Revista Sinapse Múltipla
v.12, n.1, p.213-229, Jan.\jul. 2023.
PUC Minas Betim

O DIREITO À PROTEÇÃO DE DADOS NA LEGISLAÇÃO BRASILEIRA E EUROPEIA

THE RIGHT TO DATA PROTECTION IN BRAZILIAN AND EUROPEAN LEGISLATION

Carolina Souza Novaes Gomes Teixeira[1]
Débora de Jesus Rezende Barcelos[2]

RESUMO

A tecnologia traz contradições, ao mesmo tempo em que liberta, permitindo o acesso em tempo real a todo e qualquer tipo de informação, ela também aprisiona, criando uma necessidade constante de acesso a cada vez mais novas informações, quer sejam verdadeiras, quer não. Com isso, as empresas privadas e o Poder Público, tornam-se detentoras de dados pessoais dos indivíduos, utilizando-os para a obtenção de lucro através da captura internacional de dados para a criação de interesses artificiais: o chamado Big Data. Diante desse cenário e, partindo da hipótese da utilização de dados como ferramenta de controle, o presente trabalho tem como objetivo averiguar a necessidade da proteção destes dados como um direito humano fundamental a partir da análise comparada das legislações de proteção de dados brasileira e europeia. Para tanto, a pesquisa se utilizará da metodologia da pesquisa bibliográfica e da análise comparada da legislação, além das normas internacionais de direitos humanos. O trabalho partirá de uma demonstração dos benefícios e dos malefícios da inovação tecnológica, seguindo pelo estudo da necessidade de proteção de dados como um direito humano fundamental para, posteriormente, passar à análise da legislação brasileira e europeia.

PALAVRAS-CHAVE: Inteligência artificial, Democracia e Direitos fundamentais.

[1] Doutora e mestre em Direito Material e Processual do Trabalho pela PUC Minas, Professora Adjunto I, PUC Minas. Contato: carolinasnovaes@gmail.com.
[2] Mestranda em Trabalho, Democracia e Efetividade no Programa de Pós-graduação em Direito, PUC Minas. Contato: deboradejesus.barcelos@gmail.com.

ABSTRACT:

Technology brings contradictions, while simultaneously liberating by providing real-time access to any and all types of information, it also confines by creating a constant need for access to increasingly new information, whether true or not. As a result, private companies and the government become holders of individuals' personal data, using it to profit through the international capture of data for the creation of artificial interests: the so-called Big Data. In light of this scenario and starting from the hypothesis of data utilization as a tool for control, this study aims to investigate the necessity of protecting this data as a fundamental human right through a comparative analysis of Brazilian and European data protection laws. To accomplish this, the research will employ the methodology of bibliographic research and comparative analysis of legislation, in addition to international human rights standards. The study will begin by demonstrating the benefits and harms of technological innovation, followed by an examination of the necessity of data protection as a fundamental human right, and subsequently proceed to analyze the Brazilian and European legislation.

KEYWORDS: Artificial intelligence, democracy, and fundamental rights.

1. INTRODUÇÃO

A evolução da tecnologia ao longo dos anos inaugurou uma nova era marcada pela democratização do acesso à internet e à informação. Nesse cenário nascem as redes sociais como um espaço destinado à interação global entre as mais diversas pessoas que queiram dividir suas experiências. No entanto, essa tecnologia que tinha tudo para ser emancipadora parece carregar em si uma grande contradição, pois, ao mesmo tempo em que liberta, permitindo o acesso em tempo real a todo e qualquer tipo de informação, ela também aprisiona, criando uma necessidade constante de acesso a cada vez mais novas informações, quer sejam verdadeiras, quer não. As pessoas, então, passam a ser cada vez mais alienadas e mais vigiadas, tornando-se verdadeiros “fantoches” de um sistema de manipulação de massas que opera através da captura internacional de dados para a criação de interesses artificiais: o chamado Big Data. Diante desse cenário e, partindo da hipótese da utilização de dados como ferramenta de controle, o presente trabalho tem como objetivo averiguar a necessidade da proteção destes dados como um direito humano fundamental a partir da análise comparada das legislações de proteção de dados brasileira e europeia. Para tanto, a pesquisa se utilizará da metodologia da pesquisa bibliográfica e da análise comparada da legislação, além das normas internacionais de direitos humanos. O trabalho partirá de uma demonstração dos

benefícios e dos malefícios da inovação tecnológica, seguindo pelo estudo da necessidade de proteção de dados como um direito humano fundamental para, posteriormente, passar à análise da legislação brasileira e europeia.

2. A ERA DA INFORMAÇÃO E O PANÓPTICO PÓS-MODERNO

A pós-modernidade coincide com a reorganização do cenário mundial a partir do final dos anos 60, início dos anos 70 do século passado. A evolução tecnológica, a reestruturação dos modos de organização da produção, os novos padrões societários, o individualismo exacerbado, a valorização da plasticidade, do cambiante e do efêmero marcam o início desse novo período histórico.

A digitalização do mundo da vida avança e submete as pessoas a uma mudança radical de percepção quanto às suas relações interpessoais e com o mundo. Inebriados pela facilidade e conveniência ofertadas pelos smart apps presentes nos smartphones, a comodidade dos sites de busca e dos assistentes de voz e a sensação de ininterrupta atualização e informação das redes sociais, os indivíduos ficam constantemente conectados.

Em pesquisa realizada em parceria pela DataReportal e a We Are Social (2023), dos 8,03 bilhões de indivíduos que habitam o globo terrestre em abril de 2023, 5,48 bilhões possuem telefone móvel, o que equivale a 68,3% da população mundial. Em termos de tempo em que os indivíduos se encontram conectados à internet, a média mundial é de 6 horas e 35 minutos por dia, o que equivale a aproximadamente 100 dias inteiros durante o ano. (DATAREPORTAL, 2023).

Esse elevado índice de conexão possibilita a ruptura com antigas práticas sociais em prol de um desejo de “economia” de tempo. Com efeito, atividades que outrora eram corriqueiras como ir ao banco para fazer um pagamento, se deslocar até a casa de um amigo ou familiar para conversar, ou mesmo para comprar um bem de consumo, na era do computador e da internet ficam à um clique de distância e à um milésimo de segundo, não sendo necessário mais que um “escorregar de dedos” para sua realização.

Até mesmo os locais de trabalho se desmantelam, pois, com a introdução dos aparelhos microeletrônicos no trabalho, o antigo “ambiente” de trabalho torna-se desnecessário, podendo o trabalhador executar o seu serviço em qualquer hora e em qualquer lugar. Em outras palavras, o coletivo de trabalhadores, outrora organizado segundo a ideia do panóptico de Bentham, agora é disseminado.

Para Bentham (2008), a ideia do panóptico era a de que, quanto mais constantemente as pessoas inspecionadas permanecessem às vistas do inspetor, tendo consciência disso e sob

o temor reverencial de sofrer uma sanção, mais se reprimiriam e agiriam segundo a conduta delas esperada, o que demandava, porém, a figura de um estabelecimento para inspeção. Nesse sentido, Foucault (2012), ao analisar a arquitetura do panóptico benthamiano notou três elementos: a vigilância hierárquica, a sanção normalizadora e o exame. A vigilância hierárquica consistia na presença física de um superior legitimado a vigiar; a sanção normalizadora, em punições por mal comportamento, ao passo que, o exame, era a conjugação destes dois elementos, ou seja, o processo intermediário pelo qual, a partir da vigilância, verificava-se uma conduta em desconformidade aos padrões exigidos e a punia conforme o grau de desobediência. (FOUCAULT, 2012)

A combinação destes elementos possibilitava uma influência direta e significativa sobre os indivíduos sem a necessidade de força física, o que levou Foucault (2012) a acreditar, que o panóptico poderia ser utilizado, inclusive, como uma "máquina de fazer experiências, modificar o comportamento, treinar ou retreinar os indivíduos". (FOUCAULT, 2012, p. 193)

Ocorre, que conforme observa Byung-Chul Han (2014), esse panóptico benthamiano, que consistia em uma estrutura circular com uma torre de vigilância no centro, por estar restrito a um determinado ambiente[3], prévia e cautelosamente construído tinha limitações, posto que conseguia observar seus reclusos apenas no seu exterior, isto é, permanecia estritamente ligado ao meio óptico e ao controle físico, corporal, não tendo acesso aos pensamentos ou as necessidades internas de seus vigiados.

Desta feita, o controle poderia ser extinto tão logo a pessoa desocupasse o local do confinamento, estando, após, verdadeiramente livre.

No entanto, com a evolução tecnológica, as reivindicações por liberdade e a crise dos locais de confinamento, o capital passou a demandar um controle e uma vigilância ainda mais profundos, capazes de intervir não só no corpo, mas também na mente e nos pensamentos dos indivíduos. Para tanto, o panóptico de Bentham precisava ser aperfeiçoado, com a substituição dos antigos espaços de confinamento por mecanismos de vigilância mais maleáveis, capazes de perseguir o sujeito vigiado a qualquer tempo e a qualquer lugar. A internet, o smartphone e a Google se mostraram mecanismos hábeis a cumprir tal finalidade, principalmente pelo fato de exercê-la de forma mascarada, sob a aparência de uma falsa liberdade de navegação. É então que o panóptico de Bentham se aperfeiçoa em panóptico digital.

[3] Entre os ambientes pelos quais poder-se-ia aplicar a ideia do panóptico benthamiano, citam-se as fábricas, estabelecimentos de trabalho em geral, escolas, hospitais, manicômios, presídios, etc.

Nesse contexto, Maria Cecília Máximo Teodoro e Karin Bhering Andrade (2020, p. 263) ensinam que:

> Em tempos atuais, com o desenvolvimento tecnológico, a vigilância se faz também de forma eletrônica, dentro de um contexto organizacional por meio de dispositivos tecnológicos diversos, como câmeras, microfilmes ou computadores, bem como via internet, incluindo suas redes sociais, WhatsApp, Instagram, Facebook e até mesmo por aplicativos de controle digital como a Uber. (TEODORO; ANDRADE, 2020, p. 263)

O objetivo do capital ao empreender e investir nessas novas formas de vigilância é justamente a manipulação e controle total do indivíduo, a fim de monitorar não só seu corpo e seu tempo de trabalho, tal como realizará em tempos fordistas[4], mas também, sua mente e sua alma. Assim, se no panóptico de Bentham o controle se extirpava tão logo o indivíduo deixasse o confinamento, agora, não existe mais tal possibilidade, por isso fala-se em um panóptico pós-moderno, posto que supera os limites da fábrica e adentra na própria subjetividade e na vida privada dos sujeitos.

Efetivamente, com a desestruturação e horizontalização[5] das grandes indústrias e a consequente dispersão do coletivo de trabalhadores do ambiente da empresa somada ao crescimento do setor de serviços, tornou-se imprescindível para o capital tratar de arranjar outros meios que substituíssem o controle direto mediante a presença física de uma pessoa, por um controle indireto, mas que fosse ainda mais eficiente, sobretudo, considerando a distância corporal dos trabalhadores.

Essa nova forma de controle parte da figura do "Big Data" ou "Grandes Dados" como mecanismo de vigilância e persuasão de pessoas. Por Big Data, pode-se entender, de acordo com Adriana Goulart de Sena Orsini (2020), como um sistema de Tecnologia da Informação que permite a captura, a análise e a catalogação de registros em tempo real. Nas palavras de Orsini (2020, p. 323) "[...] o Big Data proporciona o armazenamento quase ilimitado de dados textuais e a análise de tais dados, mesmo que não estejam estruturados. É possível extrair informações relevantes de uma gigantesca massa de dados não tabulados, identificando padrões e sugerindo conclusões a partir destes".

---

[4] Método de organização da produção inaugurado por Henry Ford no século XX, em sua indústria de automóveis na fabricação e montagem do famoso veículo de modelo "T". O método fordista era basicamente ancorado em um modelo industrial verticalizado, com a fragmentação de pequenas tarefas entre os empregados e a cronometrização do tempo para desenvolvê-las. O modelo fundava-se em uma vigilância rígida a partir da presença e fiscalização dos serviços desempenhados por parte de superiores hierárquicos diretos, capazes de disciplinar com sanções. (GOUNET, 1999).

[5] A desestruturação e horizontalização das fábricas envolve um processo de terceirização, pejotição, teletrabalho, intermitência, etc.

Tais dados podem ser originados a partir de diversas fontes internas e externas, como cadastros de clientes, análises de mercado, redes sociais, dispositivos eletrônicos, aplicativos, processos internos ou mesmo pesquisas em meios off-line. A partir disso, as técnicas de estatística e processamento computadorizadas começam a perceber protótipos e a criar algoritmos prevendo tendências comportamentais com maior precisão.

O capital, então, começa a extrair, mapear e a alcançar, em tempo real, informações acerca da localização e da temporização das pessoas, isto é, onde se encontram, onde poderão se encontrar e a que tempo, assim como, quantos minutos e segundos levarão para desempenhar as suas atividades. De acordo com Teodoro e Andrade (2020), esse monitoramento dos indivíduos tem como fulcro a produtividade e a lucratividade.

Além disso, o Big Data consegue, ainda, verificar as principais crenças, desejos e tendências de uma determinada população, o que permite ao capital manipulá-los da melhor maneira possível, uma vez conhecidas as suas principais paixões e fraquezas.

Percebe-se, portanto, que o panóptico digital ancorado no Big Data é, sem dúvida, uma forma de controle muito mais eficiente que o antigo panóptico de Bentham, posto que possibilita uma visão de 360 graus sobre os sujeitos objeto de vigilância.

Embora, em princípio, tenha se celebrado a rede digital como um meio de liberdade ilimitada, tal como sugeria o primeiro slogan publicitário da Microsoft “Where do you want to go today?[6]” Esta euforia inicial se mostrou, com o passar do tempo, apenas uma ilusão. A promessa de liberdade e de comunicação ilimitada se transformou, na verdade, em um controle e em uma vigilância total, embora, muitas vezes, ainda despercebida por um grande número de indivíduos. (HAN, 2014).

Enquanto no panóptico de Bentham os sujeitos tinham consciência de sua vigilância, no panóptico digital os indivíduos não se sentem vigiados ou ameaçados, ao contrário, se sentem livres, e é justamente aí que reside o problema, pois ao experimentarem o falso sentimento de liberdade se dão a revelar por completo, entregando para as grandes empresas de softwares todas as suas informações pessoais. É então que nasce uma nova forma de economia: a chamada economia orientada à dados.

3. O DIREITO À PROTEÇÃO DE DADOS COMO UM DIREITO HUMANO FUNDAMENTAL

A transformação dos dados pessoais em commodities, considerando a sua capacidade manipulatória e preditiva, têm gerado grande preocupação nos Estados soberanos, que passam

[6] Trad.“Onde você que ir hoje?”.

a legislar normas destinadas à tutela e salvaguarda destes dados na sociedade digital. À medida que a internet evoluiu, também evoluiu o debate sobre direitos e deveres cibernéticos dentro desse novo mundo ainda não muito conhecido e viu-se a necessidade de elaborar normas destinadas a regulamentar essas novas formas de interação entre usuários e provedores de softwares na tentativa de coibir abusos e deixar a relação mais simétrica.

O debate sobre a proteção de dados vislumbra um maior controle por parte dos indivíduos sobre as suas informações pessoais, bem como, a compreensão do perigo que representam quando reveladas acriticamente e utilizadas sem o seu consentimento.

As primeiras discussões sobre a privacidade no mundo virtual já se faziam presentes no meio jurídico da União Europeia (UE) desde o século passado, quando, em 1995, foi aprovada a Diretiva 95/46 CE que unificou as normas de proteção de dados entre todos os países da União. No entanto, como a internet continuou a evoluir exponencialmente, as normas redigidas no final do século XX e início do século XXI, quando seu uso ainda era tímido e limitado, já não se mostravam mais suficientes para cuidar dos novos desafios da era pós-moderna.

Assim, para que houvesse uma legislação que melhor se adequasse a realidade da democratização das redes, em 2012, foi proposta na União Europeia a Regulamentação Geral de Proteção de Dados (GDPR – General Data Protection Regulation, em inglês) e aprovada em 2016, após quatros anos de discussão, entrando em vigor em maio de 2018.

No Brasil, os debates sobre a regulamentação envolvendo questões no mundo online começaram em 2009 e resultaram na Lei nº 12.965 de 2014, também conhecida como Lei do Marco Civil da Internet, mas esta lei ainda não dispunha sobre a proteção de dados pessoais, até que em 2018 foi apresentado o Projeto de Lei da Câmara nº 53/2018, que foi aprovado e sancionado como a Lei nº 13.709 de 2018, esta sim, destinada propriamente a proteção de dados.

No entanto, as questões relativas à proteção de dados pessoais não podem se restringir à simples análise e discussão por parte de legislações infraconstitucionais ou, mesmo, constitucionais, pois transcendem esse nível e alcançam a condição de direito humano fundamental, logo, devem ser observadas e protegidas também em âmbito internacional, principalmente considerando que esses dados podem ser tratados e utilizados em qualquer lugar do globo.

Afinal, o que são esses dados pessoais? A Lei Geral de Proteção de Dados brasileira (Lei nº 13.709/18) define como dados pessoais, em seu art. 5º, “toda e qualquer informação relacionada a uma pessoa identificada ou identificável”, agregando-se na tipologia de dado

pessoal sensível a informação específica a respeito da origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (Art. 5º, inciso II).

Esses dados são considerados como informações protegíveis pelos Direitos Humanos, haja vista que estão diretamente atreladas à construção da identidade, da autonomia e da personalidade da pessoa, razão pela qual sua privacidade deve ser respeitada sob pena de violação da dignidade da pessoa humana.

Se considerarmos a mais importante formulação acerca da dignidade da pessoa humana, qual seja, a formulada por Immanuel Kant, filósofo alemão e principal teórico sobre o assunto, perceber-se-á que a dignidade da pessoa humana consiste em tratar o ser humano como um fim em si mesmo, isto é, como um valor intocável e absoluto dada a sua capacidade racional e de autodeterminação, o que o distingue de todo e qualquer outro ser vivente. Sendo assim, em outras palavras, ao ser humano, incluindo as suas informações pessoais, não se pode de modo algum ser atribuível um preço, pois seu valor vai muito além disso. Não pode, portanto, o ser humano ser mercadorizado ou instrumentalizado, reduzido a condição de um simples meio destinado a satisfação de interesses egoísticos quando considerada a condição "sacral" da sua racionalidade. Logo, é vedada qualquer tendência destinada à objetificação do ser humano ou de seus dados.

Nas palavras de Kant (2007, p. 68):

> O homem, é, duma maneira geral, todo o ser racional, existe como fim em si mesmo, não só como um meio para o uso arbitrário desta ou daquela vontade. Pelo contrário, em todas as suas ações, tanto nas que se dirigem a ele mesmo como nas que se dirigem a outros seres racionais, ele tem sempre de ser considerado simultaneamente como um fim. [...] Portanto, o valor de todos os objetos que possamos adquirir pelas nossas ações é sempre condicional. Os seres cuja existência depende, não em verdade da nossa vontade, mas da natureza, têm, contudo, se são seres irracionais, apenas um valor relativo como meios e por isso se chamam coisas, ao passo que os seres racionais se chamam pessoas, porque a sua natureza os distingue já como fins em si mesmos, quer dizer, como algo que não pode ser empregado como simples meio e que, por conseguinte, limita nessa medida todo o arbítrio. (KANT, 2007, p. 68).

A mercadorização de dados orientada pela economia do "Big Data" reduz a pessoa humana à condição de objeto, à medida em que atribui às suas informações pessoais um preço e as vende a terceiros interessados em manipular os sujeitos.

Ao agir desta forma, as empresas de softwares, incluindo as redes sociais, acabam por violar a dignidade humana de seus usuários e, juntamente com ela, uma série de direitos

humanos fundamentais destinados à sua realização, entre eles, o direito à privacidade, à vida privada, à liberdade e ao livre desenvolvimento da personalidade.

Com efeito, a Declaração Universal dos Direitos Humanos de 1948 já assegurava a tutela à vida privada como expressão e manifestação de um direito humano, ao estabelecer, em seu artigo 12, que "ninguém sofrerá intervenções arbitrárias na sua vida privada [...] contra tais intromissões ou ataques, toda pessoa tem direito à proteção da lei". Ademais, dispunha também, em seu artigo 28, sobre a importância da proteção ao pleno desenvolvimento da personalidade.

Ao capturar, tratar e comercializar dados pessoais dos indivíduos sem a sua devida ciência e consentimento, as empresas do "Data Driven" violam esse direito humano elementar de privacidade, assim como o direito à liberdade, pois não são os indivíduos verdadeiramente livres nas redes, mas sim, escravos da vigilância total.

O direito ao pleno desenvolvimento da personalidade também é violado, pois esta pressupõe autonomia e racionalidade de pensamento, coisas que são destituídas dos sujeitos na era das redes.

Ora, o caráter geral de curto prazo e celeridade da sociedade da informação impede a formação de pensamentos racionais já que a racionalidade exige tempo. Com isso, os sujeitos ficam presos aos imediatismos oferecidos pelos sistemas de "cliques" e a inteligência artificial, que encaminha respostas prontas aos sujeitos sem que precisem, sequer, "pensar".

A este respeito, Jean Baudrillard (1995) ensina, que na era do computador e do celular não há aprendizagem. Segundo ele, para cada pergunta o computador faz um quadro de cinco respostas inibindo o tempo de reflexão e induzindo a reação perante estímulos. Em suas palavras, "o aparelho não ativa processos intelectuais, mas os mecanismos reacionais imediatos" (BAUDRILLARD, 1995, p. 107). Assim, os sujeitos se mostram incapazes de desenvolver raciocínios críticos e formular verdadeiras perguntas, pois, interrogar, explorar e analisar incomoda-os perante a facilidade da internet.

Ademais, a racionalidade é também ameaçada pela comunicação afetiva na era das redes. Conforme ensina Byung-Chul Han (2022), as pessoas se deixam afetar demais por informações que se seguem apressadas umas às outras. Afetos, são mais rápidos que a racionalidade. Em uma comunicação afetiva não prevalecem os melhores argumentos, mas sim, as informações com maior potencial de estimular e gerar gatilhos emocionais.

Desse modo, assiste razão a Byung-Chul Han (2022, p. 37), quando dispõe que "[...] fake news, notícias falsas, geram mais atenção do que fatos. Um único tuíte que contenha fake

news ou fragmentos de informação descontextualizados é possivelmente mais efetivo do que um argumento fundamentado".

A partir destas artimanhas, o Big Data consegue, portanto, atuar na esfera do inconsciente, despojando os indivíduos de sua armadura natural que é a racionalidade e direcionando-os a um comportamento previamente traçado e desejado pelas empresas compradoras de dados. As decisões tomadas pelos sujeitos a partir de então, não são verdadeiramente suas, fruto da autonomia de cada um, mas produto do inconsciente-pulsional estimulado pelos detentores de poder, o que fere, logicamente, o seu direito humano fundamental à autodeterminação e ao livre desenvolvimento da personalidade.

Nesse sentido, a proteção de dados pessoais deve ser considerada um direito humano fundamental, que urge ser garantido e tutelado não só em esfera nacional, mas também, internacional. Seguindo este espectro e considerando a relevância global do tema, os próximos tópicos objetivam perfazer uma análise comparada entre as legislações de proteção de dados brasileira e europeia na tentativa de encontrar soluções e possibilidades que vislumbrem uma maior efetividade desse direito em detrimento da manipulação e vigilância generalizada em todas as esferas do globo.

4. REGULAMENTO GERAL SOBRE A PROTEÇÃO DE DADOS DO PARLAMENTO EUROPEU – CENÁRIO LEGAL

Como visto, o direito à proteção de dados pessoais decorre do direito à intimidade e privacidade, assegurado na Declaração Universal de Direitos Humanos de 1948 como um direito humano. Assim também o considera o RGPD ao determinar que "a proteção das pessoas singulares relativamente ao tratamento de dados pessoais é um direito fundamental." (EU, 2016) Além disso, é imprescindível mencionar a aplicabilidade extraterritorial das diretrizes da norma, que dispõe que a proteção das pessoas singulares quanto ao tratamento dos seus dados pessoais ocorrerá independentemente da nacionalidade ou do local de residência dessas pessoas. As diretrizes da lei abrangem, portanto, o tratamento de dados de indivíduos pertencentes à UE ou dados localizados na UE. Deste modo, não importa a origem do controlador ou processador, caso esteja analisando dados de indivíduos pertencentes à UE ou dados localizados na UE deverá se submeter às disposições do regulamento.

Quanto ao consentimento do titular dos dados, este "deverá ser dado mediante um ato positivo claro que indique uma manifestação de vontade livre, específica, informada e inequívoca de que o titular de dados consente no tratamento dos dados que lhe digam respeito (...)". (RGPD,2016) Como exemplo desses atos positivos temos uma declaração escrita,

podendo também ser em formato eletrônico, ou uma declaração oral. Ressalta-se que o silêncio e a omissão não constituem consentimentos.

No que concerne à forma de tratamento de dados pessoais, este deverá ser efetuado de forma lícita, equitativa e transparente para aqueles cujos dados pessoais recolhidos, utilizados, consultados ou sujeitos a qualquer outro tipo de tratamento lhe dizem respeito. Deverão essas informações serem de fácil acesso e compreensão, compreendendo informações sobre a identidade do responsável pelo tratamento dos dados e os fins a que esse tratamento se destina. Ressalta-se que "os dados pessoais apenas deverão ser tratados se a finalidade do tratamento não puder ser atingida de forma razoável por outros meios." Além disso, os dados deverão ser conservados apenas durante o período considerado necessário, o responsável pelo tratamento deverá fixar os prazos para o apagamento ou a revisão periódica. Lembrando que, os dados pessoais deverão ser tratados de modo a garantir "a devida segurança e confidencialidade, incluindo para evitar o acesso a dados pessoais e equipamento utilizado para o seu tratamento, ou a utilização dos mesmos, por pessoas não autorizadas."

Por fim, determina o Regulamento:

> Para que o tratamento seja lícito, os dados pessoais deverão ser tratados com base no consentimento do titular dos dados em causa ou noutro fundamento legítimo, previsto por lei, quer no presente regulamento quer noutro 4.5.2016 PT Jornal Oficial da União Europeia L 119/7 ato de direito da União ou de um Estado-Membro referido no presente regulamento, incluindo a necessidade de serem cumpridas as obrigações legais a que o responsável pelo tratamento se encontre sujeito ou a necessidade de serem executados contratos em que o titular dos dados seja parte ou a fim de serem efetuadas as diligências pré-contratuais que o titular dos dados solicitar. (RGPD, 2016).

A fim de garantir a aplicação da RGPD em toda a União Europeia foi criado o European Data Protection Board (Conselho Europeu para a Proteção de Dados), cuja principal função é emitir diretrizes sobre a interpretação dos conceitos centrais do RGPD, garantindo a aplicação uniforme das regras na UE para evitar que o mesmo caso possa ser tratado diferentemente em várias jurisdições. A possibilidade de o titular do direito violado apresentar uma reclamação junto à uma autoridade supervisora garante também a participação pública no combate contra processamento de dados indevidos. Salienta-se ainda que o RGPD determina que os países que desejam manter relações comerciais com a UE possuam uma regulamentação eficiente sobre a proteção de dados, além de uma autoridade reguladora que garanta a eficácia dessa norma.

5. ANÁLISE DA LEI GERAL DE PROTEÇÃO DE DADOS BRASILEIRA – LEI Nº 13.709 DE 2018

Expressivamente inspirada no RGPD, é possível perceber que as duas normas possuem conceitos e diretrizes similares, sendo que a LGPD se apresenta como um regulamento geral para proteção de dados pessoais, "independentemente destes passarem por fluxos da Internet ou não. Assim, quaisquer estabelecimentos que coletem dados pessoais — como farmácias, locadoras de carro, postos de gasolina — estão submetidos às disposições legais." (CAVALCANTE, 2018) Inclusive, em seu artigo 1º, ao tratar dos destinatários da norma, determina que esta é aplicável às pessoas naturais e pessoas jurídicas de direito público ou privado, tendo como objetivo proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. Dispõe ainda que as normas gerais contidas na Lei são de interesse nacional e devem ser observadas pela União, Estados, Distrito Federal e Municípios. (BRASIL, 2018)

Quanto à aplicabilidade da norma, esta aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que a operação de tratamento seja realizada no território nacional, a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional ou dados pessoais coletados no Brasil. (BRASIL, 2018).

Ressalta-se que a LGPD não se aplica ao tratamento de dados pessoais realizado por pessoa natural para fins exclusivamente particulares e não econômicos ou realizado para fins exclusivamente jornalísticos, artísticos e acadêmicos, ou de segurança pública, defesa nacional, segurança do Estado ou atividades de investigação e repressão de infrações penais. Também não se aplica a LGPD à dados provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei. (BRASIL, 2018).

A norma ainda traz em seu bojo, especificamente no art.5º, conceitos relevantes ao tratamento e proteção de dados, conceituando dado pessoal, dado pessoal sensível, banco de dados, dado anonimizado, titular, controlador, operador, entre outros. (BRASIL, 2018). Necessária atenção especial para o primeiro inciso do artigo que diz que dado pessoal é "informação relacionada a pessoa natural identificada ou identificável". (BRASIL, 2018).

Quanto aos direitos dos usuários, demonstra Laila Neves Lorenzon (2021):

> Sobre os dados, a lei assegura aos usuários alguns direitos primordiais como: solicitar exclusão permanente de seus dados, a garantia de que eles serão coletados para um fim específico e saber quais dados as empresas detêm sobre eles. No que concerne sua abrangência, a lei brasileira se aplica para o tratamento de dados feito por empresas ou instituições situadas em território brasileiro e/ou quaisquer dados referentes a cidadãos brasileiros, desse modo, empresas estrangeiras que realizam o tratamento de dados de brasileiros também devem se adequar à Lei. (LORENZON, 2021)

Assim como o RGPD, a LGPD também parte do pressuposto que a privacidade dos dados está relacionada ao consentimento do seu detentor, devendo este sempre ser requisitado pelos responsáveis pelo tratamento de dados de forma expressa e clara, de modo que o detentor tenha ciência do modo, uso e destino de suas informações nos serviços. As empresas que tratam dados pessoais também deverão ser transparentes quanto ao uso dos dados, garantindo a segurança no armazenamento e tratamentos destes.

Como instrumento de aplicação da LGPD tem-se como principal instrumento a instituição da ANPD, Agência Reguladora de Proteção de Dados, que atuará como autoridade fiscalizadora do cumprimento da lei e aplicação de sanções. A norma também impõe multas e outras formas de penalidades para aqueles que não observem a legislação, tais como advertência, publicização da infração, bloqueio e eliminação dos dados pessoais.

5. CONCLUSÃO

Vivemos atualmente a era da informação. Com a democratização do acesso à internet e às redes, as formas de relações sociais e de trabalho mudaram e, com isso, o capital precisou mudar também as suas formas de controle e vigilância para manter a sua elevada lucratividade e garantir a continuidade de seu poder. Para tanto, aquele antigo modelo de vigilância fundado no panóptico de Bentham que consistia em um confinamento circular com uma torre de vigilância no centro, amplamente aplicável em fábricas, escolas, presídios e hospitais, por estar restrito ao controle do corpo, precisava ser substituído por um novo tipo de panóptico que fosse mais além, capaz de adentrar na própria mente dos sujeitos: o chamado panóptico digital ou pós-moderno.

O panóptico digital opera com a captura, tratamento e comercialização de dados que os indivíduos ingênuos e acriticamente, sob um falso aparato de liberdade inserem nas redes todos os dias, em especial, nas redes sociais. A partir de um fortíssimo incentivo à comunicação e à praticidade, as pessoas postam o tempo todo o que estão fazendo, o que

estão comendo, para onde irão viajar, o que estão comprando ou deixaram de comprar, suas convicções religiosas e políticas, informações sobre seu trabalho, sua família, etc. Isso, aliado à ideia de inteligência artificial e de casa inteligente, possibilita às empresas do "data driven" um mapeamento integral das pessoas.

Esses dados não evaporam simplesmente dentro dos sistemas de softwares das empresas fornecedoras, ao contrário, são utilizados para a produção de um perfil de personalidade – o profiling psicométrico – para cada usuário. O profiling psicométrico torna possível prever e estimular o comportamento de uma pessoa melhor do que um familiar um ou amigo próximo poderia. Com uma quantidade suficiente de dados, é possível até mesmo gerar informações mais precisas do que uma pessoa conhece sobre ela mesma.

Esses dados são comercializados a empresas que tenham o interesse de, através de anúncios cada vez mais precisos, despertar os maiores gatilhos impulsivos e emocionais dos sujeitos para interferir e modificar as suas decisões e comportamentos que vão desde a esfera do consumo até a deliberação política.

Esse tipo de prática é extremamente nociva e viola o direito humano fundamental à privacidade e ao livre desenvolvimento da personalidade da pessoa natural, além de ferir a própria dignidade da pessoa humana, que passa a ser considerada um objeto de mercadorização. Por esta razão, a proteção de dados pessoais se mostra elementar e deve ser considerada como um direito humano fundamental.

Nesse cenário, o Estado não pode se destituir da sua função reguladora de comportamentos, deixando os cidadãos relegados à própria sorte diante da revolução digital. Não por outra razão, foram redigidos, na União Europeia e no Brasil, o Regulamento Geral sobre a Proteção de Dados – RGPD – e a Lei Geral de Proteção de Dados – LGPD – respectivamente, o que, desde logo, considera-se medidas de caráter e impacto extremamente positivos.

O RGPD foi o pioneiro na regulamentação sobre o uso de dados pessoais por qualquer empresa ou instituição, exigindo atitudes mais responsáveis e seguras dos processadores de dados e disponibilizando aos usuários diversos direitos relacionados à privacidade digital. Atualmente, já é efetivo em todo o território da União Europeia e enseja punição caso não observado. Apresenta-se como um modelo de referência mundial no tratamento da privacidade digital.

Já no Brasil, a Lei Geral de Proteção de Dados – Lei nº 13.709/2018 – tem como objetivo proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

É importante que se compreenda que a apreciação comparativa destes dois sistemas legais: Regulamento Geral sobre a Proteção de Dados do Parlamento Europeu (EU) 2016/679 de 2016 e da Lei Geral de Proteção de Dados Brasileira promulgada em 2018, deve levar em consideração âmbitos de compreensão sistêmica que perpassam pelas diferenças semânticas, culturais, epistemológicas e, até mesmo, estruturais, que, em um primeiro momento estabelecem um profundo vale na linguagem das propostas legislativas.

Nesse sentido, há que se levar em consideração que o Direito Comunitário Europeu é desenvolvido em uma construção de países com características muito peculiares, histórias completamente distintas, línguas incomuns, entre tantos outros pontos cuja objetividade do presente trabalho não nos permitiu aqui abordar. Já no que diz respeito ao Brasil, o mesmo aprimoramento legiferante perpassa uma construção que a despeito de legítima não se mostra, a princípio, tão abrangente e com tantas oportunidades fiscalizatórias.

O que visivelmente se denota entre ambas as legislações é a preocupação com a proteção do ser humano, pessoa natural que, muitas vezes, inconscientemente, tem sido manipulada pelo capital na era das redes ou do chamado capitalismo cognitivo (de dados).

Apesar de a Declaração Universal dos Direitos Humanos de 1948 e outros tratados internacionais reconhecerem o direito à privacidade, à autodeterminação e ao livre desenvolvimento da personalidade como direitos humanos fundamentais, não estabelecem normas punitivas para a sua violação, o que dificulta a proteção desses direitos na prática.

O Regulamento Geral sobre a Proteção de Dados do Parlamento Europeu e a Lei Geral de Proteção de Dados brasileira vêm, justamente, para trazer a exequibilidade efetiva desses direitos que, outrora, estavam restritos no campo do “ideal”, implementando uma série de sanções para aqueles que violem o direito fundamental à proteção de dados e adentrem na esfera subjetiva das pessoas sem a devida autorização.

Certamente, para a plena realização do direito à proteção de dados ainda há um longo caminho a se percorrer, pois, lamentavelmente, muitas empresas ainda operam de forma abusiva e irregular na sombra das redes, no entanto, O RGPD e a LGPD constituem um gigantesco avanço em direção a um futuro menos abusivo e melhor.

REFERÊNCIAS

BAUDRILLARD, Jean. A sociedade de consumo. Lisboa: Edições 70, 1995.

BENTHAM, Jeremy. **O panóptico.** Organização de Tomaz Tadeu. Trad. Guacira Lopes Louro, M. D. Magno, Tomaz Tadeu. 2.ed. Belo Horizonte: Autêntica, 2008.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. **Diário Oficial da União,** Brasília, 24 abr. 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 30 jun. 2023.

BRASIL. Lei n° 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). **Diário Oficial da União,** Brasília, 15 ago. 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 30 de junho 2023

CAVALCANTE, Pedro Peres. **Privacidade e proteção de dados pessoais**: Uma análise comparativa dos quadros regulatórios brasileiro e europeu. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Pernambuco — UFPE- Recife, 2018, p. 36.19 Artigo 5°, inciso I, do Decreto n° 13.709, 14 de agosto de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato20152018/2018/Lei/L13709compilado.htm. Acesso em: 29 de junho de 2023.

DIGITAL 2023 april global statshot report. [S.1.]: **DATAREPORTAL.** 2023. Disponível em: https://datareportal.com/reports/digital-2023-april-global-statshot. Acesso em: 29 jun. 2023.

FOUCALT, Michel. **Vigiar e punir:** nascimento da prisão. Trad. Raquel Ramalhete. 40. ed. Petrópolis: Vozes, 2012.

HAN, Byung – Chul Han. **Psicopolítica:** Neoliberalismo y nuevas técnicas de poder. Barcelona: Pensamiento Herder, 2014.

HAN, Byung – Chul. **Infocracia:** digitalização e a crise da democracia. Trad. Gabriel S. Philipson. Rio de Janeiro: Vozes, 2022.

KANT, Immanuel. **Fundamentação da metafísica dos costumes.** Trad. Paulo Quintela. Lisboa: Edições 70, 2007.

LORENZON, Laila Neves. **Análise comparada entre regulamentações de dados pessoais no Brasil e na União Europeia** (Lgpd E Gdpr) e seus respectivos instrumentos de enforcement. Disponível em Revista do Centro de Excelência Jean Monnet da FGV Direito Rio, 1 [recurso eletrônico]- Rio de Janeiro: FGV Direito Rio, 2021.1 recurso online (210 p.):

ORSINI, Adriana Goulart de Sena. Jurimetria e predição: notas sobre o uso dos algoritmos e o Poder Judiciário. In: CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da. **Futuro do trabalho:** os efeitos da revolução digital na sociedade. Brasília: ESMPU, 2020.

TEODORO, Maria Cecília Máximo; ANDRADE, Karin Bhering. O panóptico pós-moderno no trabalho. In: CARELLI, Rodrigo de Lacerda; CAVALCANTI, Tiago Muniz; FONSECA, Vanessa Patriota da. **Futuro do Trabalho:** os efeitos da revolução digital na sociedade. Brasília: ESMPU, 2020.

UNIÃO EUROPEIA. **Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016**, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados. Jornal Oficial da União Europeia, Bruxelas, v. 59, n. 79, p. 1-88, 4 maio 2016. Disponível em: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN. Acesso em: 30 de junho 2023.