V ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

DANIELLE JACON AYRES PINTO

SALETE ORO BOFF

JOÃO MARCELO DE LIMA ASSAFIM

I61

Internet: dinâmicas da segurança pública internacional [Recurso eletrônico on-line] organização CONPEDI

Coordenadores: Danielle Jacon Ayres Pinto; João Marcelo de Lima Assafim; Salete Oro Boff – Florianópolis: CONPEDI, 2022.

Inclui bibliografia
ISBN: 978-65-5648-463-1
Modo de acesso: www.conpedi.org.br em publicações
Tema: Inovação, Direito e Sustentabilidade

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Internet. 3. Segurança pública internacional. V Encontro Virtual do CONPEDI (1: 2022 : Florianópolis, Brasil).

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

V ENCONTRO VIRTUAL DO CONPEDI

INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL

Apresentação

Apresentamos nessa oportunidade os primeiros artigos do novo grupo de trabalho do CONPEDI que visa debater tema contemporâneo de extrema importância para o tecido social, jurídico, político e tecnológico brasileiro. O GT - INTERNET: DINÂMICAS DA SEGURANÇA PÚBLICA E INTERNACIONAL I é o resultado da percepção do CONPEDI da importância da Internet como locus essencial da sociabilidade humana e como, a partir dessa dinâmica, tanto a segurança pública nacional como a segurança internacional passaram a ter novos desafios que antes não se colocavam à burocracia do Estado e a própria ideia de proteção, ameaça e justiça até então compreendidas como centrais ao redor do mundo.

Assim, esse primeiro GT nasce com um debate excelente de temas que vão desde da comunicação de massa, proteção de dados, governança digital, big data e direitos de quinta geração.

Com esses temas, tivemos nessa versão virtual do CONPEDI os seguintes textos apresentados: a) A AUSÊNCIA DE MECANISMOS DE SEGURANÇA NOS APLICATIVOS DE COMUNICAÇÃO EM MASSA: O CASO TELEGRAM E A DECISÃO DO SUPREMO TRIBUNAL FEDERAL; b) A LEI GERAL DE PROTEÇÃO DE DADOS E OS DIREITOS DE QUINTA DIMENSÃO; c) GOVERNANÇA E REGULAÇÃO DO FLUXO DE DADOS PESSOAIS: OBSERVANDO OS CASOS SCHREMS (TJUE); d) SORRIA, VOCÊ ESTÁ SENDO ENGANADO: UMA ANÁLISE SOBRE A EVOLUÇÃO DAS LEIS DE PROTEÇÃO DE DADOS E O USO ILIMITADO DE BIG DATA.

Desejamos a todas e todos uma excelente leitura e uma participação cada vez mais efetiva nesse debate central para a promoção da segurança e proteção dos direitos humanos no espaço virtual tanto ao nível nacional como internacional.

SORRIA, VOCÊ ESTÁ SENDO ENGANADO: UMA ANÁLISE SOBRE A EVOLUÇÃO DAS LEIS DE PROTEÇÃO DE DADOS E O USO ILIMITADO DE BIG DATA

SMILE, YOU ARE BEING DECEIVED: AN ANALYSIS ON THE EVOLUTION OF DATA PROTECTION LAWS AND THE UNLIMITED USE OF BIG DATAS

Adriana Rossini [1]
Natalia Maria Ventura da Silva Alfaya [2]

Resumo

O trabalho é uma reflexão sobre o big data e seus usos atuais. Tem por objetivo analisar as formas como esses metadados têm sido aplicados e suas consequências quanto ao seu mau uso. Através da evolução das leis de proteção de dados no mundo e no Brasil, apresenta uma visão sobre a necessária proteção dos dados pessoais do ser humano. Adota o método hipotético-dedutivo, utilizando-se de livros e artigos científicos produzidos no Brasil e no exterior. A pesquisa aponta para a necessidade de aprofundamento nesses estudos, uma vez que as inovações da tecnologia não podem ser freadas.

Palavras-chave: Big data, Leis de proteção de dados, Modelo ocean, Psicometria, Manipulação de opinião pública

Abstract/Resumen/Résumé

The work is a reflection on big data and its current uses. It aims to analyze how this metadata has been applied and its consequences for its misuse. Through the evolution of data protection laws in the world and in Brazil, it presents a vision on the necessary protection of human personal data. It adopts the hypothetical-deductive method, using books and scientific articles produced in Brazil and abroad. The research points to the need to deepen these studies, since the innovations of technology cannot be braked.

Keywords/Palabras-claves/Mots-clés: Big data, Data protection laws, Ocean model, Psychometrics, Manipulation of public opinion

[1] Pós-graduada e Mestranda no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias das Faculdades Londrina. E-mail: adrianarossini.adv@gmail.com

[2] Doutora em Ciências Sociais e Jurídicas pela UFF. Professora no Programa de Mestrado Profissional em Direito, Sociedade e Tecnologias das Faculdades Londrina. E-mail: naty.alfaya@gmail.com

1. INTRODUÇÃO

O *BIG DATA* é um fenômeno que emerge das relações interpessoais entre o homem e a internet e seu uso indiscriminado tem trazido inúmeras transformações sociais. A rápida evolução tecnológica implica a produção de um volume massivo de dados que geram esses metadados.

O artigo discute o impacto do *BIG DATA* na vida do ser humano e o analisa através de três aspectos: a evolução natural das leis de proteção aos dados pessoais no mundo e no Brasil; Conceitos, Aplicações e Mau Uso do *BIG DATA* e Manipulação de dados dos usuários nas redes, através dos modelos *Ocean* de Psicometria.

O tema-problema da pesquisa que se pretende desenvolver é como o escândalo *Cambridge Analytica* trouxe a preocupação com a manipulação de dados de usuários na internet e até qual ponto as empresas podem invadir a privacidade individual e violar direitos fundamentais.

O presente estudo busca responder à pergunta através da reflexão sobre as consequências do escândalo *Facebook-Cambridge Analytica* e a submissão alienante a mídia pelos usuários, viciados em exposição e costumes consumeristas. Alerta ainda para o uso de psicometria nas redes sociais, para traçar o perfil psicológico dos usuários e assim manipulá-los.

No mundo contemporâneo, a informação tornou-se o bem mais valioso. O ser humano não tem como fugir dos avanços tecnológicos que lhe são impostos todos os dias. O recolhimento em massa de todas essas informações pessoais, uma vez organizados e analisados, tornam-se um poderoso instrumento de influência de opinião e processos de escolha de milhões de usuários.

O que pretendemos neste trabalho é não só alertar para o mau uso do *BIG DATA* como ferramenta de influência, mas também fomentar o estudo de soluções legislativas e jurídicas para a defesa e manutenção de um efetivo Estado de Direito Democrático.

2. EVOLUÇÃO HISTÓRICA DA LEGISLAÇÃO DE PROTEÇÃO DE DADOS

Embora o tema pareça novo, assuntos relativos à proteção de nossos dados e a privacidade no uso da internet são discutidos há anos.

Frise-se que a preocupação com o *"right of privacy"* (ZANINI, 2015, p. 3) foi uma das principais teses do direito estadunidense e já estava presente no seu sistema jurídico desde o

século XIX. Em textos e decisões da Suprema Corte (*in casu, Wheaton v. Peters*), é possível identificar a expressão "ser deixado só"[1], surgindo as primeiras ideias e conceitos de direito à privacidade, como inerentes a personalidade jurídica, não se limitando somente a terminologia da palavra privacidade, mas ampliando seu conceito. Destacam-se também, os casos *Schuyler v. Curtis* (1891) e *Marks v. Jaffa* (1893) como aqueles que teriam iniciado as discussões a respeito do *right of privacy* nos tribunais dos Estados Unidos (ZANINI, 2015, p. 4 e 5).

O tema - proteção de dados pessoais - se entrelaça de diversas formas com o inerente direito fundamental a privacidade e, embora a segurança de nossas informações não seja novidade na legislação mundial, as primeiras leis especificas para a proteção desses dados surgiram em meados dos anos 70.

2.1. Breve Evolução Histórica no Mundo

Existe uma tendência em se acreditar que as primeiras normas de proteção aos dados surgiram nos Estados Unidos da América, mas, a bem da verdade, a primeira lei oficialmente relevante ao tema, surgiu em *Hessen*, na Alemanha, na década de 70[2] (CANCELIER, 2016).

Durante esse período histórico, os inúmeros avanços da computação e da indústria nos países mais desenvolvidos, impulsionaram o Estado Alemão a criar normas para regulamentar a privacidade no país. Também foi a primeira vez que o termo "proteção de dados" foi inserido no cenário jurídico da Alemanha.

Embora todo o conceito tenha surgido e se desenvolvido no início da década de 70, a legislação só foi finalizada e implementada em 1978. Nesse ano, outros países, como França, Suécia, Áustria e Noruega, também criaram suas próprias legislações de como seriam utilizados os dados pessoais de seus cidadãos.

Já em 1981, os países que eram membros do então Conselho da Europa, elaboraram a chamada Convenção 108[3], que fomentou a adoção de normas específicas para o uso de dados, trazendo uma perspectiva universal do conceito, ampliando-o para outros países.

---

[1] Antes do artigo de Warren e Brandeis, vamos encontrar na obra do Juiz Thomas Cooley, publicada em 1880, sob o título *A Treatise on the Law of Torts*, a primeira utilização da expressão *"right to be let alone"*. Apesar de ter cunhado a expressão, Cooley não a relacionou com a noção de *privacy* (RIGAUX, 1990, p. 272), mencionando-a em seu trabalho sobre responsabilidade civil (torts) como parte do seguinte trecho: *"The right to one's person may be said to be a right of* complete *immunity: to be let alone"* (COOLEY, 1880, p. 29).

[2] Na década de 60 do século XX, a crescente automatização de processos de produção levou à preocupação sobre a regulação de dados pessoais, particularmente no continente Europeu. O estado de Hesse, na região central da Alemanha foi o primeiro a introduzir uma legislação de proteção de dados pessoais em âmbito local, em 1970.

[3] A Convenção 108/1981 entrou em vigor em 1985. A Convenção foi pioneira ao estabelecer princípios, conceitos e direitos sobre o tema.

Em 1995, surge a Diretiva 95/46/CE, que estabeleceu uma definição básica para o que são dados pessoais e outras delimitações de extrema importância para a normatização e discussão do tema, além de grande incentivo ao comércio.

Nesses textos, conceitos como o recolhimento de dados de acordo com uma finalidade específica, direito de acesso dos dados por parte do consumidor e responsabilidade das empresas sobre a segurança das informações armazenadas, já estão abordadas na lei, aproximando-se cada vez mais das legislações atuais.

No ano 2000, o *Safe Harbor* foi um dos mais eminentes acordos estabelecidos entre Estados Unidos e Europa, tendo como principal fundamento facilitar a troca de informações e dados pessoais entre os dois continentes. Entretanto, foi revogado em 2015 sob a suspeita de espionagens por parte da Agência Nacional dos Estados Unidos, sendo substituído no ano seguinte, pelo *Privacy Shield*, um novo programa de transferência internacional de dados entre as empresas norte americanas que garantiam maior segurança aos cidadãos europeus.

Mas foi somente em 2018, com a criação do Regulamento Geral de Proteção de Dados (GDPR) que tanto norte-americanos, quanto membros da União Europeia, tiveram maior amparo nas tratativas de segurança de dados, com a substituição da diretiva anterior, por esse novo regulamento.

No contexto mundial, essas foram as primeiras leis e tratados de proteção de dados e direito à privacidade de informações.

2.2 Evolução Histórica no Brasil

No Brasil, o direito à privacidade é assegurado constitucionalmente como direito humano fundamental. A sua Constituição Federal de 1988, não se restringiu ao direito à privacidade e abrangeu à preservação da vida privada e da intimidade da pessoa, a inviolabilidade da correspondência, do domicílio e das comunicações. Correlato, mencionava de forma extensiva alguns pontos sobre a proteção de dados de seus cidadãos. No artigo 5º, inciso X: “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação” e no inciso 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” (BRASIL, 1988).

No início dos anos 90 o Brasil desenvolveu um manual específico para as relações entre empresas e clientes editando o **Código de Defesa do Consumidor, evoluindo** ainda mais a busca pela defesa de informações discriminando ainda, uma seção específica sobre cadastros e banco de dados. No texto, a legislação defende o direito do consumidor acessar os dados que uma empresa tem sobre ele e solicitar sua correção, caso alguma informação esteja errada. O artigo 13º ainda deixa claro que dificultar o acesso às suas próprias informações ou deixar de comunicar ao titular sobre o registro de seus dados são consideradas infrações.

Há ainda artigos que garantem a privacidade e responsabilizam as empresas sobre a segurança dos dados, como o artigo 11º, capítulo 3: *"Os dados pessoais do consumidor serão preservados, mantidos em sigilo e utilizados exclusivamente para os fins do atendimento"* (BRASIL, 1990).

Mas alguns anos depois, com a Lei nº 9.296 de 1996[4], a legislação viria a acrescentar ser *"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"*.

O ano de 2013 foi de extrema importância para a regulação das normas sobre privacidade *online* no Brasil, pois foi implementada a primeira lei sobre uso responsável da internet no país. Pela primeira vez foram vistos na legislação conceitos como a neutralidade de rede e a liberdade de expressão e definidas quais são as obrigações dos órgãos públicos no fornecimento de internet.

Em março de 2013 o decreto nº 7.962[5] ainda acrescentou orientações que complementam o Código de Defesa do Consumidor. O artigo 2º define que são diretrizes do Plano Nacional de Consumo e Cidadania a "autodeterminação, privacidade, confidencialidade e segurança das informações e dados pessoais prestados ou coletados, inclusive por meio eletrônico" (BRASIL, 2013).

O Marco Civil da Internet, assim chamada a Lei nº 12.965/2014[6], preocupou-se em regulamentar a forma como os direitos seriam protegidos no ambiente virtual. Tal marco foi o primeiro no Brasil a estabelecer de forma direta os *"princípios, garantias, direitos e deveres para o uso da Internet no Brasil"* (BRASIL, 2014).

[4] Regulamenta o inciso XII, parte final, do art. 5º da Constituição Federal do Brasil de 1988.
[5] Decreto nº 7.962 de 15 de Março de 2013 – Regulamenta a Lei nº 8.078, de 11 de Setembro de 1990, para dispor sobre a contratação no Comércio Eletrônico.
[6] Lei nº 12.965 de 23 de Abril de 2014 – Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

Mas com os acontecimentos internacionais de 2018, observados casos de grandes vazamentos de dados, a má utilização de informações pessoais, e com o acinte da União Europeia decidindo revisitar suas regras de proteção de dados, culminando no Regulamento Geral de Proteção de Dados (GDPR)[7], os legisladores brasileiros também viram a necessidade de compilar essas normas em um código específico, favorecendo o acesso normativo de todos.

Surgem, então, os primeiros esboços para uma lei brasileira específica à proteção dos dados pessoais, como uma alternativa ao Marco Civil da Internet.

Em 2020 entrou em vigor a Lei Geral de Proteção de Dados (LGPD)[8], sendo a resposta dos legisladores brasileiros a esta crescente necessidade de normatizar o uso dos dados pessoais no mundo todo.

Claramente influenciada pelos princípios da diretiva europeia, a LGPD vale para todas as empresas que recolhem ou tratam dados no território nacional ou de cidadãos brasileiros.

Assim como o GDPR, alguns dos principais pontos da LGPD são: o direito para o titular acessar, editar ou solicitar a exclusão de seus dados, recolhimento autorizado (com exceção em casos específicos), maior cuidado com dados sensíveis, portabilidade de dados e sanções administrativas se houver descumprimento.

Vejam que, a União Europeia e seu Regulamento Geral de Proteção de Dados (GDPR), obrigou empresas do mundo todo – incluindo-se as gigantes *Facebook* e *Google* – a mudarem a forma como coletavam e usavam os dados de seus usuários, sendo responsável pelo fomento de uma onda de novas leis sobre o tema no mundo todo, inclusive no Brasil.

Mas foi recentemente que, em 10 de Fevereiro de 2022, a proteção de dados pessoais dos usuários passou a fazer parte dos direitos e garantias fundamentais dos cidadãos, através da Emenda Constitucional (EC) 115/2022[9] (BRASIL, 2022).

A sua aprovação, realça a importância dos direitos à privacidade e à proteção de dados, principalmente no que diz respeito aos ambientes digitais. Consequentemente, espera-se um

---

[7] A legislação europeia, chamada de Regulamento Geral sobre a Proteção de Dados, ou RGPD, válida em todos os países da União Europeia e do Espaço Econômico Europeu (EEE), é considerada a mais completa regulamentação sobre segurança de dados no mundo e inspirou o próprio texto da LGPD no Brasil. O regulamento entrou em vigor em 24 de maio de 2016 e é aplicável desde 25 de maio de 2018.

[8] Lei nº 13.709, de 14 de Agosto de 2018 - Lei Geral de Proteção de Dados Pessoais (LGPD) - Redação dada pela Lei nº 13.853, de 2019 - Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.
Parágrafo único. As normas gerais contidas nesta Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios (Incluído pela Lei nº 13.853, de 2019).

[9] EMENDA CONSTITUCIONAL Nº 115, DE 10 DE FEVEREIRO DE 2022 - Altera a Constituição Federal para incluir a proteção de dados pessoais entre os direitos e garantias fundamentais e para fixar a competência privativa da União para legislar sobre proteção e tratamento de dados pessoais.

fortalecimento das liberdades individuais e uma garantia jurídica maior à aplicação da Lei Geral de Proteção de Dados (LGPD), reforçando o compromisso e a preocupação do legislador em proteger os interesses e liberdades dos cidadãos.

Além disso, o engajamento em torno da proteção de dados e da privacidade, estimula os investimentos em tecnologia no país. Elevar o *status* de proteção de dados classificando-os como direitos e garantias fundamentais dos cidadãos, também fortalece as leis que regulam as relações interpessoais do cidadão brasileiro com a internet, conferindo uma estrutura pronta, sólida e segura para coletar, tratar, armazenar e empregar as informações dos usuários de forma adequada.

3. A ERA DA INFORMAÇÃO E BIG DATA: CONCEITOS, APLICAÇÕES E MAU USO

Na internet, através do giro comercial e financeiro, são realizados diariamente um número incalculável de empreendimentos e transações entre empresas e cidadãos. O exercício diário dessas atividades gera os mais diversos e distintos rastros digitais, incluindo os dados pessoais.

A nossa sociedade vive hoje a chamada Era da Informação, onde as mudanças drásticas nas tecnologias, com o aparecimento constante de novas ferramentas, novos equipamentos e novas dinâmicas interpessoais, impulsionam tanto grandes melhorias, quanto grandes abismos na sociedade, o que se consubstanciam em grandes impactos sociais, culturais, econômicos e políticos ao homem moderno.

As inter-relações do homem na internet têm atraído a atenção regulatória dos legisladores e levantado inúmeros questionamentos. Um dos aspectos mais preocupantes tem sido a gestão do *BIG DATA*.

3.1 *World Wide Web, Internet* e a História do *BIG DATA*

Para entendermos o *BIG DATA*, faz-se necessário entendermos primeiro o que é a rede mundial de computadores.

A rede mundial de computadores é **a interligação de um grande conjunto de dados e documentos que podem ser acessados pela internet em qualquer lugar do mundo**. Também é chamada de *World Wide Web*, em inglês, ou simplesmente de web. Esses documentos podem ter textos, imagens, áudios e vídeos que, em conjunto, formam as páginas da *Web*. Porém, se estivessem isoladas, essas páginas não formariam uma rede.

Já *BIG DATA*, é o termo em Tecnologia da Informação (TI) que trata sobre os grandes e massivos conjuntos de dados, gerados pelos usuários da rede mundial de computadores[10] – internet - que precisam ser processados e armazenados.

De maneira simplista, podemos definir *BIG DATA* como um conjunto de técnicas capazes de se analisar grandes quantidades de dados que geram resultados importantes que, em volumes menores, dificilmente seria possível (STANLEY, 2019).

São informações extremamente amplas que, por isto, necessitam de ferramentas especiais para comportar o grande volume de dados que são coletados, extraídos, organizados, transformados em informações que possibilitam uma análise ampla e em tempo hábil.

Os conceitos de *BIG DATA* são relativamente novos, mas sua história iniciou-se nas décadas de 60 e 70, quando o mundo computadorizado estava só começando e os primeiros conjuntos de dados estavam se formando, com os primeiros bancos de dados e data centers (STANLEY, 2019).

Na verdade, em 1969 seria quase inconcebível imaginar que a internet seria o que é hoje, uma vez que o código-fonte capaz de vincular informações entre computadores foi lançado somente em 1989, juntamente com o primeiro site baseado na *World Wide Web*. Muito mais estranho é imaginar que em 1992, a *Web* era vista como um grande sucesso, pois já possuía 10 sites aderidos. Dois anos depois, em 1994, o número subiu para 3 mil. Já em 1996, haviam 2 milhões de sites no ar que foram beneficiados pelo surgimento do *World Wide Web*. Um deles, inclusive, era o *Google*, que anos mais tarde se tornaria o buscador mais famoso do mudo. A *Amazon* também já estava incluída neste grupo.

Mas foi com a explosão do *Facebook* e do *YouTube* entre outros serviços *online*, por volta do ano de 2005, que se começou a perceber a quantidade de dados gerados por seus usuários.

Nos anos seguintes, os volumes de informações gerados por *BIG DATA* cresceram exponencialmente e até a presente data, usuários ainda geram grandes quantidades de informação que são coletadas e analisadas por minuto, gerando um valor financeiro infindável para esses dados.

Numa melhor análise, não é simplesmente o volume de dados que define o *BIG DATA*. O conceito é calcado em três pilares: velocidade, volume e variedade.

[10] A *World Wide Web* foi criada por Tim Berners-Lee, físico e cientista da computação britânico, em 12 de março de 1989. Quando trabalhava na Organização Europeia para a Pesquisa Nuclear (CERN), ainda em 1980, Tim Berners-Lee propôs um projeto baseado em hipertexto (informações interligadas de forma não-linear), para facilitar o compartilhamento de informações entre os pesquisadores. Mais adiante, em 1989, percebeu a oportunidade de unir o projeto em hipertexto e a internet, o que deu origem à *World Wide Web*. O primeiro site do CERN foi criado em 1990, por meio de um navegador que também funcionava como editor, criado por Berners-Lee. https://tecmasters.com.br/historia-do-world-wide-web-famoso-www/

Essa tem sido a definição mais aceita sobre *BIG DATA*. São dados com maior variedade que chegam em volumes crescentes e com velocidade cada vez maior. Isso também é conhecido como os três Vs.

3.2 Os três Vs do BIG DATA: volume, velocidade e variedade

O Primeiro pilar que define o *BIG DATA* é o volume. A quantidade de dados importa. Trata-se do processamento de grandes volumes de dados não estruturados. Podem ser dados de valor desconhecido, como *feeds* de dados do *Twitter*, fluxos de cliques em uma página da *web* ou em um aplicativo para dispositivos móveis.

Para algumas empresas, isso pode utilizar dezenas de *terabytes* de dados. Para outras, podem ser centenas de *petabytes* (CASALINHO, 2018)

O Segundo pilar que define o *BIG DATA* é a velocidade. Trata-se da taxa mais rápida na qual os dados são recebidos e talvez administrados. Alguns produtos inteligentes habilitados para *internet* operam em tempo real e, por tanto, exigem avaliação e ação em tempo real, o que torna essa análise de dados necessariamente rápida.

O Terceiro pilar que define o *BIG DATA* é a variedade. Variedade refere-se aos vários tipos de dados disponíveis, sejam eles estruturados ou não.

Antes de serem transformados em informação, os dados podem ser divididos em dois grupos, segundo o armazenamento e gerenciamento. No primeiro grupo encontram-se os dados estruturados e no segundo os dados não estruturados. Os dados estruturados são organizados em linhas e colunas em um formato definido de forma rígida, de modo que os aplicativos possam recuperá-los e processá-los com eficiência. Já os dados não estruturados são os que não podem, ou são difíceis de serem armazenados em linhas e colunas. Geralmente são de difícil acesso e recuperação e requerem maior espaço e velocidade para armazenamento e gerenciamento. São muitas vezes dados que não dispõem de componentes necessários para identificação de tipo de processamento e interpretação, tornando o seu uso um desafio, principalmente em aplicativos empresariais.

Em grande parte, somos nós que alimentamos essas cadeias de informação, através das nossas conversas online, dos arquivos baixados, das inúmeras mensagens e fotos nas mídias sociais, dos likes em nosso perfil. Toda essa variedade é o que chamamos *BIG DATA.*

Tipos de dados não estruturados e semiestruturados, como textos, áudios e vídeos, exigem um pré-processamento adicional para obter significado e dar suporte a metadados. Podemos

observar a variedade de dados em *e-mails*, redes sociais, fotografias, áudios, telefones e cartões de crédito. Empresas que conseguem captar a variedade, agregam mais valor ao negócio.

Esses são os três pilares mais importantes identificados no *BIG DATA.* Entretanto, com o tempo, foi possível observar na sua escalada, mais dois Vs.

3.3 Valor e Veracidade do *BIG DATA*

Atualmente o *BIG DATA* se tornou essencial. O mundo muda em uma velocidade crescente a partir da conectividade em grande escala. E todo esse vasto material gerado, em suas interpelações sociais eletrônicas permitirão aos pesquisadores a análise do comportamento humano, sejam nas esferas econômicas, culturais ou sociais. Isso só foi possível, com o desenvolvimento das tecnologias e ferramentas de BIG DATA.

Segundo a *International Data Corporation*[11] (IDC, 2019) *"descrevem uma nova geração de tecnologias e arquiteturas projetadas para extrair economicamente o valor de volumes muito grandes e de uma variedade de dados, permitindo alta velocidade de captura, descoberta e/ou análise".*

Basta observar qualquer uma das maiores empresas tecnológicas atuais para entender que grande parte do valor econômico delas vem de seus dados, que são analisados frequentemente para produzir maior eficiência e desenvolver novos produtos a seus usuários (STANLEY, 2019).

Em razão disso, existe uma corrente que concluiu a existência de mais dois Vs que caracterizam o *BIG DATA*: valor e veracidade.

Dados possuem indubitavelmente um valor econômico. Mas tão importante quando descobrir qual é esse valor econômico é confirmar a veracidade destes dados.

Encontrar o valor em *BIG DATA* não é só uma questão de o analisar, mas um processo de descoberta completo que exige analistas, usuários, executivos, que reconhecem e interpretam padrões, fazem suposições com essas informações e preveem comportamentos de seus utilizadores.

Uma pesquisa junto a grandes empresas do mercado computacional concluiu que um em cada 3 líderes não confiam nos dados que recebem. Para colher bons frutos do processo do *BIG DATA* é necessário obter dados verídicos, de acordo com a realidade. O conceito de velocidade,

[11] É a empresa líder em inteligência de mercado, serviços de consultoria e eventos para os mercados de Tecnologia da Informação, Telecomunicações e Tecnologia de Consumo.

já descrito, é bem alinhado ao conceito de veracidade pela necessidade constante de análise em tempo real, isso significa, dados que condizem com a realidade daquele momento, pois dados passados não podem ser considerados dados verídicos para o momento em que é analisado. A relevância dos dados coletados é tão importante quanto o primeiro conceito. A verificação dos dados coletados para adequação e relevância ao propósito da análise é um ponto chave para se obter dados que agreguem valor ao processo. (HURWITZ, NUGENT, HALPER & MARCIA KAUFMAN, 2016).

3.4 Usos Comerciais do BIG DATA (Coleta de Dados Pessoais)

BIG DATA é hoje, uma das maiores tendências de tecnologia do mercado, com potencial de mudar drasticamente a maneira com que as organizações do setor público ou privado, usam a informação para melhorar a experiencia do homem e seus inter-relacionamentos.

Todas as nossas ações deixam marcas. No mundo virtual as nossas marcas são as informações e dados que deixamos registrados através dos rastros ou pegadas digitais. Os rastros digitais que dizem quem é você na internet.

Apesar do grande crescimento econômico do *BIG DATA* a sua utilidade ainda é cercada de controvérsias.

Muito disso deve-se a grandes escândalos envolvendo empresas como *Facebook* e as recentes polêmicas geradas pelo uso de algoritmos e dados de informação nas redes sociais.

Na Inglaterra e nos Estados Unidos, especialistas começaram uma verdadeira cruzada exigindo mudanças nos algoritmos da tecnologia de reconhecimento facial, alegando que o algoritmo usado pela ferramenta não só era racista, mas discriminava pobres e mulheres.

Em 2018, um grande escândalo foi denunciado pelos jornais *The New York Times* e *The Guardian*, afirmando que a empresa *Facebook* teria negociado o uso das informações de mais de 50 milhões de pessoas sem o consentimento delas pela empresa americana *Cambridge Analytica*, que a usou para propaganda política que culminou com a eleição do presidente *Donald Trump* (*SHOWMETECH*, 2017). Também revelou que a mesma empresa usou as informações dos usuários para influenciar e manipular a saída do Reino Unido da União Europeia no *Brexit*.

Em 2020, uma falha no mecanismo de *login* do *Google* deixou bilhões de usuários no mundo todo sem acesso ao *YouTube*, *Gmail* e *Google Drive*, entre outros.

Todas essas notícias e informações mostram o quão frágil e suscetível o ser humano tornou-se diante das tecnologias que o cercam.

Dificilmente uma pessoa consegue se livrar do uso de uma dessas ferramentas tecnológicas. Atualmente, estima-se que 85% (oitenta e cinco por cento) do mercado de tecnologia e serviços é controlado por 5 (cinco) grandes empresas no mundo. São elas: *Apple*, *Amazon*, *Alphabet*, *Microsoft e Facebook.* São as chamadas *Big Techs* (MOROZOV, 2018). Grandes empresas de tecnologia, inovação e serviços que, constantemente atualizam seus produtos e dispositivos para atender todas as demandas.

Outra fonte considerável de *BIG DATA*, presente desde o início da internet nos anos 90, os *cookies* só explodiram em popularidade com as recentes legislações apontando para a proteção dos dados dos usuários. Entretanto, somente avisar quando se entra numa página como esses dados podem ser usados, não é eficaz, uma vez que não o aceitar, implica em não acessar a página.

Os *cookies* são um protocolo de pacote de dados, que visam garantir a comunicação entre os sites e o usuário final. Criado como uma solução para o *e-commerce*, a ferramenta evoluiu e se tornou presente em todos os tipos de páginas na internet. Os cookies são usados para registar suas preferências na internet.

Da mesma forma os algoritmos, que estão presentes em quase todos os aplicativos e *streamings* usados atualmente.

Os rastros digitais podem ser intencionais e não intencionais. Os intencionais são aqueles que se faz com consciência, a exemplo, mensagens, *e-mails*, *post*, comentários, cadastros, fotos publicadas. Os não intencionais são as buscas em *site*s, trajetos de geolocalização, registros de visitas na *web*, termos de uso aceitos sem verificação, cookies aceitos entre inúmeros outros. Ou seja, ao contrário do que todos pensam, é praticamente impossível ser anônimo na internet. Absolutamente tudo que é feito na rede deixa algum tipo de rastro. Suas ações são registradas e podem ficar lá para sempre.

Mas quando essa informação é usada sem consentimento e de forma negativa, pode em muitos casos, tornar-se manipulação.

4. O MODELO *OCEAN*, PSICOMETRIA E A ALIENAÇÃO DO USUÁRIO

A assertiva é espantosa: *BIG DATA* significa que tudo que fazemos, seja *on* ou *offline*, deixa traços digitais. Cada compra que realizamos com nossos cartões de crédito, cada acesso

a Banco, cada compra *online*, cada busca que fazemos no *Google* ou mesmo cada movimento que fazemos com nossos celulares no bolso, cada *like* ou curtida, cada filme escolhido ou mesmo cada vez que bloqueamos ou deixamos de seguir alguma página ou pessoa, todas essas informações são armazenadas para apurar o nosso perfil psicológico.

Assim, quando inocentemente um usuário clica no botão de like de um filme ou vídeo ou música ou mesmo quando curte uma imagem ou foto de um amigo nas redes sociais, automaticamente gera dados que são coletados por algoritmos capazes de armazenar e analisar o perfil psicológico deste consumidor, transformando essa informação em resposta imediata, oferecendo a ele produtos e ferramentas interessantes às suas necessidades ou, ao seu perfil.

Durante muitos anos não era claro a finalidade de todas essas informações armazenadas e analisadas. O uso que poderia se fazer com esses dados e a quem poderia beneficiar ou alcançar. O valor econômico propriamente dito da informação e dados.

Entretanto, quando o escândalo *Facebook-Cambridge Analytica* estourou nas páginas dos principais jornais do mundo, a população estadunidense assistiu atônita como foi possível usar a informação de milhões de cidadãos manipulando-os nas eleições presidenciais de 2017.

O método usado para avaliar as informações de milhões de usuários vendidas pelo *Facebook*: o modelo *Ocean* de psicometria.

A psicometria, tem como objetivo medir os traços psicológicos que formam a personalidade das pessoas. A Psicometria foi desenvolvida na década de 1980 por duas equipes de psicólogos, que traçaram cinco grandes traços de personalidade: abertura (disposição para novas experiências); *conscientiousness* (grau de perfeccionismo); extroversão (sociabilidade); afabilidade (quão atencioso e cooperativo); e neuroticidade (se a pessoa se aborrece facilmente).

Com base nessa divisão, conhecidas também como *OCEAN* (acrônimo para essas características, em inglês) – é possível avaliar as personalidades das pessoas de forma bastante eficaz, projetando um perfil psicológico de cada uma. Isso inclui também uma predição de como ela tende a se comportar (KELSON, 2020).

Os “Cinco Grandes” tornaram-se a técnica padrão da psicometria. Mas, por muito tempo, o obstáculo dessa abordagem era a coleta de dados, porque envolvia o preenchimento de um questionário complicado e altamente pessoal.

Mas, o que os psicólogos no campo da psicometria não poderiam imaginar, era o advento das redes sociais.

Michal Kosinski, era um estudante em Varsóvia quando foi aceito na Universidade de Cambridge para fazer seu PhD no centro de Psicometria. Uniu-se ao colega de estudos David

Stillwell, que um ano antes havia lançado um pequeno aplicativo para o Facebook, nos tempos que a plataforma ainda não tinha alcançado a dimensão que tem hoje. O nome do aplicativo era *MyPersonality* [12].

Em pouco tempo, os usuários haviam preenchido e respondido ao pesquisador diversos questionários psicométricos, incluindo várias questões psicológicas baseadas no modelo *Ocean*: "Entro em pânico fácil", "Contradigo os outros com frequência". Com base na avaliação, os usuários recebiam um "perfil de personalidade" – os valores *Big Five* individuais – e podiam optar por compartilhar seus dados de perfil do *Facebook* com os pesquisadores. Mas não somente os deles, também de todas os seus contatos.

Os pesquisadores esperavam que apenas alguns amigos próximos fossem responder, mas em pouco tempo, possuíam o maior conjunto de dados psicométricos sobre os perfis do *Facebook* jamais coletados.

A partir daquelas respostas, os dois pesquisadores e sua equipe passaram a comparar as informações com todos os outros dados online dos voluntários: o que "curtiram", compartilharam ou postaram no *Facebook*, ou qual gênero, idade, local de residência especificaram. Isso permitiu que os pesquisadores fizessem correlações e deduções bastante precisas e confiáveis.

Projetadas a partir de simples ações online, era possível predizer que homens que "curtiam" a marca de cosméticos *MAC* tinham um pouco mais de probabilidades de ser gays; um dos melhores indicadores de heterossexualidade era "curtir" um grupo de *hip hop*, americano de Nova York, *Wu-Tang Clan*. Seguidores de *Lady Gaga* eram muito provavelmente extrovertidos, enquanto aqueles que "curtiam" filosofia tendiam a ser introvertidos (KOSINSKI, 2012).

Durante os anos seguintes os psicólogos aperfeiçoaram seu modelo e em 2012, Michal Kosinski e David Stillwell, provaram que, com base numa média de 68 "curtidas" no *Facebook*, era possível descobrir a cor da pele de um usuário, sua orientação sexual e sua filiação partidária. Poderia auferir sua inteligência, filiação religiosa, assim como uso de álcool, fumo ou droga. Com base em estudos e análise dos perfis através do modelo *Ocean*, afirmaram que, com 70 "curtidas" saberiam mais sobre o usuário do que seus amigos próximos, com 150 "curtidas", saberiam mais do que os pais desse usuário e se excedessem 200 "curtidas",

[12] Batizado de MyPersonality, o aplicativo foi realizado por 6 milhões de pessoas e expôs 3,1 milhões que aceitaram compartilhar dados do seu perfil no Facebook, segundo a New Scientist. O app foi criado por David Stillwell e Michael Kosinski, também pesquisadores da Universidade de Cambridge. O objetivo do teste era traçar um perfil psicológico dos usuários com base no Big Five, conceito da psicologia psicosimétrica para se referir a cinco fatores de personalidade: neuroticismo, extroversão, agradabilidade, conscienciosidade e abertura para a experiência.

saberiam mais do que seus cônjuges. Que com base nas "curtidas" de um usuário poderiam, com o tempo, saber mais sobre essa pessoa do que ela mesma (KOSINSKI, 2012).

A precisão com que podiam prever as respostas de uma determinada pessoa demonstravam a força do seu modelo de psicometria. Essencialmente, Kosinski inventou uma espécie de análise comportamental que poderia ser usada de diversas maneiras, seja para fins comerciais ou até mesmo, se usada de forma errada, para separar determinados grupos, como, em referência as eleições de 2018, democratas indecisos.

A psicometria do modelo *Ocean*, foi levada especialmente a sério pelas *BIG TECHS* e passaram a fazer parte de sua gestão de dados, especialmente pela maior rede social do mundo, *Facebook*[13].

Kosinski, que almejava contribuir e compartilhar suas descobertas na psicometria, passou a reconhecer não só o potencial, mas também o perigo inerente a essas informações, podendo ser usada de forma abusiva para manipular pessoas. Ele começou a estampar avisos na maior parte do seu trabalho científico. Sua abordagem, avisava ele próprio, *"poderia representar uma ameaça ao bem-estar individual, à liberdade ou até à vida"* (KOSINSKI, 2012).

O poder do método *ocean* pode ser observado quando, tempos depois, em 2016, um homem magro, num terno azul escuro bem cortado, caminhou para o palco da Cúpula Concordia, em um hotel em Nova York – *"Por favor, deem as boas-vindas ao Sr. Alexander Nix, CEO do Cambridge Analytica"*. O homem sorridente, anuncia: "É um privilégio para mim falar com vocês hoje sobre o poder do *BIG DATA* e da psicometria no processo eleitoral." O logo da *Cambridge Analytica* – um cérebro composto de todos nós da rede, como um mapa, aparece atrás de Alexander Nix[14] (*Das Magazin*, 2017).

A *Cambridge Analytica* era uma subsidiária da SCL, ou *Strategic Communication Laboratories* (Laboratórios de Comunicação Estratégica) e foi contratada para a campanha de marketing nas eleições de *Donald Trump*, nos Estados Unidos. A força central da empresa: marketing político inovador – micro abordagem –, medindo a personalidade das pessoas a partir de suas pegadas digitais, com base no modelo *Ocean*.

A SCL oferece marketing baseado em modelos psicológicos. Um de seus focos centrais: influenciar eleições.

---

[13] https://about.facebook.com/br/ : empresas *Facebook, Facebook Messenger, Instagram, WhatsApp, Oculus VR, Giphy e Mapillary, Jio Platforms, Onavo, Beat Games e Libra Networks e Novi (rede de criptomoedas),* e demais aquisições do grupo são comandadas pela *Meta Platforms*, conglomerado de tecnologia e mídia social.

[14] O artigo original sobre a pesquisa do Dr. Michal Kosinski apareceu originalmente na Das Magazin, em dezembro. Publicado no Showmetech em 6 de fevereiro de 2017: https://www.showmetech.com.br/big-data-trump/

4.1 Manipulação de dados de usuários nas redes (como transformar cliques em votos)

O escândalo ocorrido nas eleições presidências estadunidenses de 2017, envolvendo a campanha presidencial de *Donald Trump*[15] e a empresa de marketing *Cambridge Analytica*[16], trouxe a luz a preocupação com a manipulação de dados de usuários na internet e até qual ponto empresas podem invadir a privacidade individual e violar direitos fundamentais. A empresa *Cambridge Analytica*, através da coleta de dados individuais do *Facebook*, "transformou cliques em votos" (LAPOWSKY, 2018).

A associação entre *Facebook* e a *Cambridge Analytica*, causou enorme perplexidade nos usuários da rede no mundo todo, trazendo inúmeros questionamentos sobre a legalidade das ações de ambas as empresas.

Não entraremos aqui, nas consequências sofridas pelas empresas, seja pela falência ou o pagamento de multas multimilionárias, mas nos prezaremos em explanar, que os impactos do escândalo nas eleições dos Estados Unidos podem ser considerados um dos maiores casos de manipulação midiática comprovado que temos recentemente. A Era Digital também trouxe um conceito de anonimato que acaba preservando muitas empresas de serem de fato descobertas em uso de dados pessoais. As redes sociais foram muito importantes na estratégia de alinhar as mensagens das eleições dos EUA a favor de *Trump*, por meio de otimizações de algoritmos, dados e técnicas de comunicação (DE LLANO, 2018).

As políticas de uso das redes sociais muitas vezes permitem o compartilhamento de todos os dados pessoais de seus usuários, tornando fácil a análise comportamental de cada um. Transformados em *BIG DATA*, essas informações podem ser avaliadas e usadas para fins comerciais ou, como no caso, para manipulação de opinião pública.

O indivíduo moderno é um espectador e um consumista dos produtos e notícias, vivendo em uma submissão alienante ao império da mídia. Ao longo do século XX e princípio do século XXI, a mídia migrou do impresso para o digital, e o homem passou a ser muito mais suscetível e bombardeado com publicidade e propaganda.

Entretanto, o grande questionamento não é se a polarização da opinião pública é algo bom ou ruim, mas sim se o uso indiscriminado e compartilhamento de dados podem afetar e transformar a sociedade de um país ou grupo mundial.

---

[15] Donald John Trump é um empresário, personalidade televisiva e político americano que serviu como o 45.º presidente dos Estados Unidos.

[16] Cambridge Analytica, Ltd. foi uma empresa privada que combinava mineração e análise de dados com comunicação estratégica para o processo eleitoral. Foi criada em 2013, como um desdobramento de sua controladora britânica, a SCL Group para participar da política estadunidense.

O escândalo pode ter sido o estopim para as discussões sobre segurança digital e manipulação de dados pelo uso de *BIG DATA* em eleições com o intuito de favorecer determinadas figuras políticas. O grande acesso à informação nos coloca em posição de vulnerabilidade diante de importantes tomadas de decisões.

Ressalte-se aqui, que o pernicioso uso de ferramentas de *BIG DATA*, com a análise de dados pessoais, tecnologia e estratégia política, transformaram o que eram apenas dados em informações. Algoritmos traçaram os perfis de votos indecisos de milhares de pessoas e, com uma avassaladora estratégia política, as mídias sociais passaram a bombardear os eleitores com propagandas direcionadas e até mesmo com *Fake News*, afetando de forma direta a política dos Estados Unidos, também atingindo a política internacional.

Esse monitoramento constante sofrido pelo homem na era digital, *stalkeado*[17] no ciberespaço, o coloca em verdadeira situação de fragilidade, uma vez que o mau uso de dados pessoais e a própria submissão consumista que a sociedade lhe impõe, são pontos extremamente favoráveis para uma estratégia política e devem ser investigados de forma mais assertiva para que a essência da Democracia não se perca.

5. CONSIDERAÇÕES FINAIS

Afinal, **quanto vale o acesso aos nossos dados?** Analisando os eventos ocorridos no ano anterior podemos entender porque em 2018 surgiram as mais completas legislações acerca do uso de dados e privacidade no Brasil e no mundo.

Um dos objetivos da Lei Geral de Proteção de Dados é garantir o acesso à informação de maneira clara e transparente sobre o tratamento de dados pessoais. Sendo assim, é razoável esperar que haja uma atualização crescente nos sites e aplicativos, sempre norteando-se pela transparência do uso das informações de seus usuários. "Os dados são o novo petróleo"[18]. A máxima está sendo bradada a sete ventos e certamente faz jus a verdade. Os dados hoje são uma das *commodities*[19] mais valorizadas no mundo.

---

[17] Neologismo para o português que significa "ato de perseguir". O verbo "stalkear" foi criado e disseminado através da internet, utilizado no sentido de "perseguir" ou "espionar" as atividades e comportamentos de outros usuários em redes sociais, principalmente.

[18] A famosa frase do matemático britânico Clive Humby: *"Dados são o novo petróleo" (Data is the new oil),* bem como a publicação da The Economist: *"O recurso mais valioso do mundo não é mais o petróleo, mas dados" (The world's most valuable resource is no longer oil, but data)* tem sido muito citadas pelo mercado apontando que aqueles que possuírem dados terão um recurso muito valioso em mãos.

[19] Commodities são produtos de origem agropecuária ou de extração mineral, em estado bruto ou pequeno grau de industrialização, produzidos em larga escala e destinados ao comércio externo. Seus preços são determinados pela oferta e procura internacional da mercadoria. No Brasil, as principais commodities são o café, a soja, o trigo e o petróleo.

Para acompanhar as crescentes mudanças tecnológicas e tornarem-se competitivas no mercado, as empresas passaram a investir em medidas de segurança que protejam seus negócios e segredos, bem como os dados das pessoas que se inter-relacionam com elas. Os investimentos em tecnologia de ponta e contratação de profissionais capacitados em tecnologia de informação, passaram a receber atenção dobrada.

No mesmo caminho, os governos do mundo passaram a aprovar leis que visam a proteção dos dados pessoais de seus cidadãos, como foi o caso da União Europeia e sua pioneira *General Data Protection Regulation*, a GDRP, pioneira no regulamento legislativo para proteção dessas informações digitais.

A GDPR não só foi um marco inovador na legislação de proteção de dados, como serviu de base para que inúmeras outras leis similares fossem aprovadas, como foi o caso no Brasil e a Lei Geral de Proteção dos Dados (LGPD), em vigor desde 2020.

Entrementes, como toda nova lei, a LGPD ainda está longe de alcançar sua melhor eficácia. No Brasil, deu-se o início da era do "aceitar cookies". Os cookies são uma parte importante da LGPD, mas quando o usuário inadvertidamente os aceita, também aceita o compartilhamento de seus dados de navegação com as empresas parceiras daquele site. A problemática é que a maioria dos usuários não sabem quais dados estão sendo compartilhados e muito menos para que são usados.

Outrossim, estamos caminhamos para uma realidade onde a propriedade real dos dados significará ter todas as suas informações, como ideias políticas, preferências e histórico médico, em um único lugar para que, qualquer um, menos você, possa decidir como usá-los. Isso poderia significar vendê-los, conceder uso ilimitado em troca de um serviço, a exemplo do que fez o *Facebook*.

O uso comercial de informações pessoais na era do *BIG DATA* já é uma realidade. Nessa analogia, determinar quem tem direito a posse dos "dados pessoais" é o próximo passo da revolução de *BIG DATA*.

Estamos falando de grandes volumes de informação, em grande velocidade, variedade, veracidade e valor. Por isso, é importante entender como esses cinco Vs determinam as escolhas dos cidadãos.

O ponto polêmico é que o modelo *Ocean* usa a psicometria (ramo da psicologia baseado em estatísticas) para traçar o perfil psicológico dos usuários com incrível precisão, criando algoritmos que podem não só persuadir como determinar comportamentos. Tão certo quanto as opções clicadas tornam nossa navegabilidade mais fácil, assim trabalha o algoritmo

comportamental, que se aproveita desses traços de personalidade coletados para direcionar o consumo e incluir o usuário em grupos pré-padronizados. Quase como a mais perversa das teorias de conspirações, os algoritmos passaram a ser usados para reconhecer e padronizar hábitos diários, podendo prever necessidades e fornecer produtos e serviços e até mesmo induzir a determinados comportamentos: políticos, culturais, sociais e econômicos.

Por trás de tudo que você consome existe um algoritmo que trabalha combinando uma enxurrada de dados *online* para antecipar desejos, orientar decisões, guiar escolhas e compras. Por essa razão há quem defenda que o *BIG DATA* tenha a capacidade de prever o futuro, determinando inclusive as escolhas do mercado futuro.

As leis e regulamentos são um passo importante para dirimir o uso nefasto das informações, no entanto, é provável que sua aplicação demore um pouco para alcançar a variedade cada vez maior de dispositivos conectados à Internet. Por outro lado, ao refletirmos sobre o caráter gratuito das redes socias, não podemos negar que a moeda de troca entre a empresa e o usuário são todos os dados que o próprio utilizador fornece graciosamente.

A discussão é acirrada quanto ao uso desses dados serem legais, uma vez que os usuários foram "compelidos" a aceitar a política de uso das empresas acessadas e, por trás dessa transação, há um grande mercado em desenvolvimento.

Para o bem ou para o mal, as inovações da tecnologia não podem ser freadas. E, sendo o *BIG DATA*, o produto mais imediato da inter-relação do homem com a internet, cabe a ele gerir suas políticas públicas e privadas para a proteção dos dados pessoais de seus cidadãos. Afinal, se a tecnologia se apresenta a serviço do ser humano, a sua aplicação deve aproximar a tecnologia do seu destinatário. Como se fossem as duas faces da mesma moeda.

REFERÊNCIAS

CASALINHO, Gilmar D'Agostini Oliveira. **O IMPACTO DO USO DO BIG DATA NA INTELIGÊNCIA COMPETITIVA E NA PERCEPÇÃO DO PRODUTO PELO CLIENTE: DESENVOLVIMENTO DE PROPOSIÇÕES DE PESQUISA.** Revista Brasileira de Inteligência, 2018. Disponível em: file:///D:/MEUS%20DADOS%20NAO%20APAGAR/Downloads/660-667-1-PB%20(2).pdf; Acesso em: 21 abr. 2022.

BACHRACH, Yoram; KOSINSKI, Michal; *et al*. **Personalidade e padrões de uso do Facebook.** Publicado no Showmetech em 6 de fevereiro de 2017: https://www.showmetech.com.br/big-data-trump/; 2012. Disponível em: https://doi.org/10.1145/2380718.2380722; Acesso em: 21 abr. 2022.

BOFF, Salete Oro; FORTES, Vinícius Borges. **A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um Direito Fundamental: perspectivas de construção de um marco regulatório para o Brasil**. **Sequência (Florianópolis)**, p. 109-127, 2014. Disponível em:

https://www.scielo.br/j/seq/a/LqY93YW8FMSNPgkVBg75nbH/?format=pdf&lang=pt; Acesso em: 21 abr. 2022.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm; Acesso em: 21 abr. 2022.

BRASIL. Lei nº 9.296 de 24 de Julho de 1996. Regulamenta o inciso XII, parte final, do art. 5° da Constituição Federal.
Disponível em: http://www.planalto.gov.br/ccivil_03/leis/l9296.htm;
Acesso em: 21 abr. 2022.

BRASIL. Lei nº 12.527/2011, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5o, no inciso II do § 3o do art. 37 e no § 2o do art. 216 da Constituição Federal; altera a Lei no 8.112, de 11 de dezembro de 1990; revoga a Lei no 11.111, de 5 de maio de 2005, e dispositivos da Lei no 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm; Acesso em: 21 abr. 2022.

BRASIL. Lei nº 12.737/2012, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.
Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm;
Acesso em: 21 abr. 2022.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm; Acesso em: 21 abr. 2022.

CANCELIER, Mikhail Vieira de Lorenzi. **O Direito à Privacidade hoje: perspectiva histórica e o cenário brasileiro**. SciELO Brasil – Scientific Electronic Library Online, Universidade Federal de Santa Catarina, 2019. Disponível em:
https://www.scielo.br/j/seq/a/ZNmgSYVR8kfvZGYWW7g6nJD/?format=pdf&lang=pt; Acesso em: 21 abr. 2022.

DE LLANO, Pablo. **Consultoria que trabalhou para Trump fez maior roubo de dados da história do Facebook**. El País, 18 mar. 2018. Disponível em:
https://brasil.elpais.com/brasil/2018/03/17/internacional/1521308795_755101.amp.html; Acesso em: 21 abr. 2022.

FILHO, Adalberto Simão; SCHWARTZ, Germano André D. **BIG DATA BIG PROBLEMA!** PARADOXO ENTRE O DIREITO À PRIVACIDADE E O CRESCIMENTO SUSTENTÁVEL. Universidade Federal de Goiás - UFG. Conpedi Law Review, 2016. Disponível em:
https://www.indexlaw.org/index.php/conpedireview/article/view/3644#:~:text=Constatado%20o%20paradoxo%20existente%20entre,inten%C3%A7%C3%A3o%20%C3%A9%20instigar%20o%20pensamento; Acesso em: 21 abr. 2022.

HURWITZ, Judith, *et al*. **BIG DATA para leigos**. Alta Books Editora, 2016. Disponível em:
https://books.google.com.br/books?id=j8hYCwAAQBAJ&printsec=frontcover&hl=pt-BR#v=onepage&q&f=false; Acesso em: 21 abr. 2022.

JAMIL, George Leal; NEVEZ, Jorge Tadeu Ramos. **A era da informação:** considerações sobre o desenvolvimento das tecnologias da informação. **Perspectivas em Ciência de Informação.**
Disponível em: https://brapci.inf.br/index.php/res/v/35811; Acesso em: 21 abr. 2022.

KELSON, Pedro. **O homem nu: tecnologias de vigilância e os perigos para a democracia. Sociedade Vigiada**, Organizado por Ladislau Dowbor. Anatomia Literária e outras palavras. p. 66, 2020. Disponível em: https://dowbor.org/wp-content/uploads/2021/03/Sociedade-Vigiada.pdf#page=66; Acesso em: 21 abr. 2022.

LAPOWSKY, Isse. **How Cambridge Analytica sparked the great privacy awakening. Wired.** São Francisco: 17 mar 2018. Disponível em: https://www.wired.com/story/cambridge-analytica-facebook-privacy-awakening/; Acesso em: 21 abr. 2022.

LEITE, Henrique Specian. **A Importância da Privacidade na Internet.** Tecnologia em Análise e Desenvolvimento de Sistemas, Departamento de Tecnologia da Informação, Faculdade de Tecnologia de São Paulo, São Paulo, 2016. Disponível em: A importância da Privacidade na Internet - Brasil Escola (uol.com.br) Acesso em: 21 abr. 2022.

MACEDO, Fernanda dos Santos; BUBLITZ, Michele Dias; RUARO, Regina Linden. **A *privacy* norte-americana e a relação com o direito brasileiro**. 2013. Disponível em: file:///D:/MEUS%20DADOS%20NAO%20APAGAR/Downloads/2666-Texto%20do%20artigo%20-%20Arquivo%20Original-10746-1-10-20130715%20(4).pdf; Acesso em: 21 abr. 2022.

MAIA, Luciano Soares. **A PRIVACIDADE E OS PRINCÍPIOS DE PROTEÇÃO DO INDIVÍDUO PERANTE OS BANCOS DE DADOS PESSOAIS**. Publica Direito. Jurídica. 2011. Disponível em: http://www.publicadireito.com.br/conpedi/manaus/arquivos/anais/bh/luciano_soares_maia.pdf; Acesso em: 21 abr. 2022.

MEZZAROBA, Orides; MONTEIRO, Cláudia Servilha. **Manual de Metodologia da pesquisa no direito**. 5ª EDIÇÃO. São Paulo: Saraiva, 2009. Disponível em: https://www.academia.edu/28317145/Manual_de_Metodologia_da_pesquisa_no_Direito_Orides_Mezzaroba_Claudia_Servilha_Monteiro; Acesso em: 15 abr. 2022.

MOROZOV, Evgeny. **BIG TECH: A Ascensão dos dados e a Morte da Política**. Tradução Cláudio Marcondes. UBU EDITORA. São Paulo, 2018. Disponível em: https://edisciplinas.usp.br/pluginfile.php/5143657/mod_resource/content/1/Big%20Tech.pdf; Acesso em: 21 abr. 2022.

STANLEY, Loh. **Volume, velocidade, variedade, veracidade e valor: como os 5 Vs do BIG DATA estão impactando as organizações e a sociedade.** Porto Alegre - Rio Grande do Sul, Intext, 2019. Disponível em: https://www.intext.com.br/5vs-big-data.pdf; Acesso em: 21 abr. 2022.

SZINVELSKI, Mártin Marks; ARCENO, Taynara Silva; FRANCISCO, Lucas Baratieri. **Perspectivas jurídicas da relação entre BIG DATA e proteção de dados**. Universidade do Vale do Rio dos Sinos, São Leopoldo, RS, Brasil. Rio Grande do Sul, SciELO Brasil – Scientific Electronic Library Online, 2019. Disponível em: https://www.scielo.br/j/pci/a/HhLyd6FMjFrf6hjHnfdH8GR/?lang=pt; Acesso em: 21 abr. 2022.

ZANINI, Leonardo Estevam de Assis. **O Surgimento e o Desenvolvimento do Right of Privacy nos Estados Unidos.** Justitia, São Paulo, 70-71-72 (204/205/206), jan./dez. 2013-2014-2015; Disponível em: http://www.mpsp.mp.br/portal/page/portal/documentacao_e_divulgacao/doc_biblioteca/bibli_servicos_produtos/bibli_informativo/bibli_inf_2006/Justitia%20n.204-206.21.pdf; Acesso em: 21 abr. 2022.