o Brasil como país com autoridade nacional e leis estabelecidas de proteção de dados pessoais, mesmo sabendo que a lei ainda não está em vigor.

Mais sérios ainda são os atos protelatórios para que a LGPD entre em vigor no país.

Tendo mudado diversas vezes, a data final ainda está sob risco.

Até o presente momento, a LGPD deve entrar em vigor em agosto de 2020, porém já tramita no Congresso Nacional o Projeto de lei 5762, de 2019, que prorroga a entrada da Lei em vigor por mais dois anos, levando para agosto de 2022 o início das atividades práticas de fiscalização da ANPD.

Tal Projeto de Lei foi apresentado pelo deputado federal Carlos Bezerra, trazendo em seu texto a declaração de que nem as empresas nem o poder público está preparado para a atuação da LGPD, como se vê abaixo.

Embora os benefícios advindos da LGPD sejam inquestionáveis, é necessário tecer algumas considerações sobre a sua implementação prática. Isso porque a nova lei estabeleceu, como marco inicial de vigência dos seus dispositivos mais relevantes, o mês de agosto de 2020. Ocorre que, hoje, é pouco mais de dez meses da entrada em vigor da LGPD, apenas uma pequena parcela das empresas brasileiras iniciou o processo de adaptação ao novo cenário jurídico. [...]

Soma-se a tudo isso a morosidade do Poder Público na instalação da Autoridade Nacional de Proteção de Dados – ANPD, instituição que será responsável por editar os regulamentos e procedimentos sobre proteção de dados pessoais e privacidade, que servirão de norte para balizar as ações das empresas de adequação à LGPD. Ainda que a Autoridade seja instalada com a maior brevidade possível – cenário que não nos parece provável, decerto não haverá tempo hábil até agosto de 2020 para que todas as propostas de regulamentação sobre a matéria sejam discutidas pela sociedade e aprovadas pelo órgão. (BRASIL II, 2019)

É imperativo notar que os argumentos protegem primeiramente as empresas, que ainda não se adequaram, mesmo sabendo do vigor da lei, e em segunda instância, o próprio poder público que não se estruturou para fazer valer os próprios atos legais.

O cidadão comum que deve ser protegido pelo Estado e pela lei mal é citado no projeto de lei.

Da mesma forma, é importante perceber o aspecto realmente protelatório na medida que tal projeto fala apenas de dilação de prazo sem mencionar ou propor, em sua modificação da LGPD, qualquer ato punitivo para o próprio poder público, seja através de seus órgãos, seja na pessoa de seus gestores, no caso de nova incapacidade de aplicação da LGPD até o novo prazo estipulado.

Também não pretende ajustar o provimento de recursos ou nortear as fases de implementação.

Novamente, apenas estende o prazo com o argumento inicial de que as grandes empresas não conseguiram se preparar satisfatoriamente.

Ao compreender o sopeso da lei, na estrutura primordial do direito, tem-se que leis sobrepostas que determinam atos distintos precisarão ser colocadas lado a lado para compreender qual valor ambas protegem, e restará válida a normatização daquela que no caso de questão de lei ou questão de direito preservar o valor mais importante.

De forma heterodoxa, como exercício provocativo deste trabalho, apresenta-se lado a lado a LGPD e qualquer lei que puna o machismo, o feminicídio, o tráfico de drogas.

É possível imaginar um Projeto de Lei que peça aumento de prazo para o vigor de uma lei que intensifique as restrições sobre tráfico de drogas uma vez que os traficantes ainda não tiveram tempo de se adequar às normas mais severas?

Claro que este exemplo é completamente extremo, mas justamente por seu exagero permite compreender como tal projeto se mostra descabido, mantendo em vulnerabilidade o cidadão comum ante um interesse comercial.

A letargia do Estado não pode nem deve ser normalizada e, muito menos, ser pretexto para manter a exposição do cidadão aos riscos de invasão da privacidade.

Isto se torna ainda mais sensível na medida em que cada dado capturado pode ser mantido em centenas de servidores ao redor do mundo.

Ou seja, cada dia que se passa sem uma legislação efetiva, com métodos robustos de avaliação pela ANPD para conter crimes, torna a exposição potencialmente mais nociva.

Enquanto a Europa já dá passos sobre a questão da privacidade há décadas, consolidando recentemente na GDPR as leis que comuns a todos os países-membros, no Brasil a estrutura legislativa e executiva ainda age em leniência.

Por outro lado, o Senado Federal, meses antes do PL 5762/19 já havia apresentado um Projeto de Emenda à Constituição (PEC) que torna mais evidente e clara a proteção da privacidade também através de comunicação e dados digitais.

Art. 1º O inciso XII do art. 5º da Constituição Federal passa a vigorar com a seguinte redação:

Art. 5º [...] XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal, bem como é assegurado, nos termos da lei, o direito à proteção dos dados pessoais, inclusive nos meios digitais; [...]” (NR)

Art. 2º O caput do art. 22 da Constituição Federal passa a vigorar acrescido do seguinte inciso XXX:

Art. 22. [...] XXX – proteção e tratamento de dados pessoais. [...]” (NR) (BRASIL, 2019)

Este tipo de PEC é de extrema relevância na medida que torna evidente que a comunicação digital também está protegida legalmente de modo positivado em letras claras.

Por muito tempo a questão legal sobre comunicação digital caía em discussões infrutíferas sobre a natureza do que a constituição estava protegendo em seu Art. 5º sobre correspondências.

Em alguns casos, os tribunais se encontravam em extensas discussões se a coleta de e-mails e mensagens digitais era dado ou correspondência, claramente

limitando a compreensão de correspondência mencionada na constituição àquela postada nos correios.

Um sinal claro de subversão positivista que se dedica fortemente ao texto e não ao que cada lei busca proteger.

Como tal debate ainda segue sem pacificação, se mostra completamente necessária a positivação deste desdobramento de proteção da lei.

Outro ponto importante da proposta é que o Estado passa a ser o claro detentor da prerrogativa de ditar os limites da coleta de dados e de seu tratamento, devendo expressamente assumir, como tal, este posto ativo na definição dos limites de tais práticas.

De todo modo, a mudança poderia, da mesma forma que se indica acima, alterar a forma de provisionamento de recursos para fazer esta emenda se tornar vigente e efetiva.

Ainda assim, isso não tira a relevância da inserção destes ajustes no cerne da constituição, dando ao tema a relevância primordial.

Note-se que tal projeto fora apresentado pelo Senado, o que significa que é uma proposta liderada pelos representantes legislativos dos Estados Federativos, em contraste com os atos protelatórios da Câmara dos Deputados Federais, que representa legislativamente os cidadãos.

Peculiar que os representantes do povo, que deve ser protegido pela LGPD, estejam avaliando como alargar os prazos em benefício do mercado que, mesmo sabendo da chegada da lei, não se preparou do modo devido, e os representantes dos Estados Federativos seguem o caminho da proteção dentro do campo mais precioso do sistema positivo-legal que é a Constituição Federal, a fim de limitar no topo os abusos e relegar aos Estados, então, arbitrariedades menores sobre a prática não tratada na Carta Magna.

Para os fins de provocação deste trabalho, destaca-se mais um ponto relevante.

A atuação dos representantes legislativos dos estados que tomam o espaço não ocupado tanto pelos representantes populares na esfera federal quanto das demais forças de pressão da opinião pública.

Além da visão sobre os textos legais apresentados, é necessário retomar o Contrato para a Web (BERNERS-LEE, 2019) como carta propositiva de relevo, não apenas pelo peso de seu criador, mas também pela relevância das empresas signatárias no cenário infotécnico.

Considere-se, todavia, que mesmo sendo as empresas signatárias praticamente a grande parte do oligopólio na bolsa de valores, no cenário global, não basta estas empresas, sozinhas, praticarem a ética informacional com foco na preservação da individualidade e da identidade das pessoas se as microempresas seguirem com práticas escusas. Como pequenos vírus, podem se tornar capazes de fazer ruir a privacidade com ataques tão pequenos e silenciosos que, somados, multiplicados, poderão correr os limites do que é privativo e ainda forçar mercadologicamente empresas maiores a se posicionarem de modo mais flexível, e assim, mais intrusivo quanto à privacidade.

Os itens de privacidade do Contrato também são tríplices, com foco em garantir que as pessoas possam usar a internet de modo livre, seguro e sem receios.

Para tanto, o primeiro item busca estabelecer e reforçar os protocolos e estruturas de proteção de dados de modo compreensível.

Esta última palavra é realmente importante. Compreensível.

Neste instante percebe-se que Berners-Lee (2019) não está apenas preocupado com o objeto, a privacidade em si, e com o momento atual. A compreensibilidade das leis e das iniciativas é um modo de envolver os diversos públicos no debate, nas atividades, na concretização das implementações e também na defesa atual e futura da rede.

Não há, nas propostas de Berners-Lee (2019) uma conduta única ou um público mais importante na atuação do que outro.

O autor e seus colaboradores apresentam a necessidade de proteção por todos os setores, e isso inclui o governo, dos direitos fundamentais da pessoa humana. Mas aqui lidam com o direito a privacidade como se ele fosse um fato na sociedade contemporânea.

Isso pode parecer lógico dentro de um pensamento humanista, mas não necessariamente é uma realidade positivada no direito de todos os países, como visto anteriormente.

Assim, muitos países podem defender legalmente um tipo de privacidade enquanto invadem os outros. O mercado pode narrar proteções em respeito às normas legais, mas usar as brechas para seduzir e convencer as pessoas para a prática e-vasiva.

Dentro da proposta, Berners-Lee (2019) vai dizer que a proteção de dados precisa se aplicar tanto aos dados pessoais que foram providos, ou seja, informados pela própria pessoa, quanto sobre dados observados pelas entidades, quanto sobre os dados inferidos.

As três esferas da coleta de dados estão sob a mira não apenas do autor e seus colegas, mas de muitos movimentos vinculados à privacidade.

Além disso, a proporcionalidade dos pedidos de dados entra em questão.

Isso significa que pedidos de dados feitos na justiça não devem ultrapassar a proporcionalidade do que se investiga, muito menos servir de modo de ameaça e coerção, entendendo que o simples fato de pedir na justiça informações de foro íntimo, ou que avancem sobre áreas da vida privada que não coadunam com o objeto da ação pode ser uma forma de fazer com que um investigado acabe, por pressão, produzindo provas contra si ou outrem em receio do poder de invasão e violência contra si ou contra pessoas de seu convívio íntimo.

A petição, então, por si só serviria como forma de intimidação para a condução de investigações, tornando-se instrumento de vício processual.

Além disso, o escrutínio estatal da vida individual pode ser uma forma de buscar pontos vulneráveis que, da mesma forma, podem infligir ao indivíduo sofrimentos em diversos âmbitos da vida social.

Por fim, a tríade se completa com o suporte ativo do estado à privacidade, coletando e limitando a coleta de dados ao crivo da pertinência, relevância e interesse público claramente específico.

Ou seja, a coleta indiscriminada e compulsória acaba por se mostrar uma forma de exposição e (auto)censura de modo geral.

Requer, além disso, que os contratos de concessão, venda, compartilhamento de dados sejam tornados sempre públicos, além de exigir que toda quebra de segurança de dados seja publicamente reportada para que as pessoas tomem não apenas conhecimento, mas atitudes sobre a sua proteção e dos interesses públicos, sendo que aqui se aplica a mesma inocência sobre a transparência dos dados corporativos em comparação à proteção da privacidade dos indivíduos.

E dentro do aspecto penal e, com impactos também econômicos, está a proposta de que os estados garantam que qualquer pessoa tenha meios para agir contra os entes que lhe causaram dano ou invasão de sua privacidade, fator que torna sua proposta um pouco mais consistente do que os outros chamados para a construção de uma rede mais respeitosa e que fortalece os valores sociais, tais como a privacidade.

Este aspecto reclama a construção de estruturas acessíveis de requerimento e de contenda judicial, se for o caso, para remediar o mal impetrado e impedir sua perpetuidade. Contudo, a intimidade exposta dificilmente terá um remédio pleno, que solucione os impactos de modo saudável.

Faz, então, claro que as estruturas preventivas são importantes e demandam provisionamento tanto para a construção de tais caminhos de salvaguarda quanto para auditar o mercado.

Findo o pilar de privacidade pela ótica governamental, os autores propõe o 5º princípio que convida as empresas a respeitarem e protegerem a privacidade e os dados pessoais, a fim de construir a confiança no “online”, permitindo que as pessoas estejam no controle de suas vidas online, empoderando-as através de escolhas claras e significativas sobre seus dados e privacidade.

Aqui, no quinto pilar, percebe-se um ponto de risco do Contrato proposto por Berners-Lee (2019) e seus colaboradores, que é a percepção de que a privacidade evadida no digital tem impacto nas vidas online, reduzindo a complexidade de seus impactos *onlife* (FLORIDI, 2015).

De toda forma, é necessário ler o Contrato com a ressalva de que seus itens precisam ter impactos maiores do que apenas os digitais.

A proposta central é permitir que as pessoas, de modo intuitivo e acionável, saibam como tomar para si a gestão dos dados que são conhecidos sobre si através de painéis de controle que sejam de fácil compreensão e uso.

Aqui aparece um novo ponto sensível, de certa forma talvez um pouco inocente, na medida em que o convite é feito para que cada empresa permita a edição e exclusão dos dados por parte do indivíduo, porém em termos práticos, pode ser uma tarefa de difícil execução para uma pessoa comum, gerir dezenas de plataformas de conteúdo de coleta de dados.

Em um exercício prático de inteligência, basta pensar na dificuldade que seria descobrir quais plataformas possuem informações pessoais e-vadidas, descobrir o caminho para edição, dedicar tempo para a leitura, compreensão dos dados e tomada de decisão sobre quais devem seguir ativos, quais devem ser desconsiderados.

Cada rede pode ter múltiplas formas de replicar o dado, sem que necessariamente estejam sendo propostas formas de vincular a edição dos dados de acordo com a rede coletora.

Ou seja, a partir do momento em que uma rede replicou os dados de um indivíduo, mesmo de forma legal, após o opt-in, não há hoje uma forma de registro padronizada que deixe gravado no metadado a sua origem, seu momento de coleta, seu ID único e universal.

Assim, editar um dado que foi coletado pela rede A, mas encaminhado legalmente para as redes B, C e D, e que foram replicadas em redes secundárias B1, B2, B3, C1, C2 e assim sucessivamente, pode se tornar uma tarefa humanamente impossível.

De forma mais prática, cria-se o mercado do esquecimento, com terreno fértil para plataformas de exclusão de conteúdo em massa da internet com base em logins e *browser cookies*.

Para ser ter alguns exemplos, o site justdeleteme.org aponta mais de 70 sites nos quais é praticamente impossível ter apagados os dados coletados.

Entre os mais relevantes hoje em dia estão Youtube, Pinterest, Picassa, PlayStation Network, Netflix, League of Legends e Starbucks.

Os pretextos são diversos.

A Netflix, por exemplo, guarda os dados do usuário com o pretexto de que em dado momento o cliente pode decidir voltar a assinar o serviço de streaming e quererá ter seu perfil de recomendações ativo.

Já para deletar as informações do Youtube, é preciso deletar todas as contas vinculadas, como Google+, Gmail e afins.

Alguns casos chegam a chamar a atenção, como o da Starbucks.

É como se o seu café te perseguisse, mas de modo mais forte. A informação salva não é simplesmente se uma pessoa toma café ou não, mas que tipo de gosto ela tem de modo geral.

Por qual motivo uma pessoa não pode ter esquecidas todas as suas canecas de café e *brownies* consumidos dois anos atrás?

Já o Pinterest apenas oculta os pins e murais, mas somente isso.

Tudo continua lá. Apenas não está mais visível para os leigos, para os visitantes.

Mas o administrador ainda é capaz de enxergar o histórico e as conexões feitas ao longo do uso da conta.

Com tantas dificuldades, sites como o justdeleteme.com prometem varrer a internet em busca de rastros dos seus contratantes e deletá-los por pacotes que começam com o custo mensal de US\$ 10,75, que significa mais de R\$500 por ano para uma pessoa ter sua vida minimamente fora dos principais bancos de dados de modo mais automatizado.

Mas ao unir esta promessa com as informações anteriores de dificuldade de apagar informações do Youtube, League of Legends e afins, é possível perceber que o serviço de tais sites como o Justdeleteme.com atinge apenas a camada superficial da busca na internet.

Não há caminhos simplificados nem estruturados para reduzir a e-vasão de dados de modo sistematizado.

Outro ponto que o Contrato de Berners-Lee (2019) trata é da portabilidade dos dados que ainda é um princípio, e que já aparece em muitas legislações, porém como conduta prática ainda tem muitos pontos técnicos a serem resolvidos no sentido de

haver uma padronização taxonômica que dê conta de categorizar os tesouros de forma que diversas plataformas possam consumir estes dados facilmente e consiga produzir resultados relevantes para o cliente/usuário a partir dos dados portados e tratados.

De certa forma, a portabilidade ainda trata mais da possibilidade de receber o compêndio de dados e-vadidos, observados e inferidos, mas não significa ainda a possibilidade de torna-los úteis de acordo com o interesse do portador.

Desta forma, portabilidade ainda é uma proposta de intensões e perspectivas futuras, mas sem que ainda se materializa de modo distinto, através da possibilidade de requerer os dados e recebe-los sem danos ou alterações conforme o que é utilizado pelas redes.

Ainda aqui segue o mesmo questionamento já feito em outros momentos que trata da possibilidade de requerer, de fato, os dados e-vadidos e observados, mas nem todos os dados inferidos estão disponíveis, uma vez que não há formas de auditar a entrega dos dados, que estão protegidos pelo direito à propriedade intelectual, que impede o escrutínio dos algoritmos para compreender todos os resultados derivados de sua ação sobre os dados.

Além disso, os requerimentos entregam uma base datada, limitada ao tempo do requerimento, mas tais arquivos não são automaticamente atualizados com alertas de novas inferências feitas com base nos dados solicitados.

Isso significa que a partir do momento que um dado foi entregue, o pedido do cliente/cidadão foi atendido. Mas se duas semanas depois o dado que foi entregue servir de base para novas inferências, não há obrigatoriedade por parte da empresa em apresentar tais dados para o requerente.

Fica no campo das deliberações das empresas manter padrões de diálogo enquanto o estado não está convidado a legislar sobre as questões técnicas das relações infotécnicas.

Está também no quinto pilar o convite às empresa que ofereçam explicações claras sobre o uso dos dados, mas antes disso, nos pilares governamentais, não se fala em estratégias educacionais que desenvolva uma literacia baseada nas integrações de dados e na compreensão sobre os impactos possíveis no uso dos dados para e-vadir os diversos tipos de privacidade.

O processo educacional parece muitas vezes estar subentendido com a disponibilidade da informação, como se a disponibilidade dos ingredientes numa prateleira de supermercado fosse suficiente para resultar em um prato de alta gastronomia.

Sem o processo educacional, todo resultado é possível, ao acaso.

Desde a rara conquista do prato bem executado até a completa inanição por afasia. Extremos que dificilmente seriam vistos, mas que facilmente terão em seus arredores próximos cenários possíveis de acordo com certa bagagem casuística das pessoas que passam pela prateleira.

Da mesma forma, sem o processo educacional adequado quanto às questões da privacidade e das tecnologias de e-vasão, a completa consciência atuante segue em um extremo quase que impossível, oposta pela completa invasão transparente e indistinta. Nenhum dos casos parece factível, mas certos contornos próximos a estes extremos se mostram plenamente possíveis.

Convivendo nos mesmos recintos, não difícil será encontrar pessoas que se preocupem com a privacidade e pessoas que mal se questionaram qual é o valor que esta tem para suas vidas de modo mais aprofundado.

Qualquer resultado coletivo pode ser produto casuístico e ocasional, caso se considere a sociedade um fruto da panspermia, ou intencional e interessado caso se leve em conta a atuação das instituições para fomentar a e-vasão capital do eu-suporte, do eu-midiatizado, do eu-espetáculo, eu-artefato.

Many young adults experience some kind of alienation because of social media, but they are further alienated because they don't see a thriving public discussion about the struggles they are experiencing - perhaps because those struggles aren't as racy or extreme as the ones that are the stuff of newspaper and magazine headlines. Media coverage of social media often focuses only on the belief that this generation is the most narcissistic generation ever, or on the scariest examples of what happens to young people online - predatory behavior, risqué pictures that get circulated, and cyberbullying and related suicides. Clearly, these are important issues. But while young adults and college students buckling under the pressure to project a false self online may not be as sexy (literally) as teens sexting nude photos to each other, it's a pervasive struggle, and we need to talk about it with them. (FREITAS, 2017, p. 11)

O processo educacional é a camada necessária para que mais do que dromoapto, o indivíduo contemporâneo tenha tal aptidão não apenas no campo da performance estética da mídia, mas no processo de literacia que leva a um uso com

objetivos mais complexos dos meios de comunicação, além da tomada de consciência sobre a vigilância e seus impactos presentes e futuros.

Através da literacia integral, *onlife* (FLORIDI, 2016), torna-se possível articular a transformação dos artefatos de vigilância de modo mais consciente, além de buscar formas de dirimir as questões em torno das tecnologias sem apelos para a dicotomia segurança e violência.

É também por este caminho que passam os debates que provocarão mudanças atitudinais que tocam todos os entes do Contrato proposto por Berners-Lee (2019), sejam governos, empresas e cidadãos comuns.

Ineficaz tratar apenas do conceito transformado, transmutado da privacidade sem descer para as condutas práticas da sociedade.

Da mesma forma, apenas intervir direta e arbitrariamente na sociedade sem antes construir um significado compartilhado sobre o papel da privacidade na vida das pessoas individualmente, e também do seu papel na manutenção e evolução dos princípios democráticos pode ser uma via infrutífera.

Ambas as atuações precisam se dar de modo conjunto, assim como o contrato pede a articulação triádica de governos, empresas e sociedade civil, o redesenho dos limites da privacidade, seu papel e valor na sociedade só podem ser constituídos de modo robusto através da inteligência, do debate sobre qual sociedade está em construção, bem como através de ações práticas, diretas.

These humanistic concerns are inseparable from technical advancement, and a new 4IR curriculum will need to reduce the divisions between humanities [...] to create a more integrated system of education which can explore the newly emerging conceptions of self and identity within the 4IR, including discussions of autonomy, free will, and genetic vs. social determinism. The changing nature of social relations and interactions—social media, obligations to identity groups, society, nation and world needs to be central in the 4IR curriculum as all of these identities and loyalties are shifting rapidly due to increased globalization. (PENPRASE, 2018, p. 222)

A quarta revolução industrial (4IR) está, pelas palavras de Penprase (2018) a exigir das universidades e do currículo uma postura distinta, menos fragmentada, não por modismo, mas pelas transformações da própria sociedade.

A educação então não está só a responder a, mas está inserida nas transformações, como produtora e produto.

Seguindo pelo pensamento de Penprase (2018) já não se trata de discutir se a educação se transformará, uma vez que tal transformação é um fato da contemporaneidade.

De toda forma, há de se lembrar que, com Trivinho (2007), a aceleração como fio condutor já estaria agindo constantemente como fator de mudança.

Ou seja, este não é um privilégio dos tempos atuais, mas característica estruturante e estrutural.

Não se trata necessariamente, assim, de uma mudança, mas de aceleração que acentua características que já estavam encubadas.

O Contrato de Berners-Lee (2019) pode parecer uma resposta centrada na internet e em seus impactos, mas a internet ainda que tenha um papel crucial para a vida contemporânea, não inventou a privacidade nos formatos que esta têm, mas teria, agora em uma leitura sobre a dromocracia cibercultural, mas acelerou a maturação de partes distintas de seu gérmen.

Com isso, o processo educacional não está por si só se tornando algo distinto, mas sim acaba por assumir e fortalecer aspectos já presentes em suas estruturas primordiais, da mesma forma que a privacidade não está sendo destruída para ser suplantada por algo completamente diferente, mas está a assumir uma forma que já existia dentro de si, ainda que em potência.

Desta forma, o que acaba por ser mais evidente, através do pensamento sobre a aceleração, sobre a dromocracia, é que as formas de manifestação da identidade na sociedade contemporânea podem parecer contraditórias, revolucionárias frente ao passado mais imediato, mas ao largo, não necessariamente estaríamos encarando uma cisão, pois se não o excesso de algo que já mostrava seus indícios.

INFOPODER E SUAS ARTICULAÇÕES

O poder normativo de outros tempos assume a forma do infopoder contemporâneo.

Significa dizer que a forma de construção, manutenção e atuação do poder está revestida e investida das articulações e movimentos dos dados. O dado, convertido em informação, é base crucial e constitutiva do poder que prevalece na sociedade com base na aceleração dos processo do poder, que já se utilizava de dados desde períodos históricos pregressos, mas que agora insere na cibercultura o desejo e-vasivo.

Desta forma, o infopoder mobiliza o imperativo transestético através da e-vasão e da demanda sobre a dromoaptidão e-vasiva.

Infopower is a mode of power in its own right in that it operates its own distinctive set of techniques that exercise distinctive operations of power on distinctive kinds of subjects. Infopower makes use of techniques of formatting in order to operate a fastening, canalizing, and accelerating that is targeted toward the many kinds of users, accounts, and records that we informational persons have become. (KOOPMAN, 2019, p. 172)

Tal Infopoder se torna normativo, ou seja, ele permeia a sociedade de modo que sua aplicação é parte da legitimação de forças a serem postas na dinâmica social.

É através do infopoder que os actantes se apresentam socialmente e é por ele que ocorrerão as disputas.

De certo modo, este infopoder é travestido de múltiplas formas, e poderá ser visto tanto na dromocracia cibercultural de Trivinho (2007) quanto no capitalismo transestético de Lipovestky e Serroy (2015).

Desta forma, o infopoder emanará da dromoaptidão das pessoas em produzirem movimentos de dados e artefatos virtualizados de sua conduta e identidade de modo transestético e performático que possam não apenas alimentar diretamente a esfera da infoeconomia mas também que sirva ao processo catequético de convencimento, sedução e internalização das instruções simbólicas.

In the same way that infopower is irreducible to other modes of power, so too the resistance calibrated to infopower is irreducible to mainstream theories of democratic deliberation that presuppose information in such a way that they cannot confront it as a political problematic in its own right. (KOOPMAN, 2019, p. 22)

É relevante compreender que este infopoder está, de certo modo, na mesma seara em que Bruno (2013) irá colocar a questão da vigilância atrelada às plataformas

de comunicação. Cada um com seu olhar específico, mas tratando de estruturas que se tocam nos bastidores do visível. Tanto que Koopman (2019) irá aventar o que chamou de ambivalência do infopoder através das injustiças políticas e avanços morais. Mas tal afirmação não se faz sem a tensão imanente. Os avanços morais que Koopman (2019) traz como referência deixam de lado o caráter axiomático sobre a moralidade do uso dos dados atrelados ao infopoder do que se pratica nos dias atuais, tornando os dilemas éticos e morais parte ainda não solucionada.

Para nutrir o infopoder é necessária uma estrutura complexa, mas que ao mesmo tempo precisa ser sutilizada e normalizada no cotidiano da cibercultura.

Declaradamente Koopman (2019) vai indicar que o infopoder não se trata de uma subclasse do poder prevalente, mas está acima, está condicionando as outras formas de aplicação e proliferação do poder.

Floridi (2014) vai apresentar o que chama de Ciclo da Informação contendo 7 etapas, que diagramaticamente são apresentadas em sequência cíclica, mas que ao ser compreendidas de modo mais aprofundado podem ser, e são, interconectadas.

A começar pela etapa de *ocorrência*, momento no qual o dado é criado, observado ou descoberto.

A questão é que nada é observado sem que haja um aparato preconcebido para o ato da observação. Aqui, ressalta-se o fato que observar é alterar o objeto. Ser capaz de perceber a existência não significa ser capaz de compreender sua totalidade, muito menos significa ser capaz de manter sua integralidade. Observar é reduzir, restringir, interferir.

Neste caso, o autor considera que a informação pode ser desenhada, pode ser criada. Construída para um fim específico. O processo artístico é um exemplo claro, mas esta etapa não se restringe a informações profundas e complexas. Cada ação, cada movimento é uma informação sendo criada.

A existência é uma constante criação de informação, é uma constante produção de dados que se retroalimentam, que se provocam.

Mais do que isolados, a esteira dos dados é o fluxo contínuo da vida.

Dentro da discussão do infopoder (KOOPMAN, 2019), combinada com Floridi (2014), é possível compreender que tal qual o poder emana dos atos sociais, o

infopoder também o é tal emanção. A distinção feita não é a formulação de um novo poder, mas o fortalecimento de suas características infotécnicas em suas manifestações contemporâneas.

Na medida que surge dos movimentos, são tais ações da vida humana e dos demais actantes, movimentações de dados que constituirão informação.

A segunda etapa proposta por Floridi (2014), intitulada coleta, é um ato duplo. O ato de perceber a informação e o ato de direcioná-la para um fim específico.

Por mais que pareça uma tarefa simples, não o é. Coletar informação é em si um ato de curadoria. Alguns podem compreender a curadoria como um processo posterior, mas em si, a coleta já é uma curadoria. Decidir coletar ou não algo é um filtro, ainda que todos os dados passem por um segundo filtro mais rigoroso a *posteriori*, tal processo de decisão, de escolha já começa a ser feito durante a coleta.

An agent is an autonomous entity, which has the ability to sense its environment through the use of its sensors, and acts on the environment through the use of its actuators. Agents are said to be reactive because they typically react to events detected by their sensors via actions through their actuators. Notice this description is quite general, it does not restrict the agent to being a software entity, which allows it to be closely aligned to similar concepts (the controller) within the realm of cybernetics. (SKILTON; HOVSEPIAN, 2018, p. 100)

Os dois autores destacam a autonomia dos agentes que reagem a um tipo de gatilho a partir de um evento pré-determinado. Aqui já é possível perceber que a autonomia, na realidade, significa que tais agentes não dependem de uma segunda ordem, além da ordem original e precedente que foi inserida em sua programação ou em seu processo de aprendizado como evento de coleta.

A coleta através destes agentes é, então, precedida por um interesse específico no processo de programação destes agentes para que sejam capazes de perceber exatamente os eventos necessários para seu propósito.

No caso de agentes de alerta, por exemplo, há o interesse que estes, ao protegerem uma casa, disparem um alerta apenas quando um invasor apareça e entre nos domínios da propriedade.

Mas por outro lado, não é o interesse de quem contrata este tipo de serviço que os alertas ocorram quando a família que realmente mora na casa está chegando ao final do dia, ou quando uma ave passe na frente das câmeras.

Ou seja, a coleta de dados pode ser constante para estes casos, mas será uma etapa futura, o tratamento da informação, que dirá se uma ação deve ser tomada por este agente ou não.

Já a gravação é parte extremamente sensível, na medida que parte do senso comum pode considerar que tal ato possa ser apenas uma impressão, um carimbo gravado em um papel que praticamente é passivo, apenas um suporte, apenas uma estrutura que recebe os dados.

Mas ainda que o papel possa ser considerado passivo, ele não o é. Sua existência conforma coletas que possam ser gravadas nele.

A escrita, que há muito consolida histórias, sons, contos e discursos, desenvolvida para ser armazenada em uma superfície, conforma estruturas lineares de pensamento, a temporalidade cíclica, permitindo uma visão causal do mundo.

De forma ainda mais profunda, quanto menos se percebe a importância e participação do suporte na conformação da informação, mais relevante é sua análise.

O digital, como suporte material da informação armazenada em bits eletrônicos, e a capacidade de processamento de dados, dão contornos ainda mais profundos para a virtualidade. Desta forma, a gravação carrega consigo não a curadoria do coletor, mas parte da curadoria de quem construiu as formas de gravação.

O desenho do sistema que guardará as informações pode gerar condições específicas que facilitam ou dificultam determinado tipo de gravação de dados.

Tal facilidade ou custo podem ser muito relevantes para criar barreiras na construção de uma memória de dados que seja mais abrangente.

Aqui Mayer-Schönberger (2009) se torna ainda mais relevante para dialogar com a etapa de gravação.

O autor vai tratar do custo do esquecimento nos dias atuais quando comparado ao custo da memória. Para ele, lembrar hoje é mais barato na medida que tirar fotos e gravar vídeos com os aparelhos celulares não é mais algo dificultoso. Já o processo de selecionar as fotos que devem permanecer nos celulares ou as que devem ser apagadas é custoso, demorado, cansativo. Com tanta memória nos aparelhos, é mais prático manter tudo que foi fotografado e um dia, quem sabe, decidir se algo deve ser apagado.

Porém, quando se considera a questão de Floridi (2014) de modo amplo, atrelada a Mayer-Schönberger (2009), adicionada à problematização trazida neste trabalho, compreende-se que os artefatos de memória apresentados por estes autores estão dados a partir dos aparatos de comunicação, vigilância e memória.

Em outras palavras, cada pessoa que decide documentar, gravar parte da sua história ou de seu dia não precisa, para tanto, reinventar formas de arquivamento, de gravação. Utiliza-se de artefatos já existentes que possuem linguagens próprias.

Assim, gravar é compreender a estrutura dos artefatos de memória, sua linguagem e condições.

Desta forma, gravar é, em si, conformar uma realidade a uma forma de materialização de sua memória.

Chega-se então à etapa de processamento. Etapa esta que tem contornos plásticos na medida que cada banco de dados, cada estrutura de memória pode passar por diversos tratamentos, sejam automáticos e pré-definidos, sejam rotinas humanas ou algorítmicas, que tem o potencial de converter tais dados em um acumulado de informações que resulta em narrativas diferentes sobre o fato duro que tais dados representam.

A camada de processamento é ainda mais crítica na medida que seu potencial de impacto na vida das pessoas, na vida da própria informação é pouco inteligível apenas observando o dado coletado e o resultado do processamento.

Difícilmente um indivíduo de conhecimentos médios na sociedade contemporânea terá sequer a percepção de que seus dados coletados estejam sendo tratados de modo que possa trazer benefícios a ele ou mesmo afetá-lo de modo negativo.

Assim, como já se tratou em outro momento, quanto menos se percebe uma característica dos meios de comunicação e vigilância, maiores seus impactos. Sem a visão clara dos processamentos executados sobre os dados, pouco se pode contrapor ou oferecer resistência.

Além disso, é possível fazer novo paralelo ao que propõe Mayer-Schönberger (2009) na medida em que este autor irá dizer que, diferentemente do passado, as bases de dados de hoje em dia são altamente replicáveis, a um custo barato. Ou seja,

na medida em que muitos actantes podem ter acesso à mesma base de dados, cada um deles pode aplicar dezenas, centenas de processos de tratamento de dados distintos, que converterão um dado cru em informação relevante para os seus interesses próprios.

No caso apresentado brevemente acima, com o exemplo prático de um sistema de vigilância, a coleta de imagens constante dos arredores da propriedade não fará distinção sobre quem está entrando ou saindo da casa. A coleta se dá compulsoriamente. É a etapa de processamento destes dados que indicará se a pessoa que está entrando na casa faz parte de um banco de dados registrado por seus moradores ou se é um intruso. É o algoritmo de tratamento do dado que evitará os alertas indevidos quando as câmeras captarem apenas algumas aves sobrevoando o quintal.

Deste ponto de vista, a coleta e o tratamento de dados trazem um benefício muito claro para a vida cotidiana das pessoas.

Claramente, por outro lado, um dos maiores temores das metodologias de tratamento de dados é que elas possam mostrar aquilo que o cientista de dados quer ver e não parte de uma realidade. Isso se torna crítico quando governos se tornam violentos e passam a agir contra seu povo por meio de dados coletados e tratados com o objetivo último de declarar quem são os dissidentes. Mas quem audita o grande auditor? Que vigia o vigilante? Os interesses vis podem certamente influenciar a metodologia de tratamento de dados que, como qualquer metodologia, tem sua falha intrínseca. A diferença neste caso pode significar a violência do Estado incorrendo inclusive sobre pessoas que eram o erro metodológico, que mal sabiam que poderiam ser enquadradas como subversivas através de atos específicos.

Não está a se colocar juízo de valor sobre aqueles que estão a cometer atos contrários ao sistema de modo consciente, ao passo que não está sendo feita uma avaliação de casos pontuais, na medida que pode haver governos escusos sendo legitimamente combatidos por sua própria população tanto quanto do outro lado pode haver um governo legítimo sendo provocado e atacado por estruturas do crime organizado.

A questão posta rapidamente sobre a etapa de processamento é a capacidade que metodologias distintas têm de apresentarem resultados diametralmente opostos,

e com isso afetar diretamente vidas de pessoas que mal sabem que fazem parte de uma vigilância muitas vezes algorítmica.

O tratamento muda o dado por definição. O dado que é coletado e tratado se torna, em si, outro dado ao final do processo.

Ele representa não uma realidade, mas sim uma realidade tratada, uma outra forma de ver a realidade, filtrada de acordo com os interesses ao menos dos consolidadores das metodologias aplicadas, e como tal, daqueles que selecionaram também tal metodologia.

Tal visão, então, se torna amplamente mediada.

A mediação está na escolha, na coleta, na consolidação de metodologias, na seleção e aplicação de tais metodologias de modo isolado ou combinadas.

Tratar o dado é conduzi-lo para um fim determinado.

Basta lembrar que toda metodologia tem formas muito específicas de resultados. Formas específicas de apresentar as informações após sua aplicação.

Este debate é de alta relevância na medida que o empilhamento de metodologias, a inflação do uso de algoritmos sociais para construir modelos comerciais capazes de ampliar o interesse das pessoas em produtos e serviços acaba por tornar mais difícil a percepção do viés que cada método pode estar causando na vida das pessoas.

Lembre-se do caso do ocultamento dos algoritmos pelo direito de patente, o que dificulta compreender de que maneira cada plataforma digital busca interferir na percepção das pessoas.

E como o escopo deste trabalho é principalmente ser provocativo, mais do que ser elucidativo, a pergunta que pode ser feita é se o conhecimento sobre os algoritmos sociais é um direito econômico ou um direito da humanidade.

Atualmente a comunidade acadêmica só é capaz de compreender parte dos traços algoritmos através do consolidado de movimentos de dados que precisam ser primeiramente intuídos, observados, coletados e processados.

Novamente, o ciclo pode conferir ainda mais viés. E a multiplicidade de estudos é fonte de maiores chances de compreender o vetor das metodologias mais

prevalentes, mas ao mesmo tempo não é suficiente para auditar o viés infraestrutural a ponto de conseguir interferir com celeridade.

A declaração do que vem a ser patrimônio universal da humanidade poderia abarcar as formas de interferência vertical na complexa malha social. Não para que seja ditatorialmente determinada, mas para que seja amplamente conhecida a ponto de cada comunidade ter as informações necessárias para agir sobre como querem ser transformadas ao longo do tempo.

A política internacional é justamente este argumento que sustenta a existência do *Lobby*. Parte-se do princípio que públicos bem informados podem agir com maior propriedade sobre um tema de relevância pública.

Porém, na flor do tempo, está a se discutir as plataformas *onlife* apenas através de seus reflexos mais sutis e superficiais.

Ainda nestas páginas haverá de se provocar mais uma reflexão sobre a ordem prioritária do direito, que nos dias atuais até nas formas das leis de contratos um valor aparentemente maior do que os direitos civis.

A imprecisão dos direitos que carecem de proteção em relação aos interesses governamentais e corporativos sobre as características fenomenológicas da vida em sociedade fortalece os discursos divergentes e confunde a comunidade civil, além de cooptar parte da comunidade jornalística pela necessidade de subsistência de grandes veículos que nos dias de hoje fazem parte da esfera tecnoeconômica que demanda precisão algorítmica para reter a atenção em um contexto transestético espetacular.

Entra-se então na próxima categoria do fluxo de vida da informação, que é a etapa de transmissão.

Esta etapa, por sua vez, tem também suas peculiaridades e serve a interesses específicos, de modo similar ao que se debateu brevemente acima.

A etapa de transmissão está condicionada pelos suportes do processo comunicacional.

Disseminar conteúdo sempre foi um processo de comunicação que contamina o conteúdo com características do próprio meio de comunicação utilizado.

Esta percepção é mais clara desde McLuhan (1964) e auxilia no debate atual para a compreensão da complexidade desta etapa, uma vez que o meio de transmissão, disseminação da informação traz condições específicas que devem ser consideradas no processo de análise.

E ao inserir esta visão dentro do *onlife* e da contemporaneidade transestética dromocrática, é possível compreender que uma informação que aparece no telejornal não terá, de forma alguma, o mesmo valor na infosfera que uma mesma questão sendo apresentada por um influenciador digital.

As notícias dos telejornais ainda estão baseadas em uma percepção de massa, em um esforço de criar um gosto médio e atender a ele de modo eficiente.

Não há muito espaço para peculiaridades e microrrepresentações.

É preciso falar com todos ao mesmo tempo, sem grandes crises ou quebras de expectativas.

Da mesma forma, a sedução se torna também menos vertical.

Já com o produtor de conteúdo eu-midiático (TERRA, 2010), e usando dos algoritmos de curadoria de conteúdo, uma pessoa hoje pode ficar presa dentro da pauta egótica que construiu mesmo sem perceber, através de seu comportamento de cliques na internet, dos vídeos que mais assistiu, das cenas que repetiu.

Depois de um tempo, seu gosto está tão evidenciado que encontrar conteúdos similares não é algo difícil para a grande infosfera constituída sobre pilares algorítmicos de entretenimento, de entre-ter, de possuir durante, por um tempo. Quanto maior este tempo, mais dados se coleta, mais dados se trata, mais se transmite em seguida.

Ou seja, este trecho está apresentado aqui para ressaltar que os meios de transmissão e compartilhamento de informações não são neutros, de forma alguma.

Eles, como toda a cadeia produtiva de informação e conteúdo, repetem comportamentos economicamente desejados e através do fluxo repetitivo de sedução e entretenimento consolidam e reforçam condutas sistemicamente desejadas.

Em uma instância mais objetiva, a transmissão é a etapa não apenas de tornar disponível, mas de se infiltrar na vida comum para estimular o consumo compulsório das informações, na medida que consumo é produção, em um ciclo integrado.

Antes de ir para a etapa do consumo, que é a próxima na sequência cíclica de Floridi (2014), é necessário dar o destaque no pilar de transmissão que vai além do interesse objetivo do transmissor, mas está impactado, como todos os outros itens, pela técnica.

A estrutura de cada canal, de cada meio de transmissão contaminará a mensagem e trará resultados mais particulares.

E parte do que se coletará e tratará, parte do que se produz com o objetivo de ser consumido terá como filtro as formas de transmissão e a linguagem de cada meio.

Assim, uma realidade observada que se pretende ofertar para o consumo poderá ter sua forma de coleta e tratamento impactada pelas regras, políticas, campos de significação em torno do meio de transmissão.

As technicalidades do Youtube e da Vevo, plataformas majoritárias de distribuição de conteúdo em vídeo, podem ser relevantes como mentalidade de tal forma que condicionam as etapas precedentes de produção de fatos comunicáveis, coleta, armazenamento e processamento de informação.

Este ponto de vista ajuda a compreender que a técnica acaba sendo incorporada de tal modo que durante a observação, a mente de quem observa pode estar escrutinizando os artefatos em busca de fatos comunicáveis que caibam, que respondam a uma determinada tecnologia.

Quando a mentalidade está tomada por formas comunicacionais com base nas redes de transmissão, o olhar observador se torna parte do sistema produtivo em busca de cada dia mais fatos para serem transmitidos.

O consumo, então, que aparece como a sexta etapa do ciclo de vida da informação é parte crucial do ciclo de informação, mas não é, de modo algum, seu fim.

Na medida em que o consumo produz mais dados sobre preferências, retém e detém os consumidores, e este tempo é tempo de consumo, de produção, de criação de valor.

O olhar produz valor. É na economia do olhar do outro, transestético, que está produzido o valor da infoeconomia.

A dromocracia cibercultural está a acelerar os processos produtivos e, como tal, de consumo e retroprodução. E este ciclo panescópico é, mais e mais, panórgico, quando o consumo é em si produção metalinguística.

Exemplo de consumo produtor de fácil entendimento pode ser a repostagem das publicações de amigos no stories do Instagram.

A quantidade de visualizações em cada postagem amplia seu valor na infoeconomia, aumenta a relevância daquele actante dentro da malha do infopoder, ao mesmo tempo que a republicação, a replicação dá o troféu do reconhecimento ao produtor ao mesmo tempo que contamina objetivamente quem o republica com os méritos e troféus do bom curador.

Mas consumir é produzir mais do que em casos tão explícitos do que a republicação.

O olhar, acima referenciado, é a instância do valor. Na medida em que cada actante aplica tempo contemplando uma publicação, dá a ela status, valor. E em uma rede de algoritmos, cada movimento, por menor que seja, resulta em reclassificação, tratamento de dados, retroalimentação.

Cada conteúdo consumido alimenta o mesmo sistema não como uma forma de retorno simples, mas como novo produto infoeconômico.

O consumo, então, é instância de produção instantânea.

Há, então, a sétima etapa do ciclo de vida da informação de Floridi (2014) é a reciclagem, mas é a mesma etapa que o autor referencia como apagamento.

De toda forma, seguindo o pensamento aqui exposto, tal etapa é em si constante.

Por mais que o autor a coloque na etapa de transição limiar que recria o ciclo, ela está presente em todo o processo.

Primeiro, a se analisar a característica de reciclagem, que é em si a recriação. É o uso dos artefatos comunicacionais de formas diversas, ressignificadas.

Mas basta voltar algumas páginas para ser percebido que a etapa de gravação e de tratamento já era, desde então, capaz de tal reciclagem, remodelagem.

A questão, então, é o caráter plástico e multifacetado que o dado pode assumir plasmado em informação.

Informação é, então, ação objetivada.

Reciclagem é característica fundamental da vida completa da informação. Risomática, a informação seguirá testando os caminhos possíveis de sua disseminação e consumo, que neste caso não é em si um consumo do modo tradicional, no qual aquilo que é consumido se esgota, mas no sentido ecossistêmico no qual aquilo que é consumido, convertido em energia, move e recria, é assimilado, transformado e transforma.

Há ainda o aspecto referenciado como apagamento. Da mesma forma, a partir do momento da criação, escolhe-se consciente ou inconscientemente aquilo que deve estar de fora.

Em uma sociedade onde guardar é algo barato e compulsório, e apagar é algo caro, intencional, escolher não gravar, não coletar algo é decidir por seu apagamento, aplicando energia para que tal informação não sobreviva entro de determinados sistemas infotécnicos.

A coleta motivada, que exclui, não é muito diferente do sistema de transmissão que não suporta determinados formatos de arquivo.

Em seu desenho, o apagamento está previsto de acordo com o que é sua função lembrar, possuir, tratar.

O dado que é tratado e convertido em informação, por si só, tendo sido coletado e guardado, está na instância de valor.

Porém, aquele que é relegado a não ser sequer coletado pode vir a ter mais valor ainda na medida que indica o que o sistema deseja expurgar, aquilo que lhe causa reação alérgica desproporcional. Oficialmente apagado, não existe. Mas não é por estar fora da estrutura de gravação que a conduta não exista.

Dentro da cibercultura, camada sociológica emanada da estrutura infotécnica, *software* humano rodando dentro de um *hardware* de tecnologias cada dia mais conectadas, pouco se poderá excluir sem que a própria exclusão deixe algum rastro informacional.

A lacuna de informação em uma sociedade que compulsoriamente quer mais e mais registros é, em si, uma informação.

Cerca de dez anos atrás Floridi (2014) trazia uma estimativa de que até o final de 2020, cerca de 50 bilhões de dispositivos estariam conectados à internet. Este número não foi superado, mas isso não significa que este caminho não esteja sendo construído a passos largos.

Isso significa que a expectativa é que em pouco tempo haja cerca de 10 dispositivos conectados para cada habitante do planeta.

Se tomar em conta que nem todo habitante da terra tem acesso ainda à internet, haverá uma proporção ainda maior de dispositivos vestíveis, câmeras urbanas, marcadores de estacionamento por cada habitante das regiões de alta densidade de uso da rede.

Com o imperativo panórgico transestético inserido na dromocracia cibercultural, cada indivíduo passa a desejar ainda mais artefatos que possam coletar seu dia a dia e processar seus dados de modo que a edição traga *sex appeal* para seus dados, de modo que as demais pessoas que fazem parte da sua sócioinfosfera desejem consumir os produtos resultantes do ciclo informacional das novas plataformas.

Ter os dados aplicados em infográficos sedutores é parte do desejo da meia maratona no final de semana. A foto no espelho da academia de *cross fit* se torna ainda mais interessante com um infográfico de calorias queimadas no dia, total de passos dados, ritmo cardíaco médio etc.

Tantas informações que antigamente competiam somente à própria pessoa, aos seus preparadores físicos e médicos, agora fazem parte do interesse da infosfera, e como tal, foram estetizados para que, assim, fizessem parte do fluxo de sedução e retroalimentação do infopoder.

Researchers have identified the importance of approaching privacy from a behavioral perspective – particularly as it follows (or fails to follow) from users' privacy-related beliefs or prior experiences. However, most studies are based on self-report rather than actually observed behavior. Further, what little work exists has been largely concerned with assessing the relationship between privacy behavior and one additional variable, rather than modeling this behavior as the outcome of several possible processes [...] (LEWIS, 2011, p. 92)

A questão apresentada por Lewis (2011) é que não basta, no caso da privacidade, pesquisar apenas a opinião declarada das pessoas, sem descer ao nível da observação de comportamentos.

A privacidade e a e-vasão fazem parte da infraestrutura do infopoder, e como tal, passam pelos problemas de compreensão por parte da comunidade acadêmica enfrenta com base nas declarações.

As pesquisas de opinião, pura e simplesmente, não são capazes de fotografar de modo mais nítido a realidade sobre a questão, ainda mais compreendendo que parte da cibercultura está sustentada por um processo afirmativo de comportamentos específicos que interferem na privacidade de pensamento, privacidade decisional e afins muito além do que a privacidade espacial / física.

O infopoder, da mesma forma, não pode ser capturado apenas por pesquisas de opinião. O viés da pesquisa de opinião é o fato de coletar a manifestação de opinião, mas não necessariamente nem a opinião real, nem o nível de entendimento sobre os assuntos.

Esta metodologia pode auxiliar, como provocação futura deste trabalho, na compreensão de tal nível de entendimento e preocupação com os temas da privacidade, do infopoder e da autodeterminação informacional.

Para compreender como que o infopoder se dissemina através das estruturas de comunicação de modo a fortalecer a e-vasão da privacidade, é preciso compreender as trocas que são feitas, as concessões são baseadas em benefícios, ainda que sejam aparentemente marginais.

Assim como as farmácias e seus descontos em troca do CPF, sistemas mais estruturados estão aplicando técnicas integradas para coletar dados e em troca, aquecem o mercado globalizado.

Como este trabalho está centrado nas tecnologias de comunicação convertidas em tecnologias de vigilância, assim como propõe Bruno (2013), a observação dos fenômenos e-vasivos estruturados há de passar pelo ecossistema contemporâneo da publicidade, relações públicas e jornalismo, sendo a primeira a principal beneficiada pelas técnicas de coleta e tratamento de dados, e as últimas ainda muito afetadas mais menos fortalecidas para o seu uso.

Na publicidade, estruturas de compra de espaço publicitário estão cada vez mais organizadas, integradas, com o objetivo de tornar cada espaço disponível altamente comercializável.

No início, os pequenos conglomerados criaram as *Ad Networks*, que eram compostas pela reunião de diversos sites e blogs temáticos que, juntos, ofereciam os seus espaços publicitários.

Com o tempo, cada *Ad Network* foi incorporada por uma ou mais DSPs (*Demand Side Platforms*), empresas que encontraram uma forma sistemática de oferecer o inventário comunicacional de dezenas, centenas de *Ad Networks* em uma única plataforma, que permitia às agências de publicidade comprar espaços de comunicação através de uma ou duas ferramentas.

Tal simplificação no processo de negociação seguiu estruturando e sistematizando o mercado publicitário digital pouco a pouco, não apenas concentrando economicamente a mídia publicitária de grande porte nas mãos de algumas empresas, mas também criando padrões técnicos mais restritos.

Os padrões de peças, de arquivos, de especificações permitiram o ganho de escala produtiva, de um lado, e de consolidação de operação econômica de outro.

Com as plataformas (DSPs) reunindo grande parte da internet comercial, tornou-se viável definir também padrões de coleta e utilização de dados de modo comercial.

Como o campo da comunicação digital é o campo da cibernética, e como tal, wieneriana (1954), é também o campo do controle, da métrica, do dado.

Isso significa dizer que não demorou, a partir do momento em que as *Ad Networks* foram sendo reunidas pelas DSPs, para que os padrões de coleta de dados comessem a ser definidos, disseminados e aplicados.

Os padrões de mapeamento e coleta de dados começaram a ser estabelecidos com base nos navegadores, através da utilização de *cookies*, que são arquivos de texto enviados pelo servidor do site acessado para o navegador do visitante.

Estes arquivos foram criados originalmente para instruir o navegador sobre como este deveria ordenar na tela os arquivos recebidos do servidor.

Era como o mapa para um quebra-cabeças.

Com a internet lenta de décadas atrás, além de orientar sobre tal ordem, os *cookies* também guardavam informações sobre quais arquivos já foram baixados no computador do usuário, evitando assim que o mesmo arquivo fosse baixado várias vezes e consumisse tempo e banda de internet do usuário.

Ou seja, o arquivo enviado pelos servidores dos sites começou a guardar informação dentro da máquina dos usuários com o objetivo de melhorar a experiência de consumo de informação e diminuir a fricção da comunicação digital.

Ocorre, que da mesma forma que Bruno (2013) vai falar das tecnologias de comunicação sendo convertidas em tecnologias de vigilância, não demorou muito para que o ecossistema da publicidade se desse conta que tais *cookies* poderiam ser utilizados para não apenas guardar informações, mas também para oferecer informações sobre o usuário ao longo do tempo.

Os *cookies*, então, começaram a ser usados para que as DSPs pudessem contar para os anunciantes quantas vezes elas tiveram que mostrar um anúncio para a mesma pessoa até que ela se interessasse em clicar na peça publicitária.

Tanto foi assim que muitas pessoas no mercado publicitário ainda chamam estas etiquetas de código de programação pelo nome de contadores.

Mas eles são mais do que contadores nos dias atuais. São observadores, otimizadores, e já não estão sozinhos.

O vínculo contemporâneo não se dá mais somente através de *cookies*, mas de redes de compartilhamento e enriquecimento de dados que utilizam uma informação-chave para aglutinar diversas bases de dados.

O Facebook pode compreender que tipo de conteúdo seus usuários consomem não só dentro de suas plataformas, mas em todos os sites que contém os aditivos de curtidas sociais.

O Google guarda a informação de quais termos foram buscados e para quais sites cada *browser* foi direcionado até compreender um padrão de consumo de conteúdo e passar a intuir quem viria a ser a pessoa por trás da tela.

Se em algum momento desta jornada o usuário decide se logar no Gmail, por exemplo, o seu histórico de pesquisas anônimas passa a compor sua ficha, seu *profile*.

Mas apesar de olharmos para a publicidade como se esta fosse o fim do projeto mercadológico da comunicação vigilante, ela certamente é apenas uma etapa intermediária da ação do capital.

E de modo mais direto, e contemporâneo, pode-se perceber que tal publicidade pode ser apenas um treino financiado pelo capital privado para a compreensão do nível de vigilância que pode ser exercido sobre uma população pelo estado ou pelo macro-sistema.

Cada consumidor de produtos, cada consumidor de comunicação é um actante que treina algoritmos diariamente mesmo sem saber.

Cada pessoa que se expõe aos conteúdos da internet e à publicidade está educando diversos códigos que buscam compreender como interferir em seu processo decisório.

Há um vínculo comum com o caso Cambridge Analytica, mas ele não é o máximo expoente da vigilância e-vasiva, mas ainda um breve teste. A notoriedade e alarde sobre os casos mencionados se devem não apenas pelo seu impacto direto e objetivo no tempo de sua prática, mas sim no potencial que demonstra de aplicação em um futuro não muito distante.

A efeito de intelecção, ao final de junho de 2007, a Apple lançava o primeiro iPhone. Tal produto revolucionou a forma com que os aparelhos celulares eram percebidos e usados. A tela sensível ao toque com alta qualidade para a época, o processamento de dados com bom desempenho e o apelo estético foram suficientes para levar muitas pessoas ao consumo de um produto de alto valor agregado.

São, desde então, praticamente 13 anos, e de lá para cá se tornou difícil conhecer alguém que tenha deliberadamente decidido viver em sociedade sem possuir um aparelho celular.

Apenas 13 anos.

Da mesma forma, a provocação apresentada a esta altura está na possibilidade de a sociedade vivenciar, até 2033, transformações profundas que tenham sido alertadas através de casos como o da Cambridge Analytica, ou sobre o nível de vigilância denunciado por Edward Snowden.

De certa forma, é válido fazer uma pequena digressão e ressaltar a dificuldade de produzir um estudo na academia que olhe solidamente para o futuro ao invés de sustentar-se no conforto do passado. Neste caso, arriscar os palpites para o futuro é arriscar os alertas necessários. Mira-se não no alvo, com o objetivo de provar-se correto, certo, mas sim com a esperança de mudá-lo de modo humano ao longo da jornada que constrói a história no futuro próximo.

Da mesma forma que o universitário médio dos dias atuais já tenha nascido e crescido em uma sociedade onde a internet praticamente já se apresentava de modo abrangente, os recém-nascidos dos dias atuais crescerão em uma sociedade que não mais viverá a privacidade conhecida pelos oitentistas.

O tempo da resignificação acelerada, que responde à dromocracia triviana (2007), fará caminhar a sociedade em ritmo ainda mais célere, arrastando os retardatários, agitando os maratonistas da tecnologia e recompensando os poucos atletas de alto desempenho nesta jornada tecnofágica.

Um século após o modernismo gerador da Antropofagia Cultural como movimento artístico, agora a sociedade se encontra frente a formas cibertécno-sociais de resignificar o presente, passado e futuro.

Significativo compreender a origem mais recente da vigilância praticada através do treino publicitário para que se torne mais familiar a visão gradativa do fortalecimento do infopoder na sociedade contemporânea.

A sutileza das permutas entre dados e descontos, entre informação e entretenimento são mais facilmente compreendidas com o passo retrospectivo, com a vista sobre um tempo histórico maior, consolidado, resumido, reunido em um espaço de observação.

O escrutínio de pouco mais de duas décadas em poucas páginas faz com que os traços mais grossos sejam apresentados e destacados.

Assim, nota-se o infopoder se constituindo através de cada novo clique.

Os marcadores são diversos e já não respondem mais ao conceito básico dos *cookies*, nem estão lastreados apenas nos navegadores.

É de interesse dos anunciantes conhecer cada vez mais cada grupo de cliente, e é de interesse e-vasivo de muitos consumidores estarem visíveis, disponíveis para

serem escolhidos e receberem os prêmios, descontos, gratificações da visibilidade panóptica e panórgica.

Ao criar vulto, se tornar perceptível até para alguns dos usuários mais desatentos da internet, o infopoder passa a ter seu campo cerceado através de limites específicos.

Os anunciantes passam a ter que respeitar o que se convencionou chamar de PII (*Personally Identifiable Information*), ou informações pessoalmente identificáveis.

Eis que tais limites são mais um indício da publicidade como treino de coleta de dados, e não como fim em si, na medida em que as empresas passam a ser limitadas na coleta e razoabilidade do tratamento dos dados, pouco se fala sobre os limites e riscos de tal conduta através do Estado.

Assim, o caráter comunicacional tende a passar por limites performáticos, estéticos, em alguns momentos até ineficazes, criando um discurso e percepção de esforço para a proteção dos direitos humanos vinculados à privacidade. Efeito placebo oferecido através de pequenas aparas em arestas publicitárias.

Distante desta discussão ainda segue indissolúvel o debate sobre a vigilância em troca de uma segurança pública etérea.

Vigiar pela publicidade se torna recriminável.

Mas ao mesmo tempo é possível trazer mais uma questão que não necessariamente será fechada até o fim desta obra, mas seguirá aberta, uma vez que não é o objetivo deste trabalho dirimi-la, mas oportunizar ainda debates, sobre quais são os sensores, os cerceadores das grandes companhias de coletarem indistintamente os dados.

Ou seja, seria o Estado capaz de condicionar a quem pertence o infopoder e, com ele, o direito de praticá-lo?

As câmaras de deputados, a política é capaz de enfrentar contemporaneamente tais estruturas ou serve como parte do espetáculo do cabo de guerra, enquanto o capital segue buscando apenas continuar a existir, evitando dilacerar cabalmente seus suportes humanos, e como tal, mantém o curso amedrontando empresas com o risco dos clientes e acionistas fazerem ruir uma ou

outra empresa, mas com menor receio de serem os governos os seus entraves mais contundentes.

Temem as empresas qual agente? O agente público? Os agentes de articulação privada? A massa anestesiada que, no repente, pode se converter em público articulado?

Em que mãos está repousado o infopoder? Questão difícil e que não poderá ser encerrada nestas páginas, mas precisa, assim como se deveria se supor após ler as páginas introdutórias deste trabalho, que tal resposta possa aflorar não de um compêndio pretérito, mas da carne viva do debate humano ativo, constante, questionável, desafiável, passível de ser contestado e reformulado à medida em que se faz necessário ter olhos novos para estruturas antigas da sociedade, tais qual a privacidade.

Há de se considerar também que entre as formas de articular o infopoder está não apenas a informação precisa, mas também a desinformação.

Whenever an information process is defective, it can have profound epistemological and practical consequences. If we are unable to access high quality information, we may fail to acquire knowledge that it would be useful for us to have. But misinformation and disinformation can actually put us into an even worse epistemic state than we started from. Moreover, the acquisition of false beliefs can potentially cause serious financial and physical harm. (FALLIS, 2016, p. 332)

Misinformation pode ser (a) uma falta informação ou (b) uma informação inacurada ou (c) que conduz a um entendimento equivocado sobre os fatos.

De toda forma, todas elas podem servir para a manutenção da e-vasão como modo de viver em grupo.

Isso pois a falta de informação não significa que a estrutura do infopoder não tenha as informações, mas que os indivíduos pertencentes à sociedade não recebem as informações necessárias para agirem sobre a própria realidade.

Da mesma forma a acurácia da informação pressupõe um público, ou seja, um grupo de pessoas interessadas e racionalmente articuladas para a construção de algo em comum que todos concordem ser necessário.

Tal mobilização de engajamento vinculado a direitos ou visão de mundo não necessariamente é base necessária para a manutenção do infopoder e-vasivo.

São bases da democracia, mas não necessariamente da infosfera.

Em muitos momentos pode ter ficado mais claro que a infosfera se ocupa de dados e informação mas não significa que se ocupe preciosamente sobre a veracidade dos dados coletados.

Claro que há relevância na veracidade, quanto mais próximo, melhor.

Mas em muitos casos a infosfera transestética se ocupa fortemente da verossimilhança, em busca do que aparenta ser crível, mais do que aplicar energia para garantir a factibilidade dos dados e do resultado do tratamento de dados.

O importante é que a conduta e-vasiva esteja consolidada e girando o mercado financeiro, de certa forma.

Não à toa o trecho em que se demorou neste trabalho a tratar do direito deu certo destaque ao uma defesa à propriedade intelectual que protege os algoritmos e as inteligências artificiais, mas não protege tão fortemente o indivíduo que interage com elas.

Quanto à veracidade, há uma questão importante que o infopoder contemporâneo utiliza para normalizar a coleta de dados e que aparece em muitas legislações que pretendem proteger o indivíduo.

Trata-se da previsão legal que garante o direito de todo indivíduo corrigir os dados indevidamente coletados sobre si.

Este direito é, também, uma brecha de normalidade, que faz parecer um benefício, uma garantia de veracidade sobre o dado, mas que também torna comum e aceitável que bases de dados tenham classificado mal uma informação e que, por esforço individual, a população deva trabalhar para a reclassificação e o ensino gratuito e voluntário das inteligências artificiais.

O processo de reclassificação torna comum o ato de tratar o dado, prometendo em troca a chance de uma pessoa acessar plataforma por plataforma e reformar a visão digital que cada banco de dados guarda sobre si.

Aqui encontra-se um axioma. O direito de reformar o dado garante maior mobilidade para o indivíduo, mas ao mesmo tempo coloca sobre cada indivíduo a responsabilidade de estar sendo bem mapeado pelas redes e pelos algoritmos.

Por outro lado, também, é preciso compreender que atos de violência, sejam físicos ou simbólicos, podem ocorrer contra os indivíduos com base em seus perfis, e

o máximo que esta cláusula faz é garantir que as violências ocorrerão com base em fatos ou no mais próximo do conceito de verdade que um dos entes da relação de coleta e tratamento de dados possua.

De modo algum isso equilibra as forças participantes da infosfera.

Já o entendimento equivocado dos fatos também pode servir para manter desengajados os grupos de interesse que teriam influência sobre as determinações de limites na coleta e tratamento de dados.

A técnica de *spinning* nas Relações Públicas já é conhecida a décadas como forma de despistar uma pergunta indesejada, sem tocar seu cerne.

Em muitos momentos neste trabalho é possível perceber pontos similares.

Entre eles, um dos mais significativos é visto quando o Projeto de Lei 5762/19 (BRASIL II, 2019) discute o prazo adicional necessário para colocar em vigor a LGPD em proteção às empresas e governo, mas não discute a proteção do cidadão.

A cortina de fumaça tem função. Isso lembra que a desinformação, em um sistema que valoriza tanto a e-vasão da privacidade, e que se baseia no infopoder, não pode ser apenas um breve erro.

Se assim o fosse, estaria sendo dura e sistematicamente combatida.

Sem entrar aprofundadamente no mérito das *Fake News*, basta compreender qual a capacidade investigativa dos países para combater a disseminação de notícias falsas, principalmente em períodos eleitorais, ato que tem o potencial de interferir no âmago da democracia ocidental contemporânea.

Assim, a desinformação é parte de um complexo sistema da infosfera. E como tal, serve a propósitos específicos de acordo com a entidade que opera a coleta, armazenamento, tratamento e transmissão de cada informação.

Most philosophers have focused on the one specific type of misinformation known as disinformation. Other types of misinformation can sometimes be just as dangerous as disinformation (e.g., those websites that advise parents to administer aspirin to children with fever). But in the same way that acts of terrorism tend to be more troubling than natural disasters, disinformation is a particularly problematic type of misinformation because it comes from someone who is actively engaged in an attempt to mislead. Moreover, in addition to directly causing harm, disinformation can harm people indirectly by eroding trust and thereby inhibiting our ability to effectively share information with each other. Disinformation is commonly associated with government or military activity. (FALLIS, 2016, p. 337)

A desinformação, então, ganha importância para este trabalho por um motivo duplo. O interesse claro e objetivo de causar um entendimento diferente de certa realidade.

Para entender a desinformação, é preciso partir do pressuposto que a informação é base da conduta e que agir sobre a qualidade da informação é corroer os caminhos para uma tomada de decisão plenamente consciente.

Na tarefa aplicada de causar um entendimento desviado da informação, são importantes alguns actantes.

De um lado tem-se aqueles que pretendem induzir fraudulentamente a opinião pública contra ou a favor de algo que, havendo clareza dos fatos, possivelmente se posicionaria diametralmente oposta. Ou seja, busca, através da transmissão e propagação de inverdades, sabidas como inverdades pelos seus produtores e pelos disseminadores, conduzir um grupo específico a agir de forma distinta à qual imagina-se que fariam caso estivessem corretamente informados.

Já por outro lado, há a desinformação ativista, que compreende o sistema evasivo e que se propõe a confundir ao máximo os sistemas de classificação.

Porém, esta é uma batalha articulada em disparidade de forças, uma vez que grandes empresas e governos em todo o mundo estão investindo pesadamente em estratégias e técnicas cada dia mais sofisticadas para criar perfis acurados sobre a população observada.

Diversas formas de confundir os sistemas já estão sendo aplicadas, desde postagens desconexas em redes sociais digitais, a algoritmos de comportamento desviado na internet para ocultar a navegação real, além de maquiagens que dificultam o reconhecimento facial.

Várias são as estratégias, mas basta pegar o último exemplo para compreender como a e-vasão cibercultural já está internalizada na população comum.

Se na entrada de um estádio ou em meio a alguma manifestação política alguém é visto com uma maquiagem que dificulta o reconhecimento, não se mostra difícil imaginar que tal pessoa seja alvo prioritário da polícia, ou mesmo de algumas pessoas ao seu redor, justamente pelo pressuposto que foi ensinado e mencionado por Solove (2011) de que aqueles que não temem, não precisam se esconder.

Logo, se alguém está se maquiando para que as câmeras de segurança não o reconheçam, só pode estar mal-intencionado.

Porém poucos refletirão se justamente este ato não é uma forma de manter-se anônimo para diminuir o peso da repressão sobre si e ter mais liberdade de criticar o próprio sistema.

Contudo, mesmo estas estratégias já estão sendo combatidas com análises de movimentos corporais que identificam o jeito único que cada pessoa se move, como ela muda o peso do corpo enquanto anda, e vários outros marcadores, como forma de identificar uma pessoa dentro de uma multidão.

Em outras palavras, a informação e a desinformação fazem parte da infosfera de modo complementar.

Information is everywhere. Information can be mediated by the dashboard of your car, or revealed to you by reading a text, looking at a poster, seeing a film – or by interpreting fMRI scans or statistics. All are human phenomena infused with meanings understandable by a driver or a film buff, a radiologist or a mathematician. Information can be environmental – like the degrees on a thermometer, or it may come to you in the form of an alarming sound of breaking glass above our head. Information can be mediated quantitatively or qualitatively; the information may be precise, factual. Factual information is either true or untrue. If it is true it yields correct or coherent understanding. If it is untrue we are disinformed, or we might have been unintentionally misinformed (Floridi, 2009:15). (FRIIS, 2016, p. 386)

A infosfera vai se sustentar em todos os artefatos e actantes produtores de dados para constituir o seu ecossistema.

A acuracidade da informação pode ser prescindida de acordo com os interesses vinculados ao tratamento e transmissão da informação.

Com isso, as preocupações sobre a aplicabilidade das informações resultantes dos movimentos de dados em uma sociedade e-vasiva estão ancoradas no potencial de aplicar à informação algorítmica o status de verdade.

Caso isso venha a ocorrer socialmente, dificilmente um cidadão comum terá condições de contradizer as estruturas algorítmicas, uma vez que tal embate demanda energia, muito conhecimento e poder. Melhor dizendo, infopoder.

The minute somebody can create something, it is possible for somebody else to waltz in and steal it for free and then exploit it. The minute that everything you own is capable of being modified to damage you or to further somebody else's agenda with no normative barriers in place, this is a dangerous space. That is one of the things we are trying to change. This is an overarching theme of the 4th industrial revolution. Governmental policies are evolving as people are becoming more aware of what the consequences and risks. Often people

do not know what are the risks in cyber-physical spaces or where the perimeter of security is for that matter?, where it is safe to go?, what data, devices and networks should you use? I think from observing cyberattack events after they have occurred, people do not know what and where the risks areas are and how to perceive how information works across cyber-physical spaces. (SKILTON; HOVSEPIAN, 2018, p. 209)

Neste caso, quando milhares de casas estão se tornando inteligentes, um ataque de ladrões pode ser testado à distância em todas elas de uma vez só. Ou seja, cada cyberataque pode ter como alvo milhares de residências. Cada atacante deixa de se expor do lado de fora da casa para tentar arrombar uma porta. Agora pode estar mascarado em várias camadas de servidores buscando não só abrir uma porta, mas olhar para dentro das casas em busca do melhor alvo.

A hacking group might decide to target an individual responsible for server administration at the firm whose data they're interested in. After tracking that person on social media for a few days, they can build up a pretty accurate picture of his or her likes, dislikes and habits, as well as map of their recente activities. It's then a fairly simple job for someone to approach the target and pass themselves off as a casual acquaintance. For example they could refer to a recent golf tournament in which they know the target participated, claiming perhaps to be a friend of a friend met at the event. They would know the target's interests, and should, with a little social skill, be able to strike up a rapport. This could all happen in person or even over email or social media, over days, weeks or even months. (SUMNER, 2016, p. 51)

Engenharia social e técnicas de mineração de dados podem potencializar ainda mais os riscos da alta disponibilidade de dados e da fragilidade dos contrapesos oferecidos pelos Estados e empresas.

The exact impacts of such 4IR technologies on society and the planet are still unknown—but the fact that they will bring profound and rapid change seems all but certain. The need for higher education to respond is urgente as the power of 4IR technologies for either positive social impacts or devastating environmental damage is upon us, as is the potential for irreversible loss of control over networks of powerful AI agents with increasing autonomy within financial sectors and within urban infrastructure. Substantial changes to the science and technology curriculum will be required to allow for students to develop capacity in the rapidly emerging areas of genomics, data science, AI, robotics and nanomaterials. (PENPRASE, 2018, p. 217)

A mudança não só de percepção, mas de conduta global sobre o potencial transformador dos dados e da infosfera precisa ser aportada com urgência na sociedade contemporânea.

Mantido da forma como está, com disputas territoriais sobre quem pode violar a privacidade de quem, o debate será constantemente esvaziado como no caso do PL 5762/19.

Enquanto as grandes empresas seguem ajustando a lógica de coleta de dados para não serem impactadas pela União Europeia, através de seus efeitos

extraterritoriais, as pequenas empresas ou os pequenos agentes cibernéticos seguem fluando de servidor em servidor para despistar a comunidade internacional enquanto coletam e armazenam dados privados que foram invadidos, ou mesmo aqueles evadidos.

O infopoder segue articulando modos de conduzir a política global sem que o combate às práticas de tráfico de dados seja contundentemente aplicado.

Assim como se falou anteriormente, caso o interesse global fosse realmente construir caminhos para a valorização da privacidade, tantos casos de invasão e evasão teriam sido exemplarmente investigados.

Na contramão, as formas de e-vasão continuam sendo tangenciadas e até estimuladas, mesmo nos casos das legislações mais avançadas.

A articulação contemporânea segue favorecendo os movimentos de dados para fortalecimento do infopoder através do pretexto da aceitação do compartilhamento de dados, o chamado opt-in.

Como salvaguarda performática da informação e desinformação estão as proibições de coleta e armazenamento de dados chamados de informações pessoalmente identificáveis, como uma forma de bloquear a precisão da infovigilância.

Porém a peculiaridade da conduta humana faz com que mesmo sem dados como CPF, Data de nascimento ou imagem de rosto, seja possível compreender e agrupar condutas distintas dentro de um único perfil com técnicas muito simples, como a sobreposição de dados de geolocalização de um aparelho celular com os locais de abastecimento de gasolina, ou pagamento de pedágio etc.

Se com dois dados simples como a localização e o tipo de acesso à internet isso já é possível, o que se fará com o cruzamento de tantas bases robustas de dados que no presente momento não estão sob a mira da ANPD, uma vez que a LGPD segue sendo postergada constantemente.

Ou seja, atualmente o infopoder se serve de técnicas variadas para camuflar a forma como estimula a e-vasão de dados e da privacidade, mantendo as estruturas de coleta, gravação, tratamento e distribuição de dados que servem para a manutenção econômica do mercado atual sem que os Estados tenham uma atuação mais significativa.

E-VASÃO – UMA PROPOSTA CONCEITUAL

A disponibilidade de dados sobre um indivíduo, no âmbito das tecnologias, que para os devidos fins deste estudo, é considerado não como on/offline, mas sim *onlife*, assim como dito no capítulo anterior, em consonância com Floridi (2014), considerando que desta forma apresenta sincronicidade entre o plano analógico e a camada digital.

Assim, a vida cotidiana das ações físicas está acoplada, integrada à camada de dados digitais que segue observando e registrando diversos detalhes da vida comum.

Tal sincronicidade, que por vezes pode parecer complexa, se dá através de marcadores comuns ou por chaves de cruzamento de dados.

O princípio é simples e pode ser exemplificado com clareza.

Quando duas bases possuem um dado em comum que seja único, as duas bases podem ser combinadas e se enriquecerem mutuamente.

Na prática, se uma empresa de seguros compra uma base de dados de uma rede de farmácias, ao encontrar o mesmo CPF nas duas bases de dados, a empresa de seguros pode saber exatamente que tipo de medicamento seu cliente ou seu grupo de interesse está comprando, e através destes dados, fazer análise de risco para a concessão de seguros ou para o custo que cada tipo de segurado terá.

Mas este caso se mostra compreensível e, de certa forma, simplista. Sim, simplista.

Ao pensar que somente empresas que possuam os números de documento públicos das pessoas poderiam cruzar dados para saber quem são acaba-se por imaginar que tais cruzamentos se tornem limitados.

Então é preciso rumar para uma compreensão ainda mais aprofundada sobre o ecossistema de enriquecimento de dados que existe no mercado nos dias atuais e como eles podem ir além de informações simples como consumo de medicamentos ou compra em supermercados.

A estrutura básica de cruzamento de dados está dada acima. Duas bases de dados que possuam uma informação em comum podem ser unidas a partir deste dado.

Mas um caminho mais longo pode ser traçado para combinar informações.

A exemplo, uma empresa que possua apenas o número de telefone de seus clientes em potencial pode buscar serviço de empresas de enriquecimento de dados para entender, com base nestes números de telefone, quem viriam a ser estas pessoas, buscando desde informações demográficas como sexo, idade, região de residência, renda média, chegando a dados comportamentais, como sites mais visitados na internet, aplicativos mais usados, regiões da cidade que mais frequenta e tantas outras informações a mais.

Isso é tecnicamente possível pois a infraestrutura comercial de dados está aparelhada e embarcada em muitas soluções de negócios e utilizada em sites, dispositivos celulares, jogos e aplicativos.

Cada aplicativo instalado num aparelho celular pede e coleta informações distintas.

Em sua grande maioria, tais aplicativos, sejam eles gratuitos ou pagos, aplicam o chamado contrato de adesão, de modo que o usuário final não tem liberdade, ainda que esteja pagando pelo serviço, para alterar os termos contratuais, podendo apenas aceitar ou declinar o contrato. Os termos não são discutíveis.

Assim, em diversos casos, ou o usuário aceita entregar o acesso à sua agenda telefônica, mensagens enviadas, localização, redes de wi-fi, ou simplesmente não usará o aplicativo.

Além disso, muitas vezes a coleta de dados sobre uma pessoa não se dá com seu consentimento, mas sim com o consentimento de pessoas em sua rede de relacionamentos.

Neste caso, um grupo hipotético de 10 amigos, onde cada pessoa possui 20 aplicativos diferentes instalados em seus aparelhos celulares, traz consigo 200 oportunidades de evasão da privacidade e dos dados.

Imagine que tal grupo aceite um novo membro (indivíduo A), uma pessoa que tenta constantemente evitar a evasão de seus dados.

Quando cada pessoa desta rede adiciona o número de telefone deste indivíduo em seus aparelhos celulares, em uma única noite, o indivíduo A abriu 200 brechas

para que a macroestrutura tecnológica passe a integrar mais informações a respeito de sua conduta ao seu perfil.

Quando um de seus amigos se conecta com o bluetooth do celular do Indivíduo A para lhe transferir fotos, e ao mesmo tempo está conectado com o Wi-fi do estabelecimento, em instantes o Indivíduo A, que pode estar fora do wi-fi e da internet, tem sua geolocalização revelada por tabela.

Desta forma, o indivíduo A do exemplo acima se torna exposto, com seus dados evadidos sem que tenha optado por isso.

Da mesma forma, se a configuração do aplicativo de mensagens dos amigos estiver feita de modo que todas as fotos e vídeos sejam salvos automaticamente no celular ao serem recebidas, diversos aplicativos podem ter acesso ao acervo de imagens.

Em termos mais diretos, a tentativa de se proteger da exposição e evasão não depende apenas do indivíduo, mas da forma como é autorizado aos diversos actantes lidar com as informações de alguém.

Neste caso, o ponto sensível da questão é que apesar de ter o consentimento do usuário, tais aplicativos e empresas não possuem o consentimento dos seus contatos para se tornarem cientes de tal conexão.

O ocultamento, a privacidade então não é, em si, uma escolha de um indivíduo em uma sociedade que traz tais aparatos técnicos, mas sim uma decisão sobre os direitos difusos dos indivíduos.

Há muito tempo os aparelhos celulares são ótimos localizadores, mesmo que estejam sem internet ou com o GPS desligado.

Usando a mesma técnica antiga de localização de aeronaves por triangulação de torres de comunicação, cada aparelho se torna um nó único em movimento na malha das empresas de telecomunicação.

In principle, of course, a tracking unit with its own power supply could support radio triangulation. For example, networked receivers could estimate the position of a mobile transmitter from the difference in time of arrival of its signals - a process more accurately labeled trilateration because location is calculated using relative distances rather than estimated angles. (MONMONIER, 2006, p. 77)

A triangulação básica segue utilizada pelas empresas de telecomunicações, mas todos os outros segmentos chegam ao dado da geolocalização com relativa facilidade e baixo preço através dos dados coletados por diversos tipos de aplicativos de aparelhos celulares, mesmo quando o GPS está bloqueado, através do cruzamento do WI-FI do aparelho, mesmo que a pessoa não se conecte com os roteadores ao redor.

O simples fato de habilitar o wi-fi ou o bluetooth pode fazer aparecer no aparelho as redes que estão ao redor.

Ou seja, para as empresas de mineração de dados, basta saber a geolocalização de uma única pessoa que a qualquer momento se conectou a estes roteadores, para classificar todas as outras pessoas que passaram por este local.

Os pontos de exposição são múltiplos.

Cada celular mapeado no raio de alcance do bluetooth e do wi-fi pode ser um evasor de informação.

A topografia de dados é mais estruturada e facilmente vinculável do que se imagina.

Através de diversos eventos, e a transferência de dados, cada indivíduo se torna um nó rizomático que viabiliza a observação, coleta e tratamento de dados de tantas outras pessoas.

At the same time, available storage space and further digitization will make it possible for additional types of information (text, images, audio, video, spatial data) to transition to digital devices, again stimulating demand—the rise of digital cameras, for example, has fueled demand as digital camera users store photos on general-purpose hard disks. (MAYER-SCHÖNBERGER, 2009, p. 46)

É através do barateamento das tecnologias e das formas de coleta, armazenamento e tratamento de dados que a permeabilidade da vigilância assume aspectos ainda mais profundos na topografia.

O que anteriormente se definiria comumente como ciberespaço ganha a integralidade dos espaços contemporâneos, não à toa, no capítulo anterior o ciberespaço foi referenciado como o espaço em si.

Vale ressaltar, todavia, que ainda assim, nesta tese, seguirá o termo ciberespaço como forma distintiva de apresentar o espaço contemporâneo frente à visão e historicidade do espaço antes da cibernética.

Ciberespaço é, então, o novo espaço em suas dinâmicas dromocráticas transestéticas que articulam e fortalecem o infopoder através do escrutínio dos atos comuns, cotidianos, salvaguardado pelo discurso da segurança e da praticidade, do conforto, da comodidade.

A espacialidade, mesmo que não seja fator determinante, ainda segue condicionando parte das manifestações identitárias e nas formas de assediar a privacidade para que seja preservada ou e-vadida.

There is no doubt that students love the convenience smartphones offer them, the easy access to just about anything they want, the constant availability of the Internet, the GPS function, how smartphones make everything “immediate,” that smartphones make it easy for them to keep track of their busy lives and commitments, that they can play games and listen to their music on them. (FRETAS, 2017, p. 229)

No trecho acima, a autora apresenta tanto o imediatismo quanto a conveniência como agentes no processo de e-vasão da privacidade.

Seja para pedir uma comida através de aplicativos de restaurantes como o Rappi, para marcar encontro usando os aplicativos de relacionamento, seja para pedir um taxi usando o 99, todas estas ações acabam por ensinar e normalizar o compartilhamento da geolocalização.

Ainda que estes mesmos aplicativos façam uso adequado das informações que coletam, ao conviver diariamente com tais comodidades, pratica o reforço positivo vinculado ao hábito de estar encontrável pelas plataformas com o menor atrito possível, tornando a vida cotidiana mais confortável.

Ao mesmo tempo que faz sentido o aplicativo de taxis conhecer a geolocalização de seu usuário, pouco sentido faz um aplicativo de fotos ter acesso ao mesmo dado.

Porém, isso não significa que tanto Apple quanto Google não permitam que tais aplicativos coletem este dado, desde que tenham uma justificativa plausível.

No campo da funcionalidade, isso é tranquilamente solucionável, buscando um pretexto simples para converter um aplicativo de fotos em um evasor da localização de seus usuários.

Tais Aplicativos podem oferecer a praticidade de classificar as fotos nos álbuns de acordo com data e localização, criando marcações elegantes sobre a cidade visitada.

Simples. Ao prometer diminuir o trabalho de ordenação, classificação e arquivamento das fotos e vídeos produzidos em uma viagem, um aplicativo comum de filtros pode ter acesso à localização de um usuário daquele momento em diante para compartilhar com sua rede e monetizar sua publicidade de modo mais direcionado.

Enquanto a contrapartida do Rappi para ter acesso à localização do dispositivo é diminuir o tempo de espera para uma refeição e ainda garantir que ela chegará no lugar certo, a contrapartida de um aplicativo de fotos para ter a mesma informação passa a ser tanto a praticidade da memória acessível por uma determinada taxonomia quanto o campo da estética da visibilidade e-vasiva e produtora de artefatos comunicacionais que permitam uma manifestação do self vinculada à efemeridade dos espaços.

As viagens, assim como o corpo, assim como as maquiagens, tornam-se pretexto, suporte, caminho para impelir usuários ao uso e-vasivo das mídias de modo suave e sutil.

A comodidade e os serviços se tornam pretextos para a e-vasão da privacidade de modo compulsório.

At the interface of power and time, permanent remembering creates the specter of a spatial and temporal panopticon, in which everybody may constantly be tempted to self-censor. Perhaps most importantly, comprehensive digital remembering collapses history, impairing our judgment and our capacity to act in time. It denies us humans the chance to evolve, develop, and learn, leaving us helplessly oscillating between two equally troubling options: a permanent past and an ignorant present. (MAYER-SCHÖNBERGER, 2009, p. 77)

O infopoder se dá nas camadas espaciais e temporais da vida comum de modo que o panóptico se reconstitui em cada espaço-tempo no qual se habita, ainda que transitoriamente.

E para evoluir a relação já feita com Bruno (2013) este panóptico se converte, com o processo de sedução transtéstico (LIPOVETSKY; SERROY, 2015) em uma estrutura escópica e panórgica da e-vasão.

Enquanto Mayer-Schönberger (2009) vai falar do auto-sensor, dez anos depois se propõe aqui o auto-e-vasor. E-vadir é ir além da autocensura.

Esta busca não ser agredida pelo sistema prevalente. A segunda, graciosamente entrega seus dados para serem escrutinizados em público.

Uma não exclui a outra, mas se complementa como a ramificação da fécula desenvolvida através do imperativo da aceleração.

O filtro prevalente neste trabalho está relacionado à forma como as pessoas estão compartilhando suas vidas nas redes sociais digitais, principalmente, e de que forma este voluntariado para a autoexposição se torna possível.

Em páginas anteriores já foi possível ler a palavra e-vasão, com esta grafia própria, mesmo que com explicações muito breves.

Compreendendo que nos dias atuais a invasão da privacidade surge não apenas com um viés violento que venha a ser prontamente combatido pelas instituições e pelos indivíduos, mas sim através de um duplo, aquele em que tanto a invasão ocorre mas também coopta o indivíduo através de sedução para o desejo de evadir sua própria privacidade como forma de construir um eu.

As citizens have embraced social media and other platform economy applications, the data have gotten immeasurably better. The “likes,” photos, and updates on health status that people provide as part of their social lives along with the data that they leave behind in the course of their everyday activities provide information that can be fed to the maws of the machine-learning systems that both analyze behavior and help companies manipulate it.¹⁰ Whereas states used to have to demand that people provide data, consumers now voluntarily update and publicize risky behavior, including even highly intimate sexual encounters. (FARRELL; NEWMAN, 2019, p. 165)

A partir do momento em que cada pessoa deseja sua privacidade evadida, o esforço de arrancar os dados passa a ser sutilizado e suavizado na estratégia de convencimento gradativa para a e-vasão, um híbrido proposto entre a evasão, considerando aquele que quer evadir, que quer entregar algo ou expor, tirar; e a invasão como o desejo daquele que convence, que articula de modo hábil para ter ao final o dado que precisa.

Assim, o ente não deseja invadir, deseja o dado. E como tal, passa a convencer os detentores, fetichizando a evasão.

Enquanto um quer o dado, o outro quer o prazer da exposição.

Ambos se satisfazem no primeiro momento. Apenas no primeiro momento.

A proposta de compreender tais atos como e-vasão se dá como uma provocação para abarcar a sedução objetivada pela evasão para que os dados estejam pacificamente disponíveis.

E-vadir então viria a ser um verbo cujo significado duplo seria induzir, convencer um ente a liberar seus dados; ao mesmo tempo que viria a significar desejar ter seus dados expostos, sua vida, suas imagens apresentadas à audiência que é apenas a camada pueril da camuflagem e-vasiva.

Esta proposta, derivada do trabalho dos anos recentes em busca de compreensão sobre o infopoder e suas ramificações fenomenológicas, e combina mais do que os conceitos de invasão e evasão.

A e-vasão então vai além da exposição seduzida e consentida da intimidade, mas abarca os diversos campos da privacidade, passando inclusive pela e-vasão das ideias, das articulações, do pensamento e do ato decisional.

Desejada pelas redes, por seu alto valor mercadológico, e tutorada em troca da conveniência para que os indivíduos abram as portas da sua privacidade de bom grado e com alegria.

Enquanto em momentos distintos da sociedade ocidental oscilou, inclusive no Brasil, entre alguns governos democráticos e outros governos ditatoriais, a questão da privacidade foi ganhando corpo e suas violações ocorreram de modos peculiares a cada momento.

É fácil compreender que tipo de invasão um governo ditatorial pode praticar contra sua própria população, utilizando-se principalmente do pretexto da defesa da ordem e da segurança pública para a prática de atos invasivos.

Mas a distinção de tais atos ditatoriais para os atuais atos invasivos democráticos está na violência bruta aplicada por aqueles em comparação com a violência sutil aplicada por estes.

A violência direta inevitavelmente encontrará muitas barreiras e resistência, enquanto que a suavização e sutilização deste processo faz com que a entrega seja volitiva.

Na democracia contemporânea os atos invasivos são apresentados como opção de customização de serviços, como forma de combate à corrupção, como método infraestrutural de melhora das condições econômicas.

A invasão parte do pressuposto que algum ente tem interesse em obter acesso aos dados que outro ente possui, mas que resiste em liberar.

Através da força de justiça, ou do estado de exceção, um governo pode adentrar o campo da privacidade.

Da mesma forma, no campo das ações civis e mercadológicas, a invasão pode ocorrer por espionagem, de modo objetivado, ou por meio de invasão de computadores e dispositivos eletrônicos.

Há, então, ao menos dois interesses em jogo no que toca esta questão da invasão.

O interesse do invasor em obter dados, e o interesse do ente que é assediado ou atacado por aquele, que busca manter sua zona privativa protegida da visão do outro.

Já a evasão não é apenas o mesmo movimento com uma alteração no vetor do dado.

Há os casos de evasão de informação ocorrida como forma de protesto ou denúncia como no caso Snowden, Wikileaks ou, mais próximo ainda da realidade brasileira, o caso da VazaJato.

Tais informações, ao serem reveladas, contrariam o interesse de seus produtores, que pretendiam manter segredo.

A questão é que em casos assim, fala-se de informações que são de interesse público e que foram produzidas por entes também públicos, ou que impactam na república.

O trecho constitucional brasileiro que indica a transparência na gestão das coisas públicas traz apenas uma exceção para a liberação de dados das instâncias do poder público, que vem a ser casos de risco à segurança nacional.

Descartada esta condição, restam os interesses internos à democracia, e por isso, cabíveis à transparência que permite auditar e intervir para o bom andamento da

democracia e da república em si, seja no âmbito econômico, técnico, jurídico, moral, ético etc.

Assim, aqui há um paralelo de vetor inverso quando a sociedade civil, de alguma forma, obtém acesso a informações das entidades governamentais ou corporativas, que impactam a república e a democracia em qualquer de suas instâncias, à revelia de seus produtores de dados.

Tal evasão tem no detentor original do dado o desejo do sigilo, enquanto o evasor é agente externo, é um ente interessado, que se vê como um executor da lei e do direito que estaria sendo cerceado por agentes viciados.

Neste caso, não se caracterizaria invasão na medida que o que se está apresentando já deveria estar sob escrutínio público.

Porém, há uma segunda camada da evasão que não está vinculada a movimentos de dados à revelia, mas sim se dá com o objetivo de tornar públicos os dados em questão.

A esfera performática da vida pública ativa justamente o voyeurismo, o escopismo através das mídias sobre a vida das celebridades (LIPOVETSKY) alçadas ao estrelato pelas mídias de massa. Expor-se é mandatário, mesmo que seja preciso condicionar, oportunizar os meios para tanto. “A sociedade hipermoderna também é a sociedade da artificialidade, da falsificação, do falso luxo e da verdadeira pacotilha, do falso verdadeiro e do verdadeiro virtual.” (LIPOVETSKY; SERROY, 2015, p. 408)

O cinema torna pessoas mundialmente conhecidas e faz surgir ao redor delas um campo de interesse e produção de conteúdo que pode ou não estar vinculado com certa verdade.

Em certa medida, após compreender o poder que a mídia de massa tem para manter uma personalidade em destaque na agenda pública, parte das celebridades passam a construir fatos comunicáveis que tem como objetivo justamente a sua evasão. Esta é uma forma de subverter a invasão que já era praticada pelos meios de comunicação, alimentando a massa consumidora, e fazer com que tal prática servisse ao propósito da própria celebridade.

Ou seja, no caso acima o dado não é cooptado, roubado, mas sim deixado à mercê dos paparazzi e jornalistas.

Seu vazamento é uma questão de tempo e de interesse mútuo.

Aqui há um ponto de inflexão no qual é possível resgatar o conceito da dromocracia cibercultural (TRIVINHO, 2007), na medida em que tal aceleração atinge, nos tempos atuais, em concomitância com o capitalismo transestético (LIPOVETSKY; SERROY, 2015), a vida comum, tornando-a espetacular e exigindo a dromoaptidão de mantê-la exposta e performática no campo das negociações simbólicas do infopoder.

Com isso, evadir não é um ato de infração de um ente contra outro, mas um ato motivado do indivíduo sobre sua própria imagem.

Não está a se discutir o cunho verídico do que se esvai, na medida em que tal evasão se dá como representação, como imagem arquitetada.

Isso significa que a edificação dos artefatos simbólicos está sendo articulada de forma intencional pelo emissor, pelo evasor sobre sua própria imagem.

Já o que se propõe como provocação na categoria que hibridiza invasão e evasão, é a evolução de ambas em uma forma dupla de invasão e evasão que se torna desejada pelo indivíduo.

Consider a few contemporary tendencies that have recently become commonplace: online social profile management, the precision demographic categorizations of marketing analytics, unmatched levels of state-sponsored surveillance, the deceptively familiar cyberwars conducted by governments globally, powerful technologies of consumer and voter dataveillance, unprecedented levels of voluntary personal information sharing via social media, massive torrents of online file sharing, algorithmic and automated market transactions, data-driven financialization, and site after site for the production of informational aspects of ourselves from personalized genetic reporting to the quantified selves of our wristwatches. Though this is a seemingly disparate congeries of data points, there is one thing running through it: the fine thread of the power of information. (KOOPMAN, 2019, p. 155)

Isso significa que em muitos momentos o sujeito tem sua intimidade escrutinizada, mas também deseja o campo da performance. O holofote é parte do *feedback* social acelerado nos tempos atuais. Ponto de destaque, troféu efêmero que precisa ser conquistado recorrentemente.

A e-vasão proposta neste trabalho é resultado da dromocracia aplicada sobre os efeitos da espetacularização capital na consolidação do infopoder contemporâneo na instância do escopismo panórgico.

O desejo de ser visto e o interesse em ser notado são parte do resultado do percurso que se inicia com as grandes celebridades das mídias de massa e desce hoje ao nível do cidadão comum, nas micromídias, transformando o eu-mídia (TERRA, 2010) em eu-dado, em suporte dos movimentos dos dados em busca de mais um ponto de emanção da intimidade e de construção do processo de sedução que conduzirá outros ao entendimento do que é o fio condutor da vida espetacular midiaticizada nos micromomentos do cotidiano.

A vida comum passa a ser construída com o grande observador, mas não mais como o *Big Brother* que está a escrutinar para punir, mas como o *Big Partner*, o grande parceiro que promete te ajudar, te trazer o espetáculo, a luz, o holofote mais desejado.

E-vadir é, então, um ato desejado. Estar vigiado não apenas pelas pessoas, mas também, e principalmente, por todo o sistema que tem condições de alavancar um ente comum ao status de celebridade de modo instantâneo em todas as mídias e por todo o globo.

O convencimento de que agora está ainda mais próximo do sonho de ser percebido pelo público, de modo que reforça algo que vinha em curso desde a massificação da comunicação, um contínuo dromocrático que segue seu curso estratificado e que dará vazão ao contemporâneo desejo de ser seu próprio curador, de dominar, a partir dos interesses próprios, quais discursos serão tecidos sobre a própria imagem.

A potential solution, for generations to come, may be to be thriftier with anything that tends to crystallize the nature of the self, and more adept in handling new or refined skills of self-construction. Capturing, editing, saving, conserving, managing one's own memories for personal and public consumption will become increasingly importante not just in terms of protection of informational privacy [...] but also in terms of construction of a healthier personal identity. The same holds true for interactions. The onlife experience does not respect boundaries between different online and offline environments, with the result that [...] the scope for naive lying about oneself on Facebook is increasingly reduced. In this case, the solution may lie in the creation of more affordances and safer spaces for self-expression and self-construction. (FLORIDI, 2014, p. 73)

A construção do *infoself* é um ato necessário, uma demonstração de dromoaptidão mandatória nos dias atuais.

Gerir intencionalmente e objetivamente a própria manifestação identitária é condição primordial para a aceitação de um indivíduo dentro de um grupo

determinado, assim como foi apresentado de modo gradativo no primeiro capítulo desta tese.

A e-vasão é não apenas a entrega da intimidade, mas muito mais do que isso.

Ser dromoapto a e-vadir seus dados é ter a capacidade de pensar e agir em sociedade de modo que a produção de movimentos de dados seja coerente com a imagem que se deseja produzir sendo que esta, concomitantemente, deve estar em consonância com a esfera de espetacularização escópica e panórgica do capitalismo transestético.

Dromoaptidão está em ter a mentalidade, agir e reagir de modo a influenciar a coleta e tratamento de dados de actantes diversos, sejam humanos, sejam algorítmicos, para que o resultante esteja alinhado com os objetivos do e-vasor, sempre tendo em mente que tais objetivos nascem também desta relação, e como tal, fazem parte do ideal compartilhado dentro da cibercultura e da esfera do infopoder constituído através do escopismo orgasmático.

O escopismo, por sua vez, transfere a energia no ato de ser visto e reconhecido pelos actantes *onlife* para o campo da performance e da validação social na omniágora.

A performance do agente depende diretamente da forma como este será percebido pelos actantes relevantes da infosfera, na articulação do infopoder de modo espetacular.

[...] infopower as a distinctive modality of power deploys techniques of formatting to do its work of producing and refining informational persons who are subject to the operations of fastening. Even more concisely, technical formatting is na act of power that fastens its subjects to their data. By way of a comparison familiar to readers of Foucault [...], the normalizing operations and surveillance techniques of disciplinary power are analogous to the fastening operations and formatting techniques of infopower. (KOOPMAN, 2019, p. 12)

Não apenas a questão da autoexposição está dada aqui, mas sim a e-vasão, que pretende ofertar os dados, deseja ofertar tais dados para que a infosfera vigore.

A aceleração da vigilância vinculada ao infopoder está inserida na dromocracia de modo vertical, na medida em que segue o mesmo pressuposto.

Koopman (2019) vai tratar da normalização, da aceitação silenciosa de que a vigilância já faz parte da estrutura social e, como tal, vai dar contornos ainda mais

robustos ao infopoder para que siga conduzindo os comportamentos socialmente aceitos na nova consolidação cibercultural.

O indivíduo dentro da sociedade infotransestética é produto não só dos processos de tratamento de dados, mas a internalização dos valores que fazem com que considere relevante participar ativamente da observação, coleta, armazenamento e todas as outras etapas do ciclo de vida da informação (FLORIDI, 2014).

Cada participante aplica sua energia em fazer valer o infopoder através de uma mentalidade e condutas e-vasivas.

Importante ressaltar que em uma sociedade de escopismo panórgico, aquele que oculta seus dados, que recusa oferecer seus documentos está de pronto em suspeição.

Não à toa o pensador Solove (2011) intitulará seu livro com o argumento “nada a esconder”, como uma forma de resumir a expressão conformista e internalizada que muitos manifestam atualmente quando questionados sobre a vigilância.

The nothing-to-hide argument is everywhere. In Britain, for example, the government has installed millions of public surveillance cameras in cities and towns, which are watched by officials via closed-circuit television. In a campaign slogan for the program, the government declares: “If you’ve got nothing to hide, you’ve got nothing to fear.” In the United States, one anonymous individual comments: “If [government officials] need to read my e-mails... so be it. I have nothing to hide. Do you?” Variations of nothing-to-hide arguments frequently appear in blogs, letters to the editor, television news interviews, and other forums. (SOLOVE, 2011, p. 21-22)

Importante perceber o suporte, o interesse governamental no discurso sobre não ter nada a esconder, que por sua origem já coloca a opinião pública a considerar que os opositores da vigilância panóptica sejam, via de regra, pessoas com crimes a serem ocultados.

O Estado usa seu poderio comunicacional para criar um clima de animosidade que coloca sua população dentro de imperativos categóricos kantianos. Ou a pessoa não tem nada a esconder, dando a entender que simplesmente por isso é honesta e, também logicamente não agirá contra a vigilância do Estado, ou é alguém que tem algo oculto, ilícito a ser mantido em segredo, e logicamente irá combater de todas as formas a vigilância.

Este discurso dos “honestos” contra aqueles que querem esconder algo tem o apelo na segurança pública e é um dos pilares da consolidação da e-vasão como forma de agir de um período.

Mas é importante destacar que não é o único, nem o principal pilar contemporâneo que sustenta a e-vasão.

É o argumento oficial. É a camada legalista que justifica dentro da lógica, o que em outras camadas precisaria de maior esforço.

Não sem motivos Solove (2011) vai lembrar que o ponto de vista utilizado pode ser crucial para o tipo de argumento que se utiliza para refutar a questão da privacidade, principalmente quando se coloca a questão da segurança como se fossem antagônicas.

To evaluate the nothing-to-hide argument, we should begin by looking at how its adherents understand privacy. Nearly every law or policy involving privacy depends upon a particular understanding of what privacy is. The way problems are conceived has a tremendous impact on the legal and policy solutions used to solve them. (SOLOVE, 2011, p. 24)

De pronto, tal antagonismo vai colocar a pessoa que pretende ocultar seus dados na mira do sistema legal, investigativo, uma vez que o pensamento legalista consolide e reforce o argumento de que aqueles que nada devem, nada precisam temer.

Mas neste caso é possível compreender a pressão para não esconder nada. Tal pressão é diferente, em vetor, do estímulo para mostrar tudo.

Tal distinção é relevante.

Enquanto o esforço legalista ainda tem um viés invasivo, a articulação dromocrática do infopoder exige a dromoaptidão transestética e-vasiva de modo muito mais vertical, íntimo.

A conduta e-vasiva pode até usar o argumento de que nada há para esconder quando alguém é honesto, mas este não é o foco.

E-vadir é buscar os meios de visibilidade nas instâncias de reconhecimento para que a e-vasão se torne reconhecida e culmine em fortalecimento do infopoder de quem e-vade.

É preciso ter motivação para estar exposto e articulação para que esta exposição tenha retornos imagéticos desejados.

Cada pessoa é convidada sutilmente a fazer parte da cibercultura transestética. O convite pode ser sutil, mas caso haja recusa, os impactos são mais violentos.

A resposta negativa, essa recusa é respondida com exclusão, expulsão, suspeita, barreiras e dificuldades.

Tais impactos podem ser percebidos desde a dificuldade para entrevistas de emprego quando sua vida não está exposta no linkedin com inúmeras recomendações, ou o receio de ter um encontro amoroso com alguém que tem seu perfil do Facebook pouco preenchido.

Exemplo direto do imperativo transestético aplicado no escopismo panórgico é o próprio Instagram que, como plataforma, aceita quase todo tipo de imagens, apesar de fazer distinção entre fotos e vídeos violentos e bloquear imagens de nudez, mas que mesmo permitindo o upload, a comunidade usuária não retribui com curtidas e comentários a não ser que haja uma acuidade estética vinculada ao fio condutor na medida desejada pela estética inflacionária do escopismo panórgico.

The functioning of the false self/persona and the true/real self is a fundamental component in the response to the intersubjective dynamics of recognition. The seeking of recognition is foundational to relating in that it works both ways: the desire to be recognised and the desire to discover and recognise the other. This interplay of seeking recognition while at the same time seeking to recognise is a dialectical tension that commences from the very start of life within the infant–mother dyad, where initial relational templates are laid down through to adult life, where they are repeated, worked through, and, ideally, amended, repaired, and developed further towards the capacity for intimacy. (BALICK, 2014, p. 29)

Na análise psicológica este jogo entre o *self* “real” e o *self* construído é parte das forças que regem a busca por reconhecimento.

O objetivo não é adentrar a área da psicologia, mas provocar o convite a considerar que no *onlife* (FLORIDI, 2014) a comunicação não terá distinções como esta, a não ser que as mantenhamos de fato no campo da psicologia.

No plano da comunicação, no espaço da narrativa do eu, esta persona será construída não de modo unitário, mas múltiplo, porém sem que isso signifique que o discurso em si é fragmentário, quando muito, tal discurso é dinâmico, transitório, reagente.

Para que isso se dê de modo acelerado, como segue na cibercultura, é preciso que o processo de e-vasão mantenha ritmo e, como não poderia de ser diferente, siga atento aos indicadores de resultado.

Um ente e-vasivo seguirá contando seguidores, curtidas, compartilhamentos.

Os ídolos contemporâneos são medidos não mais pela quantidade de discos ou CDs vendidos, mas pelo número de pessoas que os seguem nas redes sociais e pela quantidade, e velocidade, de curtidas atingidas.

A diferença da esfera anterior é que a articulação do mercado fonográfico, para seguir o mesmo exemplo, seguia o modelo analógico e estava condicionado a decisões de ampla lateralidade dos administradores das gravadoras.

Com a proliferação das mídias sociais digitais, dos canais do Youtube, Vimeo e afins, o sonho do estrelato foi novamente vendido à custa dos dados e de muita dedicação na compreensão, obtenção da dromoaptidão e sua aplicação para criar conteúdos que praticam e convocam à e-vasão.

A distinção do modelo antigo é que agora a um artista não basta convencer e agradar produtores e editores. É preciso agradar um público verticalizado e, talvez principalmente, aos algoritmos vigentes.

O processo e-vasivo, então, se dá como matéria-prima e como substrato da cibercultura algorítmica.

A união de uma visão de cultura permeada pelo *onlife* com um adjetivo como este é fruto da compreensão de que a cultura atual assimilou e age com aceitação às aplicações de tratamentos de dados de modo algorítmico com o pretexto do aumento da conveniência e melhora na qualidade de serviços para alguns, mas como condição para o ingresso nas esferas de representação e articulação da identidade contemporânea e transitória.

I began [...] by agreeing with the common idea that capitalism is based on selfish individualism. This needs some qualification. What I will call 'free market capitalism' is based on selfish individualism, because free markets are. Markets are free when exchange is voluntary and when there is 'freedom of contract': that is, when the terms of contracts are decided by the transacting parties alone, rather than being dictated or constrained by outside parties. In other words, markets are free when individuals decide for themselves, when actions are not coerced. Free markets are simply individualism applied to economic affairs. (WHYTE, 2019, p. 40)

Em outras palavras, o infopoder pode estar fomentando um individualismo coletivo e acompanhado.

As redes sociais digitais podem atingir a fina camada de comunicação que, na realidade, torna alguém um bom emissor e que, como resposta, recebe curtidas.

De toda forma, é ainda um processo de comunicação que traz indicadores de valor, um índice de quem recebe mais curtidas do que os demais.

Contudo, quanto mais isolados, quanto mais separados uns dos outros, e em contato apenas pelas mídias, mais lógico parece ser e-vadir sua privacidade para que as pessoas possam acompanhá-la à distância.

De certa forma, a espacialidade, que apresentamos em dado momento como menos relevante, traz de forma colateral seu preço, e a distância passa a ser pretexto e contexto para que a e-vasão se intensifique, se tornando artefato de visualidade das relações mediadas.

Com base em Whyte (2019) é possível intuir que o afastamento físico pode ser um dos fatores que auxiliem e favoreçam a instauração do fluxo e-vasivo.

A distinção é que, lembrando que se trata de um imperativo dromocrático, nos tempos atuais esta atuação bebe da robustez do movimento comunicacional e econômico conhecido como globalização, e sustentado pelo seu bastião tecnológico, a saber a internet, estruturando formas de comunicação que possam prescindir da espacialidade diretamente, mas que já se percebe ainda não ser possível no campo indireto, e como tal, influencia os processos e-vasivos.

Desta forma, quanto mais afastados, mais isolados, mais o processo e-vasivo se estabelece.

Pessoas sentadas à mesa com familiares postando fotos no grupo da família dentro do Whatsapp é um exemplo que em outros tempos poderia parecer infeliz ou exagerado, mas que nos dias atuais já está normalizado pela conduta prática.

Colegas de trabalho que se falam mais por email mesmo sentando a poucos passos um do outro seguem o mesmo caminho.

Amigos que trocam mensagens de áudio e se referenciam como os mais íntimos, mas que raramente se encontram.

A distância física e a proximidade infotécnica é uma manifestação do infopoder condicionante do modo de conduta e-vasivo.

Dentro das contrapartidas que a tecnologia oferece está a assincronia das comunicações por Whatsapp, por exemplo, para que o indivíduo tenha tempo para pensar na resposta que dará. Mesmo que seja questão de segundos.

A conversa nas redes sociais digitais oferecem a licença poética da instantaneidade, mas também da descontinuidade.

Todos possuem a prerrogativa de estarem falando com mais de uma pessoa ao mesmo tempo. Isso dá tempo para pensar, para articular que forma transestética e-vasiva será apresentada para a pessoa que está do outro lado da tela.

Tal descompasso, assincronia basal, é parte não da falha, mas do fortalecimento das contrapartidas, de modo que faz com que cada indivíduo seja capaz de usar sua energia para articular detalhes da e-vasão de sua máscara social de modo dinâmico.

Por sua vez, a conversa em tempo real, lado a lado no mesmo ambiente, não permite tempos de articulação, de construção de respostas mais ajustadas ao imperativo transestético.

É preciso um nível magistral da mentalidade e-vasiva articulada para estar exposto de modo intencional em um campo de diálogo analógico, ainda que *onlife* e obter os mesmos resultados que teria com o tempo adicional para articular as respostas.

O tempo real das tecnologias pode até existir com um leve descompasso no tempo de transmissão, que por muitos é ignorado com afeto, mas a copresencialidade demanda alta performance instantânea, e nem todos estão aptos a sustentá-la após tantos anos de flacidez do exercício articulador sequencial necessário para agir no plano do verdadeiro tempo real.

What is being sought when one is inspecting another's Facebook profile, photo albums, or reading through old status updates? On the relational-unconscious level, the motivations revolve around the desire to discover and to be discovered, orbiting around polarities of narcissistic/exhibitionistic and voyeuristic desires. (BALICK, 2013, p. 44)

E-vadir é estar visível e conquistar o direito de ver. Permitir-se exposto e receber o consentimento da visualização da intimidade do outro também, além de compreender que tais plataformas e o plano da visibilidade realizará interferências sutilizadas inclusive em camadas profundas como a privacidade decisional.

Exemplo prático disso nos dias atuais, que serve para a sedução do escopismo panórgico e-vasivo de múltiplas vias, é a notificação de leitura de mensagens do Whatsapp.

Para saber se uma mensagem enviada já foi aberta pelo destinatário, é preciso que o emissor deixe sua conta configurada para realizar notificação de leitura para seus contatos também.

De certa forma é completamente justo.

Para saber se alguém está lendo suas mensagens, nada mais correto do que esta pessoa também poder saber se você leu as mensagens dela. É simétrico, deste ponto de vista.

Há, porém, um ajuste que poderia ser feito neste caso, que é a possibilidade de configurar o aviso de leitura para pessoas específicas ao invés de uma configuração única para todos os contatos.

Por outro lado, caso houvesse esta possibilidade, as pessoas seriam pressionadas por seus amigos, chefes, esposos a terem as notificações obrigatoriamente habilitadas para eles.

Seria claramente um caminho para aplicar esta forma de coerção em busca da invasão da privacidade do outro.

Então, de um lado, há um tutoramento sedutor, que faz com que em troca das notificações haja também a liberação das suas informações de leitura.

Do outro lado há a impossibilidade de configurar alertas específicos que, ao mesmo tempo, mantém certas brechas para desculpas que evitem o escrutínio de algumas pessoas sobre as notificações de leitura.

Este pensamento sobre o pêndulo da liberação dos dados e das notificações de leitura, como no exemplo prático, se dá de modo largo justamente por não haver um caminho educacional e de tomada de consciência que tenha abarcado a privacidade ao longo dos anos.

As transformações não ocorreram de modo abrupto, se não de modo gradual. Sim, acelerado, também. Mas não repentino.

Mas a agenda pública fica tomada por este assunto apenas nos momentos de grandes violações, como a invasão das contas do aplicativo Telegram pertencentes a políticos e juristas vinculados à operação Lava Jato.

Perde-se a oportunidade de construir uma agenda que abarque a e-vasão como modo constante de estar no mundo contemporâneo.

A própria mídia se alimenta do processo e-vasivo na medida em que utiliza os dados de segmentação para compreender como cada público reage aos seus programas, novelas, entretenimento.

Se décadas atrás a forma de saber se um programa tinha audiência era através de institutos de pesquisa como o IBOPE, hoje o tempo real das reações no Twitter e em outras plataformas é um termômetro com mais informações.

Agora o processo e-vasivo permite que a audiência seja conhecida de modo mais profundo e, de certa forma, atitudinal ao invés de declaratório.

Enquanto os institutos perguntam para as pessoas sobre seus interesses, e aí pode vigorar a espiral do silêncio, os movimentos dos dados da cibercultura observa condutas objetivas, como cliques, buscas na internet, visitas a estabelecimentos físicos através dos dados de geolocalização dos aparelhos celulares, tempo dedicado a filmes através das redes de *streaming*, tipo de música preferido, humor ao longo do dia.

Tudo pode se tornar informação dentro do ecossistema midiático e segue sendo utilizado como matéria-prima para os conglomerados de comunicação locais e globais.

Tal dado é ainda mais rico a cada dia e o processo e-vasivo pode se dar inclusive à revelia.

Poderia se argumentar que se a e-vasão de dados ocorre de modo compulsório e sem pleno conhecimento, não é em si uma e-vasão, mas sim uma invasão, como mencionado anteriormente.

De um ponto de vista legal, possivelmente este seja o caminho.

Ocorre que o indivíduo que tem seus dados compartilhados ne sempre está determinado a pedir ressarcimento ou de buscar a interrupção de tal ato.

Assim, lembra-se que o imperativo e-vasivo é mais do que o ato de ter os dados apresentados ao público e mais uma mentalidade que culmina em tal ato de modo constante, compulsório e normalizado socialmente.

Ao saber-se e-vadido, o cidadão médio não parte em busca da interrupção, quando muito se conforma e talvez mude comportamentos pequenos.

CONCLUSÃO

A compreensão de que o sujeito social precisa de um campo de significação e articulação que é apartado das suas manifestações foi um ponto relevante ao longo deste trabalho, para que fosse possível caracterizar o valor da privacidade como sendo social, antes de ser individual.

Este conceito, que oferece à sociedade formas preliminares de testar em microescala as críticas evolutivas da democracia, é o pano de fundo que permitiu ir além da privacidade física e íntima para descer em seus degraus mais profundos e cruciais.

Brevemente se falou do direito a autodeterminação informacional, uma vez que este tema já foi largamente tratado na monografia anterior (FELÍCIO. 2015).

Todavia, reforçou-se sobremaneira a questão da privacidade do pensamento e decisional, crucias e extremamente necessárias para a construção e manutenção do presente e futuro da democracia e da sociedade.

Urge que desta tese restem alguns alertas relevantes sobre tal tema, a serem postos em apreciação.

As formas de coleta de dados vigentes nos dias atuais estão permeando as condutas humanas de modos tanto positivos quanto negativos.

Mas a decisão de limitar os abusos e falhas precisa ocorrer de modo sistêmico e alinhada em diversos níveis da estrutura social, política, legislativa, jurídica, midiática.

Lembra-se aqui, como forma de dar ainda mais destaque à questão, que possivelmente a tutela da privacidade, como bem coletivo e difuso, aplicado às realidades individuais, deva ser aninhada no Estado para que este seja obrigado a agir sobre as violações praticadas e torne inalienável a privacidade do indivíduo em certo nível, da mesma forma que o faz com o direito de imagem, que pode ter seu uso vendido com prazos e condições determinadas, mas não de modo infundável e perpétuo.

Há também que se caminhar a passos mais largos sobre a questão de como governos e empresas poderão observar as populações, de que forma, com qual finalidade.

Manter a forma atual, ainda que com a aplicação a LGPD, pode significar apenas camuflar os problemas reais e, em alguns casos, através da sensação de proteção, aumentar ainda mais o potencial de violações da privacidade em seus vários níveis.

Da mesma forma, não basta que o Brasil considere as condutas sobre os crimes da privacidade, assim como aqueles perpetrados através da internet, como uma questão unicamente do próprio Estado, sem que haja articulação internacional para a desterritorialização dos processos em busca de criminosos, estejam onde estiverem, principalmente por compreender que os meios de comunicação desterritorializaram parte das comunidades, mas também aumentaram o potencial da violência à distância.

Para tanto, é preciso uma visão humanística dos direitos e deveres humanos, acima e anteriores aos direitos e deveres do brasileiro.

Sem cooperação e alinhamento, a legislação local muitas vezes pode ser ineficiente para fazer valor as ações corretivas e punitivas.

Buscou-se trazer à luz que tais legislações e condutas corporativas e civis estão condicionadas pela busca, fortalecimento e manutenção do infopoder, forma contemporânea do poder que se apropria dos dados e impulsiona sua geração para que haja um ciclo de fortalecimento e crescimento constante.

Os movimentos dos dados, estimulados pelos governos e pelo mercado, foram internalizados como modo de estar no mundo e ser reconhecido através da atualização as máscaras sociais como forma de garantir a transitoriedade das identidades, posicionamentos, interesses.

Os troféus passam a ser ainda mais fugazes e a necessidade de reconhecimento se torna uma busca constante e infundável, ainda mais com a inflação estética e o modo como o mercado se estabelece e premia aqueles que aceitam e propagam a e-vasão.

Alguns autores foram cruciais para compreender como que se somam diversos fatores para gerar as condições propícias para a atual sociedade e-vasiva.

Entre eles, amplo destaque deve ser dado a Trivinho (2007).

Através de seu trabalho, foi possível compreender os aspectos violentos da velocidade atualmente, mas não do modo simplista como às vezes é possível encontrar na mídia de massa.

Sua visão estrutural permitiu perceber que tal violência é sutalizada socialmente, ainda que seus impactos sejam muitas vezes percebidos, agindo de modo constante e acelerado sobre todas as esferas da vida e da sociedade.

Foi a partir da compreensão do imperativo da dromoaptidão que se deu a compreensão de que a privacidade e sua e-vasão somam-se às habilidades exigidas para se fazer parte da cibercultura contemporânea.

Sem este conceito, certamente a visão sobre a privacidade teria majoritariamente uma análise mercadológica, como se o mercado fosse o principal vetor, como estímulo, da e-vasão.

Pode-se compreender que mais do que o mercado, em si, composto por empresas e regulações, o que ocorre para tal fomento está muito mais arraigado na sociedade do que os interesses das organizações, que acabam sendo também conduzidas ao invés de liderarem estes movimentos dromocráticos de velocidade e aceleração.

É preciso ainda referenciar de modo relevante a questão da propriedade e posse das tecnologias discursivas no próprio *domo*, para que tal dromoaptidão seja desenvolvida em compasso com a aceleração sistêmica, e ainda o processo comunicacional e-vasivo se dê de modo constante, não dependendo de acessos esporádicos às redes.

Foi necessário também rumar pela questão estética que magistralmente camufla as violências da velocidade e artealiza a exposição da intimidade, sensualiza a efemeridade e, gradativamente se instala como forma de manifestação inflacionada com trações pulsionais do escopismo, que em sua e-vasão se torna ainda mais panórgico.

A estética se apresentou, através de Lipovetsky (2015), não como algo secundário e que apenas glamouriza o processo comunicacional, mas como parte do estímulo que é internalizado para gerar e-vasores e, ao mesmo tempo, convencer os demais de que este é o caminho por excelência, e que a exposição de si, sua reapresentação diferentemente estetizada a cada momento deve ser desejada, admirada, buscada, conquistada.

Unindo Trivinho (2007) e Lipovetsky (2015) foi possível criar uma lente mais apropriada para compreender como se dá o processo gradativo de convencimento que faz e-vadir não apenas a privacidade física, corpórea, mas também como através deste imperativo de velocidade tecnocrática e transestética foi possível e-vadir aos poucos aspectos do livre-pensar e a privacidade decisional em troca de confortos simplórios e baixos retornos econômicos, em busca da promessa de estar em destaque na infosfera.

Foi ainda importante compreender que a sociedade e-vasiva está a consolidar e fortalecer o infopoder, não infraestrutural do poder, mas pelo contrário, forma contemporânea do poder que se manifesta e articula através do exercício da produção constante e compulsória de dados, de sua observação interessada, coleta pervasiva e, de forma ainda mais violenta e ao mesmo tempo sutil, a sua modelagem para que

consolide uma visão de mundo interessada a partir do ponto de vista do próprio infopoder.

As análises narradas por cada um dos três principais autores se coadunam em um fato social afiado, a saber, o infopoder dromocrático cibercultural transestético que exercerá sua força para conduzir a sociedade à produção, tratamento e disseminação de mais dados e informações, como se a sociedade seguisse sendo um suporte informacional.

Com todos os apontamentos feitos ao longo deste trabalho, conclui-se justamente com a proposta de que se constitua um termo para um processo de apropriação do imaginário das pessoas em busca de brechas e da exposição da privacidade que seja mais complexo do que apenas um desejo de se expor na sociedade pura e simplesmente, com traços mais profundos e mais sutilizados do que a banalidade de atos menores.

É preciso reconhecer a luta simbólica, psicológica, social e, principalmente, mercadológica que há na configuração do novo modo de estar no mundo através da espetacularização da esfera privada exposta ao escrutínio público.

Reforça-se que, ainda que não seja o termo final grafado como e-vasão nos tempos vindouros, que ainda assim seja constituído um termo que possa significar a tal luta de interesses que permeia mais do que as redes sociais digitais.

A e-vasão proposta, então, se mostra um termo intersticial que acopla em si (1) o interesse sistêmico pela invasão da privacidade física, mental, emocional e decisional do outro somado às estratégias de facilitação de tal acesso através da (2) sedução e artealização da violência simbólica que é a interferência no pensamento, visão de si e do mundo, e capacidade de decidir sobre si para que haja um (3) desejo de evasão de dados, imagens, informações e comportamentos através da (4) gratificação efêmera pelos atos de autoexposição que devem se aglutinar a um (5) discurso identitário multimodal apresentado através de (6) diversos meios de comunicação, convertidos gradativamente em formas de entretenimento informacional, e seguindo (7) ritmo acelerado e arquitetado.

Ao combinar todos estes fatores, o que se obtém como resultado, então, não vem mais a ser um ato impulsivo de liberação de dados ou de autopropagandismo, mas algo muito mais profundo e sistêmico que se apresenta como comportamento e mentalidade epocal, e como tal, estará sujeito a transformações presentes e futuras,

ainda sob a dromocracia cibercultural, mas que tem potencial para se converter em muitas realidades distintas.

Com a proposta atual, a concepção do ato de e-vadir está vinculada a um ato complexo composto por diversas forças concomitantes, que seguirá interferindo em diversos níveis sociais e que precisa, como tal, ter seus limites definidos através de análises e debates sociais criteriosos.

Sem a tomada de consciência, tal violência seguirá seu vetor de violências sutilizadas a extremos ainda não praticados.

Ao mesmo tempo, será necessário vencer as barreiras dos interesses econômicos imediatistas para que seja salvaguardada a sociedade ao invés das pessoas jurídicas e dos governos transitórios atuais.

O convite está feito para uma reflexão ativa, provocativa, sobre a vida contemporânea e sobre os limites situacionais e morais da interferência no pensamento, na vida íntima e na habilidade e capacidade de tomar decisão.

Tendo comido do fruto da árvore do conhecimento, resta viver com as consequências de compreender as falhas e as violências que sustentam os processos sutis.

Vendo-se exposto, vulnerável, objetificado, resta a provocação sobre qual atitude será tomada a partir de tal conhecimento para que as formas de condução estejam condicionadas aos interesses da sociedade democrática e dos indivíduos de modo aberto, claro, e que o espaço criativo e fecundo da privacidade possa ser conduzido à categoria de inalienável, protegido e fortalecido ao longo de cada ciclo cibercultural.

REFERÊNCIAS

BALDWIN, Tom. **Ctrl Alt Delete**: How politics and the media crashed our democracy. London: Hurst & Company, 2018. 383 p.

BALICK, Aaron. **THE PSYCHODYNAMICS OF SOCIAL NETWORKING**: Connected-up Instantaneous Culture and the Self. London: Karnac Books, 2014. 225 p.

BERNERS-LEE, Tim. **Contract for the Web**: A global plan of action to make our online world safe and empowering for everyone. 2019. Disponível em: <<https://contractfortheweb.org/principles/principle-3-respect-and-protect-peoples-fundamental-online-privacy-and-data-rights/>>. Acesso em: 25 nov. 2019.

BAUDRILLARD, Jean. **De um fragmento a outro**. São Paulo: Zouk, 2003.

BEHRENDT, Ralf-peter. **Narcissism and the Self**: Dynamics of Self-Preservation in Social Interaction, Personality Structure, Subjective Experience, and Psychopathology. Guernsey: Palgrave Macmillan, 2015. 423 p.

BOÉTIE, Étienne de la. **Discurso da servidão voluntária**. São Paulo: Martin Claret, 2009.

BOURDIEU, Pierre. **Coisas ditas**. São Paulo: Editora Brasiliense, 1987. 235 p.

BRASIL. Constituição (2019). Proposta de Emenda Constitucional nº 17, de 03 de julho de 2019. **Pec 17/2019**. Brasília, DF.

BRASIL II. Projeto de Lei nº 5762/19, de 30 de outubro de 2019. **PL 5762/19**. Brasília, DF.

BRUNO, Fernanda. **MÁQUINAS DE VER, MODOS DE SER::** vigilância, tecnologia e subjetividade. Porto Alegre: Editora Sulina, 2013. 194 p.

CALIFORNIA (Estado). Constituição (2018). Ato nº 375, de 28 de junho de 2018. **Assembly Bill No. 375**. California, 28 jun. 2018. Disponível em: <https://leginfo.legislature.ca.gov/faces/billTextClient.xhtml?bill_id=201720180AB375>. Acesso em: 01 ago. 2018.

COVER, Rob. **DIGITAL IDENTITIES**: Creating and Communicating the Online Self. Crawley: Elsevier, 2016. 308 p.

CURY, Lucilene. **O dilema da pesquisa**. São Paulo: Edusp, 2008.

DAMASIO, Antonio R. **O erro de descartes**: Emoção, razão e cérebro humano. São Paulo: Companhia das Letras, 1994.

DEBORD, Guy. **A sociedade do espetáculo**. Rio de Janeiro: Editora Contraponto, 1997.

FALLIS, Don. MIS- AND DISINFORMATION. In: FLORIDI, Luciano. **THE ROUTLEDGE HANDBOOK OF PHILOSOPHY OF INFORMATION**. New York: Routledge, 2016. Cap. 27. p. 332-346.

FARRELL, Henry; NEWMAN, Abraham L.. **Of Privacy and Power**: The Transatlantic Struggle over freedom and Security. Oxfordshire: Princeton University Press, 2019. 247 p.

FLORIDI, Luciano. **The 4th revolution**: how the infosphere is reshaping human reality. Oxford: Oxford University Press, 2014. 265 p.

_____. **The Onlife Manifesto**: Being Human in a Hyperconnected Era. London: Spinger, 2015. 255 p.

FOUCAULT, Michel. **Vigiar e punir: nascimento da prisão**. Petrópolis: Vozes, 2013.

FREITAS, Donna. **The Happiness Effect**: How social media is driving a generation to appear perfect at any cost. New York: Oxford University Press, 2017. 369 p.

FRIIS, Jan Kyrre Berg. THE INTERPRETATIVE VALUE OF INFORMATION. In: FLORIDI, Luciano. **THE ROUTLEDGE HANDBOOK OF PHILOSOPHY OF INFORMATION**. New York: Routledge, 2016. Cap. 31. p. 386-395.

FUREDÍ, Frank (Ed.). New Forms of Alienation. In: KENNEDY, Angus; PANTON, James. **From Self to Selfie**: A Critique of Contemporary Forms of Alienation. Gewerbestrasse: Palgrave Macmillan, 2019. p. 193-206.

GIBBS, Samuel. **Shops can track you via your smartphone, privacy watchdog warns**: UK retailers are able to follow and target customers using facial recognition software and handset identifiers broadcast via Wi-Fi. 2016. Disponível em: <<https://www.theguardian.com/technology/2016/jan/21/shops-track-smartphone-uk-privacy-watchdog-warns>>. Acesso em: 01 mar. 2019.

GOFFMAN, Erving. **A representação do eu na vida cotidiana**. Petrópolis: Vozes, 1975.

GUNTHER, André (Aut.). The Consecration of the Selfie: A Cultural History. In: ECKEL, Julia; RUCHATZ, Jens; WIRTH, Sabine. **Exploring the Selfie: Historical, Theoretical, and Analytical Approaches to Digital Self-Photography**. Cham: Palgrave Macmillan, 2018. p. 27-48.

HALL, Stuart. **A identidade cultural na pós-modernidade**. 10^a ed. Rio de Janeiro: DP&A, 2005.

IBRAHIM, Yasmin. **Production of the 'Self' in the Digital Age**. London: Palgrave Macmillan, 2018.

KERCKHOVE, Derrick de. **A pele da cultura: Uma Investigação sobre a Nova Realidade Electrónica**. Lisboa: Ed. Relógio D'Água, 1997.

KOOPMAN, Colin. **How We Became Our Data: A Genealogy of the Informational Person**. Chicago: The University Of Chicago Press, 2019. 281 p.

KUMAR, Kaushik; ZINDANI, Divya; DAVIM, J. Paulo. **Industry 4.0: Developments towards the Fourth Industrial Revolution**. Singapura: Springer, 2019. 69 p.

LATOUR, Bruno. **We Have Never Been Modern**. Cambridge: Harvard University Press, 1993. 162 p.

LÈVY, Pierre. **O que é o virtual?** São Paulo: Editora 34, 1996.

_____. **Cibercultura**. São Paulo, Editora 34, 1999.

LEWANDOWSKI, Dirk. Is Google Responsible for Providing Fair and Unbiased Results? In: TADDEO, Mariarosaria; FLORIDI, Luciano. **The Responsibilities of Online Service Providers**. Cham: Springer, 2017. p. 61-78.

LEWIS, Kevin. The Co-evolution of Social Network Ties and Online Privacy Behavior. In: TREPTE, Sabine; REINECKE, Leonard (Ed.). **Privacy Online: Perspectives on Privacy and Self-Disclosure in the Social Web**. Hamburg: Springer, 2011. Cap. 8. p. 91-110.

LIPOVETSKY, Gilles; SERROY, Jean. **A estetização do mundo: Viver na era do capitalismo artista**. São Paulo: Companhia das Letras, 2015. 467 p.

MCLUHAN, Marshall. **Os meios de comunicação como extensões do homem**. Trad. Décio Pignatari. São Paulo: Cultrix, 1964

MASUR, Philipp K.. **Situational Privacy and Self-Disclosure: Communication Processes in Online Environments**. Stuttgart: Springer, 2017.

MAYER-SCHÖNBERGER, Viktor. **Delete: The Virtue of Forgetting in the Digital Age**. Princeton: Princeton University Press, 2009. 149 p.

NAÇÕES UNIDAS. **Declaração Universal dos Direitos Humanos**.

NICOLELIS, Miguel. **Muito além do nosso eu: A nova neurociência que une cérebro e máquinas - e como ela pode mudar nossas vidas**. São Paulo: Companhia das Letras, 2011.

PARISER, Eli. **O filtro invisível: O que a internet está escondendo de você**. Rio de Janeiro: Zahar, 2012.

PENPRASE, Bryan Edward. The Fourth Industrial Revolution and Higher Education. In: GLEASON, Nancy W.. **HIGHER EDUCATION IN THE ERA OF THE FOURTH INDUSTRIAL REVOLUTION**. Singapura: Springer, 2018. Cap. 9. p. 207-238.

PRIMIERO, Giuseppe. INFORMATION IN THE PHILOSOPHY OF COMPUTER SCIENCE. In: FLORIDI, Luciano. **THE ROUTLEDGE HANDBOOK OF PHILOSOPHY OF INFORMATION**. New York: Routledge, 2016. Cap. 10. p. 90-106.

ROMÊNIA (País). Lei (2004), Lei 506/2004. **Processing of personal data and the protection of privacy in the electronic communications sector**. Romênia. Disponível em: <<https://fra.europa.eu/en/law-reference/law-no5062004-processing-personal-data-and-protection-privacy-electronic>>. Acesso em: 01 ago. 2018.

RUCHATZ, Jens. Selfie Reflexivity: Pictures of People Taking Photographs. In: ECKEL, Julia; RUCHATZ, Jens; WIRTH, Sabine. **Exploring the Selfie: Historical, Theoretical, and Analytical Approaches to Digital Self-Photography**. Cham: Palgrave Macmillan, 2018. p. 49-82.

SANTAELLA, Lúcia. **Corpo e comunicação: sintoma da cultura**. São Paulo: Paulus, 2004.

SCHWAB, Klaus. **The fourth industrial revolution**. Cologny: World Economic Forum, 2016. 172 p.

SHEAFF, Mike. **Secrecy, Privacy and Accountability: Challenges for Social Research**. Plymouth: Palgrave Macmillan, 2019. 156 p.

SKILTON, Mark; HOVSEPIAN, Felix. **The 4th Industrial Revolution: Responding to the Impact of Artificial Intelligence on Business**. Cham: Springer, 2018. 342 p.

ŚLEDZIEWSKA, Katarzyna; WŁOCH, Renata. Should We Treat Big Data as a Public Good? In: TADDEO, Mariarosaria; FLORIDI, Luciano. **The Responsibilities of Online Service Providers**. Cham: Springer, 2017. Cap. 14. p. 263-274.

SOLOVE, Daniel J.. **Nothing to Hide: The False Tradeoff between Privacy and Security**. Yale: Yale University Press, 2011. 256 p.

STRANDBURG, Katherine J. Social Norms, Self Control and Privacy in the Online World. In: STRANDBURG, Katherine J.; RAICU, Danela Stan (Ed.). **Privacy and Technologies of Identity: A Cross-Disciplinary Conversation**. Illinois: Springer, 2006. Cap. 3. p. 31-53.

SUÍÇA (País). Constituição (1999), de 18 de abril de 1999. **Federal Constitution of the Swiss Confederation**. Suíça, 18 abr. 1999. Disponível em: <<https://www.admin.ch/opc/en/classified-compilation/19995395/index.html>>. Acesso em: 01 ago. 2018.

_____. Constituição (1999), Ato 235.1, de 19 de junho de 1992. **Federal Act on Data Protection**. Suíça, 19 jun. 1992. Disponível em: <<https://www.admin.ch/opc/en/classified-compilation/19920153/index.html>>. Acesso em: 01 ago. 2018.

SUMNER, Stuart. **You: For Sale: Protecting Your Personal Data and Privacy Online**. Waltham: Elsevier, 2016. 214 p.

SUPREMO TRIBUNAL FEDERAL. **DIREITO AO ESQUECIMENTO**: Bibliografia, Legislação e Jurisprudência Temática. Brasília: Stf, 2017. 81 p. Disponível em: <http://www.stf.jus.br/arquivo/cms/bibliotecaConsultaProdutoBibliotecaBibliografia/ano_direito_ao_esquecimento2.pdf>. Acesso em: 01 mar. 2018.

TERRA, Carolina Frazon. **Usuário-mídia: A relação entre a comunicação organizacional e o conteúdo gerado pelo internauta nas redes sociais**. 2010. 217 f. Tese (Doutorado) - Curso de Comunicação, Ppgcom, Universidade de São Paulo, São Paulo, 2010.

TRIVINHO, Eugênio. **A dromocracia cibercultural: lógica da vida humana na civilização mediática avançada**. São Paulo: Paulus, 2007. 456 p.

UNIÃO EUROPEIA. Regulamento (2016). **Regulamento (EU) 2016/679 do Parlamento Europeu e do Conselho**. União Europeia. Disponível em: <[https://eur-lex.europa.eu/legal-](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3417-1-1)

[content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3417-1-1](https://eur-lex.europa.eu/legal-content/PT/TXT/HTML/?uri=CELEX:32016R0679&from=EN#d1e3417-1-1)>. Acesso em: 01 ago. 2018.

WHYTE, Jamie (Ed.). In *Prise of Selfish Individualism*. In: KENNEDY, Angus; PANTON, James. **From Self to Selfie: A Critique of Contemporary Forms of Alienation**. Gewerbestrasse: Palgrave Macmillan, 2019. p. 193-206.

WIENER, Norbert. **Cibernética e sociedade: O uso humano de seres humanos**. São Paulo: Cultrix, 1954.

WOLF, Mauro. **Teorias das comunicações de massa**. São Paulo: Martins Fontes, 2009.

WOLTON, Dominique. **Internet, e depois? Uma teoria crítica das novas mídias**. Porto Alegre: Sulina, 2003.

ZAHARI, Mohamad Kuzahier Mohd; ZAABA, Zarul Fitri. Intelligent Responsive Indoor System (IRIS): A Potential Shoplifter Security Alert System. **Journal Of Information And Communication Technology**. *, p. 262-282. 2 mar. 2017.