O ENQUADRAMENTO NACIONAL E A CULTURA DIGITAL EM RELAÇÃO A PROTEÇÃO DE DADOS PESSOAIS

THE NATIONAL FRAMEWORK AND DIGITAL CULTURE IN RELATION TO PERSONAL DATA PROTECTION

Artigo recebido em 03/05/2022
Artigo aceito em 20/05/2022
Artigo publicado em 28/01/2023

Lucas Corrêa dos Santos
Graduando em Direito– Universidade Tiradentes – UNIT. Orcid: https://orcid.org/0001-6922-051X.
E-mail: lucascorrea.jud@gmail.com.

Patrícia Verônica Nunes Carvalho Sobral de Souza
Pós-Doutora em Direito pela Mediterranea International Centre for Human Rights Research dell Università Mediterranea di Reggio Calabria (Itália). Pós-Doutora em Direito e Doutora em Direito Público pela Universidade Federal da Bahia-UFBA. Doutora em Educação e Mestra em Direito Público pela Universidade Federal de Sergipe - UFS. Instituição de origem: PPGD da Universidade Tiradentes – UNIT. Orcid: https://orcid.org/0000-0002-3725-6339. E-mail: patncss@gmail.com.

RESUMO: Observando as constantes mudanças tecnológicas no atual cenário digital, surgiram novos riscos à privacidade do cidadão, e analisando essa problemática, o presente estudo buscou fomentar o debate sobre a proteção de dados pessoais, além de elencar a necessidade de aplicação de medidas urgentes de conformidade. O método utilizado foi a pesquisa bibliográfica, a fim de promover uma abordagem qualitativa e exploratória, baseado no atual do cenário de tratamento de dados em âmbito nacional. Como resultado, notou-se que grande parte da população pode até saber que possui o direito à privacidade, mas não sabem como se proteger no meio digital. Isso se deve muito ao ambiente de insegurança e fragilidade presente no Brasil ao que diz respeito à garantia e aplicabilidade das normas de proteção de dados, mesmo com a proeminente possibilidade de aplicação das sanções já existentes. O que leva a conclusão de que o Brasil pouco avançou em relação aos demais países comprometidos com a aplicação da proteção de dados na prática. A grande massa das empresas nacionais não tem como prioridades ou sequer sabem sobre a proteção dos dados pessoais. Dado este que expõe a falta de consciência no meio social em relação aos seus dados pessoais, uma vez que, se todos entendessem o valor das informações no modelo de mercado atual, mais criteriosa e comprometida com o cumprimento da segurança seria a sociedade em geral, promovendo a garantia da ordem e o desenvolvimento econômico com maior eficiência.

PALAVRAS-CHAVE: Autodeterminação informativa, Cultura Digital, Privacidade, Proteção de dados.

ABSTRACT: Observing the constant technological changes in the current digital scenario, new risks to the privacy of the citizen have emerged, and observing this issue, this study seeks to foster the debate on the protection of personal data, in addition to listing the need to apply urgent compliance measures. The method used was a bibliographic research, in order to promote a qualitative and exploratory approach, based on the current scenario of data processing in Brazil. As a result, it was noted that there is an environment of insecurity and very great fragility in Brazil, not related to the guarantee and applicability of data protection rules, even with a prominent possibility of application of sanctions existing for 2 months. Which leads to the conclusion that Brazil has made little progress in relation to other countries committed to applying data protection in practice. The vast mass of national companies do not prioritize or even know about the protection of personal data. Given that this exposes the lack of awareness in the social environment in relation to your personal data, since, if everyone understood the value of information in the current market model, society in general would be more discerning and committed to compliance with security, promoting the guarantee of order and economic development with greater co-efficiency.

KEYWORDS: Privacy, Data Protection, Digital Culture, Information Self-Determination.

1 INTRODUÇÃO

Da mesma forma que a Revolução industrial mudou o cenário econômico mundial em 1760, o capitalismo moderno aprimora-se com a evolução exponencial das novas tecnologias, desenvolvendo um ambiente fértil para a inovação e ideias *disruptivas*[1]. Uma era de inovações constantes fez com que a tecnologia se tornasse um vetor condicionante do modelo de sociedade moderno, que, no seu sentido econômico, é indissolúvel do processamento de dados.

[1] Disrupção é um termo criado por Clayton Christensen, professor de Harvard, e autor do livro *O Dilema da Inovação*, que o conceitua como uma inovação de ruptura que transforma um produto que historicamente era tão caro e complexo que só uma pequena parte da população podia ter e usar, em algo que é tão acessível e simples que uma parcela bem maior da população agora pode ter e usar. (CHRISTENSEN, 2012, p. 17)

O coração do mundo contemporâneo e de economia globalizada pulsa através do capitalismo de vigilância e bombeia o que hoje é chamado de mercantilização dos dados. Dados pessoais se tornaram a nova moeda de troca entre organizações e titulares, gerando uma quantidade imensurável de dados trafegados. Mas é no processo de tratamento dessas informações que se produz o conteúdo de extremo valor para as empresas, motivo que gerou o compromisso de salvaguardar as informações pessoais.

Visando obstar os riscos que podem surgir desse novo cenário de tratamento de dados, surgiu a ânsia por firmar um compromisso entre as organizações e titulares, permitindo a garantia de proteção aos direitos humanos fundamentais, previstos na Declaração Universal Dos Direito Humanos (DUDH) de 1948. A partir daí buscou-se gerar um dispositivo legal que estabelecesse parâmetros de segurança e confiança para todo o caminho traçado pelos dados pessoais, desde a coleta, tratamento, compartilhamento, descarte, entre outras práticas que envolvam os dados pessoais, garantido transparência e privacidade aos indivíduos titulares. Seguindo essa trilha, a União Europeia desenvolveu o General Data Protection Regulation (Regulamento Geral de Proteção de Dados - GDPR), um conjunto de normas que regula a proteção de dados em toda a União Europeia e seu espaço econômico. O dispositivo serviu de espelho para diversas legislações no mundo, inclusive no Brasil para elaboração da tão discutida Lei nº 13.709/2018 ou Lei Geral De Proteção de Dados (LGPD).

Nesta medida, o presente trabalho possui o escopo de fomentar a discussão sobre a importância da cultura digital no atual cenário de constantes evoluções tecnológicas, observando o panorama nacional de enquadramento das organizações em relação as normas regulamentares de proteção de dados. Busca ainda, questionar se o cidadão comum possui consciência da necessidade de proteger seus dados e da importância da autodeterminação informativa. Além de elucidar se a aplicação de medidas urgentes de conformidade por parte das empresas ao exemplo do *compliance*[2], a cultura do *Privacy By Desing*[3] e *Privacy By Default* [4], entre outros métodos e ferramentas, contribuiriam com a formação de uma

[2] De acordo com o entendimento do Conselho Administrativo de Defesa Econômica (Cade), "compliance *é um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios ou colaboradores*". (CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA, 2021)

[3] Significa que todas as etapas do processo de desenvolvimento de um produto ou serviço de uma empresa devem ter a privacidade em primeiro lugar, criado pela Dra. Ann Cavoukian, diretora executiva do Instituto de Privacidade e Big Data da Universidade de Ryerson em Ontário, no Canadá. (DANTAS, 2019)

[4] Significa que um produto ou serviço, ao ser lançado no mercado, deve vir com as configurações de privacidade no modo mais restrito possível por padrão, e o usuário deve liberar acesso à coleta de mais informações caso julgue necessário, como entende a Dra. Ann Cavoukian. (DANTAS, 2019)

consciência social a respeito da proteção de dados pessoais e seus impactos diretos na vida de cada cidadão.

O método de pesquisa utilizado foi a pesquisa bibliográfica, a fim de promover uma abordagem qualitativa e exploratória, baseado no atual do cenário de tratamento de dados em âmbito nacional.

O Presente trabalho foi norteado pelos seguintes questionamentos: Os titulares de dados possuem real consciência da vulnerabilidade e das consequências a que estão expostos ao trafegarem no ambiente digital com suas informações? Como após a vigência completa da LGPD o cenário de proteção de dados brasileiro poderá promover uma estrutura protetiva e conscientizadora?

Como resultado, nota-se que mesmo em absoluta vigência da LGPD, um marco legal em relação a proteção de dados e a garantia de direitos fundamentais no Brasil, ainda há um ambiente de insegurança e fragilidade muito grande no que diz respeito à garantia e aplicabilidade das normas de proteção de dados, mesmo com a existência do órgão fiscalizador (ANPD) e a proeminente possibilidade de aplicação das sanções, atrapalhando o avanço social a respeito da autodeterminação informativa.

O que leva à conclusão de que o Brasil pouco avançou em relação aos demais países comprometidos com a aplicação da proteção de dados na prática. A grande massa das empresas nacionais não tem como prioridades ou sequer sabem sobre a proteção dos dados pessoais. Dado que expõe a falta de consciência no meio social em relação aos dados pessoais, visto que, se todos entendessem o valor das informações no modelo de mercado atual, mais criteriosa e comprometida com o cumprimento da segurança seria a sociedade em geral, promovendo a garantia da ordem e o desenvolvimento econômico com maior eficiência.

2 ASPECTOS INTRODUTÓRIOS DA LEI GERAL DE PROTEÇÃO DE DADOS - LGPD

A economia atual é orientada pela utilização de dados pessoais. Cada dia novas tecnologias disruptivas nascem e reformulam a ideia do que antes era impossível. Neste cenário, em meio a uma sociedade mais conectada, surgiu a necessidade de possuir um regulamento especializado, que buscasse coordenar, estabelecer regras e impor limites ao cruzamento de informações e o seu tratamento descontrolado.

Em 1948 a Declaração Universal Dos Direitos Humanos (DUDH), em seu art. 12º já ensejava a proteção da lei e garantia de direitos, como a proteção à vida privada, à família, ao domicilio ou sua correspondência e até mesmo a ataques à usa honra e reputação. Sua importância para a garantia da proteção dos dados pessoais atualmente é inestimável, pois foi o dispositivo matriz para a inspiração dos demais em todo o mundo.

Passados 4 anos, surgiu a Declaração Europeia de Direitos Humanos (DEDH), com o propósito de proteger os direitos humanos, mas em especial a vida privada, familiar, domicilio e correspondência em toda a União Europeia. Em 1973 e 1974 o conselho da Europa lançou as Resolução 22 e 29, respectivamente, que tratavam da proteção das personalidades de pessoas físicas perante bancos eletrônicos de dados nos setores Privados e Públicos, respectivamente. Em 1981 o Conselho da Europa propôs a convenção nº 108, com a ideia ensejar a proteção dos indivíduos referente ao processamento automático de dados pessoais. Foi o primeiro instrumento a tratar a temática com força legal e vinculante. Em 1995 a comissão Europeia editou a DIRETIVA nº 46, que foi por mais de duas décadas o principal dispositivo sobre proteção de dados pessoais e privacidade. Porém, possuía lacunas, pois traçava um objetivo geral para os países, cabendo a eles estabelecerem uma legislação interna mais específica, a qual se mostraram conflitantes entre si, promovendo insegurança jurídica.

Depois de longo período de debates e com demasiada bagagem histórica sobre o tema, a União Europeia colocou em vigor no dia 25 de maio de 2018 a GDPR - *General Data Protection Regulation*, regulamento único do direito europeu sobre privacidade e proteção de dados pessoais, aplicável em 27 países da União Europeia e mais 3 outros (Liechtenstein, Islândia e Noruega). O dispositivo serviu de grande influência para legislações protetivas em inúmeros países, inclusive Estados Unidos e Brasil.

Apresentado ao calor externo oriundo das novas condutas internacionais de tratamento de dados, o Brasil publicou no dia 14 de agosto de 2018 a Lei 13.709/2018, ou, também chamada de LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS – LGPD, contudo, somente entrou em vigor em 18 de setembro de 2020. O referido dispositivo surgiu alterando o Marco Civil da Internet (Lei nº 12.965/2014), criando uma regulamentação que padroniza os atributos qualitativos de proteção de dados pessoais, com o objetivo de proteger os direitos fundamentais de liberdade, privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Diferente do que é compartilhado, a LGPD não foi "motivada" pela GDPR, o correto a dizer seria que ela foi "espelhada" no dispositivo Europeu. Devido à grande pressão externa, proveniente principalmente dos países do bloco europeu que possuem regras de governança

corporativa e proteção de dados pessoais a qual as empresas devem tomar bastante cuidado com suas relações internacionais em razão dos riscos de compartilhar dados do cidadão europeu em um ambiente desprotegido. A medida tornou obrigatória que países do mundo estabelecessem suas próprias normas com vistas a manterem suas relações internacionais com a União Europeia, e assim foi com o Brasil.

Nesse sentido, a

> Regulação da Internet (Lei 12.965/2014), da Proteção de Dados Pessoais (Lei 13.709/2018) e da Internet das Coisas (Plano Nacional da Internet das Coisas – Decreto 9.854/2019) são alguns dos exemplos mais atuais de novas tecnologias na esfera jurídica (SOBRAL DE SOUZA; FERRARO, p. 2).

Ocorre que, o mundo vive a "Quarta Revolução Industrial"[5] e o Brasil ainda se encontra atrasado no que diz respeito à corrida da proteção de dados. Para que seja possível avançar de forma evolutiva, é necessário investir não só em medidas protetivas, mas ensinar a usá-las, engajar a promoção da cultura digital afim de promover o conhecimento do direito aos titulares.

3 A DUALIDADE ENTRE A PRIVACIDADE E A PROTEÇÃO DE DADOS

Em 1890, Samuel D. Warren e Louis D. Brandeis, no artigo *The Right To Privacy* (1890), já debatiam a questão ao direito à privacidade, e relacionando com as problemáticas da época chegaram à conclusão que a privacidade seria "*apenas uma instância da aplicação do direito mais geral do indivíduo para ser deixado sozinho*". Na época, as questões que exigiam a proteção da privacidade eram muito diferentes das atuais, contudo, os autores apresentaram relato bastante contemporâneo, como é visto em seu artigo a nota do caso Wyatt v. Wilson, de 1820, a respeito da proteção do que seria chamado hoje de "dados sensíveis[6]" do monarca George III.

---

[5] Termo usado por Martha Gabriel em seu livro "Você, eu e os robôs: pequeno manual do mundo digital": "*Estamos vivendo a Quarta Revolução Industrial, em que o modelo de sociedade baseado em máquinas mecânicas dá lugar a um modelo baseado em máquinas computacionais, fragmentado em bits e bytes, hipertextual, complexo, não linear."* (GABRIEL, 2019, p. 20)

[6] Art. 5º, II, da Lei 13.709/2018: "*dado pessoal sensível: dado pessoal sobre 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*" (BRASIL, 2018)

> Lord Cottenham afirmou que um homem "é aquele que é exclusivamente seu" e citou com aprovação a opinião de Lord Eldon, conforme relatado em uma nota manuscrita do caso Wyatt v. Wilson, em 1820, a respeito de uma gravura de George III durante sua doença, no sentido de que "se um dos médicos do falecido rei tivesse mantido um diário do que ouviu e viu, a corte não teria, durante a vida do rei, permitido que ele o imprimisse e publicasse; (THE RIGH TO PRIVACY, 1890. p. 10)

Já no mar de inovações tecnológicas e disruptivas que se tornou o século XXI, muito se fala em privacidade e proteção de dados pessoais. Constantemente surgem novas e grandes ideias que modificam o convívio social. Nesse contexto, a privacidade, devido a sua função social e política para além da esfera privada, começa a moldar também a cidadania, afastando-se de ser simplesmente "o direito de ser deixado só" e "volta-se para a direção da ideia de uma tutela global das escolhas da vida contra qualquer forma de controle público e de estigmatização social, em um quadro caracterizado pela liberdade das escolhas existenciais e políticas." (RODOTÀ, 2008, p. 129).

Com a proteção das informações pessoais o estado resguarda e protege a privacidade do cidadão contra ingerências ou investidas injustas à sua esfera pessoal e íntima, seja por parte do próprio estado ou por terceiro particular. Surge daí uma relação simbiótica, mas que jamais se confunde. Tornando a proteção de dados pessoais em apenas um dos meios em quem se busca garantir o direito à privacidade.

No Brasil a constituição federal de 1988 estabeleceu por definitivo a inviolabilidade da intimidade e da vida privada, em seu art. 5º, X, garantindo a promoção do direito à privacidade.

> 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; (BRASIL, 1988, Art. 5º).

Em 2018, já influenciada pela enorme necessidade de proteção das informações pessoais derivadas das novas tecnologias, criou-se a Lei 13.709/2018 - Lei Geral de Proteção de Dados (LGPD). Inspirada no Regulamento Europeu, o *General Data Protection Regulation* (GRPD) de 2016. A LGPD considera a proteção de dados um direito inerente aos indivíduos e é indispensável para o desenvolvimento individual e coletivo. Busca resguardar os direitos básicos de liberdade, privacidade e personalidade presentes na Constituição.

> 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. (BRASIL, 2018, s/n).

Nesse sentido, Paulo Lôbo preleciona que:

> [...] sob a denominação, "privacidade" cabem os direitos da personalidade que resguardam de interferências externas os fatos da intimidade e da reserva da pessoa, que não devem ser levados à público" além de que "incluem-se nos direitos à privacidade os direitos à intimidade, à vida privada, ao sigilo e à imagem. (LÔBO, 2012, p. 141)

A partir das definições supracitadas sobre o que é a privacidade, assim como sua distinção da proteção de dados, vejamos a seguir a sua importância no campo das tecnológicas de informação.

Em seu livro "Você, eu e os Robôs: pequeno manual do mundo digital", Martha Gabriel (2019, p 66) torna lúcido o poder da privacidade e a necessidade de proteger o controle sobre "quem" ou "o que" você apresenta. Como se vê:

> A questão do controle da privacidade é essencial devido ao poder que outorga, não formal, mas inquestionável, a quem detém as informações do indivíduo. A preocupação é que esse poder pode ser usado de forma benéfica ou não, ética ou não, legal ou ilegal, ajudando ou prejudicando aquele indivíduo. Conhecer aquilo que motiva as pessoas a agir possibilita: a) influenciar essas pessoas - tanto para o bem (melhorar serviços, produtos, tratamento dessas pessoas) como para o mal (manipulando-as) e; b) prever ou analisar seus comportamentos. (GABRIEL, 2019, p.66)

Ana Paula Moraes Cantos de Lima, Almeida e Maroso (2020, p. 19) também elucidam a importância e o cuidado que se deve ter com relação as pegadas (*footprint*[7]), rastros (*traces*[8]) e as chamadas sombras digitais (*shadows*[9]).

> Dados que estruturados são capazes de prever comportamentos e preferências e até de manipular as pessoas, tudo com base nas pegadas digitais que os cidadãos deixam ao usar a Internet e diversos aplicativos. (LIMA; ALMEIDA; MAROSO, 2020, p. 19).

A título de exemplo, suponha-se que determinada pessoa publicou um dado em sua página pessoal em certa rede social, ao compartilhá-lo ela o torna público. No entanto, isso não significa que a informação possa ser tratada de maneira indiscriminada. A partir desse

7 Informações pessoais compartilhadas ativa ou intencionalmente na internet, como as publicações e comentários nas mídias sociais, fotos, etc. (GABRIEL, 2019, p. 76)

8 Informações pessoais compartilhadas passiva ou inconscientemente, como histórico de buscas na rede, IP, localização, configuração de browser, entre outras. (GABRIEL, 2019, p. 76)

9 Informações pessoais que são compartilhadas por terceiros, como fotos, menções, depoimentos, opiniões etc. (GABRIEL, 2019, p. 76)

exemplo se constata com clareza como ambos conceitos de privacidade e proteção de dados andam juntos, uma vez que, para que seja mantida a privacidade do titular (direito à intimidade, à vida privada, ao sigilo e à imagem) é imprescindível que sejam adotadas medidas protetivas aos dados, mesmo que públicos.

Portanto, é necessária uma mudança de cultura: o titular da informação deve ser a base para proteção da privacidade, assim como é fundamental que as organizações estabeleçam também uma cultura corporativa interna.

4 A IMPLEMENTAÇÃO DA CULTURA DIGITAL NO AMBIENTE CORPORATIVO E ORGANIZACIONAL

Com o inédito regulamento protetivo de dados pessoais brasileiro, a LGPD, as empresas que possuem tratamento de informações pessoais são obrigadas a adotar uma Política de Segurança da Informação (PSI). Um conjunto de orientações e regras que deve ser seguido, cujo o objetivo é garantir ao titular a confidencialidade, integridade, disponibilidade, autenticidade e legalidade do tratamento dos dados.

Estabelecer procedimentos para a referida finalidade não é tarefa fácil, mas para que seja concluído com sucesso todo o processo de enquadramento de uma organização é necessário que haja a conscientização e comprometimento do todos os funcionários e principalmente do dono, líder ou equivalente. Porém, além de treiná-los para agirem de forma técnica e responsável é preciso reformular a cultura interna da empresa. Ou seja, antes de mais nada é necessário naturalizar o compromisso interno com privacidade e a proteção dos dados.

A Lei Geral de Proteção de dados traçou algumas diretrizes a serem cumpridas pelas empresas, a fim de atender com o compromisso alegado, entre elas estão as boas práticas e a governança, previstas no art. 50 da referida lei.

> Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais.

> § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. (BRASIL, 2018).

Segundo Camilla Do Vale Jimene (2019):

> Ainda, podem ser igualmente considerados como boas práticas e de governança: a metodologia do *privacy by design,* os instrumentos de governança corporativa, tais como políticas internas de segurança da informação e de proteção de dados pessoais, os contratos e acordos de confidencialidade, a capacitação dos empregados, o monitoramento dos controles etc. (JIMENE, 2019, p. 394)

Adotar novas medidas dentro da empresa por vezes pode acarretar em novos custos, fugindo até mesmo do controle orçamentário, caso seja algo inesperado. Contudo, adotar esse novo modelo de cultura trará benefícios incalculáveis. Haja vista que, além de mitigar os riscos e evitar as penalidades previstas em lei, a organização atraíra uma percepção diferente de seus clientes, os quais se sentirão mais seguros e confortáveis com relação ao tratamento dos seus dados com a empresa, melhorando a sua imagem (marca) no mercado.

> Essencial ter em mente que ajustes serão inevitáveis. É preciso compreender que os pilares dessa construção passam por processos, pessoas e tecnologia. A empresa ganhará com a mudança, estará mais organizada, *compliant* com a LGPD e demais legislações que devem ser observadas no seu segmento. Limites e obrigações estarão bem definidos, pautados pela ética e pela integridade. A mudança será percebida pelos clientes, titulares dos dados pessoais e tornar-se-á um diferencial competitivo. (LIMA; ALMEIDA; MAROSO, 2020, p. 37).

Patrícia Peck Pinheiro (2018) também realça a importância da implementação dos novos requisitos postos pela LGPD, mas sobretudo a necessidade de transformação da cultura.

> Atender aos requisitos da LGPD exige adequação dos processos de governança corporativa, com implementação de um programa mais consistente de *compliance* digital, o que demanda investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de procedimentos e fluxos internos e externos de dados pessoais, com aplicação de mecanismos de controle e trilhas de auditoria e, acima de tudo, mudança de cultura. (PINHEIRO, 2018, p.33)

Todavia, necessário salientar que, quando o presente estudo se refere a mudança de cultura não se trata apenas da cultura protetiva dos dados pessoais, mas da cultura digital, ou como conceitua o grande sociólogo Pierre Levy, a “cibercultura”:

> Como uso diversas vezes os termos "ciberespaço" e "cibercultura", parece-me adequado defini-los brevemente aqui. O ciberespaço (que também

> chamarei de "rede") é o novo meio de comunicação que surge da interconexão mundial dos computadores. O termo especifica não apenas a infraestrutura material da comunicação digital, mas também o universo oceânico de informações que ela abriga, assim como os seres humanos que navegam e alimentam esse universo. Quanto ao neologismo "cibercultura", especifica aqui o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço. (LÉVY PIERRE, 1999, p.13)

Entretanto, se considerar todo o período de discussão mundial acerca do assunto, inclusive contando o tempo de promulgação da LGPD até o presente momento, é notável que o avanço do Brasil ainda é tímido em comparação aos demais países no que diz respeito ao enquadramento das organizações quanto às regras de proteção de dados. Um estudo realizado pela ICTS Protiviti (2020) com 104 empresas brasileiras, das quais 33% são de grande porte, 27,5% médias e 39,6% são micros e pequenas empresas, revela que 84% delas não estão preparadas paras as novas regras de privacidade de dados (PROTIVITI, 2020).

Pode-se dizer então, que esse dado é o reflexo da cultura digital no país. Grande parte da população ainda não conhece o valor das suas informações pessoais. Assim, as empresas continuam a tratar os dados de forma negligente e situações corriqueiras que condicionam riscos à privacidade continuam acontecendo normalmente, como por exemplo: Receber e-mail de remetente desconhecido; informar o CPF em uma farmácia para obter desconto; preencher cadastro para receber brindes ou promoções; ao entrar em site clicar em “concordo” para aceitar as políticas de privacidade e os termos de uso sem mesmo ler, etc.

5 DA AUTODETERMINAÇÃO INFORMATIVA À CONSCIENCIA DOS RISCOS

No mundo contemporâneo, onde o consumo e produção de dados em massa são primordiais na atual sociedade da informação, o indivíduo transfigura-se em um “HyperASW3

Humano”, expressão de David Lyon na introdução de Vigilância Líquida, de Zygmunt Bauman (2013). Como no diz o autor “Use um bracelete de silício com um QR como acessório da moda, e basta sussurrar “me escaneie”. Isso faz com que se abra uma página da web com seus dados de contato, links de mídia social e todo o resto. Você é um hyperlink humano.”.

> Tudo que se faz no mundo digital ou no plano real produz algum tipo de dado que pode ser convertido em informação útil. Essa utilidade, apesar de todos os benefícios, concedeu à população um "telhado de vidro". Como discorre o ilustre professor Stefano Rodotà: [...]assediados por computadores, espiados por olhos furtivos, filmados por telecâmeras invisíveis. Os cidadãos da sociedade da informação correm o risco de parecer homens de vidro: uma sociedade que a informática e a telemática estão deixando transparente. (RODOTÀ, 2008, p. 8)

O que Rodotà (2008) quis dizer com a expressão "homens de vidro" é que a privacidade do indivíduo da sociedade de informação está em risco a todo momento. O indivíduo está imerso em mundo absolutamente conectado, que experimenta o que Shoshana Zobuff (2019) apresenta como "capitalismo de vigilância", onde o capitalismo que é conhecido enxergou nos dados a oportunidade de transformar o comportamento humano em informações úteis a monetização de suas atividades. A consequência desse novo modelo é a formação da mercantilização dos dados, ou, "mercado de comportamentos futuros", cujo objetivo é prever e determinar comportamentos (ZUBOFF, 2015, p. 14-15).

Nas palavras de Ricardo Bioni, "os dados pessoais são o petróleo, insumo ou uma *commodity*, estando para a economia da informação como a destruição do meio ambiente estava para a economia industrial." (BIONI, 2019, p. 132).

Apresentado este panorama com a importância das informações do contexto atual, é preciso abordar a questão da consciência do cidadão nesse mundo. Onde com o passar dos anos e os olhares do mundo se voltando a proteção dos dados pessoais, a necessidade de fazer com o que o titular tivesse o absoluto controle das suas informações foi aprimorando-se. Resultando, então, na necessidade da autodeterminação informativa, um dos fundamentos presentes na Lei Geral de Proteção de Dados (ar.2º, II).

Para Rony Vainzof (2019, p. 27) a autodeterminação informativa é:

> [...] o controle pessoal sobre o trânsito de dados relativo ao próprio titular – e, portanto, uma extensão de liberdades do indivíduo – conjuga as duas já mencionadas concepções de privacidade de dados: a primeira de caráter negativo e estático; e a moderna, em que a intervenção (proteção) é dinâmica, durante todo o ciclo de vida dos dados nos mais variados meios em que possa circular. (VAINZOF, 2019, p. 27)

Segundo Bruno Ricardo Bioni:

> O principal vetor para alcançar tal objetivo é franquear ao cidadão *controle* sobre seus dados pessoais. Essa estratégia vai além do consentimento do titular dos dados, pelo qual ele autorizaria o seu uso. Tão importante quanto esse elemento volitivo é assegurar que o fluxo informacional atenda às suas

> legítimas expectativas e, sobretudo, não seja corrosivo ao livre desenvolvimento da sua personalidade. (BIONI, 2019, p. 134)

Como bem aponta Bioni (2019), para alcançar autodeterminação informativa é preciso olhar além do consentimento do titular. O consentimento, definido pela LGPD como "*manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada*" é o fator indispensável que permite que os agentes de tratamento deem início a operação (realizar coleta, classificação, utilização, reprodução, transmissão e armazenamento).

Porém, caso haja vício no consentimento do titular, o mesmo será inválido e o tratamento dos dados passará a ser considerado ilícito, conforme exposto pelo art. 8º, §3º, da LGPD.

Neste sentido, é nítido que para haver o tratamento das informações não basta apenas a confirmação do titular, essa deve ser munida de manifestação de vontade livre, informada e inequívoca.

Bioni (2019, p. 213) ainda acrescenta:

> A crença de que o cidadão é um sujeito racional e capaz de desempenhar um processo genuíno de tomada de decisão para controlar seus dados pessoais é posta em xeque por toda essa complexidade envolta ao fluxo das informações pessoais. Ele está em uma situação de *vulnerabilidade específica* em meio a uma *relação assimétrica* que salta aos olhos, havendo uma série de evidências empíricas a esse respeito. (BIONI, 2019, p. 213)

O autor apresenta uma problemática no protagonismo do consentimento do titular como sendo refratário, visto que coloca em dúvida a capacidade do titular de dados em exercer um controle efetivo sobre seus dados pessoais. Apresenta ainda, vários argumentos como a hipervulnerabilidade do titular e o questionamento de sua racionalidade ao consentir com o tratamento dos dados.

Um estudo realizado pelas pesquisadoras Lorrie Cranor e Aleecia McDonald (2010), com o título de "Crenças e comportamentos: compreensão dos usuários da Internet sobre publicidade comportamental" em tradução livre, investigou através de uma pesquisa empírica o conhecimento e as percepções dos usuários americanos adultos sobre as técnicas de publicidade no campo virtual, a fim de analisar a capacidade dos usuários nas tomadas de decisões.

A pesquisa realizou diversos questionamentos aos participantes e, através desses pôde-se obter algumas constatações importantes. Entre elas, vale destacar algumas de caráter super curiosos e importantes para o presente trabalho. A primeira revelação do estudo demonstra

que apenas 23% dos usuários utilizam a navegação privada, quando 50% não fazem uso e os outros 27% não tem certeza. Ademais, apenas 17% apagam os *cookies*[10], 23% não tem certeza, e o assustador número de 60% de usuários que não deletam. Esses dados iniciais já demonstram que os usuários não possuem o conhecimento técnico necessário para fazer valer a autodeterminação de seus dados pessoais.

Ainda na mesma linha de raciocínio, a pesquisa faz uma análise das razões pela qual a pequena parcela de 17% dos usuários deleta os *cookies*. Foram obtidos, a partir daí, algumas respostas surpreendentes que refletem mais uma vez a falta de conhecimento do cidadão, como por exemplo: **i.** "*Alguém me recomendou uma vez e eu tenho feito isso desde então*"; **ii.** "*Não tenho muita certeza do que são [cookies]*. **iii.** "*Minha filha me disse para fazer*".

O estudo entrevistou um total de 314 participantes e obteve 390 respostas. Dessas, 80 revelaram que não excluem os *cookies*, sendo que 27% alegaram que possuem software que exclui sozinho; 20% não tinham certeza do que são cookies ou por que os excluíam; 31% foram alguma forma de apatia, seja porque os cookies não incomodam os participantes ou eles não se importam com os cookies; 19% não tinham certeza de como excluir cookies; 3% (duas pessoas) escreveram que não se importam em ser rastreados online. Já no massivo número de 278 pessoas que optaram por excluir 33% basearam-se na ideia de que muitos cookies tornariam o computador lento; 30% teriam a ver com privacidade e segurança; 28% estavam relacionados à liberação de espaço no disco rígido, redução da desordem ou uma noção de limpeza; 8% mencionam vírus, spam ou malware. Já que alguns cookies de rastreamento são classificados como spyware pelo Norton Anti-virus e outros programas anti-malware. (CRANOR; MCDONALD, 2010, p. 12)

Através do estudo as autoras Lorrie Cranor e Aleecia McDonald (2010, p. 27) obtiveram a seguinte conclusão:

> Em primeiro lugar, os consumidores não podem se proteger de riscos que não entendem. Encontramos uma lacuna entre o conhecimento que os usuários têm atualmente e o conhecimento que eles precisariam possuir para tomar decisões eficazes sobre sua privacidade online. Isso tem implicações para políticas públicas, comércio e tecnólogos. Uma participante mais jovem disse, frustrada, que não aprendeu como proteger sua privacidade online na escola, ela apenas aprendeu a digitar. Acreditamos que haja uma necessidade séria não apenas para melhorar a notificação de práticas, mas para o requisito de educação para entender as divulgações. A maioria das abordagens não regulamentares exige que os consumidores entendam as compensações e saibam o suficiente para

[10] Segundo Maria Cecília Gomes, os cookies são "*identificadores que podem ser gerados ou coletadosa partir do navegador ou dispositivo que você usa, a fim de disponibilizar uma página para você acessar ou ainda identificar o seu perfil de navegação*". (GOMES, 2019, p. 9)

> tomar quaisquer ações que permitam suas preferências de privacidade. No momento atual isso parece irreal, mas as perspectivas podem melhorar no futuro. (CRANOR; MCDONALD, 2010, p. 27)

Portanto, a partir dessa pesquisa, é possível concluir que os usuários não estão capacitados para realizar decisões relacionadas ao controle dos seus dados pessoais. Alguns desejam proteger sua privacidade, mas não sabem como. Outros realizam tarefas desnecessárias imaginando resultados diversos, porém inexistente, ou até mesmo confundem com o *modus operandi* de outras ferramentas. Existe aí uma grande confusão quanto ao uso seguro de ferramentas que coletam dados pessoais, com o agravante de serem implementadas em contexto de publicidade comportamental. Evidenciando a vulnerabilidade dos indivíduos em exercer sua autodeterminação informativa no ambiente digital.

6 CONSIDERAÇÕES FINAIS

Na Era Digital é incontestável que o número de pessoas engajadas em saber como são tratados seus dados aumentem. Contudo, ínfimo é ainda o número de pessoas que buscam realmente satisfazer seu interesse em proteger suas informações. Ademais, tende a corroborar com isso as constantes mudanças tecnológicas que utilizam dados e personalizam as relações sociais.

Observado esse novo e intrigante cenário de sociedade de vigilância e mercantilização dos dados é imprescindível que seja reformulada a cultura de utilização e proteção dados pessoais, inclusive, por observar que se trata de algo relativamente novo para grande número de pessoais, as quais muitas não contavam com essa necessidade há décadas atrás.

Para que seja possível imaginar um horizonte de abundante consciência e de conhecimento do titular a respeito dos seus dados e de sua utilização no Brasil, é preciso agir de forma pragmática desde logo. Contando também com a participação primordial de todos os setores sociais.

No sentido legislativo, já são perceptíveis alguns avanços em torno do tema, mas ainda falta muito trabalho no que diz respeito à aplicabilidade prática das normas. O legislador ao construir a Lei Geral de Proteção de Dados (Lei 13.709/2018) já previu essa demanda e então estabeleceu a criação da ANPD – Autoridade Nacional de Proteção de Dados – órgão que possui a competência fiscalizar a aplicabilidade do regulamento (LGPD) e de promover na população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e das medidas de segurança, prevista em seu art. 55-J, VI (BRASIL, 2018).

Compartilhando da mesma intenção que possui a Lei 12.965/2014, chamada também de Marco Civil da Internet, o qual prevê em seu art. 26, o dever constitucional do Estado de prestar educação, em todos os níveis de ensino, incluindo a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico (BRASIL, 2014).

Contudo, é nítido ver que mesmo que as referidas medidas já estejam sendo tomadas, sua eficácia ainda é mínima. O Número de pessoais que desconhecem a necessidade de proteção de seus dados pessoais, assim como a quantidade de organizações que não se enquadram às regras da LGPD é majoritário, mesmo passados dois anos da vigência desse do dispositivo.

A partir daí é possível reconhecer a necessidade inadiável de pôr em prática por completo a atuação do órgão fiscalizador que é a ANPD. Tendo em vista que estabelecer esse ponto de convergência para cultura digital é uma tarefa de longo prazo, mas sempre reconhecendo que o titular deve ser a base da proteção da privacidade e proteção de dados pessoais.

REFERÊNCIAS

BAUMAN, Zygmunt. ***Vida para consumo*: a transformação das pessoas em mercadoria.** Rio de Janeiro: Zahar, 2008.

BAUMAN, Zygmunt. **Vigilância líquida**: diálogos com David Lyon. Rio de Janeiro: Zahar, 2013, versão Kindle.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BRANDELS, Louis. WARREN, Samuel. **The right to privacy**. Disponível em: http://civilistica.com/the-right-to-privacy/. Acesso em 11 de novembro de 2021.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em:http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 22 julho 2021.

BRASIL. **Lei 12.965, de 23 de abril de 2014**. Marco Civil da Internet. 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: 15 de novembro de 2021.

BRASIL**. Lei nº 13.709, de 14 de agosto de 2018**. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2018/Lei/L13709.htm. Acesso em: 16 de novembro de 2021.

BRASIL. **Lei nº 13.853, de 8 de julho de 2019**. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados, e dá outras providências. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 15 de novembro de 2021.

CHRISTENSEN, Clayton M. O Dilema da Inovação: **Quando as Novas Tecnologias Levam Empresas ao Fracasso/Clayton M. Christensen 2012** – São Paulo – M.Books do Brasil Editora Ltda. 2012 – São Paulo – M.Books do Brasil Editora Ltda.

CRANOR, Lorrie Faith; MCDONALD, Aleecia M. **Beliefs and Behaviors: Internet Users' Understanding of Behavioral Advertising**. Disponível em: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092. Acesso em 16 de novembro de 2021.

DANTAS, Henrique. **LGPD: O que é Privacy by Design e Privacy by Defaul**t. 15 de junho de 2019. Disponivel em: https://www.advogatech.com.br/blog/@HenriqueDantas/lgpd-o-que-e-privacy-by-design-e-privacy-by-default-vc4zyjv. Acesso em 16 de novembro de 2021.

Doneda, Danilo Cesar Maganhoto. **Da privacidade à proteção de dados pessoais [livro eletrônico]: elementos da formação da Lei Geral de Proteção de Dados / Danilo Cesar Maganhoto Doneda.** -- 2. ed. -- São Paulo : Thomson Reuters Brasil, 2020.

Estatísticas do nível de adequação das empresas. **Proviti.** publicado em março de 2020. Disponível em: https://www.protiviti.com/BR-por/protecao-de-dados-pessoais. Acesso em: 26 de julho de 2021.

FRANCO, Isabel. **Guia prático de compliance / organização Isabel Franco**. – 1. ed. – Rio de Janeiro: Forense, 2020.

Gabriel, Martha. **Você, eu e os robôs: pequeno manual do mundo digital / Martha Gabriel.** – [3. Reimpr.]. – São Paulo: Atlas, 2019.

GOMES, Maria Cecília de Oliveira. **Cookie notice: o que é e por que é importante?** Disponível em: https://baptistaluz.com.br/institucional/midia-publicidade/. Acesso em 11 de novembro

Guia para programas de compliance. Disponível em: http://www.cade.gov.br/acesso-a-informacao/publicacoesinstitucionais/guias_do_Cade/guia-complian-ce-versao-oficial.pdf. Acesso em: 15 de novembro de 2021.

JIMENE, Camilla Do Vale. **Capítulo VII – Das Seguranças e das Boas Práticas**. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. ***LGPD*: Lei Geral de Proteção de Dados**. 1. ed. São Paulo: Revista dos Tribunais, 2019.

LÉVY, Pierre. **Cibercultura / Pierre Lévy; tradução de Carlos Irineu da Costa**. - São Paulo: Ed. 34, 1999. (Coleção TRANS)

LIMA, Ana Paula Moraes Canto de; ALMEIDA, Dionice de; MAROSO, Eduado Pereira. **LGPD – Lei Geral De Proteção De Dados:sua empresa está pronta?** – São Paulo, SP: Literare Books International, 2020.

LÔBO, Paulo. **Direito civil:** parte geral. 3. ed. São Paulo: Saraiva, 2012.

MALDONADO, Viviane Nóbrega; BLUM, Renato Opice. (coord). **LGPD: Lei geral de proteção de dados comentada.** 1. ed. São Paulo: Revista dos Tribunais, 2019.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais:** comentários à lei n. 13.709/2018 (LGPD). São Paulo: Saraiva Educação, 2018, p.16

Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho (General Data Protection Regulation). **EUR-Lex.** Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A32016R0679. Acesso em: 12 de novembro de 2021.

RODOTÁ, Stefano**. A vida na sociedade da vigilância: a privacidade hoje**. Organização, seleção e apresentação: Maria Celina Bodin de Moraes. Trad. Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Ed.Renovar, 2008.

VAINZOF, Rony. **Capítulo I - Disposição preliminares**. In: MALDONADO, Viviane Nóbrega; OPICE BLUM, Renato. ***LGPD*: Lei Geral de Proteção de Dados**. 1. ed. São Paulo: Revista dos Tribunais, 2019.

ZUBOFF, Shoshana. **Big other: surveillance capitalism and the prospects of an** information civilization. Journal of Information Technology. v. 30, n. 1, 2015.