Acta Scientiarum. Human and Social Sciences
ISSN: 1679-7361
ISSN: 1807-8656
actahuman@uem.br
Universidade Estadual de Maringá
Brasil

Souza, Edna Alves de; Villa, Rômulo Maldonado; Gonzalez, Everaldo Tadeu Quilici
Privacidade e autonomia na era de Big Data
Acta Scientiarum. Human and Social Sciences, vol. 42, núm. 3, e56202, 2020, -
Universidade Estadual de Maringá
Maringá, Brasil

DOI: https://doi.org/10.4025/actascihumansoc.v42i3.56202

Disponible en: http://www.redalyc.org/articulo.oa?id=307365949010

Acta Scientiarum
http://periodicos.uem.br/ojs/acta
ISSN on-line: 1807-8656
Doi: 10.4025/actascihumansoc.v42i3.56202

Privacidade e autonomia na era de *Big Data*

Edna Alves de Souza[1*], Rômulo Maldonado Villa[2] e Everaldo Tadeu Quilici Gonzalez[3]

[1]Faculdade de Filosofia e Ciências, Universidade Estadual Paulista "Julio de Mesquita Filho", Av. Hygino Muzzi Filho, 737, 17525-900, Marília, São Paulo, Brasil. [2]Centro Universitário Eurípides de Marília, Marília, São Paulo, Brasil. [3]Universidade Metodista, Piracicaba, São Paulo, Brasil. *Autora para correspondencia. E-mail: ednalves@alumni.usp.br

RESUMO. Neste artigo, temos por objetivo analisar alguns dos desafios atuais colocados pelas Tecnologias da Informação e Comunicação (TIC), quanto às questões de privacidade e autonomia no que concerne ao controle de dados pessoais, através de recursos de *Big Data*. Nossa análise se restringe aos dados pessoais que identificam ou que podem identificar uma pessoa, de modo a colocar em xeque sua privacidade e autonomia. Inspirados em hipóteses elaboradas por John Stuart Mill sobre a influência que a sociedade exerce sobre os indivíduos, argumentamos que há que se proteger a independência individual em face de práticas impositivas, e por vezes irracionais, que a opinião coletiva pode exercer sobre os indivíduos. Uma dificuldade sugerida por Mill estaria em se identificar, na prática, o limite entre a autonomia da pessoa e o controle social. Argumentamos que, ainda que em contextos distintos, essa dificuldade não só persiste na Sociedade da Informação contemporânea como se mostra premente com o acelerado desenvolvimento de TIC, *Big Data*, *Internet* das Coisas e Computação Ubíqua que integram parte significativa da vida dos indivíduos. Admitimos que as possibilidades apresentadas pelas TIC são, em muitos casos, consolidadoras de direitos básicos como o de acesso à informação, entre outros; contudo a vigilância e o controle governamental e empresarial, facilitada pelo desenvolvimento das TIC, por sua vez, nos conduz à indagação sobre possíveis consequências negativas sobre a autonomia individual na Sociedade da Informação vigente. Considerando os três Vs característicos dos *Big Data*: volume, velocidade, em tempo real, e variedade (Laney, 2011), discutimos neste artigo aspectos positivos e negativos do emprego de recursos de *Big Data*, especialmente, por governos e grandes corporações, no que diz respeito à sua influência na privacidade e autonomia humana.

Palavras-chave: *Big Data;* controle; computação ubíqua; sociedade da informação; ética.

Privacy and autonomy in the Big Data era

ABSTRACT. In this article, we aim to analyze some of the current challenges posed by Information and Communication Technologies (ICT), regarding issues of privacy and autonomy with regard to the control of personal data, through Big Data resources. Our analysis is restricted to the personal data that identifies or can identify a person, in order to put their privacy and autonomy in check. Inspired by hypotheses made by John Stuart Mill about the influence that society has on individuals, we argue that individual independence must be protected in the face of imposing, and sometimes irrational, practices that collective opinion can have on individuals. A difficulty suggested by Mill would be to identify, in practice, the limit between the person's autonomy and social control. We argue that, even in different contexts, this difficulty not only persists in the contemporary Information Society, but is also pressing with the accelerated development of ICT, Big Data, Internet of Things and Ubiquitous Computing that make up a significant part of the lives of individuals. We admit that the possibilities presented by the ICT are, in many cases, consolidators of basic rights such as the access to information, among others; however, governmental and business surveillance and control, facilitated by the development of ICT, in turn, leads us to inquire about possible negative consequences on individual autonomy in the current Information Society. Considering the three Vs characteristic of Big Data: volume, speed, in real time, and variety (Laney, 2011), we discuss in this article positive and negative aspects of the use of Big Data resources, especially by governments and large corporations, with regard to their influence pricy and human autonomy.

Keywords: Big Data; control; ubiquitous computing; information society; ethics.

Received on October 30, 2020.
Accepted on November 27, 2020.

Introdução

A existência de uma sociedade em que os indivíduos são continuamente observados e vigiados deixou de ser uma ficção, como o romance *1984* de George Orwell ([1949] 2009), para se tornar não só uma possibilidade, mas uma forte tendência na atualidade. A vigilância e o controle governamental e empresarial hoje são uma realidade, tornada possível pelo desenvolvimento de Computação Ubíqua, *Big Data*, *Machine Learning*, *Internet* das Coisas e Tecnologias da Informação e Comunicação (TIC) em geral. Essas tecnologias pervasivas permitem a captação (e manuseio) de rastros digitais deixados pelas pessoas em seu dia-dia em um ambiente cada vez mais tecnológico. Daí significativa razão de vivermos hoje na chamada Sociedade da Informação, em que quase tudo é datificado; atos corriqueiros presentes nas redes sociais, no uso de celular e de pesquisas em sites de busca, já nos colocam em interação com o universo de coleta, registro e análise de massiva quantidade dados, característica da Era de *Big Data*.

No presente artigo temos por objetivo analisar alguns dos desafios atuais colocados pelas técnicas de análise de *Big Data* e outras tecnologias pervasivas, quanto às questões de privacidade e autonomia no que concerne ao controle de dados pessoais.

Por um lado, muitas das possibilidades atrativas apresentadas pelas tecnologias digitais, como o fácil e rápido contato com pessoas, acesso a textos, livros, notícias, filmes, compras e outros, representam comodidades que podem otimizar o dia-a-dia dos usuários. Essas possibilidades são, em muitos casos, consolidadoras de direitos básicos, como o acesso à informação. Por outro lado, o desenvolvimento tecnológico apresenta também novos desafios, ampliando possibilidades de exploração de vulnerabilidades no ciberespaço. Diante desse impasse, entre benefícios e prejuízos causados pelo uso de tecnologias digitais e sua constante evolução, aparecem questões que incitam a reflexão e o debate em diversas áreas do saber, como destacam os atuais indicadores bibliométricos.

Nesse contexto, duas questões-chave guiam a presente reflexão: 1) Que subsídios pode a filosofia oferecer para a compreensão do conceito de liberdade de expressão na Sociedade da Informação? 2) Técnicas de *Big Data* podem viabilizar o controle ético e legal, que garanta o direito à privacidade e à autonomia de usuários das TIC?

As questões 1 e 2 serão discutidas em duas etapas. Na primeira, intitulada 'Liberdade, privacidade e controle de dados pessoais', resgatamos o conceito de liberdade proposto por Mill, para analisar questões sobre invasão de privacidade e perda de autonomia em um contexto de vigilância social. Na segunda seção, 'Desafios da Era de *Big Data*: aspectos éticos e epistemológicos', tecemos considerações sobre o dilema ético da fluidez da privacidade e da autonomia em sociedades controladas por recursos de *Big Data*. Por fim, esperamos apresentar contribuições, de cunho ético, propondo formas de regulamentação do uso de tecnologias pervasivas, que seja viável (sustentável) para a realidade contemporânea.

Privacidade, autonomia e controle de dados pessoais

Um dos autores que mais influenciou o pensamento filosófico no tocante à questão da liberdade individual foi John Stuart Mill (1806-1873). Em sua obra *Sobre a liberdade* ([1859] 1991), Mill elaborou hipóteses sobre a liberdade individual, argumentando que o Estado deveria garantir aos indivíduos toda liberdade possível, limitando-se apenas a controlar aqueles comportamentos e ações que causassem danos ou prejuízos a terceiros. Para Mill, todo indivíduo deveria ter a garantia da lei, de que poderia viver, agir e pensar como bem lhe aprouvesse, pois essa liberdade seria fundamental para a construção de uma vida feliz. E construir uma teoria racionalista sobre a liberdade individual aplicada à sociedade, estava diretamente relacionada à busca por uma vida feliz ao maior número possível de pessoas, ou seja, ao papel da filosofia prática.

Atrelar ao conceito de liberdade individual a condição para a busca da felicidade foi a resposta oferecida por Mill a uma das problematizações fundamentais por ele mesmo apresentada, que diz respeito aos limites e alcances de uma vida feliz dos cidadãos no meio social. A ideia de liberdade com poucas restrições pode ser denominada de liberdade positiva, ao passo que a ideia de que as leis e o Estado devem impor limites, apenas e tão somente, aos comportamentos que causem danos a terceiros, pode ser, por sua vez, associada à chamada liberdade negativa. Com efeito, para o escritor e filósofo contemporâneo Isaiah Berlin ([1969] 2002), que examinou e defendeu tal distinção, o desenvolvimento das concepções de liberdade positiva e negativa se deve, em grande medida, ao pensamento de Mill sobre a questão da liberdade. Enfim, Mill defendeu que somente por meio da liberdade individual é que a sociedade humana poderia encontrar o florescimento do espírito humano e os fundamentos para uma vida feliz, apesar da dificuldade em se identificar, na prática, o

limite entre a liberdade da pessoa e o controle social, entre o que hoje podemos entender como liberdades positiva e negativa.

Inspirados em Mill[1], entendemos que há que se proteger a liberdade individual em face de ideias e práticas impositivas, e por vezes irracionais, da opinião coletiva. Por liberdade aqui, não nos referimos à liberdade do querer ou o livre arbítrio, mas a liberdade civil ou social demarcadora da autonomia do indivíduo frente ao tipo de poder que a sociedade, legitimamente, pode exercer sobre ele. Quanto à dificuldade em se identificar, na prática, o limite entre a autonomia da pessoa e o controle social, ela não só persiste como se mostra premente na era de *Big Data*. Considerada em termos da sociedade contemporânea informatizada, essa dificuldade residiria em se identificar, na prática, o limite entre privacidade e autonomia no que concerne ao controle de dados pessoais.

Por *Big Data* atualmente se entende mais do que quantidades massivas de dados; mas inclui a capacidade de registro, mineração, agregação, análise e referência cruzada de grandes conjuntos de dados. A análise de dados, por sua vez, pode também ser realizada de forma automatizada por algoritmos, capazes de manipular ampla variedade, volume e velocidade dos mesmos com vistas à obtenção, em geral de resultados práticos, e nem sempre de conhecimento propriamente dito. Como ressaltam Mayer-Schonberger and Cukie (2013): com *Big Data*, os dados se tornaram a matéria-prima da produção; como produto mercadológico, os dados têm imenso valor econômico e social. Nesse sentido, por *Big Data* pode se entender os dados massivos, associados a uma nova forma de coleta, processamento, análise, armazenamento e extração de valor das informações contidas em grandes bancos de dados, que permitem a tomada de decisão (humana ou automatizada), propiciando eficiência a grandes corporações públicas e privadas.

Embora atualmente existam tecnologias específicas para criar bancos de dados que alimentam os *Big Data*, em geral, o recurso a estes ocorre em função de um uso secundário de bancos de dados já existentes para finalidades específicas. Por exemplo, quando preenchemos um formulário *online* para fazer uma compra, podemos estar alimentando os *Big Data*, uma vez que as informações ali disponibilizadas podem ser captadas, analisadas e utilizadas para propósitos diferentes daquele que lhe deram origem.

Cabe observar que, em nossa Sociedade da Informação, não só as pessoas geram dados que são disponibilizados na internet. Com a Internet das Coisas (IoT, de *Internet of Things*), sensores de diversos tipos são acoplados/adaptados em aparelhos tecnológicos espalhados no ambiente, captando continuamente dados como imagens, sons e localização de objetos e pessoas, que ficam disponíveis para possíveis usos futuros.

A tomada de decisão nos negócios, na administração governamental, na pesquisa científica e até mesmo em pesquisas pessoais pode ser significativamente manipulada e modelada pela análise de dados a partir de técnicas inferenciais usadas com e através de recursos de *Big Data*. Uma questão relevante para a nossa investigação é: O que representam essas possibilidades de manipulação e modelagem no que diz respeito à autonomia da ação humana? Elas trazem, de fato, melhorias ou adversidades no que concerne à privacidade e autonomia pessoais?

É justificável o temor de que os recursos de *Big Data* possam ser mal utilizados ao dar, especialmente, aos governos e às grandes corporações, novas habilidades para competir deslealmente na política e no mercado ou induzir pessoas irrefletidamente à ideologias desumanas (contrárias ao florescimento humano) e ao consumo desenfreado.

No contexto acima delineado, de emprego de recursos de *Big Data* para manipulação de dados, entre eles dados pessoais de usuários de TIC, entendemos que se faz atual a reflexão de Mill ([1859] 1991, p. 102) segundo a qual "[...] o perigo que ameaça a natureza humana não é o excesso, mas a deficiência dos impulsos e preferências pessoais". E ainda:

> Uma pessoa cujos desejos e impulsos são autônomos – expressões da própria natureza como a desenvolveu e modificou a cultura – é dita de caráter. Outra, cujos desejos e impulsos não possuem essa autonomia, não tem caráter, não o tem mais do que uma máquina a vapor (Mill, [1859] 1991, p. 102).

Um dos pilares da concepção milliana de 'liberdade' consiste na defesa da legitimidade de se exercer a faculdade de exprimir a opinião, proporcionada pelo livre pensamento e pela livre discussão. A liberdade de expressão do pensamento é um importante ponto de passagem do ser humano da categoria de súdito para a de cidadão, garantida pelo uso da razão. Entretanto, a defesa da liberdade de exprimir o pensamento deve ser

[1] Estamos cientes do risco de anacronismo ao trazer o conceito de liberdade milliano para o tratamento da privacidade em uma época e contexto tão distintos daqueles do pensador. Contudo, uma vez que o pensamento de Mill nos serviu como fonte de inspiração, não poderia deixar de ser mencionado aqui.

lida em conformidade com certas restrições sociais que são contexto dependentes. A intervenção na liberdade de opinião, expressão e ação de outrem é legítima quando (e somente quando) servir para a autoproteção ou proteção de outras pessoas. Nas palavras de Mill ([1859] 1991, p. 124), "[...] quando se verifica um prejuízo definido, ou existe um risco definido de prejuízo, a um indivíduo, ou ao público, o caso sai do setor da liberdade, e recai no da moralidade ou no da lei", raciocínio que analogicamente pode ser estendido tanto à privacidade como ao controle de dados pessoais.

'Dados pessoais', no presente contexto, referem-se àquilo que identifica/individualiza ou que pode vir a identificar/individualizar uma pessoa, como credenciais, dados de consumo, dados médicos, dados de crédito, dados de navegação, dados de geolocalização e assim por diante.

A privacidade, por sua vez, pode ser aqui entendida como o direito de ficar só ou ser deixado só, sem exposição publica. Nesse sentido, a proteção da privacidade dos indivíduos envolve a garantia de seu isolamento, anonimato, sigilo. Por exemplo, no Artigo 12 da Declaração Universal dos Direitos Humanos (Unesco, 1948) lê-se:

> Ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. Toda pessoa tem direito à proteção da lei contra tais interferências ou ataques.

Na Sociedade da Informação, no entanto, o conceito de privacidade está sendo ressignificado. A 'privacidade' está sendo concebida também de forma funcional, como "[...] o direito de manter o controle sobre as próprias informações" (Rodotà, 2008, p. 92). O uso das TIC, *Big Data* e outras tecnologias pervasivas, com o intuito de satisfazer interesses, sejam comerciais ou ideológicos, pode ameaçar o direito da pessoa à privacidade. Contudo, na Sociedade da Informação a privacidade, paradoxalmente também está ligada à vigilância.

Entendemos por vigilância a utilização de meios ou mecanismos para observação, monitoramento, rastreamento, controle, classificação, apreciação e outras formas de atenção sistemática dirigida a um alvo, que pode ser uma pessoa, situação, fenômeno ou um objeto qualquer. Com recursos de *Big Data*, o potencial de vigilância tem aumentado; suas técnicas permitem violações da privacidade, segurança/controle civil e manipulação do consumidor, ao possibilitar a captação, muitas vezes ilícita e abusiva, de dados pessoais pela onipresença da tecnologia digital que desempenha agora um papel fundamental na vida diária das pessoas. Além do vigilantismo, os *Big Data* podem fomentar práticas discriminatórias, uma vez que dados pessoais são submetidos à análise algorítmica que por vezes carregam uma programação segregativa (Starr, 2013). Visando coibir ações discriminatórias, no Brasil, foram elaborados regramentos (seguindo a tendência internacional) como o Marco Civil da Internet (Lei nº 12.965, de 23 de abril de 2014) e o Decreto 8.771/16, em que pese não haver uma solução jurídica, de fato, completa e eficaz para o enfrentamento dos problemas colocados pelos avanços de técnicas de *Big Data*.

Para Bauman (2013), a vigilância é um dos pilares da Modernidade e, juntamente com ela, sofre transformações ao longo do tempo. A pós-modernidade ou modernidade líquida (em sua terminologia) traz consigo uma vigilância também líquida, que, silenciosamente, se espalha por toda parte, adentrando os vários setores da vida. Na modernidade líquida, com a ascensão dos *Big Data*, foram alteradas também as relações de poder. O poder agora se manifesta em um espaço global e extraterritorial, tendo seu alcance ampliado e gerando grande incerteza, haja vista que apenas se sabe que ele é exercido por aqueles que detêm os dados. Ironicamente, à medida que detalhes de nossa vida cotidiana se tornam cada vez mais acessíveis ao poder vigilante, as atividades de vigilância se tornam para nós, de modo proporcionalmente inverso, menos transparentes e difíceis de discernir. Nas palavras de Lyon (2013, p. 13, grifos do autor): "Se Bauman está certo, fechou-se a cortina de uma era de 'engajamento mútuo', em que administradores e administrados confrontavam-se. O novo espetáculo é um drama mais ardiloso, em que 'o poder pode mover-se à velocidade de um sinal eletrônico'".

Não queremos sugerir que a obscuridade da vigilância líquida seja, necessariamente, intencional ou conspiratória. Acreditamos que, pelo menos, parte da dificuldade de entendimento dos novos mecanismos de vigilância reside no caráter tecnicamente sofisticado dos algoritmos por eles utilizados e do complexo fluxo de dados no contexto de *Big Data*. Além disso, a replicabilidade, um dos cânones da ciência tradicional, se vê limitada não só pela transitoriedade dos dados, mas também pelo sigilo que envolve a competição comercial e as questões de segurança.

Em suma, algumas possibilidades apresentadas pelas tecnologias informacionais são atrativas, trazendo facilidades não só para o mundo dos negócios e organizações, mas também para a ciência e a vida cotidiana. Tais facilidades conduzem a uma aceitação tão profunda e generalizada desse tipo de tecnologia, que não

apenas desfrutamos dela, mas nos tornamos a cada dia mais seus dependentes. Justamente devido a esse motivo de dependência que, de uma perspectiva ética, não se pode deixar de analisar os possíveis perigos trazidos pela era de *Big Data*. Mais especificamente, o constante estado de vigilância a que estamos diariamente submetidos, independente de nossa consciente anuência ou não a ele, tem suscitado muitas reflexões de cunho ético. Até mesmo quando não se está 'conscientemente' conectado à rede tem-se a vida observada, pois dispositivos eletrônicos, que captam dados, estão espalhados nos mais diversos ambientes e de várias maneiras nos produtos tecnológicos dos quais nos servimos inescapavelmente. Assim, pessoas se tornam presas fáceis para o controle e manipulação, tendo em vista a identificação (mesmo que mecânica) de seus desejos de compras, preferências partidárias, propensões religiosas e de uma miríade de outras informações. Nesse contexto, consideramos que uma das tarefas da filosofia, enquanto atividade que visa favorecer a autonomia e a criticidade humanas, consiste em auxiliar na compreensão do conceito de liberdade de expressão na Sociedade da Informação. Esforço esse ao qual nos empenhamos apoiados em algumas das ideias de Mill ([1859] 1991) e Bauman (2013).

Um dos desafios da Era de *Big Data*, discutido na próxima seção, consiste em manter a defesa da liberdade individual ao mesmo tempo em que se lida com determinadas restrições sociais contexto dependentes. Entendemos esse desafio a partir na concepção de fluidez da privacidade e da autonomia em sociedades controladas por recursos de *Big Data*.

Desafios da era de *Big Data*: aspectos éticos e epistemológicos

A problematização de Mill ([1859] 1991), sumarizada na seção anterior, está na agenda de filósofos e outros pensadores críticos que refletem sobre os antagonismos éticos da Sociedade da Informação.

A fluidez do que se 'produz' na rede e a consequente dificuldade de atribuição de responsabilidade a um indivíduo específico ou coletivo ilustram a falta de controle a que a Sociedade da Informação está sujeita, e suscitam, dentre outras, considerações éticas. Hijmans (2016, p. 96), por exemplo, reflete que "[...] [a] evolução da Era dos *Big Data* implica, por sua própria natureza, uma falta de controle". Um exemplo ilustrativo da falta de controle do que se produz nesse contexto pode ser visto com as recentes eleições presidenciais, em que *fake news* (ou desinformações propositalmente difundidas), reverberadas pelas redes, e outros recursos provenientes das TIC, parecem ter reforçado, se não moldado, indicadores capazes de influenciar as opiniões dos eleitores e seus resultados.

O papel desempenhado pelas *fake news* no exemplo acima indica uma dificuldade encontrada para diagnosticar, identificar, penalizar e, mais importante, reverter o quadro de crenças por elas gerado, criando-se um espectro de desinformação. É extremamente difícil se identificar um sujeito ou coletivo responsável por mobilizar as pessoas em torno de uma determinada causa, quando a mobilização se dá por meio das novas TIC, uma vez que consubstancia fluxo interminável de mensagens transmitidas e retransmitidas instantaneamente em indeterminados grupos da sociedade visando impactar a comoção e agregação social. No caso exemplificado, a rede tornou-se o espaço para planejar – pensar, preparar, incentivar, apoiar e até mesmo denegrir – uma espécie de mobilização virtual com consequências materializadas na realidade político-social do país[2].

Por mais que se discutam os perigos do rumo tomado pela Sociedade da Informação e, particularmente, pela metodologia adotada nas técnicas de análise de *Big Data*, há poucas dúvidas de que os *Big Data* possam ajudar a identificar tendências emergentes, melhorar a tomada de decisões de negócios e desenvolver novas estratégias de geração de receita. Os *Big Data* têm o potencial de descobrir novas regularidades de macro-comportamentos; padrões esses que amiúde eram ignorados no passado em razão da escassez de dados disponíveis para manipulação.

Talvez a maior inovação do uso de *Big Data* esteja no trato de dados em tempo real para descrever atividades, antes mesmo que fontes de dados oficiais estejam disponíveis. Tem-se uma variável em tempo real fornecida, por exemplo, por consultas em mecanismos de pesquisa, como o Google, monitoramento dos sinais de celulares pelos Serviços de Telecomunicações ou do uso de cartão de crédito. O fluxo de dados desses sistemas é praticamente contínuo e agora podem ser analisados, concomitantemente à sua geração, por técnicas de análise de *Big Data*. Para entendermos tal procedimento, consideremos o exemplo da política de contenção do Covid-19.

[2] Epstein and Robertson (2015) apresentam um estudo esclarecedor de como eleições podem ser manipuladas por mecanismos de buscas.

Recursos de *Big Data* estão sendo utilizados recentemente como uma das ferramentas para conter a expansão pandêmica do Covid-19, através, por exemplo, do monitoramento da adesão à medida preventiva de isolamento social. Um dos recursos adotados consiste no uso de códigos, uma espécie de chave, para entrada em transportes, repartições e outros ambientes, fornecidos por um aplicativo em *Smartphone*, cujo sistema cruza dados de Ministérios, como o da Saúde e do Transporte, de Organizações Comunitárias e Empresas. Por meio do *App* é possível alertar para áreas de riscos e mesmo identificar se um vizinho ou colega de trabalho ficou doente, o que poderá alterar o estado do portador do aparelho para o de mais um caso suspeito, de risco. Tal medida visa inibir a mobilidade de pessoas em caso de suspeita de contaminação e proibir, efetivamente, qualquer mobilidade daquelas comprovadamente infectadas, impedindo a transmissão e proliferação do vírus. De acordo com o grau de risco apresentado por uma pessoa, apontado pelo aplicativo (ilustrativamente, como código vermelho, amarelo ou verde), ela está sujeita às correspondentes medidas de segurança e isolamento (Gan & Culver, 2020). Embora o aplicativo atribua um grau de risco apresentado pela pessoa, automaticamente, via análise estatística e correlacional, a comprovação da contaminação ou não é feita pelos procedimentos científicos tradicionais, baseados na noção de causalidade. Nesse sentido, também argumentamos que as técnicas de análise de *Big Data* são utilizadas como um complemento dos procedimentos científicos tradicionais e não como um substituto deles, como alguns, nomeadamente Anderson (2008), têm defendido apressadamente.

Empresas, por motivos econômicos, também usufruem de técnicas de análise de *Big Data* para tratarem dados em tempo real. A adaptabilidade dos anúncios de sites comerciais para um indivíduo, com base em seu comportamento na *Web*, é exemplar desse procedimento. Empresas têm se empenhado para oferecer, por exemplo, produtos e serviços personalizados, a partir de informações resultantes de coletas instantâneas de dados dos consumidores. Enquanto as empresas tendem a acumular os benefícios da personalização, danos são infligidos aos indivíduos que têm sua privacidade invadida e autonomia reduzida. Os consumidores, por sua vez, têm pouco conhecimento do que está por trás desse processo de personalização, tendo maior dificuldade para responder à altura a esse tipo de apelo de *marketing*. Desse modo, um dos principais diferenciais ou inovação do uso de *Big Data*, ou seja, o trato de dados em tempo real, agrava, em muito, a situação de perda de autonomia e privacidade da pessoa na contemporaneidade.

Há de se considerar dois lados na personalização. Empresas, como a Amazon, usam seus bancos de dados de consumidores (e possivelmente outros) para fazer recomendações a possíveis clientes de compra de um livro, por exemplo, que parece de seu interesse. Tal recomendação, por um lado, pode ajudar na identificação de um livro desejado ou desejável pelo consumidor. Por outro lado, essa prática pode conduzir à segmentação comportamental, colocando pessoas em situações desconfortáveis, ao deixar transparecer uma espécie de rotulagem (e não de personalização propriamente dita), como a de alguém com perfil, por exemplo, marcadamente machista ou homofóbico, devido a alguns cliques anteriores.

É muito comum ouvirmos reclamações do tipo 'Só porque pesquisei malas na internet, agora fico recebendo propagandas não apenas de malas, mas também de agências de viagem, redes hoteleiras e assim por diante'. Algumas pesquisas corroboram esse tipo de descontentamento em relação ao rastreamento *online* de anunciantes, principalmente quando se trata de usuários adultos[3]. Sendo assim, podemos prever que a publicidade encontrará novas maneiras, mais eficazes e discretas, de usufruir os benefícios da 'personalização' sem causar aborrecimentos, inconvenientes ou outros descontentamentos por parte de seus usuários/consumidores. Acreditamos que essa adaptação, em que a personalização seja feita em um segundo plano, pode ter consequências mais graves em termos de invasão da privacidade e da perda de autonomia das pessoas, ainda mais quando consideramos que a aplicação desses recursos tecnológicos perpassa as mais diversas áreas, do mercado à política.

Alguns recursos de *Big Data*, além de permitir o direcionamento instantâneo de informações quando se acessa a rede, guiam, em um nível mais básico, os indivíduos e a própria sociedade, ao detectarem padrões que são fortalecidos em detrimentos de outros, os quais aos poucos colapsam (Merrill, 2016). Ilustrativamente, plataformas de *delivery*, como a da *startup* iFood, que tem seu aplicativo tão comumente baixado pelos usuários em *smartphones*, parece, à primeira vista, apenas um meio de ligar fornecedores de alimentos às pessoas que os querem consumir. Mas, o iFood tem condições de saber quais os alimentos que mais vendem, qual é a base desses alimentos e pode usar esse banco de dados, inclusive, para fazer transações

[3] O boicote ao Facebook neste ano de 2020 é um caso ilustrativo da expressão de descontentamento por parte dos usuários/consumidores ao rastreamento abusivo de dados pessoais.

comerciais diversas, como investimentos em empresas de determinado segmento ou vender esses dados, sem que seus usuários saibam disso.

Poderíamos ter utilizado os já tão citados exemplos de empresas de seguro ou de convênios de saúde, cuja utilização dos dados pessoais fornecidos, e mesmo de rastros digitais identificados de seus usuários, permitem uma interferência no custo do serviço oferecido, dentre outras coisas, de modo a ferir, em algum sentido, eticamente falando, a lisura contratual, pois afeta diretamente a vida de seus usuários, sem que os mesmos tenham clareza do processo como um todo. Mas o que gostaríamos de destacar, com o exemplo acima do iFood, é que mesmo nos casos em que os dados pessoais aparentemente não são os protagonistas, dada a infinidade de possibilidades de reutilização de dados, mesmo que sejam não-sensíveis, poderá afetar diretamente a vida das pessoas, ter impacto na sociedade. A questão comercial não é simples, como pode sugerir à primeira vista. As questões comerciais são aquelas que, atualmente, pautam basicamente a sociedade. Se você permite que uma empresa como a iFood dite o preço de um produto ou o estabeleça como sendo o padrão, você pode, por exemplo, acabar com outros tipos de produtos e todo a rede comercial a ele atrelada. Daí hoje o monopólio presente em quase todos os segmentos comerciais. Sem dúvida, esse tipo de uso da informação que, conscientemente ou não, disponibilizamos na rede, pode ter um impacto nocivo na sociedade e-capitalista.

À medida que os *Big Data* se tornaram uma ferramenta comum nas decisões corporativas, públicas e privadas, surgiram vários novos riscos sociais a eles relacionados. O mais óbvio é o risco de violação da privacidade, como temos discutido até aqui. Portanto, precisamos refletir sobre a forma como as políticas públicas devem responder a esses desafios, senão como a sociedade, por meio de outros esquemas, pode lidar efetivamente com eles.

Para lidar com o problema da violação da privacidade, dentre outros, na literatura especializada, a abordagem mais comum consiste em explorar a criação e/ou aperfeiçoamento de estatutos e regulamentos governamentais, que consideramos um passo importante (se não necessário) e eficaz em certos aspectos, mas não suficiente para impedir tal violação. Assim como a lei que sustenta o direito à dignidade da pessoa humana é necessária, mas não garante, efetivamente, a mesma dignidade a todas as pessoas.

O fato de que alguns agentes nem sempre respeitam os limites impostos por controles regulatórios sugere que a nova regulamentação, para atender aos desafios da sociedade informacional, deve tentar antecipar os problemas e não esperar que eles se materializem.

Para alguns pensadores, outra saída para o problema da violação da privacidade e o controle dos dados pode estar no Direito Privado. Contratos de empresas com fornecedores, outras empresas e indivíduos, por exemplo, podem oferecer respostas mais rápidas a alguns dos desafios da era de *Big Data*. Com efeito, a tendência em curso da auto-regulação do setor, independentemente de regulamentação governamental, pode se tornar o padrão vigente nessa área. A aposta aqui está fundada na correlação estatística que conduz à previsão de que a diminuição da probabilidade de violações da privacidade em empresas acompanha a diminuição de sua vulnerabilidade legal. Com efeito, talvez do *insight* dessa correlação possamos tirar uma prova ou explicação causal do comportamento de sistemas complexos onde há ou não algum tipo de regulamentação.

Existem ainda especulações sobre esquemas para 'monetizar' os dados privados das pessoas, para que possam controlá-los e vendê-los, quando, e se for o caso, de seu interesse particular.

Seja como for, parece haver consenso na literatura geral sobre a importância ou obrigatoriedade da transparência. Corporações públicas e privadas que mantêm bancos de dados pessoais devem ser transparentes a respeito de como e o que sabe sobre as pessoas.

Consideramos alguns princípios basilares:

1. Temos direito a nossos próprios dados pessoais.
2. Temos o direito de tomar posse de uma cópia completa de nossos dados pessoais, sem demora e sem custo.
3. Temos o direito de compartilhar nossos dados pessoais com outras pessoas, conforme entendermos que for o caso.
4. Plataformas devem ser responsáveis pelos dados coletados, bem como pelos metadados deles extraídos.
5. Plataformas devem permitir que os dados, sob sua responsabilidade, tenham uma vida útil, ou seja, um tempo de duração, para que sua eliminação respeite o chamado direito de esquecimento.

Esses princípios 1, 2, 3, 4 e 5 expressam direitos humanos básicos. Nenhuma lei ou política deveria restringir esses direitos. Podemos nos empenhar, em termos teóricos e práticos, para que as técnicas de *Big Data* possam viabilizar o controle ético e legal, que garanta o direito à privacidade e à autonomia de usuários das TIC, e não restringi-lo como visto atualmente.

Em síntese, a Sociedade da Informação nos coloca a dificuldade de garantir o direito à privacidade e à autonomia em um contexto de vigilância fluida, instantânea e ubíqua. Sociedades controladas por recursos de *Big Data* necessitam de formas de regulamentação especial do uso de tecnologias pervasivas, que seja viável (sustentável) para os desafios da realidade contemporânea. Considerar as formas de liberdades positiva e negativa no contexto de uso de recursos de *Big Data* e de TIC em geral, talvez seja o primeiro passo para a garantia de direitos humanos tão básicos como o da privacidade e autonomia, acima discutidos.

Considerações finais

Procuramos indicar neste artigo aspectos positivos e negativos do uso de recursos de *Big Data* na manipulação de dados de usuários de TIC. No que diz respeito aos aspectos positivos, ressaltamos que esses recursos representam uma ferramenta oportuna para diversos tipos de ganho na Sociedade da Informação; nos negócios, por exemplo, o êxito na combinação do emprego de técnicas de mineração de dados e *marketing* está alinhado ao sucesso de grandes empresas e corporações. As técnicas de análise de *Big Data* também podem auxiliar a pesquisa científica, ao acelerar descobertas e inovações. Na vida cotidiana, com os *Big Data* pode-se desfrutar de recursos, na área do laser, da saúde e do trabalho, que diminuem distâncias, tempo e procedimentos antes complicados e dispendiosos. A administração do Estado também é facilitada e pode tornar-se mais eficiente com o uso de técnicas de *Big Data* na prestação de serviços governamentais, como o monitoramento e contenção de ameaças à segurança publica.

Apesar de produzirem bons instrumentos para o mundo dos negócios, ciência e tecnologia, vida cotidiana e governo, o emprego de recursos de *Big Data* também apresenta grandes desafios éticos. As técnicas de análise de *Big Data* têm se tornado muito difundidas, intrusivas e difíceis de entender para a classe de pessoas pouco familiarizadas com as TIC. Para os indivíduos pertencentes a essa classe, quais recursos estão disponíveis que possam fornecer garantias de proteção aos usos indevidos ou abusivos de dados pessoais? Como definir sistemas regulatórios para o que é social e legalmente aceitável nesse novo contexto de *Big Data*?

Uma conclusão possível, que apresentamos no presente artigo, não sem dificuldades, é que, o controle estatal e legal sobre o que é produzido no ambiente da *Big Data* deveria seguir os parâmetros apresentados – inspirados em Mill ([1859] 1991) e Berlin ([1969] 2002) – de liberdade positiva e liberdade negativa. Manifestações de pensamento e atividades que se apresentam no ambiente da *Big Data* devem, idealmente, pautar-se pela ideia de liberdade positiva. Todavia, a liberdade negativa como direito legal da autoridade estatal, deve estar presente sempre que manifestações e expressões de opiniões e atividades apresentadas no ambiente da *Big Data* causarem danos ou prejuízos a outrem ou às próprias instituições fundamentais ao Estado Democrático de Direito. Nesse sentido, seria prudente que não apenas filósofos e legisladores, mas governantes, empresários, cientistas, consumidores e cidadãos em geral direcionem atenção às implicações econômicas, e, sobretudo, às éticas utilitaristas, trazidas pelo uso de técnicas de análise de *Big Data*. Por si só, tal atenção não garante, mas, ao menos, aumenta as chances de que o emprego de técnicas de *Big Data* seja pautado em responsabilidade social. Essa atenção cuidadosa poderia capacitar os usuários de TIC a um maior entendimento e controle sobre o acesso e uso de seus dados.

Considerando a premissa vigente entre pesquisadores de *Big Data,* segundo a qual 'mais é melhor', posto que algoritmos permitem identificar padrões que criam respostas para perguntas que nem sequer foram ainda formuladas (Anderson, 2008), não parece ser o caso de limitar a coleta de dados, pois isso poderia minar os benefícios potenciais das técnicas de análise de *Big Data*.

No entanto, não confiamos na mão pesada do Estado, tampouco na mão invisível do Mercado para (auto)regular a coleta e o uso de dados pessoais. O mais prudente talvez seja exercermos nossa maioridade, em termos kantianos, e confiarmos em nossa própria mão, na atenção cuidadosa em busca de regulamentação tecnológica (não apenas de proteção legal dos dados). A exigência de desenvolvimento de tecnologias voltadas para o controle do uso de *Big Data,* e outras tecnologias pervasivas, talvez nos indique uma espécie de contrapartida às ameaças de um desenvolvimento descontrolado das TIC.

Nesse sentido, entendemos que, se não podemos frear ou alterar o rumo tomado pela Sociedade da Informação, podemos, ao menos, intervir no estabelecimento de regulamentação tecnológica, visando salvaguardar a privacidade individual, bem como a autonomia da pessoa humana. A proteção da privacidade, visando permitir o exercício da autonomia individual, talvez não seja o foco da Indústria de Dados, dos detentores de seu poder. Talvez o que se pretende é salvaguardar/monopolizar o 'novo petróleo', segundo o pressuposto de que os dados preservam seu valor porque poucos os detêm. Esse pressuposto deve ser levado em consideração quando refletimos e propomos uma regulamentação tecnológica.

Agradecimentos

Os autores agradem aos membros dos grupos de pesquisa OpLaDyn, GAEC (UNESP) e CLE (UNICAMP) por suas discussões inspiradoras. Edna A. de Souza agradece, especialmente, à professora Dra. Maria Eunice Q. Gonzalez, pela leitura crítica do artigo e comentários enriquecedores tanto para a pesquisa como para a vida. Esta pesquisa foi financiada pelas agências FAPESP (2016 / 50256-0) e CAPES (PNPD) a quem também expressa gratidão.

Referências

Anderson, C. (2008, June 23). The end of theory: The data deluge makes the scientific method obsolete. *Wired*,. Retrieved on Sept. 30, 2018 from https://www.wired.com/2008/06/pb-theory/

Bauman, Z. (2013). *Vigilância líquida - Diálogos com David Lyon* (Carlos Alberto Medeiros, Trad.) Rio de Janeiro, RJ: Zahar.

Berlin, I. (2002). Two concepts of liberty. In H. Hardy (Ed.), *Liberty* (p. 166-217). Oxford, UK: Oxford University Press.

Decreto nº 8.771. (2016, 11 de maio). Regulamenta a Lei nº 12.965, de 23 de abril de 2014. Recuperado em 14 de junho de 2020 de http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2016/Decreto/D8771.htm

Epistein, R., & Robertson, R. (2015). The search engine manipulation effect (SEME) and its possible impact on the outcomes of elections. *Proceedings of the National Academy of Sciences*., e4512-e4521. Retrieved on July 08, 2020 from http://www.pnas.org/content/112/33/E4512.full.pdf

Gan, N., & Culver, D. (2020). China usa QR code digital para combater o coronavírus. Saiba como funciona. *CNN Brasil*. Recuperado em 21 de abril de 2020 de https://bitlybr.com/ogZJu

Hijmans, H. (2016). *The European Union as guardian of internet privacy: The story of art 16 TFEU*. Brussels, BE: Springer International Publishing. doi: 10.1007/978-3-319-34090-6

Laney, D. (2001). *3D Data management controlling data volume velocity and variety*. Retrieved on Sept 05, 2018 from https://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf.

Lei nº 12.965. (2014, 23 de abril). Estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil (Lei conhecida como Marco Civil da Internet). Recuperado em 14 de junho de 2020 de http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/112965.htm

Lyon, D. (2013). Introdução. In Z. Bauman, *Vigilância líquida - Diálogos com David Lyon* (p. 4-17, Carlos Alberto Medeiros, Trad.). Rio de Janeiro, RJ: Zahar.

Mayer-Schonberger, V., & Cukier, K. (2013). *Big Data: A revolution that will transform how we live, work, and think*. Boston, MA: Houghton Mifflin Harcourt.

Merrill, J. B. (2016, Aug. 23). Liberal, moderate or conservative? See how facebook labels you. *The New York Times*. Retrieved on Sept 05, 2018 from https://bitlybr.com/6ajVAIt

Mill, J. S. (1991). *Sobre a liberdade* (Clássicos do Pensamento Político, 2a. ed., Alberto da Rocha Barros, Trad.). Petrópolis, RJ: Editora Vozes.

Orwell, G. (2009). *1984* (Heloisa Jahn e Alexandre Hubner, Trad.). São Paulo, SP: Companhia das Letras.

Rodotà, S. (2008). *A vida na sociedade da vigilância: a privacidade hoje* (Danilo Doneda e Luciana Cabral Doneda, Trad.). Rio de Janeiro, RJ: Renovar.

Starr, S. B. (2013, Sept. 01). Evidence-based sentencing and the scientific rationalization of discrimination. *Forthcoming, Stanford Law Review*, *66*. Retrieved on Sept. 05, 2018, from http://www.ssrn.com/abstract=2318940

Unesco (1948). *Declaração Universal dos Direitos Humanos* (Resolução 217 A (III) da Assembléia Geral das Nações Unidas, de 10 de dezembro de 1948). Recuperado em 14 de junho de 2020 de https://brasil.un.org/pt-br/91601-declaracao-universal-dos-direitos-humanos