



Revista do Mestrado em Direito da UFS

O COLONIALISMO DIGITAL COMO NOVA FORMA DE IMPERIALISMO NA SOCIEDADE EM REDE

Alessandra Cristina de Mendonça Siqueira¹

RESUMO

No momento atual, as fronteiras entre “mundo digital e mundo real” encontram-se cada vez menos visíveis, e, até mesmo, incabíveis. Está ocorrendo uma migração para uma forma de abstração social, onde os meios digitais são os responsáveis por integrar justamente o conceito de individualismo e identidade. Nesse toar, temas como privacidade e vigilância são palavras-chave para a noção de proteção de direitos individuais, referentes aos próximos anos. Existe um confronto verdadeiro entre controle e liberdade, segurança e privacidade, onde não se sabe ao certo quais os limites e extensões das práticas que estão acontecendo, seja referente à captura e análise massiva de dados, como também uma forma de controle tecnológico muito menos observável. É nesse contexto que se enquadra a noção de “colonialismo digital e capitalismo de vigilância”, a serem analisadas no trabalho em questão, onde os novos atores, situados em polos tecnológicos, impõem uma nova forma de imperialismo, não apenas à sociedade, mas a Estado como um todo. A discussão de medidas, políticas e intervenções, é não apenas necessária, mas urgente, a fim de colocar uma luz às práticas que acontecem antes das mesmas se infiltrarem como a normalidade passiva.

Palavras-chave: Colonialismo Digital. Privacidade. Internet. Controle de dados. Capitalismo de vigilância.

¹ Graduada em Direito. Advogada. Fundadora do Aracaju Legal Hackers, criadora do JurisData, ativista na proteção de direitos fundamentais no ambiente cibernético, membro da Internet Society, membro da Comissão De Ética, Direito e Conformidade em Ambiente Digital e Internet do Instituto Brasileiro de Direito e Ética Empresarial, membro do GT da ISOC e do IBDEE. Email: ale_mendonc@hotmail.com.

ABSTRACT

In the present moment, the frontiers between “digital world and real world” are less and less visible, and even not there anymore. It is happening a migration to a new form of social abstraction, where digital are the responsible to integrate the concepts of individualism and identity. Therefore, themes like privacy and surveillance are the keywords to the notion of protection of individual rights for the next years. There is a real conflict between control and freedom, security and privacy, where no one knows the limits and extensions of the practices that are happening, about capture and massive data analysis, and also a new form of tech control, that is less and less observable. This is the context where you can put the notion of “digital colonialism and surveillance capitalism”, terms that are going to be analyzed in the present work, where new actors in tech poles are imposing a new form of imperialism, not only to a society, but to a whole State. The discussion of what to do, politics and interventions, it is not only necessary, but urgent, so it can shine a light in the things that are happening, before they can be the new normal.

Keywords: Digital colonialism. Privacy. Internet. Data control. Surveillance capitalism.

Introdução

Muito se falou acerca de uma mudança iminente nas relações sociais. No entanto, enquanto se conversava acerca dessas mudanças, elas chegaram em velocidade exponencial, o que é condizente com a própria natureza da principal matriz desse desenvolvimento: a tecnologia, especialmente, a internet.

A Era Digital trouxe uma nova gama de pontos de vista e viradas estruturais em vários contextos, como por exemplo, economia, cultura, sistemas jurídicos, e a própria cultura social em si. Há, atualmente, uma interrelação indissociável entre tecnologia e sociedade, a ponto de não poder haver uma divisão entre “real” e “virtual”, visto que é quase incompreensível ter pleno acesso à própria ideia de sociedade em si, sem que haja o uso de novas tecnologias interconectadas para tanto. O cotidiano se virtualizou de uma maneira que permeou a vida social de maneiras imperceptíveis. Se anteriormente havia a necessidade de ir pessoalmente ao banco para abrir uma conta, hoje isso pode ser alcançado em um simples aplicativo no celular. A vida social também é quase inexistente sem o uso da internet, seja para marcar um encontro entre amigos, como também para conhecer novas pessoas. A virtualização do “eu”, já é real.

Nesse contexto, surgem também novos desafios, como por exemplo, conceitos de “capitalismo de vigilância”, “sociedade da informação”, “colonialismo digital”, e a redefinição de proteção de direitos que parecem intangíveis, como por exemplo, o direito à proteção de dados. É nesse teor que esse trabalho tenta encontrar seu estaque, buscando retratar essas novas nuances, e a necessidade de uma visão internacional acerca do assunto, posto que a problemática apresentada perpassa os limites territoriais, tornando-se uma questão humana de forma geral.

O presente estudo teve forma utilizando o método dedutivo, em pesquisa bibliográfica, onde, após partir de premissas gerais, chega-se ao particular, por meio de teorias, normas e princípios. Existem três eixos principais nos quais se desenvolve o tema, quais sejam: primeiramente, irá tratar do acesso à internet como Direito Humano na era da Sociedade em Rede, usando, para esta última nomenclatura, os ensinamentos de Manuel Castells. Após, falar-se-á acerca de conceitos atuais, especialmente de colonialismo digital e capitalismo de vigilância. Ao final, haverá a interlocução entre os dois temas retratados,

com a especificação da necessidade de proteção de direitos individuais na esfera da internet, especialmente no que trata ao direito à proteção de dados. Finaliza-se, portanto, com o arremate geral sobre as novas perspectivas, e como a solução deve se firmar no âmbito internacional.

2. O acesso à internet como direito fundamental na era da sociedade em rede

O conceito de superioridade da matriz constitucional, é de extrema importância para a consecução da proteção de direitos a membros de uma mesma sociedade de forma igualitária. A noção de direitos fundamentais pode ser definida como um sistema de relações jurídicas básicas entre indivíduo e o Estado, fundamento de toda a ordem jurídica (Fernandes, 2017). São a forma física da proteção (ou abstenção) estatal, frente à sociedade, frutos de lutas pelo reconhecimento desses direitos.

No que concerne a classificação dos direitos fundamentais, muito se foi ventilado a respeito do assunto, porém, hoje há uma importância à definição dada por Paulo Bonavides, o qual categorizou em gerações de direitos fundamentais. Abre-se aqui um adendo para demonstrar uma crítica doutrinária moderna ao uso da palavra “gerações”, visto que pode caracterizar a ideia de abandono das conquistas da geração anterior, sendo a palavra “dimensão” a escolhida para retratar melhor essa classificação.

Por direitos de primeira dimensão, tem-se que são os direitos de liberdade (civis e políticos), os quais encontram um dever de abstenção por parte do Estado. Após, fala-se no surgimento dos direitos de segunda dimensão, quais sejam: os direitos sociais, culturais e econômicos, abarcando a noção de igualdade, exigindo do Estado prestações materiais. Ao final do século XX, cunhou-se o pensar de uma nova dimensão de direitos fundamentais, a terceira, a qual abarca os ideais de direitos que têm como destinatários todo o gênero humano, transindividuais, ou seja, o direito ao desenvolvimento, à paz, ao meio ambiente (Bonavides, 2011).

É no diapasão do reconhecimento de outras dimensões de direitos humanos, que este trabalho encontra o marco inicial para seu deslinde. Apesar de haver divergências doutrinárias ao que seriam os direitos de quarta e quinta dimensão dos direitos

fundamentais, Paulo Bonavides declara que o fator histórico dos direitos quarta dimensão seria a globalização política o que os definiriam como: a proteção do direito à democracia, à informação e ao pluralismo (Bonavides, 2011).

É no direito de quinta dimensão, segundo os ensinamentos de Augusto Zimmermann, que se encontra o escopo principal deste projeto. De acordo com o autor, são direitos de quinta dimensão aqueles que inerentes à realidade virtual, compreendendo o grande desenvolvimento da internet (Zimmermann, 2002).

Não é difícil de vislumbrar o porquê de haver doutrinadores colocando a internet como uma dimensão de direitos fundamentais. A revolução tecnológica remodelou a base material da sociedade, de forma a ser indissociável da mesma. O avanço das máquinas deixou de ser algo elitista ou privativo a temas de ficção científica, para ser algo do cotidiano, levando ao fato de que os processos de existência social e coletiva são moldados diretamente pelo meio tecnológico (Castells, 2000).

Hoje em dia, o movimento geral de virtualização afeta não apenas a informação e a comunicação, mas também aos corpos, ao funcionamento econômico, aos marcos coletivos da sensibilidade e o exercício da inteligência. A virtualização alcança inclusive as formas de estar junto, a formação do “nós”: comunidades virtuais, empresas virtuais, democracia virtual, etc. (Lévy, 1998).

A internet se apresenta como um “eu” descentralizado. Um local onde um indivíduo pode descobrir semelhantes, criar projetos, aumentar a rede de conexões, exercer seu ofício. No cyberspaço a noção de minoria é reduzida, e começa a haver uma pluralidade de semelhantes reunidos em prol de um objetivo comum. Não há espaço que coloque a funcionar as engrenagens do reconhecimento, como o espaço virtual. A integração social nesse ambiente foi tamanha, que hoje há pouco espaço para delimitação de o que é real e o que é virtual. São todos parte da universalização do indivíduo.

A internet moldou, de certa forma, o comportamento do sujeito, que deixou de ser passivo, meramente receptor do conteúdo emitido pelos meios de comunicação de massa, tornando-se um usuário ativo, participante do processo de disseminação e produção da informação que é veiculada na web (Chagas, 2011).

Todos integrantes da rede podem ser atores de uma grande peça mundial, que não conhece fronteiras ou padronagens usuais, nem definição de tempo e espaço da maneira como é conhecida. A internet é o ambiente para estudo, negócios, entretenimento, ativismo, crimes. Não é um ambiente dissociável da realidade palpável, mas sim, faz parte da mesma, em um macro organismo tão material quanto a própria existência social.

Quando se tem um ambiente determinante dos próprios anseios humanos, em um papel descentralizado, cujo funcionamento ainda é misterioso para grande parte da sociedade, não é impossível perceber o potencial de difusão do mesmo. O avanço da internet por todos os aspectos da vida cresce em escala exponencial. Se há vinte e oito anos era quase impossível abrir uma imagem no meio virtual sem que demorassem vários minutos, hoje a sociedade, via de regra, já acorda conectada, em uma teia espiralada de bits e algoritmos. Essa mesma conexão é necessária para que se faça simples atos do cotidiano, como abrir uma conta no banco ou conversar com algum amigo.

O crescimento alargado da internet trouxe também uma face obscura da mesma. Não demorou muito tempo para que houvesse a notícia de crimes cometidos por esse meio digital. Invasões de dispositivo, crimes contra a honra, espionagem, cyberbullying, são apenas alguns dos poucos exemplos de comportamentos desviantes que ocorrem nesse cenário. Por muito tempo, a jurisprudência moderna tratou a internet apenas como meio, amoldando as condutas praticadas a delitos pré-existentes, já positivados, no entanto, os casos foram ficando mais rebuscados, e já não havia mais como haver a subsunção, sem que princípios como a legalidade e a taxatividade fossem violados, havendo a necessidade de criação de delitos próprios, como aquele previsto no art. 154-A do Código Penal (invasão de dispositivo informático), indiciando que a internet não poderia ser tratada meramente como um meio, mas que deveria ser vista como um ambiente integrado ao conceito de sociedade, porém com regramentos individuais.

De outra forma, não há espaço mais propício a luta e proteção de direitos fundamentais como o meio digital. Por suas características, há fácil e rápida formatação que permite o agrupamento de ativistas em diversas searas. Não se fala apenas de abaixo-assinados virtuais, mas sim de verdadeiras revoluções moldadas em um ambiente tecnológico.

Parece se tratar de uma distopia, mas em verdade, a internet pode derrubar governos (ou elegê-los).

Os exemplos são muitos, e os movimentos sociais conseguem um misto de instantaneidade e alcance, que é peculiar à internet. A propagação do que seria conhecida posteriormente como “Primavera Árabe”, teve como mote propulsor, as redes sociais. Um relatório divulgado pela Dubai School of Government, indica a importância de serviços como twitter e facebook na disseminação e fortalecimento das manifestações populares.

A organização transacional WikiLeaks é outro exemplo do uso da internet para mudanças globais. Com suas postagens de conteúdos sensíveis e informações confidenciais, ela se traduz em uma das maiores e mais importantes contribuições para a liberdade de expressão e transparência que se pode observar nesse novo advento digital.

O plano de fundo do funcionamento da internet ainda é de curto alcance. Pode haver violações de direitos como privacidade e liberdade, sem que o usuário tenha sequer noção do que está acontecendo. E o potencial de dano é incalculável. Um dos grandes exemplos, foi a situação ocorrida na eleição americana de 2016, quando houve a descoberta da venda de dados sensíveis e informações pessoais para a empresa de consultoria política Cambridge Analytics. De posse desses dados (angariados em uma rede social), a empresa conseguiu usar técnicas para direcionar mensagens nas redes sociais de forma a chegar aos eleitores e favorecer o candidato republicano Donald Trump, influenciando diretamente na sua vitória eleitoral.

Não apenas os agentes privados são uma ameaça potencial, mas também o próprio governo. Nos Estados Unidos, a vigilância online é fortemente utilizada, especialmente sob o manto do Ato Patriota. Há relatos de casos de prisões e invasões domiciliares ilegais, que foram determinadas por análise de dados de geolocalização e pesquisa online. No Paquistão, ativistas foram mortos depois de ter sua identidade revelada por conteúdo postado na internet.

Depreende-se, portanto, que o acesso à internet é essencial para a sociedade, não se consubstanciando em privilégio, mas sim em um direito geral. Novos modelos democráticos e novas formas de mobilização social têm seu berço no cyberspaço. Negar

esta inclusão, é ir ao contraponto de conceitos basilares como a própria dignidade da pessoa humana.

Proteger o acesso à internet como direito fundamental é colocar uma lupa em questões sedimentares para o presente e o futuro, tais como: vigilância, privacidade, liberdade de expressão, assim como muitos outros, sendo também o primeiro passo para a engrenagem de um conceito de governança da internet. O “eu digital” não se dissocia do “eu real”, e o perigo que existe para um, existe para outro. A internet está se tornando cada vez menos livre ao redor do mundo, levantando perigo pra direitos individuais, e para a democracia, necessitando de proteção.

Destarte, o acesso à internet não pode ser visto como um privilégio, mas sim como um direito ao alcance de todos. Ao determinar a importância da internet para novos contextos (como acesso a informação e proteção de direito individuais, por exemplo), não há como dissociar a sua integração no próprio escopo da Dignidade da Pessoa Humana e do Estado Democrático de Direito. Com base na visão pragmática e fenomenológica da acepção dos direitos fundamentais e na realidade, tem-se que se é necessário que haja uma internalização do acesso à internet como direito fundamental positivado.

A tendência de proteção maior já existe no cenário internacional, que se encontra mais atualizado com as novas sistemáticas protecionistas. A ONU, em 2016, pronunciando-se na sua Assembléia Geral, declarou, no documento A/HRC/32/L.20 que a internet (consubstanciada pelo seu acesso), é um direito humano, que deve ser protegido e tornado acessível a todos. Países como a Islândia (que foi a primeira a colocar em prática do conceito de “constituição virtual”) e a Noruega, explicitamente já colocaram uma obrigação positivada de conectividade social.

Não é difícil de perceber por que o acesso à internet deve ser considerado um direito humano, e positivado internamente nos ordenamentos jurídicos. A virtualização da vida humana como movimento propulsor que consubstancia a integração e proteção de demais direitos, como por exemplo, o acesso à informação, é indiscutível. A constitucionalização do acesso à internet serviria como conceituação única e irradiação vertical dessa proteção contra ingerências, sejam elas estatais ou privadas. Haveria a necessidade de uma maior transparência e resposta e a obrigação negativa de insurgência

contra abusos, além de uma observação a conceitos como colonialismo digital, vigilância, censura, liberdade de expressão, privacidade, espionagem cibernética, segurança digital, dentre outros.

3. Capitalismo de vigilância e colonialismo digital: o novo imperialismo

3.1. Capitalismo de vigilância

A internet se consubstancia na base tecnológica para a nova forma organizacional na Era da Informação. Por essa nova forma, temos que seria exatamente a rede. Por rede, entende-se não apenas no sentido técnico da palavra, mas sim, de forma mais abrangente, no sentido de conexão, inclusive, falando de interconexão subjetiva entre pessoas.

A procura por conexão social é uma prática de sobrevivência evolutiva. Sempre houve a busca de viver entre iguais, e de extrair dessas convivências, laços afetivos. Com a internet, essa conexão tornou-se cada vez mais fácil, e cada vez mais rápida, quase que instantânea. Não é difícil, portanto, perceber que não havia nenhum modo pelo qual os potenciais da internet não se achassem em pleno desenvolvimento, na sociedade. A internet é um meio de comunicação que permite, pela primeira vez, a comunicação de muitos com muitos, num momento escolhido, em escala global (Castells, 2000).

A velocidade da transformação fez com que ficasse difícil de prever as mudanças estruturais que ocorreriam com a internet disseminada em escala mundial, e com tanto alcance. A projeção do futuro, por vezes se baseava em uma distopia dissociada da realidade, mais parecida com os livros de ficção científica. O grande diferencial da tecnologia, especialmente de uma tecnologia informacional como a internet, é que não existe um momento de ruptura, um momento de transformação que seja palatável. Enquanto se espera por um momento específico que mudança, ele já aconteceu, e está indo em direção a um novo modelo.

Portanto, até se perceber o que estava acontecendo, as práticas determinadas no presente capítulo, já estavam enraizadas no cotidiano digital, sem que a maioria das pessoas pudesse analisar o real perigo das novas práticas.

O termo “capitalismo de vigilância” tem suas origens mais determinadas, nas pesquisas de Shoshana Zuboff. Para essa estudiosa, o diferencial dessa nova faceta do capitalismo, é exatamente o fato de usar o comportamento humano (e não a mão de obra) como meio de produzir lucro e controle de mercado. O modo mais claro de fazer isso, é por meio de tecnologias digitais, onde se vigia e prevê o comportamento humano, tendo bases, portanto, para, com esses dados, modificá-lo.

O diferencial nesse modelo é justamente o uso de dados dos usuários (geralmente a captação de dados é feita de forma não clara), para que haja uma padronização, um modelo preditivo de comportamento, a fim de, ao mesmo tempo, saber exatamente qual o hábito de determinada pessoa, e também poder manipulá-lo, ao ponto de modificar esse mesmo hábito, com fins determinados.

É importante frisar que o capitalismo de vigilância não significa tecnologia. Muitas vezes, a captação de dados é colocada como pressuposto para que determinada tecnologia ou determinado produto, funcione. O que se coloca aqui, como capitalismo de vigilância, é uma norma forma de mercado, mas que não encontra vida fora da tecnologia, mas não é “a” tecnologia em si. Imperativos comerciais não são a mesma coisa que necessidades tecnológicas.

Portanto, usando movimentações tecnológicas como, por exemplo, a análise massiva de dados (big data), essa forma de capitalismo busca prever e modificar o comportamento humano, como forma de produzir lucro e controle de mercado, não apenas impondo a informação, mas também produzindo a informação em escala massiva.

As primeiras facetas da hegemonia e controle de mercado que começam a se delinear, podem ser vistas de forma concreta, levando em consideração o Google, considerado como percussor desse novo movimento, como exemplo. De acordo com o projeto Atlas of digital hegemony, que desenvolve um estudo acerca do controle digital, o gigante do mecanismo de buscas, é o mais usado em quase todos os países do mundo, com exceção da China.

Aqui, demonstra-se um aspecto especial dessa nova sistemática, que é justamente a busca pela hegemonia. Se algo se torna o status quo informático, ele adquire o potencial de

coletar mais dados, operando de forma a capturar todo aspecto do cotidiano de uma pessoa, a qual, muitas vezes, submete de forma “voluntária” (aqui a expressão encontra-se em aspas, visto que a submissão é voluntária, porém o uso dos dados muitas vezes encontra-se obscuro, por isso não se pode dizer que existe uma voluntariedade completa) por meio das redes sociais.

E o que acontece com esses dados? Eles podem ser coletados em prol da própria rede em si, como o Google sabendo seus hábitos de pesquisa e moldando os resultados das buscas para algo mais apelativo, como também podem ser vendidos a terceiros, com fins comerciais. Ou, ainda de forma mais assustadora, entregue a agências governamentais, como por exemplo, serviços de inteligência.

Essa nova lógica é sedutora, e muito mais difícil de ser detectada, visto que ela explora as necessidades de forma muito concreta, promovendo informação ilimitada e maneiras de antecipar o que as pessoas querem, de forma fácil e simples, sendo que esse novo mercado é uma lógica diferenciada, onde a vigilância e os padrões comportamentais são transformados em lucro (Zuboff, 2019).

O capitalismo de vigilância se baseia em uma assimetria de conhecimento. Pela primeira vez, há maneiras possíveis de se obter uma quantidade de dados sobre determinadas pessoas, e, não apenas isso se pode processar, analisar, padronizar e prever comportamentos de acordo com esses dados. No entanto, não é apenas para o mercado que esses dados são usados. Com a previsão de padrões comportamentais, surge uma maneira de ter o controle dos mesmos, e modificá-los, de forma que não há nem a percepção do que está acontecendo. O que pode comprometer até mesmo a ideia de democracia, visto que os dados podem ser manipulados em prol de um fim comercial, e até mesmo político.

Uma das principais polêmicas ao colocar um holofote sobre como os dados dos usuários são capturados, refere-se ao escândalo do Facebook e da empresa Cambridge Analytica. A empresa referida teria usado dados disponíveis na rede social, a fim de traçar perfis de eleitores nos Estados Unidos. No entanto, foi noticiado que os dados usados foram obtidos de forma ilegal.

Em 2014, um teste de personalidade inofensivo, teve sucesso na rede social. O funcionamento é bem simples: os usuários, ao realizar o teste, dentro da plataforma do Facebook, dava permissões para que ele acessasse alguns dados. O grande problema começa a partir do momento que não se dá uma atenção especial para o tipo de acesso que determinado programa ou aplicativo pede. Assim como os termos e condições, os acessos de terceiros contém fatos que, se fossem mais públicos, provavelmente não seriam permitidos por todos.

No caso em questão, o teste requisitava acesso não apenas aos dados de quem o fazia, mas também de toda a rede de contatos do usuário. Nesse contexto, esses dados foram vendidos para a empresa Cambridge Analytica, de forma que ela agora detinha informações sobre cerca de 50 milhões de pessoas que se encontravam com cadastro no Facebook. De porte desses dados, a empresa conseguiu realizar a análise e traçar padrões psicológicos, criando uma campanha digital hiper-segmentada para seus clientes, especialmente o que viria a ser o presidente norte-americano, Donald Trump, oferecendo aos eleitores, publicidade distribuída no Facebook em forma de anúncios patrocinados no feed.

Desta forma, pode-se apresentar que, pela primeira vez, tem-se registro de uma mudança específica em uma manipulação eleitoral, por meio da captura de dados e projeção de perfis. Ao levarmos em consideração que as eleições, consubstanciada pelo ato de votar, é um dos pilares de um Estado democrático, quando se está diante de uma forma de alienação sorrateira, com base em uso de dados que nem ao menos foram coletados de forma pública e consentida, tem-se que a própria esteia democrática se encontra em risco.

A sociedade se encontra muito atrasada em relação à essa nova forma de exploração, especialmente porque ela seduz no contorno da facilidade e da individualidade de seus produtos e serviços. Tão importante quando uma questão de saber o que está acontecendo, deve-se cuidar para que o véu da facilidade caia, e que seja demonstrado que a própria individualidade e autonomia comportamental estão sendo colocadas em risco, tudo isso pela facilidade de ter um produto específico em uma propaganda já direcionada.

Aos poucos existe um movimento de contenção de danos. Há uma importância maior no cenário mundial (e também nacional), com a proteção de dados individuais. Esse assunto será tratado com mais profundidade no capítulo posterior, quando irá haver uma incursão de proteção social nessa nova sistemática.

3.2. Colonialismo digital

A datificação da sociedade não remete apenas a uma nova forma de capitalismo, mas também a uma nova forma de colonialismo. Essa nova ordem cria a dependência de plataformas, as quais usam os dados para continuar a recriar o círculo de dependência, assim como uma nova forma de discriminação social.

Se no passado os impérios definiam seu controle por meio da ocupação de rotas e matérias-primas, a nova forma de dominação é por meio do uso da tecnologia, dados e poder computacional. Muito se fala acerca dos dados serem o novo “petróleo”, no entanto, diferentemente do combustível fóssil, a extração de dados é feita de maneira muito menos definida e contornada. Na verdade, muitas vezes nem existe o conhecimento de que essa extração está ocorrendo.

A luta entre controle e liberdade não é nova, mas diferentemente do passado, não existe a noção de que não há liberdade na internet, até o momento dela deixar de existir completamente, posto que todas as engrenagens rodam de modo encoberto. E não apenas isso, mas, dessa vez, os donos do poder não se encontram em Impérios e Países, mas sim em empresas. A colonização ocorre precipuamente no Vale do Silício, e até mesmo os Estados estão sob controle do poder tecnológico de poucos. Nesse momento de dominação global, existe a penetração em governos, em movimentos dos cidadãos, em predição de comportamentos de todos que se encontram, de alguma forma, conectados. E se a tendência é a conexão global, então pouco se pode fazer para mudar esse cenário, a não se que as atitudes comecem a ocorrer agora.

Sartre (1968) define o colonialismo enquanto sistema econômico, atuando conforme os interesses e necessidades, com objetivos de explorar os recursos sociais e naturais da colônia, em benefício do colonizador. É um dos parâmetros da colonização também, impor

os parâmetros de diferenciação e hierarquia, além da ideia de que há uma necessidade da colônia, em ser colonizada. Explica-se: com a ideia de hierarquia, pressupõe o fato de que existe um poder maior (no caso, o ator explorador). Incutindo essa ideia, ajuda a conceituação de que existe algo em troca, como por exemplo, ajudar a construir casas em prol de uma extração de recursos minerais em determinada localidade. Há uma falsa percepção da realidade.

Quando tratamos dos ambientes digitais, percebe-se que não é muito diferente. Os recursos de dados são extraídos de forma exploratória, manifestando-se em uma conotação de controle. O colonialismo digital comina as práticas predatórias extrativistas, com a quantificação abstrata da internet (Coldry, 2018.), criando uma situação de dependência.

Existe uma extração racional, que trata da extração de dados de maneira que não há valor na mesma, é apenas um compartilhamento, operando na sociedade ao ponto de apresentar que as pessoas se beneficiam dessa manifestação na rede. Ou seja, não existe nada de ruim no fato de uma pessoa compartilhar sua localização, sendo que ela irá se beneficiar com um cupom de desconto para almoçar em um local perto de onde esteja, por exemplo. É justamente nesse contexto que o colonialismo digital é perigoso: porque não é tão perceptível.

Os principais atores do colonialismo de dados (ou colonialismo digital) podem ser denominados de “setores de quantificação social”, que são as corporações envolvidas em capturar o dia a dia e transformar em dados quantificados que são analisados a fim de gerar lucro (Coldry, 2018). Podemos citar empresas como Amazon, Facebook e Google no ocidente, e grandes como Baidu e Alibaba no oriente, mais precisamente na China. Apesar de haver essa divisão entre oriente e ocidente, percebe-se que ela não se mantém de forma essencial, visto que, basicamente, essas empresas atuam em todos os locais, em virtude da falta de fronteiras quando se fala em atuação pela internet.

As grandes corporações, detentoras das fronteiras tecnológicas, usam todas as ferramentas à sua disposição para centralizar os serviços de internet, vigiar seus usuários, processar seus dados, e usar esses mecanismos para fazer com que esses continuem reféns de seus serviços. A população, por sua vez, se encontra pouco preocupada com essa

questão, posto que concorda com esses abusos, visto que, em contrapartida, utiliza serviços gratuitos e que melhoram sua experiência.

Essas Big Tech conseguem reunir características que impedem que mais atores consigam adentrar nesse cenário: primeiro, recursos e materiais (como servidores e controle de cabeamento, por exemplo), e também o recurso intelectual à tecnologia de ponta e às melhores mentes capacitadas para lidar com ela. Ademais, também a política internacional, como também as engrenagens jurídicas, funcionam em prol do poder ativo, fazendo com que seja muito difícil se livrar do giro dessa roda, haja vista a limitação de capacidade de pesquisa e inovação.

As grandes empresas vêm os países subdesenvolvidos como o grande mercado em expansão. Geralmente adentram neste cenário, utilizando-se de um plano de fundo social, como por exemplo, o caso do Free Basics, serviço do Facebook. No contexto, a empresa disponibilizou o conceito de conectividade às pessoas que não poderiam ter acesso à isso. Criaram suas próprias redes e servidores em países que não tinha a infraestrutura necessária, e ofereceram o serviço de finalmente, conectar às pessoas a uma nova era. No entanto, o que realmente existe é uma captura massiva de dados (que se transformam em análise comportamental), além de conteúdo direcionado. As pessoas não vêem uma internet livre, mas sim uma rede com conteúdo pré-definido, o que pode mudar drasticamente a forma de ver o mundo. Um mundo pelos olhos das grandes corporações, permitindo novas formas de exploração e subordinação.

4. Breves linhas acerca da proteção de dados na esfera digital

Como visto em linhas anteriores, as novas mudanças sociais e tecnológicas estão modificando as estruturas de conteúdos que já se encontravam quase que estratificados. Novas formas de capitalismo e colonização enquadram esse novo panorama, e os dados pessoais são o novo alvo de países e corporações (Rodota, 2008).

Há, hoje, a possibilidade de indivíduos e grupos controlarem o exercício dos poderes baseados em disponibilização de informações, com novas formas de coleta e tratamento de dados. O aumento na quantidade de informações pessoais coletadas pode visar alguns

objetivos, e alguns deles podem não ser necessariamente ruins, como por exemplo, o uso pela administração pública para preparação de programas de gestão e intervenção social, por exemplo.

A coleta de dados não é necessariamente algo maléfico, e em alguns casos, é necessária para o próprio funcionamento de algum programa ou plataforma, como por exemplo, usar dados de músicas mais ouvidas para formar uma lista de novas músicas que o usuário pode usar.

O maior problema dessa extração é a falta de consciência da sociedade a respeito de como isso está acontecendo. A falta de transparência acerca do assunto, é assombrosa. Não se sabe como os dados estão sendo coletados, para que, e para quem eles estão sendo vendidos ou compartilhados.

Essa passividade a respeito do que está acontecendo, parece que encontra mudança aos poucos. Um dos diplomas pioneiros referentes ao assunto, é a GDPR. O Regulamento Geral sobre a Proteção de Dados é um conjunto de regras válido para a União Européia, porém, pelo aspecto descentralizado da internet, tem impactos em todo o mundo, seja de forma incisiva ou colateral.

A proteção de dados pessoais é considerada um direito, portanto, as empresas e organizações deverão seguir regras rígidas para coletar, processar, compartilhar e resguardar dados pessoais, devendo o usuário saber quais dados estão sendo coletados e para quais finalidades, assim como maneiras de haver a solicitação para que a haja a exclusão das informações já coletadas, ou a interrupção da coleta. Dentre outras normativas, o uso de linguagem clara, concisa e transparente para que as pessoas possam compreender as comunicações a respeito de seus dados, incluindo termos e condições de privacidade.

O regramento europeu foi pioneiro em uma regulamentação extensiva, mas o Brasil não demorou muito a ter sua própria normativa neste sentido. Em agosto de 2018 foi publicada a Lei 13079 (2018), denominada de Lei Geral de Proteção de Dados. Em muitos aspectos têm uma proteção análoga à diretriz europeia, sendo mais protetiva em outros.

Segundo a referida lei, a disciplina da proteção de dados pessoais tem como fundamentos: o respeito à privacidade, a autodeterminação informativa, a liberdade de expressão, informação, comunicação e opinião, a inviolabilidade da intimidade, honra e imagem, o desenvolvimento econômico e tecnológico e a inovação, a livre iniciativa, livre concorrência e a defesa do consumidor, como também os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Também se incute na lei que as atividades de tratamento de dados deverão observar alguns princípios, sendo o corolário deles a boa-fé. Dentre os princípios citamos, finalidade: propósitos legítimos, específicos, explícitos e informados ao titular; adequação: compatibilidade do tratamento ao mínimo necessário para a realização de suas finalidades; necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos; livre acesso: garantia de consulta facilidade e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados; qualidade dos dados: garantia de exatidão, clareza, relevância e atualização e dados; transparência: informações claras, precisas e facilmente acessíveis sobre a realização do tratamento; segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados; prevenção: prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; não discriminação; responsabilização e prestação de contas.

Percebe-se, portanto, o rol extensão de direitos e princípios que se encontram no referido diploma, demonstrando que é necessário que se olhe de uma maneira mais protetiva para a questão do uso, coleta e tratamento de dados pessoais. Obviamente que é complicado, tecnicamente falando, apontar que há uma coleta indevida e uma transferência ilegal desses dados, sem uma perícia ou auditoria, porém, a legislação já cria um enfoque protetivo nessa seara.

Deve haver um profundo processo de revisão dos critérios do que se hoje conhece por: privacidade, vigilância e controle, para que se possa olhar de modo ressignificado essas novas diretrizes que são colocadas em uma Sociedade em Rede. Deve haver uma reclassificação das informações pessoais, segundo uma escala de valores renovada, na

qual deveria ser garantido o máximo de opacidade às informações (Rodota, 2008), posto que elas são suscetíveis de moldar as sociedades para se curvarem a seus interesses.

5. Conclusão

Este ponto tecnológico em que hoje se encontra o mundo era impensável apenas há poucos anos. As inovações mudaram a forma de pensar e de se relacionar, consubstanciando-se inclusive em um novo tipo de sociedade: A Sociedade em Rede. E o povo começou a descobrir também as potencialidades dessa nova esfera pública que se encontra em meio digital, acabando com a dicotomia entre real e virtual.

A internet ajudou a derrubar regimes. A mudar a legislação. A fazer com que governantes se curvassem a uma imposição da maioria do povo que clamava por mudanças. O potencial da internet para a legitimação de democracia é gigante.

De repente, todos estão conectados. A espaço de poucos cliques, pode-se saber o que está acontecendo em qualquer lugar do mundo, e tomar ação em situações onde a passividade antes predominava. O lugar de fala aumentou. Não existe ferramenta que tenha tanto alcance para aproximar um povo ao seu governo, do que a internet. E aproximar o restante do mundo também.

No entanto, com as mudanças, novos meios de exploração também surgem nesse domínio. A captação e o uso de dados têm efeitos que não conseguimos vislumbrar ainda. O que pode acontecer se uma futura empregadora souber dos hábitos de saúde de um candidato? O que pode acontecer se ela tiver acesso às preferências políticas daquele que pleiteia uma vaga em sua empresa? O que as grandes corporações fazem com todos esses dados coletados, preferências, e descobertas de coisas que não se conta para ninguém, mas se pesquisa no Google? Estamos vendo apenas a ponta do iceberg no que se refere ao que a Big Data pode trazer nesses anos porvir. O potencial danoso de quem tem o poder por trás dos dados, é de difícil constatação. E não se fala apenas em uma massa de propagandas direcionadas, mas sim de manipulação a ponto de haver medo de ruptura até mesmo em sistemas democráticos.

Chegou-se a um ponto crítico, devendo haver a conscientização da população acerca do tratamento de seus dados. Ver a manipulação por trás dos benefícios e da imediatividade. Para tanto, a transparência e a uniformização de regramentos internacionais deve acontecer. O fomento à pesquisa e a ajuda a novos atores na área tecnológica é de vital importância para combater a hegemonia do mercado.

A internet é plural, imediata, descentralizada. A fim de combater os danos advindos do mau uso dessas novas plataformas, as ações devem seguir o mesmo padrão: plural, imediata e descentralizada. Cabe ao direito, nacional e internacional, e à sociedade como um todo, se enquadrar nesses novos padrões de combate, a fim de que não se chegue a um ponto de controle e vigilância sem volta.

Referências

Alexy, Robert. (2008). Teoria dos Direitos Fundamentais, Tradução de Virgílio Affonso da Silva, 1ª Ed., Malheiros Editores.

Almeida de Evangelista, R. Capitalismo de Vigilância no Sul Global: Por uma perspectiva situada. Recuperado de: <http://lavits.org/wp-content/uploads/2018/04/08-Rafael-Evangelista.pdf>. Acesso em 15 de abril de 2019.

Almeida Filho, J. C. de Araújo. (2015). Direito Eletrônico ou Direito da Informática? Informática Pública vol. 7 (2): 11-18. Recuperado de: http://www.ip.pbh.gov.br/ANO7_N2_PDF/IP7N2_almeida.pdf. Acesso em 10 de setembro de 2018.

Alves, Marcelo de Camilo Tavares. (2009). Direito Digital. Goiânia. 9-10 pp. em <http://aldeia3.computacao.net/greenstone/collect/trabalho/import/Direito%20Digital.pdf>. Acesso em 10 de setembro de 2018.

Bauman, Z. (2014). Vigilância líquida. Rio de Janeiro. 1ª edição. Editora Zahar.

Bertoldi, M. R., & Santos de Oliveira, K. C. (2011) de (coords.) Direitos Humanos: entre a utopia e a contemporaneidade. Belo Horizonte: Fórum.

Blum, Renato M. S. (2006). Opice. Manual de Direito Eletrônico e Internet. São Paulo: Aduaneiras, 680p.

Bonavides, P. (2011). Curso de Direito Constitucional. 26ª edição. São Paulo: Malheiros.

Budapeste, 23 nov. 2001. Convention on Cybercrime. Recuperado de: <http://conventions.coe.int/Treaty/EN/Treaties/html/185.htm>. Acesso em 23 de outubro de 2018.

Castells, M. (1999). *A Sociedade em Rede. A era da informação: economia, sociedade e cultura volume I*, São Paulo, Editora Paz e Terra.

Comparato, F. K. (2011). *A afirmação histórica dos direitos humanos*. São Paulo: Saraiva.

Couldry, N. & Meijas, U. (2018). Data colonialism: rethinking big data's relation to the contemporary subject. Recuperado de <https://journals.sagepub.com/doi/abs/10.1177/1527476418796632?journalCode=tvna>. Acesso em 20 de maio de 2019.

Declaração Universal dos Direitos Humanos. Recuperado de: <http://www.humanrights.com/pt/what-are-human-rights/universal-declaration-of-human-rights/articles-11-20.html>. Acesso em 11 de outubro de 2018.

Fernandes, B. G. (2017). *Curso de Direito Constitucional*, Salvador: Ed. JusPodivm.

Gelman, M. (2007). *Direitos Humanos: a sociedade civil no monitoramento*. Curitiba: Juruá.

Herkenhoff, J. B. (2002). *Direitos Humanos: a construção universal de uma utopia*. São Paulo: Santuário.

Ihering, R. V. (1993). *A luta pelo direito*. Tradução de João Vasconcelos. 17. ed. Rio de Janeiro: Forense.

Lei 7.232/84: LEI N.º 7.232, de 29 de outubro de 1984. Dispõe sobre a Política Nacional de Informática, e dá outras providências. Recuperado de: <http://presrepublica.jusbrasil.com.br/legislacao/109644/lei-7232-84>. Acesso em 29 de outubro de 2018.

Lei N.º12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.. Recuperado de: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em 29 de abril de 2018.

Lei N.º13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Recuperado de: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em 20 de maio de 2019.

_____. Internet e regulação: o bom exemplo do Marco Civil da Internet. *Revista do Advogado*, São Paulo, n. 115, ano XXXII, pp. 99-112, abr. 2012. LÉVY, Pierre. O que é o virtual? São Paulo: 34, 1997.

Lehtiniemi, Tuukka. Personal Data Spaces: an intervention in surveillance capitalism?. Recuperado de: <https://ojs.library.queensu.ca/index.php/surveillance-and-society/article/view/6424/6678>. Acesso em 10 de maio de 2019.

Lévy, P. (1999). Cibercultura. São Paulo: 34.

Medeiros, Claudio Melquiades. (2006). Os Direitos Fundamentais e a atuação do magistrado: neoconstitucionalismo e garantismo jurídico. 2006. 135 p. Dissertação (Mestrado em Ciência Jurídica)- Universidade do Vale do Itajaí – UNIVALI, Itajaí. Recuperado em: <http://www.dominiopublico.gov.br/download/teste/arqs/cp038905.pdf>. Acesso em 29 de outubro de 2018.

Monteiro, V. Cibernética, Direito, ciberespaço. Ciberdireito? Recuperado de <http://www.datavenia.net/entrevistas/00001092001.htm>. Acesso em 12 de fevereiro de 2018.

Peck, Patrícia Pinheiro. (2009). Direito Digital: em defesa do mundo virtual. Fevereiro. Recuperado de: http://www.ambito-juridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=2901 . Acesso em 29 de fevereiro de 2018.

Polli, V. Mas, afinal, o que é Direito Digital?. Recuperado de: <http://www.meon.com.br/opiniao/opiniao/colunas/mas-afinal-o-que-e-direito-digital>. Acesso em 29 de fevereiro de 2018.

Rodota, S. (2008). A vida na Sociedade da Vigilância: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro. Renovar.

Sarlet, I. W. (2003). A Eficácia dos Direitos Fundamentais. Porto Alegre: Livraria do Advogado.

Sartre, Jean Paul. (1968). Colonialismo e Neocolonialismo. Rio de Janeiro: Tempo Brasileiro.

Schaff, Adam. (1995). A sociedade informática: as consequências sociais da segunda revolução industrial. Tradução Carlos Eduardo Jordão Machado e Luiz Antônio Obojes. São Paulo: Universidade Paulista Brasileira.

Segal, I. E. (1992). Norbert Wiener. National Academy of Sciences. Washington: National Academy Press.

Zimmermann, A. (2002). Curso de Direito Constitucional. 2.ed. rev.ampl. e atual. Rio de Janeiro: Lumen Juris.

Zuboff, S. Big Other: Surveillance Capitalism and the Prospects of an Information Civilization. Recuperado de: <http://papers.ssrn.com/abstract=2594754>. Acesso em 18 de abril de 2019.

Zuboff, S. (2019). *The Age of Surveillance Capitalism: the fight for a human future at the new frontier of power*. Nova Iorque: Public Affairs.