UNIVERSIDADE FEDERAL DO RIO DE JANEIRO - UFRJ
CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS - CCJE
FACULDADE NACIONAL DE DIREITO - FND

BRENDA CRISTINA RIBEIRO NERY

A IMPORTÂNCIA DO PROCESSO DE CONSCIENTIZAÇÃO DA POPULAÇÃO EM RELAÇÃO A LGPD E O PAPEL DA ANPD NESSE PROCESSO

RIO DE JANEIRO

2023

BRENDA CRISTINA RIBEIRO NERY

A IMPORTÂNCIA DO PROCESSO DE CONSCIENTIZAÇÃO DA POPULAÇÃO EM RELAÇÃO A LGPD E O PAPEL DA ANPD NESSE PROCESSO

Monografia apresentada como requisito necessário para a obtenção do título de Bacharel em Direito.

Orientadora: Dra. Veronica Lagassi

RIO DE JANEIRO

2023

CIP - Catalogação na Publicação

N456i

Nery, Brenda Cristina Ribeiro
A IMPORTÂNCIA DO PROCESSO DE CONSCIENTIZAÇÃO DA POPULAÇÃO EM RELAÇÃO A LGPD E O PAPEL DA ANPD NESSE PROCESSO / Brenda Cristina Ribeiro Nery. -- Rio de Janeiro, 2023.
57 f.

Orientador: Veronica Lagassi.
Trabalho de conclusão de curso (graduação) - Universidade Federal do Rio de Janeiro, Faculdade Nacional de Direito, Bacharel em Direito, 2023.

1. LGPD. 2. Direito . 3. Universidade Federal do Rio de Janeiro. I. Lagassi, Veronica , orient. II. Título.

Elaborado pelo Sistema de Geração Automática da UFRJ com os dados fornecidos pelo(a) autor(a), sob a responsabilidade de Miguel Romeu Amorim Neto - CRB-7/6283.

AGRADECIMENTOS

Em primeiro lugar, gostaria de agradecer aos meus pais e a minha irmã, por todo o apoio e amor que me dedicaram ao longo da vida. Vocês foram primordiais para essa conquista.

Também, agradeço à minha avó Irene, exemplo de força e resiliência, cuja vida dedicou ao sustento e à felicidade da família.

Aos familiares, por todo o apoio e pela ajuda.

Aos meus amigos que, mesmo espalhados por todo o Brasil, sempre se fizeram presentes e demonstraram apoio durante toda essa jornada.

Por fim, aos professores, pela paciência com a qual guiaram o meu aprendizado. E, especialmente, à professora Dra. Veronica Lagassi, por ter sido minha orientadora.

RESUMO

O contexto atual da tecnologia e a sua influência sob a economia provocou a criação de legislações com a finalidade de regular o tratamento de dados pessoais, como é o caso da Lei Geral de Proteção de Dados. O desenvolvimento na tecnologia permitiu que a capacidade de armazenamento de dados no meios digitais aumentasse, possibilitando não só a criação de redes sociais e afins, como também a coleta intensa dos dados dos usuários. Ocorre que, esses dados coletados refletem aspectos singulares das personalidade de seus titulares, tornando-os em matérias extremamente valiosas, mas ao mesmo tempo, perigosas também. Isto porque, por retratar o âmbito privado do cidadão, os dados são utilizados pelo meio sociopolítico para induzir o cidadão a determinados comportamentos. O poder provocado pelos dados pessoais permitem que essas instituições alcancem seus objetivos por meio da violação da privacidade do indivíduo, tornando-os extremamente vulneráveis. Dessa forma, o cenário exposto exigiu a criação de um dispositivo legislativo específico para regular o tratamento de dados e consolidar a importância de determinado tema na vida cotidiana dos cidadãos.

Palavras-chaves: Dados Pessoais; Tratamento de Dados; Privacidade; Lei Geral de Proteção de Dados.

ABSTRACT

The current context of technology and its influence on the economy have led to the creation of legislation with the purpose of regulating the processing of personal data, as is the case with the General Data Protection Law. The development of technology has allowed the data storage capacity in digital media to increase, enabling not only the creation of social networks and the like, but also the intense collection of user data. It turns out that these collected data reflect unique aspects of the personality of their holders, making them extremely valuable materials, but at the same time, dangerous as well. This is because, to portray the private sphere of the citizen, the data are used by the sociopolitical environment to induce the citizen to certain behaviors. The power demonstrated by personal data allows these institutions to achieve their objectives by violating individual privacy, making them extremely vulnerable. Thus, the exposed scenario presents the creation of a specific legislative device to regulate data processing and consolidate the importance of a certain topic in the daily lives of citizens.

Palavras-chaves: Personal data; Data Processing; Privacy; General Data Protection Law.

LISTA DE ABREVIATURAS E DE SIGLAS

LGPD	Lei Geral de Proteção de Dados
GPDR	General Data Protection Regulation
ANPD	Agência Nacional de Proteção de Dados
CDC	Código do Consumidor
IBGE	Instituto Brasileiro de Geografia e Estatística
OAB	Organização dos Advogados Brasileiros
STF	Supremo Tribunal Federal
FTC	Federal Trade Commission
FIPPs	Fair Information Practice Principles
PROCON	Programa de Proteção e Defesa do Consumidor
MERCOSUL	Mercado Comum do Sul

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

Cativados pelas facilidades imediatas provenientes das tecnologias, os indivíduos dificilmente se questionam sobre o funcionamento das plataformas digitais ou se alertam em entender as dinâmicas socioeconômicas que ocorrem nos bastidores da internet, sem o conhecimento dos usuários.

É inegável que o avanço da tecnologia facilitou muito a vida dos cidadãos no dia a dia, auxiliando a execução de tarefas em todos os âmbitos, do social ao profissional. No entanto, todo esse cenário só foi possível em razão do desenvolvimento da tecnologia que proporciona o tratamento de dados digitais mais efetivo.

A evolução do armazenamento de informações nos meios digitais possibilitou a criação do sistema digital que usufruímos atualmente, composto por redes sociais, aplicativos diversos, entre outros. E, ao utilizarem as plataformas e os aplicativos virtuais, os cidadãos possibilitam a criação de dados pessoais, que podem refletir aspectos singulares sobre sua personalidade.

Ocorre que, após a coleta, na maioria das vezes, sem o consentimento do usuário, esses dados são vendidos a instituições públicas e privadas.

Em que pese essa dinâmica parecer inofensiva, suas consequências podem ser muito mais negativas e prejudiciais ao usuário do que o esperado. Isto porque, por serem extremamente sensíveis e carregarem características específicas sobre determinado usuário, como gostos e preferências, os dados equivalem ao âmbito pessoal do usuário, que não deveria ser coletado ou disponibilizado a terceiros sem autorização.

Com o passar do tempo, histórias sobre vazamento e venda de dados pessoais se tornaram cada vez mais frequentes nas manchetes de jornais, pois, os dados pessoais, que refletem características singulares do titular, passaram a ser vistas como matéria valiosa, proporcionando um desenvolvimento econômico às empresas.

As informações provenientes dos tratamento de dados pessoais facilitam a vida das empresas e as guiam para um caminho ao lucro de uma maneira mais fácil.

Torna-se imprescindível a criação de uma consciência social efetiva sobre a importância dos dados pessoais e, por consequência, a criação de uma legislação e autoridade específicas também.

Logo, em 2020, entrou em vigor a Lei Geral de Proteção da Dados Pessoais e, em 2021, a sua autoridade, a Agência Geral de Proteção de Dados Pessoais, que tem o papel significativo de concretizar a efetividade da tutela de proteção de dados, tanto no âmbito público-privado como no individual.

Desta maneira, a presente monografia tem como intuito demonstrar a importância e os reflexos, positivos e negativos, do tratamento de dados, e expor o papel da LGPD na missão de tutelar a proteção de dados pessoais no Brasil.

1. CAPÍTULO I

a) O surgimento do tratamento de dados digitais

Em decorrência dos avanços tecnológicos e da ascensão dos dados digitais, a forma de comunicação e de consumo da sociedade atual mudaram completamente.

Tal porque a tecnologia moderna permitiu que a sistematização e o armazenamento desses dados evoluíssem, tornando sua manipulação mais fácil e, por consequência, sua funcionalidade mais aprimorada.

Paralelamente, os meios de comunicação e entretenimento também mudaram. Houve o surgimento das redes sociais e meios de comunicação digitais, que passaram a fazer parte do cotidiano do cidadão.

Ao utilizar esses meios de forma constante, o indivíduo ampliou o âmbito de coleta e fluxo de seus dados, permitindo que terceiros os analisem, transformem em informações úteis acerca da sua personalidade e conduta e apliquem em objetivos socioeconômicos.

Segundo Bruno Bioni (2021, p.34), esse novo fluxo informacional proporciona a informação um novo papel:

> "Por isso, a informação avoca um papel central e adjetivante da sociedade: *sociedade da informação*. A informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como fizeram a terra, as máquinas a vapor e eletricidade, bem como os serviços, respectivamente, nas sociedades agrícolas, industrial e pós-industrial." [1]

No entanto, ainda que esteja em destaque atualmente, a coleta de dados não é uma novidade do mundo atual. Há décadas existe uma concepção acerca da utilidade das informações derivadas das análises de dados.

Antes mesmo do surgimento dos dados digitais, já era recorrente a criação de banco de dados, nos quais, após coletados, os dados eram armazenados com base em uma determinada lógica a fim de permitir uma proveitosa obtenção de informações.

Utilizados por governantes, por exemplo, o censo ilustra bem a serventia desse determinado instrumento, que por meio da coleta de dados, sistematiza os dados e adquire um senso populacional, que é utilizado para embasar determinadas decisões institucionais.

[1] BIONI, Bruno Ricardo. RIELLI, Mariana Marques. A Construção multissetorial da LGPD: histórias e aprendizados. Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF

Os dados nada mais são do que a matéria-prima das informações que, desde o capitalismo industrial, já tinha com uma posição de relevância devido à ciência da sociedade acerca da importância da informação, visto que, no sistema de produção taylorismo, analisa-se cada processo de produção a fim de atingir uma maior produtividade.

No decorrer dos anos, aumentando seu âmbito de aplicação, os dados passaram a ser utilizados não só pelo Estado, mas também pelo mercado. Assim, quando houve a evolução do banco de dados digitais, provocou-se a instauração de uma nova conjunção socioeconômica.

b) Mudanças socioeconômicas subsequentes

A ascensão dos dados iniciou quando ocorreu evolução do armazenamento digital desses. Anteriormente, os dados eram armazenados como se fossem átomos, que em conjunto resultam em material mais denso, como uma espécie de livro, agora, no entanto com o *Big Data* e *Big Analytics*, o armazenamento ocorre em forma de bits, o que possibilita que as informações se estruturem em unidades menores de matéria, permitindo, consequentemente, a digitalização de diversas espécies de informações, como vídeos e áudios.

Ao mudar a forma de armazenamento dos dados, permitiu-se não só que uma maior quantidade desses fosse arquivada, mas também possibilitou, proporcionalmente, melhoria na organização e qualidade deles. Por se tornarem mais volumosos e significativos, a análise dos dados passou a conceber informações corretas, aumentando a sua funcionalidade e tornando os dados uma matéria-prima extremamente valiosa.

Isto é, a melhora direta no armazenamento e na organização desses que proporcionou uma maior qualidade aos dados e o aperfeiçoamento na análise desses, provocou a transição da sociedade pré-informacional para a informacional, criando um novo modelo de organização de empresas em rede e fazendo com que os indivíduos deixassem de estar em uma posição passiva na relação de consumo e passassem a ser integrantes ativos dessa dinâmica.

Durante a coleta, os dados são considerados como uma espécie de pré-informação, uma forma mais primitiva e fragmentada da informação, que só geram valor após serem processados em informações.

Ao utilizar a internet, os indivíduos produzem dados digitais, ou seja, pré-informações que formam um conjunto de dados, *o big data*, que serão compartilhados e lidos por dispositivos receptores e transformados em dados, que podem ser pessoais, pessoais sensíveis ou anônimos.

O primeiro é identificado como um dado relacionado a uma pessoa humana identificável ou identificada, enquanto o segundo representa o âmbito mais privado do indivíduo, aspecto singulares de determinada pessoa, abrangendo até convicções pessoais. Por fim, o terceiro é um dado que não é capaz de ser associado a qualquer pessoa.

Esse novo modelo descentralizou a atividade empresarial e a tornando horizontal. As empresas passaram a trabalhar de forma colaborativa e a analisar os dados de vendas a fim de se aperfeiçoar e aumentar os lucros. Isto é, a evolução do banco de dados acarretou a instauração de uma nova conjunção, dado que os usuários, ao utilizarem a internet, proporcionam às empresas um direcionamento para as suas ações publicitárias.

Dessa forma, percebe-se que em razão do conteúdo proveniente do processamento de um determinado dado ser capaz de tornar suscetível a identificação de uma pessoa singular, o dado coletado é pessoal.

Isto é, dependendo de qual dado foi coletado, este estará diretamente ligado não só ao âmbito de privacidade de determinado indivíduo, como também sua autonomia, identidade e liberdade.

Assim, aos poucos, certas comunidades vêm passando a perceber os perigos das coletas de dados, percebendo a necessidade da proteção de dados e, por conseguinte, desenvolvendo leis para regular a coleta e análise desses.

2. CAPÍTULO II

a) A interferência da nova dinâmica de tratamento de dados pessoais sobre o cidadão

As informações provenientes do tratamento de um banco de dados pessoais mais estruturado e organizado conseguem apresentar, de forma mais verídica, as preferências, interesses e características da personalidade de determinado indivíduo, dentre outras informações relevantes.

De acordo com a Lei de Proteção de Dados Pessoais, definem-se os dados pessoais como qualquer informação vinculada ao usuário que permite a identificação, direta ou indireta.

E os dados pessoais sensíveis:

> "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 a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural."[2]

Este resultado é proveniente da utilização do algoritmo, um conjunto de passos determinados que, ao seguirem uma ordem lógica predeterminada, originam uma ação. Por exemplo, quando acessamos uma rede social e assistimos alguns vídeos ali disponíveis, dados são criados e analisados, possibilitando ao algoritmo criar uma percepção de quais são nossos gostos e, a partir disso, a rede social passará a sugerir e apresentar vídeos que acredita estar consoante a nossa preferência, fazendo com que mais vídeos de nossa preferência sejam apresentados e mais dados nossos coletados.

Paralelamente, a variedade de sistemas digitais que utilizamos permite que os dados sejam produzidos em maior número e rastreados com mais facilidade pelo *data brokers*[3]. Esses dados são tratados e geram informações, que se tornam produtos a serem consumidos por empresas, governos, partidos políticos, dentre outros[4].

---

[2] Brasil. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10.11.2022.

[3] Data brokers são "entidades dedicadas a compilar informações diversas, organizá-las, classificá-las e comercializá-las para terceiros, que passarão a usar todo esse banco de dados qualificado para suas próprias finalidades (sejam elas benignas ou malignas)". https://canaltech.com.br/seguranca/o-que-sao-data-brokers-e-como-eles-funcionam-176757/

[4] TAYLOR, Linnet. O que é justiça de dados? Conectando direitos digitais e liberdades globalmente.Construindo caminhos para a justiça de dados no Brasil: o papel das defensorias públicas na proteção de dados pessoais. 1.ed. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. PDF, p. 20.

E, com a crescente utilização da tecnologia como ferramenta essencial para o cotidiano dos indivíduos, os usuários não conseguem evitar a disponibilização de seus dados pessoais e, por conseguinte, rastreamento digital feito a partir desses. O processamento desse grande volume de dados pessoais possibilitam a terceiros o conhecimento da conduta não só pública, como também privada, de determinada pessoa.

Segundo Martin Hilbert, especialista de Big Data, ao curtir 150 posts, os algoritmos já conseguem entender mais um indivíduo que o companheiro dele e, ao curtir 250 posts, o algoritmo é capaz de entender mais o indivíduo que ele próprio[5].

Percebendo a sensível matéria-prima disponível, o mercado se volta para a utilização dos dados de forma acentuada e, por conseguinte, torna-se uma instituição baseada em controle de dados pessoais.

Mesmo que conscientes da visibilidade ilimitada dos seus dados, em razão da necessidade da utilização de serviços movidos a dados para atividades sociais e profissionais, os usuários apenas se acostumam e se conformam com a visibilidade, abdicando de seus direitos e deixando de se engajar de forma política acerca de seus dados[6].

Coletados diariamente sem e com consentimento, os dados pessoais dos cidadãos são coletados e utilizados por autoridades públicas e privadas de forma incontrolada.E, a ausência de uma separação forte entre os dados coletados voluntariamente (por pesquisas diretas e com a ciência do indivíduo) e automaticamente (provenientes de sensores da vigilância digital) agrava o presente cenário.[7]

Consoante a esse pensamento, Linnet afirma:

> "A crescente disponibilidade de dados digitais que refletem o desenvolvimento econômico e humano, em particular a chamada "fumaça dos dados" ou *data fumes* (Thatcher, 2014) - isto é, dados produzidos como subproduto da utilização de dispositivos e serviços tecnológicos - está provocando de uma mudança de paradigma na elaboração de políticas públicas, que deixam de ser informadas por dados (*data informed*) para se tornarem orientadas por dados (*data driven*) (Kitchin, 2016)."[8]

Assim, diante do cenário em questão, surge o *mobile marketing*, derivado da comunicação entre a publicidade, os consumidores e os fornecedores. O indivíduo, por ser

---

[5] FRAZÃO, Ana. TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Ed. Revistas dos Tribunais, 2019, p.26.
[6] Idem, p.22.
[7] Idem, p.20
[8] Idem, p.16.

usuário da internet e dos seus meios de comunicação digitais, terá seus dados coletados utilizados pelas empresas, que a partir da análise desses, saberão os direcionamentos para potencializar mensagens publicitárias[9]. O consumidor passa a ser telespectador das suas próprias informações[10].

Isto porque, os dados representam o cidadão e, por isso, transmitem aspectos singulares de sua personalidade. Assim, mais que um bem econômico ou uma matéria-prima, o dado passa a ser um produto analisado sob um ponto de vista comportamental.

As informações resultantes dos dados apresentam aspectos singulares do âmbito privado, ou seja, são o reflexo do cidadão, espelhando a sua individualidade. Assim, ao serem compartilhados com as instituições privadas, transforma-se não só os dados em mercadoria como também os cidadãos, atingindo os direitos de personalidade desses.

É muito comum que essas informações sejam utilizadas por terceiros sem o consentimento do titular e, ainda que ciente da coleta, o cidadão dificilmente tem noção das consequências do tratamento, pois as instituições não informam o porquê ou a finalidade do tratamento.

Logo, a ausência de um controle efetivo dos cidadãos sobre os dados permite a utilização desses de forma abusiva por terceiros, prejudicando os próprios titulares.

Consonante a esse pensamento, Bioni (2021, p.150) destaca a fala de Anderson Schreiber:

> "o destino de uma pessoa pode ser decidido com base em seus dados coletados na internet, podendo ser eliminada de um certo progresso por conta da sua opção político, partidária, religiosa ou das mais variáveis."

A visibilidade provocada pela maior disponibilidade dos dados digitais atinge principalmente as populações de baixa renda[11], que geralmente são completamente ignorantes sobre a exploração dos dados e as suas consequências, tornando a situação ainda mais complexa, pois a autonomia e o poder para proteger seus dados geralmente se restringe aos indivíduos pertencentes a classes econômicas superiores.

---

[9] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites de consentimento. Ed 1. Rio de Janeiro: Forense, 2019, p. 46.
[10] Idem, p.39
[11] TAYLOR, Linnet. O que é justiça de dados? Conectando direitos digitais e liberdades globalmente.Construindo caminhos para a justiça de dados no Brasil: o papel das defensorias públicas na proteção de dados pessoais. 1.ed. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. PDF, p. 16.

Estabelece-se o "one mirror way" que, segundo Frank Pasquale, é um cenário no qual os dados pessoais ao serem utilizados pelos Estado e pelo mercado possibilita a esses um conhecimento profundo, do âmbito privado e público, dos cidadãos, enquanto esses não têm consciência da presente situação[12].

A utilização desses dados pessoais permite a concretização de uma estrutura muito mais sofisticada e operativa, visto que, ao moldar-se a partir dos interesses dos indivíduos, o mercado apresenta exatamente o que os consumidores querem, facilitando sua manipulação sob a sociedade.

Ocorre o que Jeff Connaughton chama de The Blob. Segundo Ana Frazão[13], em sua pesquisa, Connaughton descreve este como "*um network* de atores que age às sombras, mobilizando dinheiro e mídia para ganhos privados, mesmo quando agem oficialmente em nome do negócio ou do governo".

Logo, o lucro obtido da vigilância proporcionada coleta e análise de dados pessoais, tornam os dados insumos de extremo valor. Por conseguinte, surge uma nova era do capitalismo, o capitalismo da vigilância.

A extração absurda de dados que, mesmo sendo muito mais do que o necessário, é justificada pelo objetivo de melhoria do serviço, pois, coletados, os dados alimentam *machines learning*, uma espécie de novo meio de produção, originando predições de excelência acerca do comportamento dos indivíduos[14].

Assim, o cenário de vigilância permitido pelos coleta e análises de dados pessoais se concretiza por meio de uma relação desbalanceada, pois todo o processo é feito de forma escondida, sem que os cidadãos tenham ciência que seus dados estão sendo coletados ou com qual finalidade serão analisados, podendo criar consequência extremamente negativas aos titulares.

Em seu texto, Caitlin Mulholland destaca um caso em que o perfilamento derivado da análise de dados pessoais gerou um tratamento discriminatório. Nos Estados Unidos, após informações obtidas da análise de dados, as seguradoras impediam a contratação de mulheres

---

[12] Idem, p.41.
[13] Idem, p.28.
[14] Idem, p.33.

vítimas de violência doméstica, isto é, os dados dos usuários foram utilizados não sem seu consentimento como também os prejudicaram[15].

Também, no mesmo texto, destaca um caso apresentado por Rodotà (2008, P.70):

> "Na dúvida de que o conhecimento, por parte do empregador ou de uma companhia seguradora, de informações sobre uma pessoa infectada pelo HIV, ou que apresente características genéticas particulares, pode gerar discriminações. Estas podem assumir a forma da demissão, da não admissão, da recusa em estipular um contrato de seguro especialmente elevado."[16]

A falta de transparência na coleta de dados permite a ignorância dos indivíduos acerca da concretização da sociedade da vigilância, tornando o cenário atual extremamente perigoso, visto que coloca em jogo não só o tratamento isonômico entre os indivíduos mas também a autonomia individual dos cidadãos.

Como Ana Frazão bem coloca, dados pessoais e o capitalismo da vigilância são lados da mesma moeda. Ao escrever sobre os perigos dos fenômenos tecnológicos e sociais, Richard Thomas descreveu o cenário como "a *sleepwalking into a surveillance society*", no qual afirma que os indivíduos estão cada vez mais caminhando para uma sociedade vigilantes sem estar conscientes do local de chegada[17].

E, por se tornarem cada vez mais valiosos, os dados passam a ser mais cobiçados, convertendo-se em alvos constantes de tentativas ilícitas de acesso e de vazamentos.

A quantidade de dados pessoais disponibilizados a essas entidades e o poder dessas são diretamente proporcionais, quanto mais fácil for o processo de coleta maior será a extração e o lucro proveniente da análise desses.

Insumo principal do capitalismo atual, os dados pessoais permitem tanto um rendimento econômico para as grandes empresas, quanto permitem um controle intenso e diário da parceria público-privada sob a sociedade.

Por isso, é certo que o conhecimento pleno dos cidadãos acerca da importância dos dados pessoais e sua extração tornaria o processo de coleta muito mais difícil, afetando diretamente os lucros dessas grandes entidades estatais e privadas.

---

[15] MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709.18). R. Dir. Gar. Fund., Vitória, V.19, n.3, p.159-180, set - dez 2018, p. 174

[16] Idem, p. 175

[17] FRAZÃO, Ana. TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Ed. Revistas dos Tribunais, 2019, p.26.

A violação de dados torna-se intencionalmente um problema pormenorizado e de certa forma escondido por essa parceria público-privada. É possível ter uma melhor compreensão de como ocorre o procedimento supracitado pela autora Ana Frazão (2019, p.29):

Devido a quantidade de etapas presentes no processo acima, esse é composto por diversos agentes, contendo desde aqueles que exercem apenas a coleta de dados até aqueles que processam e vendem, chamados de data brokers.

Ainda, segundo um relatório redigido em 2014 pela Federal Trade Commission[18] norte americana, dentre as conclusões alcançadas, destacaram-se: a) a fonte utilizada de dados utilizadas abrange canais comerciais, governamentais e públicos, como: mídias sociais, blogs, dentre outros, b) para atingir melhores resultados, combina-se dados obtidos de forma online e offline, c) grande parte da coleta de dados pessoais ocorre sem a ciência dos cidadãos, d) o número de dados coletados e maior do que o número de dados utilizados, e) em sua grande maioria das vezes os dados são aplicados para resultarem em predições acerca do comportamento dos consumidores, f) dependendo da finalidade da coleta, a análise dos dados pode acarretar riscos negativos ao indivíduo.

Segundo Frazão, alguns doutrinadores já destacam os perigos provenientes da utilização descontrolada das predições:

> "Como advertem Agrawal, Joshua Gabs e Avi Goldfarb, há limites para a habilidade das máquinas na predição de julgamentos humanos, até porque o poder preditivo das

[18] FEDERAL TRADE COMMISSION. Data Brokers. A call for transparency and accountability. Disponível em: [https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf]. Acesso em: 22.11.2022.

> máquinas é ruim em se tratando de eventos raros ou que não tenham ocorrido muitas vezes no passado.
>
> Mesmo quando o raciocínio estatístico estiver certo, e forçoso concordar m que este, em si, não deixa de apresentar uma espécie de discriminação, medida em que o julgamento a respeito de uma pessoa e feito a partir de critérios gerais que desconsideram a sua individualidade."[19]

Ao não serem capazes de identificar as particularidades, as predições apresentam malefícios tanto ao acertar quanto ao errar. Isso ocorre pois os acertos permitem que terceiros passem a ter conhecimento de aspectos extremamente íntimos do indivíduo analisado, enquanto os erros atribuem a esse indivíduo características que não lhe são pertencentes, sem que ele tenha o poder de refutar essas predições.

Ademais, por proverem informações sensíveis, as predições permitem que os algoritmos nos regulam e nos definem, como confirma Frazão:

> "Os algoritmos- ou aqueles que os criam e utilizam- tanto podem determinar os destinos das pessoas como também podem ser desenhadas para influenciar e modificar o comportamento humano. O conhecimento profundo das características do usuário, inclusive no que diz a respeito das suas fragilidades, pode ser utilizado para toda sorte de discriminações e abusos, além da manipulação de suas emoções, crenças e opiniões para os fins mais diversos, inclusive políticos."[20]

A falta de transparência do processo o torna ainda mais perigoso, dado que, perfis traçados a partir da análise de dados são vendidos como produtos para companhias e empresas, sem qualquer consentimento do usuário ou refutações acerca da sua qualidade, permitem que preconceitos presente em uma sociedade se perpetuem ainda mais. Isto e, quanto mais enraizado seja o preconceito, mais o algoritmo vai extraí-lo, estabelecê-lo como um padrão e, por conseguinte, replicá-lo.[21]

Também, Caitlin Sampaio Mulholland destaca o segundo ponto em seu texto:

> "De acordo com Celina Bodin e Chiara de Teffé (2016, p.21), "uma vez munidas de tais informações (dados pessoais), entidades privadas e governamentais tornam-se capazes de "rotular" e relacionar cada pessoa a um determinado padrão de hábitos e de comportamentos, situação que pode fornecer inclusive graves discriminações, principalmente se analisando dados sensíveis".[22]

---

[19] FRAZÃO, Ana. TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Ed. Revistas dos Tribunais, 2019, p.34.
[20] Idem, p.37.
[21] Idem, p.40.
[22] MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709.18). R. Dir. Gar. Fund., Vitória, V.19, n.3, p.159-180, set - dez 2018, p. 174.

Dessa forma, evidencia-se que, mais do que invasão à privacidade, a coleta e análise de dados se concretizam como um controle institucional que, ao ocorrerem de forma opaca, inibem a mudança social, facilitando a manipulação.[23]

Consoante a esse pensamento, Frazão afirma:

> "O problema é que essa estratégia compromete todo o potencial de liberdade e difusão de informação na internet, colocando em risco os direitos individuais e o próprio crescimento econômico, na medida em que se torna instrumento para consolidar o poder e riqueza dos grandes agentes, cujas atividades não são nem monitoradas nem reguladas."[24]

E, as redes sociais entram como personagens da determinada dinâmica que permitem a concretização do mercado de dados, visto que conseguem não só coletar os dados de forma "natural" e indolor, mas também influenciar seus usuários, praticando a forma mais fundamental do poder e perpetuando a doutrinação da elite econômica sob a sociedade.[25]

Com isso, percebe-se assim grande influência da visão utilitarista, pois, segundo o ponto de vista dos grandes atores econômicos, a inovação e seus resultados justificam o sacrifício de certos direitos fundamentais, como a privacidade e autonomia. A indústria atual não só se concretiza utilizando-se de um insumo que não é sua propriedade, como também não a coleta de forma lícita, sendo um processo de exploração realizado de forma escondida e desleal.

Conjuntamente, os próprios cidadãos não se preocupam com a proteção de seus dados devido a névoa de otimismo promovida pelos benefícios imediatos que a economia digital lhe promove e a falta de ciência dos reais impactos que a violação de dados pode ocasionar.

Esse cenário cria um ônus difícil de ser contornado pelos reguladores, que se veem diante de dificuldades para conter as condutas ilícitas dos agentes e proteger os dados dos cidadãos de forma efetiva.

O desequilíbrio na relação jurídica atual entre os cidadãos e a indústria diverge da relação jurídica obrigacional ideal entre credor e devedor e isso se dá pois há a aplicação equivocada do conceito de obrigação.

---

[23] FRAZÃO, Ana. TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Ed. Revistas dos Tribunais, 2019, p.40.
[24] Idem, p.41.
[25] Idem, p. 44-45.

Anteriormente, a aplicação de obrigação utilizada era a concepção estática da obrigação, no entanto, a complexidade intra-obrigacional aplicada atualmente, em decorrência da boa-fé objetiva, estabelece diversos deveres anexos além do estabelecido no vínculo obrigacional simples, considerando também os acessórios, secundários, gravitacionais ou satelitários.

Consoante a esse pensamento, Bruno Bioni afirma:

> "Há, portanto, uma coordenação recíproca que remete à ideia de processo: de uma prática de atos coordenados em que o vínculo obrigacional se extingue-se desenvolve, contribuindo os dois polos da relação obrigacional para todo esse desencadeamento.
>
> Em síntese, seja qual for a nomenclatura: obrigação como organismos (Heinrich Siber e Savigny), relação-quadro, complexidade intra-obrigacional, obrigação como processo, concepção dinâmica da obrigação ou regra moral nas obrigações, há uma convergência da doutrina que se afasta de uma análise rarefeita, simples e estática do plexo obrigacional para a concepção dinâmica em que há um feixe de direitos e deveres entre os polos da relação obrigacional conclamados para a extinção do vínculo obrigacional. " [26]

Isto posto, divergindo do conceito estático de obrigação, o princípio de transparência e a imprescindibilidade da informação passam a ser destaque dentro de qualquer relação jurídica proveniente do mercado de consumo e a integrar lugar dentro das legislações, principalmente a consumerista, compondo "a própria licitude da atividade do fornecimento de produtos ou serviços" [27](BIONI, p.140).

E, ainda que existam mecanismos que podem ser utilizados a fim de diminuir esse controle proporcionados pela análise indevida e descontrolada dos dados pessoais, como a anonimização, os estudos recentes destacam cada vez mais os riscos presentes em tais procedimentos e a sua reversibilidade.

Como mencionado anteriormente, um dado pode ser anônimo, isto é, "incapaz de revelar a identidade de uma pessoa"[28], ainda que originalmente fosse um dado pessoal. Isso ocorre em razão do processo de anonimização, cujo objetivo é romper o vínculo existente entre a pessoa e o dado, não sendo possível identificá-la por meio dele.

---

[26]BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergência e divergências a partir da análise da ação coletiva promovida contra o Facebook e aplicativo "Lulu". Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF, p. 137.

[27] Idem, p.140.

[28]BIONI, Bruno Ricardo. Compreendendo o conceito de anonimização e dado anonimizado. Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF. p.245.

No entanto, esses procedimentos não são infalíveis e há possibilidade dos dados pessoais anonimizados serem identificados. Assim, é possível que mesmo o dado anonimizado ser vinculado à pessoa após esforço, o efeito mosaico.

É evidente que o procedimento não basta, necessitando outras formas mais efetivas de proteção, mas pode auxiliar na minimização dos riscos provocados pelo tratamento de dados.

Assim, um dos principais meios de prover uma relação jurídica mais equilibrada ao titular é a informação. O dever-direito de informar que dá ao cidadão o verdadeiro controle sobre seus dados, mas, para que o ato de informar seja efetivo, é necessário que a informação preencha determinados requisitos.

Segundo Claudia Lima Marques[29]:

> "Informar é "dar" forma, é colocar (in) em uma "forma", aquilo que um sabe ou deveria saber (o expert) e que o outro (leigo) ainda não sabe (o consumidor), donde se constata dois substratos iniciais para dissecar o objeto de análise - a informação."

Não basta dar qualquer informação, primeiramente, é necessário se dar forma, ou seja, tornar o ato de informar evidente a quem recebe a informação. E, segundamente, é a imprescindibilidade da informação, isto é, ela precisa ser original e útil.

Dessa forma, ao adquirir mais conhecimento, o cidadão passa a ter uma visão mais crítica acerca das situações que o cercam, principalmente das decisões por ele a serem tomadas.

A informação bem elaborada, útil e completa permite que o cidadão tenha uma relação menos desequilibrada com o fornecedor, dado que, a perspectiva crítica proporcionada pela informação, possibilita que o diálogo estabelecido entre os dois seja menos obscuro, dado que a disparidade informacional entre os dois não vai ser tão evidente.

Destaca-se que informar não é transmitir uma quantidade excessiva de informação. O ato de informar se torna efetivo quando se exprime a quantidade ideal de informações, dado que a racionalidade limitada do ser humano o impede de assimilar informações dadas em excesso[30].

---

[29] BIONI, Bruno Ricardo. O dever de informar e a teoria do diálogo das fontes para a aplicação da autodeterminação informacional como sistematização para a proteção dos dados pessoais dos consumidores: convergência e divergências a partir da análise da ação coletiva promovida contra o Facebook e o aplicativo "Lulu". Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF. p.143-144.

[30] Idem, p.145.

Então, o foco deve ser concretizar esse pensamento dentro do âmbito privado, tornando a informação um fator presente nas relações dos cidadãos e das empresas. Isso ocorre, pois, a relação entre público e privado nesse cenário é inevitável dado que muitas das funções do Estado são realizadas pelo setor privado.

Os números de integrantes da equipe pública são pequenos comparado ao corpo de indivíduos do meio privado que trabalham com o Big Data, na maioria das vezes, a ratificação do Estado é realizada pelo âmbito privado.[31] Por conseguinte, o mercado se torna o ponto central das discussões de proteção de dados para diminuir as assimetrias ocasionadas pelo abuso aos direitos, provocados por indevidos tratamentos de dados.

No entanto, conforme a circulação dos dados digitais aumenta entre os âmbitos público e privado, as ferramentas que podem ser utilizadas pelos cidadãos para a representação democrática não são disponibilizadas de maneira efetiva, fazendo com que esses não possam reparar determinados danos[32].

A complexidade existente na relação de vigilância, relacionando vários indivíduos, sendo de "muitos" para "muitos"[33], não sendo possível a análise da proteção de dados apenas por uma perspectiva individual.

Mesmo que a proteção de dados seja analisada por uma ótica de infração aos direitos fundamentais como privacidade informacional e liberdade de comunicação, essa interpretação gera alguns problemas pois não só aplicação dos Direitos Humanos exige que a infração gera clara e evidentes como também determina que a reparação ocorra em âmbito individual.

Assim, ao evidenciar-se que o abuso da coleta e tratamento de dados atinge não só o âmbito privado como também o coletivo, percebe-se a necessidade de uma proteção multifacetada por meio de legislação e criação de diversas autoridades independentes a fim de promover essa dinâmica de proteção público- privada.[34]

---

[31] TAYLOR, Linnet. O que é justiça de dados? Conectando direitos digitais e liberdades globalmente.Construindo caminhos para a justiça de dados no Brasil: o papel das defensorias públicas na proteção de dados pessoais. 1.ed. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. PDF, p. 20.
[32] Idem, p. 21.
[33] Idem, p.21.
[34] Idem, p. 22.

b) O porquê da necessidade de proteção do princípio da dignidade humana e dos direitos de personalidade por meio da proteção de dados

Conforme mencionado, a proteção de dados é vista com uma outra perspectiva, que deixa de abranger apenas aspectos computacionais e passa a envolver privacidade, liberdade e autonomia do cidadão. Isso se deve, pois, a proteção de dados passa a ser vista como um direito fundamental inerente ao princípio da dignidade humana.

Em seu texto, Caitlin Sampaio Mulholland divide o princípio da dignidade humana:

> "Este princípio possui duas acepções: uma no sentido de garantir a todas as pessoas um tratamento humano, não degradante, e, portanto, protetivo da integridade psicofísica de cada um; e outra; no sentido de realizar projetos e propostas que possibilitem a cada pessoa a concretização de sua humanidade, por meio de ações visíveis."[35]

Isto posto, destaca-se a ligação de determinado princípio com os direitos de personalidade humana. Segundo Cristiano Chaves e Nelson Rosenvald[36], sem esse direito "a análise da teoria da personalidade e da proteção fundamental que dela decorre tornar-se-iam vazias, caindo em verdadeiro marasmo formalismo, despido de significado concreto".

É imprescindível que esse macro princípio constitucional esteja inerente ao direito de personalidade do indivíduo, permitindo-o a tutela da privacidade, liberdade, autonomia, dentre outros direitos basilares à pessoa humana.

Ainda, embasando-se na Constituição de 1988, os doutrinadores reconhecem a pessoa humana como integrante principal do âmbito jurídico:

> "Nessa trilha de raciocínio, repita-se à saciedade que o mais precioso valor da ordem jurídica brasileira, erigido como fundamental pela Constituição de 1988, e a dignidade humana, vinculando o conteúdo das regras acerca da personalidade jurídica. Assim, como consectário, impõe reconhecer a elevação do ser humano ao centro de todo o sistema jurídico, no sentido de que as normas são feitas para a pessoa e para a sua realização existencial, devendo garantir um mínimo de direitos fundamentais que sejam vocacionados para lhe proporcionar vida com dignidade.
>
> Enfim, o postulado fundamental da ordem jurídica brasileira e a dignidade humana, enfeixando todos os valores e direitos que podem ser reconhecidos à pessoa humana, englobando a afirmação da sua integridade física, psíquica e

[35] MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709.18). R. Dir. Gar. Fund., Vitória, V.19, n.3, p.159-180, set - dez 2018, p. 169.

[36] ROSENVALD, Nelson. FARIAS, Cristiano Chaves de Farias. Curso de Direito Civil: Parte Geral e LINDB. Ed. 16. Salvador: Ed. JusPodivm, 2018, p.180.

> intelectual, além de garantir a sua autonomia e livre desenvolvimento da personalidade".[37]

Também, inerente aos direitos de personalidade, como qualquer outro conceito jurídico, o direito à privacidade está vulnerável a modificações promovidas pelas mudanças sociais que ocorrem ao longo do tempo.

Inicialmente, via-se a proteção à privacidade como um direito a ser deixado só, ou seja, "*the right to be alone"*, no entanto, a contemporaneidade expandiu determinada concepção, incluindo a proteção e tutela de dados pessoais como ferramentas a garantir o direito à privacidade, visto que, atualmente, os dados apresentem predições do comportamento do indivíduo, suas preferências e, até mesmo, características da sua personalidade. Os dados pessoais representam a esfera privada do cidadão, por conseguinte, caso haja acesso ilícito a esses dados, atinge-se o direito à privacidade do cidadão.

Ainda, o direito à privacidade passa a ter um aspecto mais ativo, que não só determina o direito negativo de não ser molestado, mas também permite ao cidadão um controle sob a coleta e análise de seus dados e, por conseguinte, o exercício da autodeterminação informativa e da liberdade existencial.[38]

Assim, por meio do consentimento gradual e o dever informacional, a autodeterminação informacional pode ser o principal aspecto de solução para os infortúnios provocados pela exploração indevida de dados pessoais. Assim, deve-se criar uma tutela dinâmica a fim de permitir que a tecnologia tenha seu fluxo natural ao mesmo que os direitos da personalidade sejam preservados durante esse processo.

Isto posto, a chave para que esse cenário seja possível é a informação que, ao tornar a dinâmica mais equilibrada e transparente, permite a comunicação mais equilibrada e eficiente entre os cidadãos e quem está coletando seus dados.

Dado que a proteção de dados se relaciona diretamente com a intimidade, direito à informação e privacidade, como exemplificado acima, é evidente que, a sua presença na estrutura constitucional é inquestionável.

---

[37] Idem, p.180.

[38] MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709.18). R. Dir. Gar. Fund., Vitória, V.19, n.3, p.159-180, set - dez 2018, p. 173.

Tão logo, em reflexo a essa mudança de concepção, o Supremo Tribunal Federal, em 2020, proferiu decisão reconhecendo a proteção de dados como um direito fundamental. Isso ocorreu devido a Medida Provisória 954, que em um dos seus dispositivos, exigia que as empresas de telecomunicações compartilhassem dados pessoais dos usuários, como: nome, número de telefone, endereço, com o IBGE. Logo após a edição da determinada medida, o Conselho Federal da OAB e diversos partidos políticos ajuizaram Ações Diretas de Inconstitucionalidade a fim de declarar a inconstitucionalidade do regulamento.

Mesmo que a pandemia estivesse ocasionando situações adversas que precisassem de medidas mais precisas e intensas, a fim de controlar os danos causados, direitos fundamentais não podiam ser infringidos, causando mais problemas a uma população cuja situação já estava crítica.

Consoante a esse pensamento, a ministra Rosa Weber votou pela suspensão da Medida Provisória, sob a seguinte fundamentação:

> "Não se subestima a gravidade do cenário de urgência decorrente da crise sanitária nem a necessidade de formulação de políticas públicas que demandam dados específicos para o desenho dos diversos quadros de enfrentamento. O seu combate, todavia, não pode legitimar o atropelo de garantias fundamentais consagradas na Constituição."[39]

Ainda, evidenciou a sensibilidade de dados, que ao primeiro olhar podem parecer insignificantes, no entanto, ao serem cruzados com outras informações promovem informações muito significativas acerca do cidadão. Por conseguinte, o Ministro Luiz Fux destacou o caso da Cambridge Analytics, empresa processadora de dados alvo de escândalo e investigação que utilizava seu modelo de negócio para vender dados dos cidadãos para candidatos a cargos executivos no poder público na finalidade de prover informações determinantes a suas vitórias, lesando a democracia.

Atualmente, a proteção de dados encontra-se expressa no texto constitucional. Em 2022, foi incluído no artigo 5º o inciso LXXIX, acrescentando o direito à proteção de dados pessoais.

Considerada como direito fundamental autônomo na Carta de Direitos Fundamentais da União Europeia, Rodotà também destaca a proteção de dados como "uma ferramenta

[39] MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. STF reconhece direito fundamental à proteção de dados. Revista de Direito do Consumidor | vol. 130/2020 | p. 471 - 478 | Jul - Ago / 2020, p.3.

essencial para o livre desenvolvimento da personalidade" e destaca-a "como a soma de um conjunto de direitos que configuram a cidadania do novo milênio".[40]

Cria-se uma concepção de importância acerca dos dados pessoais, na qual a proteção desses torna-se imprescindível para que não só o direito à privacidade fique protegido, mas também que os direitos de personalidade dos cidadãos possam ser exercidos da maneira devida e viável.

Os dados representam as características privadas e públicas do indivíduo, originando predições que permitem a terceiros o conhecimento de suas preferências, personalidade, inclinações até análises sobre propensão à criminalidade, detectar sinais de doença, como depressão[41]. Dessa forma, o acesso ilícito a essas determinadas informações afeta absurdamente o direito da personalidade do indivíduo e imprescindem de regulação.

[40] MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709.18). R. Dir. Gar. Fund., Vitória, V.19, n.3, p.159-180, set - dez 2018, p. 171.

[41] FRAZÃO, Ana. TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Ed. Revistas dos Tribunais, 2019, p. 32.

3. CAPÍTULO III

a) O desenvolvimento de leis acerca da proteção de dados

Segundo Viktor Mayer-Schonberger[42], existem quatro gerações de desenvolvimento de leis. Na primeira, havia uma extrema centralização dos dados, ou seja, os grandes centros elaboradores ficavam responsáveis tanto pela coleta dos dados quanto pela sua análise. Ademais, a primeira fase de leis tinha como enfoque regular o processamento dos dados, dando mais destaque às questões tecnocráticas, sobre a informática do processo, sem que houvesse lugar para a discussão sobre a privacidade.

Isto posto, as leis eram restritas, concentrando o poder no Estado, visto que, impunham autorizações por órgãos estatais para a criação de banco de dados e de seu controle. Evidencia-se, assim, que o principal controlador do uso dos dados nesse período era o Estado.

No entanto, logo, essas leis são rapidamente ultrapassadas, pois, os centros de processamento foram aumentando consideravelmente, tornando inviável um sistema centralizado baseado em autorizações estatais.

Tem-se como representação do marco final da primeira fase a criação da lei alemã federal *Bundesdatenschutzgesetz* em 1917. O governo alemão executou uma coleta de dados da população a fim de que depois da análise desses, eles não só conseguissem ter uma informação concisa sobre a distribuição geográfica da população, como haviam justificado aos cidadãos, mas também, aplicar possíveis execuções administrativas.

Ao perceberem as intenções escondidas do governo e a falta de transparência desses acerca da finalidade do processamento dos dados, os cidadãos entraram com uma ação coletiva, que originou a lei supracitada e o conceito de autodeterminação informativa.

Isso ocorreu pois, ao terem seus dados solicitados, os cidadãos perceberam que a partir do processamento desses poderiam surgir óbices ao exercício pleno do direito à personalidade. O problema apresentado era muito mais complexo que a determinação da esfera da privacidade, pois, a questão apresentada não era se os dados eram públicos ou privados, e sim quais seriam as consequências aos indivíduos a partir da análise desses.

---

[42] DONEDA, D. (2011). A proteção dos dados pessoais como um direito fundamental. *Espaço Jurídico Journal of Law [EJJL]*, *12*(2), 91–108.

Em decisão, o Tribunal concordou que determinada ação poderia atingir a esfera de ação individual do cidadão, pois, ao fornecer seus dados a terceiros, o processamento iria prover um perfil completo sobre sua personalidade que seria compartilhado ilimitadamente sem que o indivíduo pudesse questionar a veracidade das informações apresentadas ou impedir o compartilhamento.

> "Tal utilização ampliaria a influência do Estado sobre o comportamento do indivíduo, que não seria mais capaz de tomar decisões livres em virtude "pressão psíquica de participação pública". Uma sociedade, "na qual os cidadãos não são mais capazes de saber quem sabe o que sobre eles, quando e em que situação", seria contrária ao direito à autodeterminação informativa, algo prejudicial tanto para a personalidade quanto para o bem comum de uma sociedade democrática."

Isto posto, o tribunal decidiu que, ainda que a lei do recenseamento não tivesse como finalidade catalogar cada cidadão, violaria a Lei Fundamental, dado que este deve ter o poder de tutelar os seus dados, por serem uma extensão da sua personalidade, por conseguinte, diretamente ligados ao direito de privacidade. Então, cria-se um novo direito fundamental, à autodeterminação informativa, a fim de abranger a evolução do direito de personalidade.

Surge, assim, o conceito de autodeterminação informativa, cujo qual o cidadão tem o poder e o direito de exercer a decisão acerca da coleta e análise de seus dados, a fim de proteger plenamente o direito de desenvolvimento de personalidade e dignidade do ser humano[43].

Então, no final da década de 70, inicia-se a segunda fase das leis de proteção de dados, que distintamente da primeira, coloca em mais evidência o aspecto da privacidade do indivíduo e não focando apenas no fenômeno computacional.

Consequência do descontentamento dos cidadãos acerca da utilização indevida de seus dados por terceiros e da falta de instrumentos disponíveis para a defesa de sua privacidade, essa nova era de proteção determina a privacidade e proteção de dados como uma liberdade negativa que devia ser exercida pelo próprio cidadão, o proprietário dos dados deveria ficar responsável pela defesa desses. Por conseguinte, foi criado instrumentos e meios para tutela a fim de que o cidadão conseguisse identificar utilizações indevidas de seus dados e defendê-los.

Entretanto, mais um problema foi identificado, dado que, com o passar do tempo, o fornecimento de dados tornou-se aspecto indispensável para a participação do âmbito social

[43] MENDES, Laura Schertel Ferreira. Autodeterminação informativa: a história de um conceito. Revista de Ciências Jurídicas Pensar. p.11.

pelo cidadão, por conseguinte, quando esse questionava a utilização de determinado dado, surgia um entroncamento em sua vida social, que o impossibilitava o fluxo de funcionamento ocorrer da maneira devida e o exclui do meio social.

Logo, surge a terceira fase que, diante dos problemas apresentados, abrangeu o âmbito de ação do cidadão, não limitando-o apenas à liberdade negativa de proteção e seus dados, mas também evidenciando a efetividade dessa liberdade e promovendo o devido exercício da autodeterminação efetiva. Porém, ainda que a mudança fosse bem colocada, colocar em prática a prerrogativa exigia custos econômicos e sociais, tornando-a um privilégio disponível a poucos. Para a devida efetivação pelos cidadãos, é imprescindível que todos tenham acesso aos instrumentos de tutela, criando um padrão coletivo de proteção, surge então a quarta geração de leis de proteção de dados.

Nesta, a fim de estabelecer uma isonomia na relação entre as entidades responsáveis pela coleta e análise de dados e os cidadãos que permita o exercício efetivo da autodeterminação informativa, as novas leis fortalecem o papel dos indivíduos nas determinadas relações e, paralelamente, diminui-se a função da decisão individual de autodeterminação informativa. Para uma efetiva proteção de determinadas modalidades de uso de dados, faz-se necessário uma proteção mais elevada, além da decisão individual do cidadão.

Além disso, na determinada era, a criação de regulações conexas, isto é, direcionadas a determinados setores do processamento de dados, e, criação e expansão de moldes de autoridades independentes.

b) O surgimento de legislações específicas diante das novas dinâmicas provocadas pela tecnologia e a criação de autoridades para a concretização da nova legislação

Tendo em vista o determinado cenário, surge a necessidade de criação de regulações com o objetivo exclusivo de proteger os dados pessoais.

Devido à influência da Convenção de 108 de 1980, é criada a GDPR, *General Data Protection Regulation*, lei que rege a proteção de dados pessoais na Europa. A partir dessa, determinou que toda empresa que exercer alguma atividade em território europeu deverá

tratar dados pessoais de maneira transparente e cautelosa, dado que o determinado regulamento estabeleceu a proteção desses dados como um direito fundamental[44].

Em que pese os cidadãos tivessem seus dados protegidos em território europeu, ao interagirem com economias estrangeiras, as empresas europeias teriam seus dados acessados por empresas estrangeiras, colocando os dados dos cidadãos europeus em risco em razão de grande parte do mundo ainda não ter consciência da relevância dos dados pessoais e sua necessidade de proteção.

Com isso, os países europeus sentiram a necessidade de exigir de outros países que criassem os seus respectivos dispositivos legislativos acerca da proteção de dados com a finalidade de dar mais destaque ao papel do titular dos dados e ao seu consentimento. Dessa forma, países, como o Brasil, foram impulsionados a criar sua legislação para proteger os dados pessoais de seus cidadãos.

E, ainda que já houvesse dispositivos dentro do ordenamento brasileiro que contemplasse direitos relacionados à proteção de dados, como o Habeas Data e o artigo 43 do Código de Defesa do Consumidor, a complexidade do cenário demanda uma regulação mais específica que complete as lacunas jurídicas.

Além disso, a participação do Brasil nas negociações do Mercosul, impulsionou a criação de uma lei voltada exclusivamente a proteção de dados pessoais, dado que havia um movimento de pressão entre os países integrantes para a formação de uma normal em comum entre os países integrantes do grupo comercial, o que não ocorreu, mas provocou a criação da lei no Brasil.

Consoante, em 2011, Doneda já destacava que a proteção de dados não era exercida de maneira efetiva por meio dos dispositivos já existentes, visto que, como o *habeas data*, ao perfil desses estarem muito mais direcionados em estabelecer liberdades negativas, a tutela de dados se tornava ineficaz[45].

Como disposto no artigo 5 incisos X, XII, destaca-se que apenas a comunicação dos dados era regulada, ocasionando uma grande permissividade em relação aos dados pessoais.

---

[44] ANDRÉA, Gianfranco Faggin Mastro. ARQUITE, Higor Roberto Leite. Proteção dos Dados Pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil.Revista de Direito Constitucional e Internacional | vol. 121/2020 | p. 115 - 139 | Set - Out / 2020, p. 5.

[45] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental, p. 104.

Consoante a esse pensamento, havia decisões do STF declarando que não havia infração à privacidade em casos "apenas" de armazenamento de dados de terceiros[46].

Assim, além do escândalo da Cambridge Analytica e a entrada em vigor do Regulamento Geral de Proteção de Dados, destaca-se também tanto intuito de efetivar a ingressão a Organização para a Cooperação e Desenvolvimento Econômico, cujo a regulamentação de dados pessoais era imprescindível, quanto o processo de aprovação da Lei Geral do Cadastro Positivo, impulsionam a aprovação da lei.

Ainda que tivessem uma legislação considerável acerca da proteção de dados, como o Código de Defesa do Consumidor e o Marco Civil da Internet, esses não conseguem preencher todas as lacunas criadas pelo avanço da tecnologia, sendo imprescindível a criação de uma lei voltada unicamente para determinada questão.

A partir disso, anos depois, no Brasil, inspirada na GDPR, iniciou-se o processo legislativo da Lei Geral de Proteção de Dados, Lei 13.709, a fim de tutelar a proteção de dados, tanto sua comunicação quanto seu armazenamento e, por consequência, o direito à personalidade, a privacidade, autodeterminação informativa, dentre outros[47]. Dessa forma, o exercício da autonomia informativa permite aos cidadãos que possam ter o devido controle sobre seus dados, com o objetivo de frear as disfunções do mercado de dados atual[48].

Iniciada como um projeto multisetorial, a Lei de Câmera nº 53 foi impulsionada a se tornar a lei nº 13.709 de 2018 após impulso inicial do Manifesto pela Aprovação da Lei de Proteção de Dados Pessoais, ocasionando um marco para a legislação Brasileira.

No entanto, a LGPD foi uma das primeiras precursoras acerca do tema de tecnologia e apresenta diversas concepções que ainda não são comuns a maior parte da sociedade, fazendo com que leis de proteção de dados sejam uma espécie de Leviatã, como destaca Gianfranco em seu texto:

> "Sua abrangência, ambição legislativa e maturidade conceitual corroboram a ideia de que esse é um autêntico regulamento-modelo, no qual diversas outras iniciativas nacionais, regionais e intracomunitárias também serão espelhadas em busca de padrões normativos uniformes na proteção de dados pessoais. Não seria exagero afirmar que o GDPR nasce como um "monstro normativo", um Leviatã a induzir

[46] DONEDA, Danilo. A proteção dos dados pessoais como um direito fundamental, p. 105.
[47] MULHOLLAND, Caitlin Sampaio. Dados Pessoais Sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709.18). R. Dir. Gar. Fund., Vitória, V.19, n.3, p.159-180, set - dez 2018, p. 162.
[48] FRAZÃO, Ana. TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Ed. Revistas dos Tribunais, 2019, p. 31.

> condutas de conformidade (compliance) por parte de agentes nas esferas públicas e privada no campo da proteção de dados e especialmente identificáveis nos ambientes informacional e digital."[49]

Isto posto, em que pese tenha ocorrido uma mudança legislativa ao redor da proteção de dados pessoais, é evidente que essa questão segue não sendo uma prioridade para as autoridades públicas:

> "a revolução dos dados é até agora primeiramente técnica: o poder dos dados para classificar, categorizar e intervir ainda não foi explicitamente vinculado a uma agenda de justiça social pelas agências e autoridades que coletam, geram e utilizam dados. Tampouco existe um nível de conscientização elevado entre agentes de políticas públicas sobre como as novas tecnologias orientadas por danos não podem ser neutras em termos de acesso, utilização ou impactos, conforme demonstram pesquisas sobre este fenômeno (Dalton et al., 2016)"

Apesar de tudo, é importante destacar que a LGPD resistiu a diversos contratempos. Sua vigência não só postergada algumas vezes como também segmentada, fazendo que a lei viesse a vigorar "aos poucos". Com isso, a LGPD entrou em vigor sem que um dos órgãos mais importantes, a Autoridade Nacional de Proteção de Dados, estivesse formado e em funcionamento.

ANPD é a autoridade responsável por ajudar a concretizar a cultura social de proteção de dados pessoais, por meio do estabelecimento de diretrizes, possibilitando diálogos entre os órgãos de cooperação, entre outras funções. Dessa forma, muito além de aplicar sanções, a ANPD tem como papel principal viabilizar a consolidação LGPD, tornando-a um instituto imbuído na mentalidade dos cidadãos brasileiros, a fim de que estes a coloquem em prática e consigam proteger seus dados de forma efetiva.

Concomitantemente, criou-se conjuntamente o Conselho Nacional de Proteção de Dados (CNPD), a fim de, como órgão consultivo, auxiliar a ANPD nas questões procedimentais, como realizar estudos, estabelecer diretrizes, entre outros, materializando a proteção de dados conjuntamente com outros órgãos e o órgão regulador principal. Em cooperação com outros órgãos, a ANPD deverá exercer a correlação, isto é, o equilíbrio entre um processo estatal e privado.

No entanto, mesmo que a estrutura estabelecida pela LGPD seja de descentralizar e não estabelecer todo o poder em uma única autoridade, ainda sim é importante que a agência

[49] ANDRÉA, Gianfranco Faggin Mastro. ARQUITE, Higor Roberto Leite. Proteção dos Dados Pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil.Revista de Direito Constitucional e Internacional | vol. 121/2020 | p. 115 - 139 | Set - Out / 2020, p. 6.

reguladora principal seja vista como uma autoridade forte, delegando as funções de forma devida.

A relevância se intensifica em razão da falta de conscientização do brasileiro em relação aos seus dados pessoais que torna a introdução da LGPD mais difícil.

Diferentemente do Brasil, a Europa tem uma cultura social acerca da proteção de dados muito forte, em razão do histórico existente de utilização dos dados pessoais sem o consentimento dos cidadãos. Para exemplificar, um caso bastante emblemático foi o da decisão da Corte Constitucional Alemã sobre a Lei do Censo de 1983, pois abriu os olhos da sociedade europeia acerca da importância dos dados pessoais e de como sua proteção é fundamental.

Em vista disso, o processo de conscientização da GDPR na sociedade europeia não foi tão árduo e, por consequência, a efetividade da lei foi alcançada mais facilmente. Não basta a promulgação da norma, é necessária a sua efetiva aplicação para que a sociedade a veja como um suporte a seus direitos.

Por conseguinte, devido a LGPD introduzir novos conceitos e uma nova concepção acerca do uso de dados pessoais, conclui-se que a introdução de determinada norma pode ser mais difícil, fazendo com que institutos como a ANPD tenha um papel importante para a consolidação da LGPD.

Por muitas vezes, quando países empregam normas originadas em países de primeiro mundo a fim de tentar se equivaler a estes de forma rápida e econômica, os atos de criação da lei e promulgação já são vistos como uma conquista, no entanto, não necessariamente esse dispositivo vai se tornar uma cultura social, já que a recepção da população em relação a lei pode ser distinta devido ao histórico de contato dos indivíduos com determinado tema. Para ilustrar o cenário com mais propriedade, cita-se o estudo de Martin De Jong, Konstantinos Lalenis e Virginie Mamadouh: "*The Theory and Practice of Institutional Transplantation*".

De acordo com essa teoria, ao uma norma ser criada baseada em uma legislação estrangeira, ocorre um "transplante institucional", isto é, da mesma forma que um órgão de uma pessoa pode ser transplantado em outro, uma norma também pode ser transplantada em outro lugar diverso daquele de origem.

Entretanto, o estudo também levanta as consequências derivadas deste ato, pois, por não se ter mesmo histórico que o país de origem da determinada legislação, não necessariamente a simples transplantação irá surgir efeito. Em que pese, o procedimento de transplante ser feito da maneira correta, é importante que haja um acompanhamento posterior a fim de que o corpo não reaja de forma negativa e rejeite o novo órgão.

Assim, se aplicarmos o mesmo pensamento para o procedimento de transplante institucional, no qual a sociedade é o corpo humano e, a lei, o órgão transplantado, verifica-se a relevância da continuidade do trabalho de introdução da nova norma, moldando, simultaneamente, por meio de instrumentos como a ANPD, a legislação e a sociedade para que o dispositivo se torne realmente efetivo.

Diante dessa situação a ANPD se destaca, no cenário da LGPD, em conjunto com outros operadores. A Autoridade deve ser o meio para que a lei realmente se consolide e seja utilizada pela população como suporte de seus direitos, como ocorreu com o Código do Consumidor.

Para atingir a consolidação atual, o Código do Consumidor precisou ser extremamente trabalhado e disseminado na mentalidade da população brasileira, pois apenas a criação da lei não bastava, foi necessário dar um estímulo à conscientização de todas as partes dessa relação. Assim, conjuntamente com o CDC, foi criado o Sistema Estadual de Defesa do Consumidor, também conhecido como Procon, sendo uma das suas funções educar a população acerca de seus direitos e deveres dentro de uma relação de consumo.

No entanto, ressalta-se que a função da ANPD não deve ser apenas resumir a conscientização dos indivíduos, mas também das instituições públicas e privadas.

Além disso, o avanço da utilização dos dados pessoais e a criação da LGPD não deve apenas impulsionar mudanças aos indivíduos como também as empresas e instituições. Isto se deve porque para estar ao patamar dos países desenvolvidos, o país deve acompanhar as mudanças mundiais e é evidente que o mercado de dados já ocasionou diversas mudanças não só no meio social como também no econômico.

Países europeus já estão muito à frente no mercado de dados devido à preocupação acerca do assunto estar presente há muito tempo, no entanto, ainda que o Brasil tenha muito que andar para estar no mesmo patamar que esses países, é necessário que haja um esforço efetivo para que o brasil se torne um país competitivo dentro do mercado de dados

internacional e, por conseguinte, mais desenvolvido, por isso a necessidade de uma legislação bem estruturada e uma aplicação efetiva.

4. CAPÍTULO IV

a) A importância da aplicação efetiva da LGPD

O surgimento da LGPD permitiu que houvesse uma maior simetria legislativa acerca da proteção de dados pessoais no país, visto que, antes da sua criação, as questões relacionadas aos dados eram regidas por leis provenientes de diferentes regulamentos, provocando uma insegurança jurídica e legislativa, conforme fala de Bioni[50]:

> "Era uma verdadeira colcha de retalhos que não cobria setores importantes da economia e, dentro aqueles cobertos, não havia uniformidade em seu regramento. Essa assimetria gerava insegurança para que os mais diversos setores produtivos trocassem dados entre si com o objetivo de desenvolver novos modelos de negócios, bem como desestimulava a formulação de políticas e parcerias público-privada."

A Lei Geral permitiu a existência de um cenário orgânico no qual os direitos e deveres foram devidamente delimitados, estabelecendo uma maior segurança jurídica à sociedade brasileira.

Torna-se imprescindível uma infraestrutura forte e eficiente para pôr o regulamento em prática e torná-lo útil a todos aos cidadãos e às instituições financeiras, bem como para consolidar o papel das autoridades como um dos requisitos essenciais para um sistema legislativo eficiente.

Apenas a legislação não basta, sendo necessário um sistema de aplicação e fiscalização eficaz.

É incontestável a necessidade de autoridades eficientes para concretizar a nova legislação, pois, além de permitirem uma maior consolidação, também permitem uma fiscalização uniforme, provocando uma maior integração econômica da sociedade com um todo.

Uma legislação eficiente e autoridades presentes são o caminho para que o Brasil integre o grupo de países cujo nível de proteção de dados é considerado adequado para transferência internacional de dados. E, ainda que existam outros meios para participar da transferência internacional, as opções alternativas são muito mais caras de um ponto de vista operacional do que a aplicação efetiva da legislação.

---

[50] BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites de consentimento. Ed 1. Rio de Janeiro: Forense, 2019, p.60.

Percebe-se que a consolidação eficiente da infraestrutura legal e institucional são essenciais para o Brasil se tornar competitivo dentro do mercado de dados. E, diferente do que muitos pensam, esse caminho deve ser visto como um investimento para a economia brasileira.

A LGDP não deve ser vista como uma forma de dificultar a fluidez da economia de dados, mas sim o suporte necessário para que ela funcione de forma eficiente e segura, conforme BIONI afirma[51]:

> "Todo o sistema gira em torno da lógica em se criar uma trilha auditável do dado, pelo qual o cidadão e os demais agentes econômicos enxerguem todo o seu ciclo de vida e principalmente a sua repercussão nas atividades econômicas e relações sociais que fazem parte. A nova lei não veio para travar o fluxo informacional, mas, muito pelo contrário, estimulá-lo dentro de uma lógica de sustentabilidade entre quem produz essa matéria prima e quem a explora."

Deve haver uma mudança de mentalidade das empresas, para que se organizem de acordo com o novo ordenamento.

Caso haja um maior investimento por parte do mercado de dados com a finalidade de adequar seu funcionamento à infraestrutura legal, haverá a criação de novos meios de trabalho, como produtos e serviços, novos modelos de negócios, geração de valor de avaliação de riscos regulatórios[52].

Consoante a esse pensamento, as empresas europeias já agem de acordo com o previsto em lei, engajando-se em estar à frente das outras empresas, pois, assim, valorizam seus serviços em comparação com as outras empresas, retardatárias.[53] As empresas pararam de ir contra a legislação e a utilizaram para tornar o mercado mais fluido e estratégico, passando a ver a regulação como um caminho de oportunidades, como Bioni confirma[54]:

> "Quem compreender e catalisar o processo de conformidade como um dos pilares de um plano estratégico de inovação, coloca ordem em casa e colherá frutos que extrapolam o mero estado de compliance. É um efeito secundário e desejado da nova regulação, o que os economistas costumam chamar de externalidade positiva."

Em sua criação, a regulação de dados adotou uma abordagem de equilíbrio entre os direitos e deveres do processamento de dados para com os cidadãos. Assim, na década de 80

---

[51] BIONI, Bruno Ricardo. Regular de Dados é uma janela de oportunidade. A Construção multissetorial da LGPD: histórias e aprendizados. Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF, p.70

[52] Idem, p.71.

[53] Idem, p.71.

[54] Idem, p.72.

foi criada a *Fair Information Practice Principles (FIPPs)*, um conjunto de princípios que rege as leis de proteção de dados cuja criação e permitiu tanto a expansão dos ideais de proteção a nível internacional quanto estabeleceu um equilíbrio entre a proteção dos direitos fundamentais dos cidadãos e o estímulo ao desenvolvido econômico (BIONI, p.75).

Nesse sentido, a atenção com a LGPD deve ser ainda maior, dado que a lei abrange diversos aspectos da sociedade além da internet, como também as relações trabalhistas e até o vínculo entre o cidadão e o poder público. Assim, a legislação impacta muito mais do que o código de defesa do consumidor (BIONI, p.76).

Soma-se isso ao fator de desigualdade social, a atuação das autoridades torna-se imprescindível. Diferentemente dos cidadãos de classes sociais mais altas, os mais pobres são tanto os mais vulneráveis aos abusos da coleta de dados quanto os que menos têm acesso à proteção de seus direitos[55].

Como destacado acima, os dados coletados podem ser reunidos e interseccionados, interligando diversas características, como: etnia, gênero, raça, entre outros, tornando-os em sujeitos de direitos, esses dados são utilizados por agentes decisórios e a interferência desses irá depender da qual grupo social esse indivíduo é pertencente. Dessa forma, por exemplo, um adolescente de baixa renda não tem as mesmas oportunidades para resistir a vigilância que um adulto de classe alta[56].

Isto posto, e claro que ainda a LGPD sendo um divisor de águas para a proteção de dados, estabelecendo um regramento aos cidadãos para a tutela de seus direitos, a lei por si só não é o suficiente para conter os vícios existentes acerca do capitalismo da vigilância, visto que seus atuantes se encontram em posições dominantes no mercado atual[57]. Torna-se importante que os dispositivos já existentes trabalhem em conjunto e consoantes a LGPD.

Por conseguinte, a grandiosidade desse impacto exige que ocorra uma transformação da sociedade como um todo para adaptar seu funcionamento de acordo com as mudanças e avanços estabelecidas pela LGPD. Dessa forma, torna-se primordial que a sociedade em geral veja a necessidade dessas mudanças e suas repercussões nas relações sociais e econômicas[58].

---

[55] TAYLOR, Linnet. O que é justiça de dados? Conectando direitos digitais e liberdades globalmente.Construindo caminhos para a justiça de dados no Brasil: o papel das defensorias públicas na proteção de dados pessoais. 1.ed. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. PDF, p. 19.
[56] Idem, p.20.
[57] FRAZÃO, Ana. TEPEDINO, Gustavo. Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro. São Paulo: Ed. Revistas dos Tribunais, 2019, p. 48
[58] Idem,p.78.

A título de exemplo, o Código do Consumidor levou décadas até ser estabelecido de forma concreta entre os cidadãos brasileiro e as empresas. As leis estabeleceram mais limites às empresas, diante de seus clientes, lado mais hipossuficiente da relação, tornando o mercado de consumo mais "civilizado" e mais seguro para os consumidores.

b) A LGPD como um instrumento de mudança socioeconômico

A LGPD é uma legislação criada em detrimento do tratamento de dados pessoais, abrangendo pessoas físicas ou jurídicas do meio privado ou público. Todo documento ou informação que contenha algum dado pessoal estará protegido por ela, ainda que em estado físico ou meio digital.

Em seu artigo primeiro, a LGPD afirma:

> **Art. 1°** 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.

Com objetivo de atingir seu objetivo, a LGPD definiu determinados aspectos a serem seguidos pela sociedade como um todo que não só tem o objetivo de estabelecer equilibrio da dinâmica economica atual, como tambem tem como enfoque proteger os direitos fundamentais de liberdade e de privacidade, além do livre desenvolvimento da personalidade da pessoa natural.

Como Rony Vainzof destaca:

> "Assim, a LGPD busca a proteção de direitos e garantias fundamentais da pessoa natural, equilibradamente, mediante a harmonização e atualização de conceitos de modo a mitigar riscos e estabelecer regras bem definidas sobre o tratamento de dados pessoais."[59]

Assim, a lei em questão baseia-se no conceito de "*privacy by design*" que consiste na utilização da tecnologia como mecanismo de moldar comportamentos sociais, sendo uma infraestrutura informacional orquestrando os comportamentos dos indivíduos[60].

---

[59] BORELLI, Alessandra. GUTIERREZ, Andriei. Lei Geral de Proteção de Dados. Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.25.

[60] BIONI, Bruno Ricardo. ZANATTA, Rafael A. F. A infraestrutura jurídica da economia dos dados: dos princípios de justiça às leis de dados pessoais. A Construção multissetorial da LGPD: histórias e aprendizados. Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDFp.112

Em seu sexto artigo, a LGPD estabelece medidas para prevenir danos e direcioná-las como missão para os controladores e operadores e, ainda que não exista uma menção explícita acerca da "*privacy by design*", é bastante evidente que a legislação deixa a sua presença subentendida.

Além disso, para guiar o tratamento de dados, surgem as bases legais que consistem em fatores concessórios do tratamento, sendo um deles o legítimo interesse, que vai ter sua aplicação guiada por diversos princípios, como o da boa-fé e o da transparência.

Isso se deu em razão da Fair Information Practice Principles (FIPPs), conjunto de princípios determinados para a aplicação do tratamento de dados, como discorre Vainzof:

> "Os princípios nelas estabelecidos, como transparência, finalidade,necessidade, proporcionalidade, qualidade, livre acesso e segurança formam a espinha dorsal de inúmeras normas existentes atualmente, como o GDPR, que sucedeu a Diretiva 95/46, e a LGPD, sendo importante ressaltar que os princípios deverão ser cumpridos, independentemente das bases legais para o tratamento de dados pessoais."[61]

Ao estabelecer direitos e deveres, o legítimo interesse exige uma ponderação maior, dado que não vai estar vinculado a uma finalidade *a priori* e demanda a presença de finalidade a cada situação de tratamento. Tal determinação tem como intuito exigir que o operador, ao tratar os dados, delimite mais seu interesse a fim de evitar o tratamento excessivo de dados, processando mais do que o necessário para o determinado objetivo.

Inserido na sessão de dispositivos preliminares, apresentado no artigo 6 da LGPD, o princípio da boa-fé faz parte do grupo de princípios direcionadores do legítimo interesse e orientadores da normativa de todos os outros dispositivos presentes na lei.

A sua inclusão no texto legislativo vincula conceitos jurídicos novos e indeterminados da nova legislação a um princípio bastante tradicional no âmbito jurídico brasileiro, o que é essencial, dado que, as discussões acerca da regulação dos avanços da tecnologia precisam de um direcionamento ético (BIONI, p.221).

O princípio da boa-fé vai demonstrar a tentativa do legislador em evitar o transplante legal inadequado do conceito de legítimo interesse europeu, pois permite um debate sobre os novos conceitos jurídicos, modulando-os.

---

[61] BORELLI, Alessandra. GUTIERREZ, Andriei. Lei Geral de Proteção de Dados. Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 127.

Ainda, dentre os princípios norteadores do legítimo interesse, os três primeiros: finalidade, adequação e necessidade, que podem ser considerados conexos, e quando aplicados conjuntamente ao princípio da transparência formam o cerne principal da legislação.

> **Art. 6º** As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> **I** - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> **II** - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> **III** - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

O princípio da finalidade permite ao titular o conhecimento prévio da demilitação e os propositos dos tratatamento de seus dados, devendo o motivo da coleta ser compatível com o objetivo final do tratamento, como realça Doneda.[62]

Conforme Vainzof:

> "A sua utilização sempre estará vinculada ao motivo que fundamentou essa coleta, nascendo uma ligação entre a informação e a sua origem, vinculando-a ao fim de sua coleta, de modo que esta deva ser levada em consideração em qualquer tratamento posterior. Como o dado pessoal é expressão direta da personalidade do indivíduo, nunca perde seu elo com este, pois sua utilização pode refletir diretamente para o seu titular."[63]

Vinculado ao princípio da finalidade, o princípio da adequação estebele que o tratamento de dados deve ser compatível às finalidades informadas ao titular. Já o princípio da necessidade enfatiza a necessidade de delimitação do tratamento, ou seja, devem ser coletados e analisados apenas os dados pertinentes à finalidade estabelecida. Logo, estabelece-se um prazo e conservação, obrigando o controlador a sempre revisar o banco de dados e descartar dados que não estão mais alinhados à necessidade do tratamento.

Alinhado a esse pensamento, já se criam algumas jurisprudências, como a seguir:

---

[62] Idem, p. 128.
[63] Idem, p. 128.

> "O já citado caso julgado pelo STJ menciona expressamente o princípio da minimização dos dados do GDPR para declarar abusiva e ilegal cláusula prevista em contrato de prestação de serviços de cartão de crédito, que autoriza o banco contratante a compartilhar dados dos consumidores com outras entidades financeiras, sem que seja dada opção de discordar daquele compartilhamento."[64]

Leonardo Roscoe Bessa afirma[65]:

> "se pode ser verdadeiro que, sob a ótica econômica, quanto mais informações, melhor a avaliação de crédito (more is better), para o direito, para proteção jurídica da privacidade, é fundamental restringir, tanto no tempo, como na qualidade e quantidade, as informações que circulam pelos bancos de dados de proteção ao crédito. A primeira forma de limitar a qualidade da informação que circula em arquivos de consumo é exigir que ela esteja vinculada ao propósito específico do banco de dados. Os dados coletados devem ser visivelmente úteis para os objetivos específicos do arquivo. Se não atenderem a esse pressuposto, a coleta e o tratamento da informação devem ser considerados ilegais, ilegítimos e ofensivos à privacidade (art. 5°, X, da CF). […] De fato, para conferir significado mínimo à inviolabilidade da privacidade, prevista tanto na Constituição Federal (art. 5°, X) como no Código Civil (art. 21), há que ser estabelecidas restrições positivas. Não se cuida de desconsiderar a possibilidade de restrição ou conformação de direito fundamental, mas do cuidado em preservar o núcleo essencial do direito. É imprescindível, no âmbito da moderna concepção de proteção de dados, limitar tanto o conteúdo como a quantidade de informação que é tratada pelas entidades de proteção ao crédito."

Conjuntamente, destaca-se o princípio da transparência, presente no artigo 6, inciso VI e artigo 10, parágrafo segundo.

> **Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:**
>
> **VI** - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> **Art. 10. O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:**
>
> I - apoio e promoção de atividades do controlador; e
>
> II - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.
>
> § 1º Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.

[64] Idem, p. 135.
[65] Idem, p. 136.

> **§ 2º O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.**
>
> § 3º A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Assim, o princípio tem como intuito mitigar a possibilidade de desequilíbrio dentro da relação entre o titular dos dados e o controlador, fazendo parte do teste de balanceamento do legítimo interesse após a ponderação de interesse.

Sendo essencial para a tutela dos direitos fundamentais, o princípio da transparência permite ao titular do de dados o acesso ao conhecimento acerca do tratamento, podendo refletir de forma consciente sobre o acesso aos seus dados pessoais.

Vainzof afirma:

> "O titular dos dados carece da ampla informação sobre o tratamento dos seus dados para que consiga enxergar, cristalinamente, a legalidade, a legitimidade e a segurança do tratamento de acordo com o seu propósito, adequação e necessidade. Assim, terá condições para refletir sobre o tratamento e tomar decisões de acordo com os seus direitos."[66]

E, ainda que possa haver a relativização do princípio, a sua existência é imprescindível para o tratamento de dados correto, pois incentiva a entrega espontânea de informações importantes ao titular dos dados, isto é, informações explícitas e claras acerca dos dados utilizados e analisados vão ser comunicadas ao titular e, também, dependendo da situação, a grupos de interesse e até a autoridade nacional de dados, sem a necessidade de requisição dos mesmos[67].

Isso ocorre, pois, esse não protege apenas interesses privados como também coletivos, como a dignidade humana e a publicidade. E, como mencionado anteriormente, o tratamento indevido de dados pode ocasionar sérios danos sociais e individuais, tornando práticas de tratamento, como a transparência, imprescindíveis.

Em consonância com esse pensamento, Bioni afirma:

> "Há casos em que o tratamento abusivo de dados leva a violações de direitos afetos a todo um segmento populacional, sendo conhecidas as situações de discriminação por raça, gênero e perfil socioeconômico em virtude de usos abusivos de dados pessoais.

---

[66] Idem, p. 139.

[67] BIONI, Bruno Ricardo. KITAYAMA, Marina.Colocando em movimento o legítimo interesse. A Construção multissetorial da LGPD: histórias e aprendizados. Proteção de dados: contexto, narrativas e elementos fundantes. São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF, p.229.

> A transparência ativa das empresas desempenha também um papel de responsabilidade social, sujeitando suas próprias práticas à apreciação pública, de um lado, e criando uma cultura que padroniza essa atitude nos mercados, de outro."

Sendo assim, ao ser comunicado sobre as medidas de tratamento, o titular discorde de alguma, o mesmo tem o direito de oposição (*opt-out*), que consiste na dispensa de consentimento, ou seja, na oposição ao tratamento realizado, conforme o artigo 18, parágrafo segundo da LGPD. No entanto, destaca-se que esse direito não é absoluto, sendo o descumprimento da lei requisito para a sua aplicação, não podendo ser exercido sem a condição necessária[68].

Conforme destaca o seguinte trecho:

> "A mudança cultural é enorme, especialmente em países, como o Brasil, que não guardam laços históricos com a tradição de proteção de dados. É comum procedimentos, por ausência de percepção dos riscos, comodidade e custos envolvidos, de coleta massiva de dados pessoais para depois se pensar nos possíveis usos, o que é diametralmente oposto ao que o princípio em estudo comanda."[69]

Distintamente das outras legislações já existentes no ordenamento jurídico, a LGPD atua de uma maneira específica. Assim, por exemplo, ainda que o Marco Civil já determinasse a necessidade de alguns registros por parte dos provedores de conexão e aplicação, tendo como objetivo a segurança da informação, a LGPD determina a imprescindibilidade dos registros tendo como finalidade um motivo maior, cultivar a cultura de responsabilidade no uso e tratamento de dados.

Por conseguinte, segundo a LGPD, é obrigatório o registro de todo o processo de tratamento de dados, desde a coleta até o descarte, isto porque, a intenção não é só a segurança da informação, mas que, ao registrar os processos realizados com os dados, criar uma consciência nos agentes econômicos acerca das atividades realizadas durante o tratamento, fazendo-os refletir e tornar o processo mais correto.

Além dos fatores apresentados, também se destaca outros aspectos como a *accountability*. Esse mecanismo estabelece a criação de relatórios de impacto à proteção de dados pessoais a fim de que o controlador possa tomar decisões acerca da cadeia de tratamento com mais propriedade.

Assim, da mesma forma que a GRPD, a LGPD estabelece em seu corpo legislativo a necessidade de relatórios de impacto, no entanto, diferente da legislação europeia, o

[68] Idem, p.233.
[69] BORELLI, Alessandra. GUTIERREZ, Andriei. Lei Geral de Proteção de Dados. Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.452.

dispositivo brasileiro não codificou todo o procedimento de criação do relatório, tarefa que ficou estabelecida a ANPD. Dessa forma, no Brasil, o relatório não é uma obrigação, mas sim uma possibilidade.

Ainda, além da diferença normativa, há também diferenças nos aspectos culturais de aplicação de determinado mecanismo que pode afetar diretamente na efetividade em território brasileiro, pois, a Europa tem uma cultura regulatória bem mais transparente e colaborativa que a brasileira. No entanto, ainda que haja a diferença cultural e histórica dos países europeus e dos Estados Unidos em relação ao Brasil, nada o impede de trabalhar nos mecanismos apresentados a fim de tornar a LGPD mais fluida e enraizada ao funcionamento da sociedade.

Dessa forma, para a LGPD pode alcançar um equilíbrio entre seus objetivos- proteção ao direito dos titulares dos dados e o desenvolvimento econômico- foi necessário estabelecer diretrizes específicas acerca do legítimo interesse a fim de permitir a criação de direito de manipulação de dados por parte do controlador ou de terceiros, cumpridos os requisitos estabelecidos por lei.

A partir disso, é necessário destacar o conceito correto de legítimo interesse e diferenciá-lo do conceito de finalidade. Segundo o artigo 29 do Grupo de Trabalho, determinou finalidade como o propósito específico da ação, enquanto o interesse consiste em algo valoroso mais amplo, como, por exemplo, a garantia de segurança de determinado grupo. E, o legítimo é a consonância com as leis, deve estar de acordo com o determinado por lei e, também, estar relacionado a uma situação concreta.

Dessa forma, o artigo 10 da LGPD estabelece requisitos cumulativos:

> **Art. 10.** O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a:
>
> **I** - apoio e promoção de atividades do controlador; e
>
> **II** - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei.

> **§ 1º** Quando o tratamento for baseado no legítimo interesse do controlador, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados.
>
> **§ 2º** O controlador deverá adotar medidas para garantir a transparência do tratamento de dados baseado em seu legítimo interesse.
>
> **§ 3º** A autoridade nacional poderá solicitar ao controlador relatório de impacto à proteção de dados pessoais, quando o tratamento tiver como fundamento seu interesse legítimo, observados os segredos comercial e industrial.

Percebe-se que o legislador apresentou um rol exemplificativo, permitindo uma interpretação mais aberta do conceito, bem como uma adaptação a diversas situações que possam vir a existir nas experiências concretas.

Ocorre também que esses deveres não estão vinculados apenas ao controlador, mas também, a terceiro. Isso ocorre pois o controlador pode fazer tratamento por determinações de terceiros, ou seja, que não são baseadas em seu próprio interesse.

E, tanto o parágrafo primeiro quanto o segundo interligam o legítimo interesse aos princípios da adequação, necessidade e transparência.

No mais, ainda que diversos aspectos direcionadores já estejam definidos na Lei, há algumas determinações que só podem ser estabelecidas pela ANPD. Como Gutierrez afirma, a LGPD é uma carta principiológica, logo, traz uma indicação que será regulamentada pela ANPD.

Por exemplo, no artigo 10 da LGPD, não esclarece se as regras de legítimo interesse também vão abranger microempresas e empresas de pequeno porte, cabendo à ANPD a tarefa de delimitar essa abrangência por meio de uma regulação específica.[70] Assim, demonstra-se claramente a necessidade da autoridade se tornar um instituto forte e ativo, mesmo não exercendo um poder centralizado.

c) O papel da ANPD no processo de consolidação da LGPD

A ANPD, como Autoridade Nacional de Proteção de Dados, tem uma grande responsabilidade em assumir um papel de destaque na conscientização da Lei Geral de

[70] BIONI, Bruno Ricardo. **A Construção multissetorial da LGPD: histórias e aprendizados. Proteção de dados: contexto, narrativas e elementos fundantes.** São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF, p. 241.

Proteção de Dados. Ainda que o intuito de sua criação não seja centralizar todas as tarefas, a ANPD pode e deve guiar tanto as autoridades públicas e privadas quanto a população a fim de que todos se tornem cientes da dinâmica socioeconômica atual e possam se posicionar acerca da proteção de dados. Dessa forma, a ANPD deve ser uma ferramenta para que a justiça de dados seja alcançada por todos.

Segundo Andriei Gutierrez:

> "Uma sociedade na qual os dados assumem importância crescente precisa de regras claras e maior transparência sobre a maneira como eles são coletados, armazenados, tratados, compartilhados e até descartados. Regras, quando equilibradas, trazem previsibilidade para os setores produtivos e confiança para os cidadãos e consumidores. E a despeito de críticas pontuais que possa receber, a LGPD traz essa confiança e previsibilidade permitindo que a transformação digital brasileira avance de maneira sustentável.
>
> Tão importante quanto a existência de leis e regulamentações é a maneira institucional pela qual estas se farão respeitadas. E aqui chegamos na Autoridade Nacional de Proteção de Dados Pessoais (ANPD).
>
> [...] a criação da ANPD é um passo importante e essencial para a efetiva garantia à proteção dos dados pessoais assim como para a segurança jurídica para organizações, sejam elas públicas ou privadas. Dada a relevância desse papel, é também relevante que, além da autonomia técnica e decisória, a ANPD também desfrute de autonomia funcional, financeira e administrativa."[71]

As autoridades administrativas independentes são um recurso bastante utilizado por Governos a fim de atualizar sociedades diante de novos marcos regulatórios que apresentam obstáculos para concretização, como é o caso da Lei Geral de Proteção de Dados Pessoais[72]. Consoante a esse pensamento, a Carta de Direitos Fundamentais da União Europeia de 2000 indica a imprescindibilidade da autoridade de fiscalização como um fator fundamental do direito fundamental à proteção de dados pessoais. Até mesmo países que não apresentam uma lei geral de proteção de dados, apresentam órgãos fiscalizadores, como é o caso dos Estados Unidos, que tem a FTC (Federal Trade Commission)[73].

Dessa forma, dentre as funções exercidas pelas autoridades independentes destaca-se o de estreitamento da relação dos âmbitos do setor público e privado com a população. Isso ocorre, pois, as autoridades se dedicam exclusivamente a se especializar para atender as demandas provocadas por singularidades da nova dinâmica social, promovendo a defesa dos

[71] BORELLI, Alessandra. GUTIERREZ, Andriei. Lei Geral de Proteção de Dados. Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p.443.
[72] DONEDA, Danilo. Da privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados. 2 ed. São Paulo: Thomson Reuters Brasil, 2020, p. 301.
[73] Idem, p. 302.

direitos dos cidadãos e, por consequência, posicionando-se como uma autoridade de garantia.[74]

E, ainda que ocorra uma descentralização de centros de decisões, o papel central da lei não é atingido, pois, por meio de medidas que aproximam o interesse do cidadão ao interesse público, tendo como objetivo o equilíbrio, conforme confirma Doneda:

> "Nesse espaço, uma autoridade de garantia de direitos fundamentais encontra sua razão de ser, na promoção de um equilíbrio dinâmico entre essas situações subjetivas - organizando uma convivência plural dos valores que se referem à pessoa."[75]

E essa atuação da autoridade deve praticar uma justiça de dados que enquadre tanto aspectos positivos da proteção de dados quanto aspectos negativos. A conscientização da sociedade brasileira deve percorrer um caminho que tente conciliar os riscos e os benefícios dessa nova dinâmica social.

Ainda que esse objetivo não seja fácil, dado que exige uma conciliação entre aspectos extremamente contrastantes, como o engajamento tecnológico e os princípios fundamentais, é importante que ocorra esses atritos tanto para a evolução da sociedade como do governo, estabelecendo parâmetros de como queremos viver na sociedade do conhecimento[76].

Consoante, Bioni expõe:

> "Devemos ser capazes de determinar nossas interações com a tecnologia debatendo e, se necessário, resistindo e propondo caminhos diferentes. Se não podemos imaginar modos de recobrar o tipo de privacidade que gostaríamos, ou como permitir que as pessoas optem por não serem vigiadas através de seus dados - ou mesmo produzir esses dados em primeiro lugar- talvez tenhamos que, além de renegociar, também reinventar.
>
> Isso também pode envolver demandas diferentes a autoridades - sejam comerciais ou governamentais - com relação a governança de, e por meio das, tecnologias de dados."[77]

Com isso, percebe-se que, nessa concepção, há um deslocamento da responsabilidade de compreensão do indivíduo para as autoridades governamentais. Por exigir alterações

---

[74] Idem, p. 303.
[75] DONEDA, Danilo. **Da privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2 ed. São Paulo: Thomson Reuters Brasil, 2020 p. 309
[76] TAYLOR, Linnet. O que é justiça de dados? Conectando direitos digitais e liberdades globalmente.Construindo caminhos para a justiça de dados no Brasil: o papel das defensorias públicas na proteção de dados pessoais. 1.ed. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. PDF, p. 40.
[77] BIONI, Bruno Ricardo. **A Construção multissetorial da LGPD: histórias e aprendizados. Proteção de dados: contexto, narrativas e elementos fundantes.** São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF, p. 41

estruturais, esse enquadramento que exige um engajamento ativo da sociedade como um todo, principalmente das instituições que regem o funcionamento de uma população[78].

O papel de uma constituição democrática consiste tanto em delimitar as liberdades civis como também criar órgãos e leis que concretizem e torne alcançadas essas liberdades por todos.[79] Assim, autoridades independentes, como a ANPD, são criadas a fim de concretizar leis e liberdades e torná-las efetivas a todos os integrantes da sociedade, ainda que diante das novas dinâmicas sociais.

Conforme Gutierrez afirma:

> "A fiscalização e possibilidade de aplicação de sanções é parte essencial da institucionalização da proteção dos dados pessoais materializada pela criação da ANPD. Mas é necessário que se construa um arcabouço de estímulo às boas práticas por parte das organizações de modo a reduzir ao máximo a necessidade de se recorrer ao expediente da punição.
>
> Nesse campo, a publicação de diversos guias, orientações e estudos por parte da ANPD pode trazer uma baliza importante para que controladores e operadores possam adequar suas práticas e processos internos da maneira mais eficiente possível de modo a evitar que sejam alvo de processos administrativos e, eventualmente, de sanções.[80]"

Assim, atuação da ANPD vai constituir principalmente em um papel de autoridade de garantia dado que só o controle individual não é capaz de tutelar os direitos fundamentais de maneira efetiva, sendo imprescindível a atuação a Agência Nacional para a proteção dos interesses dos cidadãos, conforme afirma Doneda:

> "Conforme observado, trata-se de seara na qual os danos de reduzidíssima monta são comuns, o que diminui a propensão para postular sua reparação e, por distorção, incentiva as práticas de utilização indevida de dados pessoais. Além disso, o recurso a uma tutela baseada na responsabilidade civil não é, por si só, capaz de proporcionar uma tutela eficiente para o direito fundamental que representa a proteção de dados pessoais - como não o é a tutela exercida somente pelo interessado ou a autorregulação pelo mercado. A ação de uma autoridade para a proteção de dados pessoais representa, portanto, a realização de uma garantia institucional." [81]

Vale destacar que, diferentemente do Regulamento Europeu de Proteção de Dados, a LGPD não identificou quais informações devem compor esse inventário, cabendo, assim, dentre várias medidas, a ANPD regulamentar e especificar quais informações são imprescindíveis.

---

[78] Idem, p. 42.
[79] Idem, p. 300.
[80] BORELLI, Alessandra. GUTIERREZ, Andriei. Lei Geral de Proteção de Dados. Comentada. 2. ed. São Paulo: Thomson Reuters Brasil, 2020, p. 452.
[81] DONEDA, Danilo. **Da privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2 ed. São Paulo: Thomson Reuters Brasil, 2020, p.310

Confirmando a importância das autoridades independentes na concretização da legislação acerca da proteção de dados, a GPDR utiliza das suas autoridades para facilitar a concretização da legislação conforme o trecho abaixo:

> *"The GDPR asserts that the primary responsibility of DPAs concerns the monitoring and consistency of its application 'in order to protect the fundamental rights and freedoms of natural persons in relation to processing and to facilitate the free flow of personal data within the Union'."*[82]

Dessa forma, se mesmo com toda a familiaridade da sociedade europeia com o tratamento de dados e necessidade de proteção, ainda é necessário a instauração das *DPAs* para proteger os direitos fundamentais e as liberdades intrínsecas aos indivíduos, a sociedade brasileira vai ser ainda mais carecida de uma autoridade de proteção de dados.

Ademais, o próprio estudo em questão também destaca o papel das autoridades responsáveis pela proteção de dados no papel de orientar as instituições privadas, principalmente em relação às empresas de médio e pequeno porte:

> *"Yet recognising that 'DPAs are multi-taskers', we seem it necessary to reflect on DPAs' duties toward SMEs beyond enforcement, such as their duties concerning the monitoring and consistency of GDPR application. To this end, we consider within this contribution how DPAs can appropriately function in their role as educators to aid SMEs with clear and targeted guidance allowing them to begin their GDPR compliance journey."*[83]

Isso ocorre, pois, as grandes empresas têm uma infraestrutura com muito mais recursos permitindo que se adaptem de acordo com a lei de uma maneira mais fácil e ágil, no entanto, empresas de médio e pequeno porte não têm acesso a mudanças de maneira não rápida visto que seus recursos são mais limitados. Assim, a ANPD tem a função de guiar mais especificamente essas empresas a fim de prover um equilíbrio maior entre essas e as empresas de grande porte, pois, caso não sejam auxiliadas, vão ser extremamente prejudicadas.

Por isso, a importância da ANPD forte e ativa, pois, ainda que a LGPD não tenha como objetivo centralizar as medidas concretizadoras em uma só autoridade, é necessário que a Agência trabalhe de maneira ágil para preencher as lacunas deixadas pela legislação e impulsionar a concretização da LGPD na sociedade brasileira como um todo, conforme o autor afirma:

---

[82] COCHRANE, Leanne. JASMONTAITE-ZANIEWICZ. Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises.p.352-364, p.2

[83] Idem, p.2.

> "Although DPAs report the imperative of having direct contact with SME representatives to understand SME needs, we argue that SME Associations are often better placed to identify and communicate such needs to DPAs on behalf of SMEs. This is because SMEs, unlike SME Associations, tend to lack the time and the resources necessary to communicate their business needs to DPAs.[84]"

Ademais, ao estabelecer os objetivos dessas autoridades da proteção de dados, permite-se que a legislação seja aplicada de forma efetiva e uniforme:

> "In practice this means that formalizing awareness raising duties of DPAs could be seen as an attempt to ensure that regulators can enforce the applicable framework 'in a more uniform and effective way' and in a way that updates the enforcement practices of DPAs."[85]

Deve agir como uma líder a fim de guiar a sociedade para a concretização da legislação, e não de uma forma centralizadora:

> "In principle, some among this group suggest that DPAs' awareness-raising role among SMEs should be regarded as a form of leadership, 'where the emphasis is on the expertise, authority, influence of and information from DPA'. Christopher Hodges asserts that successful leadership, and consequently the success of awareness raising activities of DPAs, depends on trusted relationships which entail constructive engagement by DPAs with regulated entities[86]."

Assim, a CNPD pode estabelecer medidas a fim de alcançar essas empresas de pequeno-médio porte a fim de integrá-las às mudanças que estão ocorrendo na sociedade, tanto no âmbito econômico quanto legislativo. De acordo com a pesquisa feita com as empresas de pequeno-médio porte, essas acreditam que determinadas medidas podem ser mais eficientes para aproximá-las da nova legislação, como diferentes meios de comunicação-rádio, tv, redes sociais, entre outros-, eventos dedicados às empresas de pequeno médio porte, além da publicação de materiais voltados a proteção de dados.

Essas medidas permitem uma aproximação do mercado como um todo da nova legislação, melhorando e tornando sua aplicação mais alcançável. Assim, apenas a lei e a autoridade tendo uma atuação mais contida não vai gerar os resultados esperados. Em consonances:

> "Some of the respondents noted that DPA guidance often raises more questions that it answers and further that it arrived too late, i.e., after the time the legislation should have been implemented. Furthermore, some SME representatives shared the opinion that DPA guidance is too academic and focused on legal to be useful for everyday use, particularly for SMEs. This point was highlighted by one interviewee who stated that, 'the rules and guidance are designed for much bigger companies, where

[84] Idem, p.3.
[85] Idem, p.4.
[86] Idem, p.4.

> there is one or two specialist people doing paperwork late at night at the kitchen table after being in the field all day'.[87]"

Nesse mesmo pensamento, é possível reconhecer semelhança entre o papel das autoridades na concretização das leis dos consumidores:

> "Existing national arrangements of key Union consumer laws are not sufficient in a cross-border context. Effective Union-wide cross-border enforcement cooperation among public authorities is therefore crucial to prevent non-compliant traders from exploiting gaps, territorial and other limitations in the enforcement capacity of each Member State."[88]

Dessa forma, demonstra-se que apenas a promulgação da lei não basta, fazendo-se necessário a consolidação dessa na mentalidade do brasileiro a fim que esse a veja como suporte na busca de proteção de seus dados, tornando um tema alcançável a todos os integrantes da sociedade, seja um cidadão pertencente a qualquer classe social, como também empresas, das de pequeno porte até as de ampla estrutura. Assim, a atuação da Agência Nacional de Proteção de Dados se estabelece como pilar da consolidação da LGPD.

[87] Idem, p.6.
[88] Idem, p.3.

CONCLUSÃO

Conforme o trabalho apresentado, destacamos a importância dos dados digitais na dinâmica socioeconômica atual e como o tratamento indevido desses pode afetar diretamente os cidadãos, atingindo aspectos sensíveis.

Não só demonstramos o lugar de importância dos direitos fundamentais e dos direitos da personalidade nessa discussão, como também demonstramos que essa perspectiva individual não é suficiente para tutelar a proteção do tratamento de dados pessoais em razão da complexidade da discussão que exige uma análise sob uma ótica ampla, abrangendo mais de um indivíduo.

A partir disso, destacou-se o papel da Lei Geral de Proteção de Dados como instrumento de desenvolvimento socioeconômico, e a responsabilidade da sua respectiva autoridade, a Agência Nacional de Proteção de Dados, de introduzir a nova legislação a população brasileira e sedimentar uma consciência sobre a tutela de dados tanto no âmbito público, abrangendo instituições estatais e privadas, quanto aos cidadãos brasileiros.

Tendo em vista que os brasileiros não tiveram muito contato com a história do tratamento de dados, existe uma dificuldade maior da sociedade como um todo entender a importância da LGPD, tornando a aplicação mais difícil e aumentando a importância da concretização por meio da ANPD.

Isto porque, a resistência a essa nova legislação só ocasiona atrasos ao mercado brasileiro, tornando-o inapto a participar das dinâmicas econômicas internacionais.

Além disso, a ausência de concretização da LGPD não só afeta o ambito econômico, como tambem afeta o ambtio dos direitos fundamentais dos indivíduos, visto que esses são lesionados pelo tratamento indevido.

Em que pese, não se possa erradicar todos os abusos provocados pelo tratamento indevido de dados pessoais, é possível minimizar os danos causados por ele. A atuação das autoridades independentes na consolidação da LGPD se torna imprescindível para a sociedade atual, visto que os dados são vistos como uma mercadoria pela presente economia, precisando da devida proteção.

A discussão sobre os benefícios e malefícios do tratamento de dados deve ser exposto a todos cidadãos, pois, apenas por meio da informação e o debate, os membros da sociedade são capazes de defender seus direitos e influenciar no modo funcionamento da sociedade que são pertencentes.

Isto posto, é imprescindível a atuação efetiva da Agência Nacional de Dados como um meio de concretização efetiva não só da LGPD, como também, de uma consciencia sobre a necessidade de proteção dos tratamentos de dados pessoais, pois não basta que as empresas apliquem a legislação da maneira correta, mas sim que os cidadãoes, independente de classe social, tenham o mínimo de ciência da dinâmica do tratamento de dados pessoais e quais as consequencias.

Logo, as autoridades independentes são aspectos primordiais no processo de consolidação de novas legislações. E, ainda que o almejado pareça um pouco inalcancável, para justificar a viabilidade do objetivo, citamos um caso análogo: o Código do Consumidor.

Isto porque, o processo de concretização do CDC exemplifica bem o papel de autoridades, como o PROCON, para disseminar e consolidar os dispositivos do Código no raciocínio do cidadão, auxiliando-o a proteger seus direitos como consumidor.

Dessa forma, em que pese a criação da Lei Geral de Proteção de Dados já ter sido um grande avanço, a importância dessa ainda não faz parte do conhecimento da população brasileira.

Atualmente, encontra-se completamente fora do alcance da comunidade mais humilde o conhecimento acerca do tratamento de dados ou da LGPD e, ainda que outra parcela da população tenha mais ciência do assunto em questão, dificilmente tem uma nocao completa das consequencias que o tratamento indevido de dados pode proporcionar.

Por ser um tema que ainda não atinge a todos os brasileiros, presentes apenas em discussões de classes sociais mais altas e nem ao menos beirando o conhecimento de classes sociais mais baixas, a LGPD é sim restrita a uma parcela da sociedade brasileira, tornando relevante o papel da ANDP.

Por fim, destaca-se a ANPD como um órgão extremamente responsável pela fixação da LGPD como um dispositivo efetivo e útil ao cidadão brasileiro na proteção de seus dados pessoais, independente da classe social a que seja pertencente.

REFERÊNCIAS

ANDRÉA, Gianfranco Faggin Mastro. ARQUITE, Higor Roberto Leite. **Proteção dos Dados Pessoais como direito fundamental: a evolução da tecnologia da informação e a Lei Geral de Proteção de Dados no Brasil.** Revista de Direito Constitucional e Internacional | vol. 121/2020 | p. 115 - 139 | Set - Out / 2020

Brasil. **Lei Geral de Proteção de Dados Pessoais (LGPD).** Brasília, DF: Presidência da República, [2020]. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 10.11.2022.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites de consentimento.** Ed 1. Rio de Janeiro: Forense, 2019.

BIONI, Bruno Ricardo. **A Construção multissetorial da LGPD: histórias e aprendizados. Proteção de dados: contexto, narrativas e elementos fundantes.** São Paulo: B. R. Sociedade Individual de Advocacia, 2021. PDF

BORELLI, Alessandra. GUTIERREZ, Andriei. **Lei Geral de Proteção de Dados. Comentada.** 2. ed. São Paulo: Thomson Reuters Brasil, 2020.

COCHRANE, Leanne. JASMONTAITE-ZANIEWICZ. **Data Protection Authorities and their Awareness-raising Duties under the GDPR: The Case for Engaging Umbrella Organisations to Disseminate Guidance for Small and Medium-size Enterprises.**p.352-364, p.2.

DONEDA, D. (2011). **A proteção dos dados pessoais como um direito fundamental.** *Espaço Jurídico Journal of Law [EJJL]*, *12*(2), 91–108.

DONEDA, Danilo. **Da privacidade à Proteção de Dados Pessoais: fundamentos da Lei Geral de Proteção de Dados.** 2 ed. São Paulo: Thomson Reuters Brasil, 2020.

FEDERAL TRADE COMMISSION. **Data Brokers. A call for transparency and accountability.** Disponível em: [https://www.ftc.gov/system/files/documents/reports/data-brokers-call-transparency-accountability-report-federal-trade-commission-may-2014/140527databrokerreport.pdf]. Acesso em: 22.11.2022.

FRAZÃO, Ana. TEPEDINO, Gustavo. **Lei Geral de Proteção de Dados Pessoais e suas repercussões no Direito Brasileiro**. São Paulo: Ed. Revistas dos Tribunais, 2019.

MENDES, Laura Schertel. FONSECA, Gabriel Campos Soares da. **STF reconhece direito fundamental à proteção de dados.** Revista de Direito do Consumidor | vol. 130/2020 | p. 471 - 478 | Jul - Ago / 2020.

MULHOLLAND, Caitlin Sampaio. **Dados Pessoais Sensíveis e a tutela de direitos fundamentais: uma análise à luz da Lei Geral de Proteção de Dados (Lei 13.709.18)**. R. Dir. Gar. Fund., Vitória, V.19, n.3, p.159-180, set - dez 2018.

ROSENVALD, Nelson. FARIAS, Cristiano Chaves de Farias. **Curso de Direito Civil: Parte Geral e LINDB**. Ed. 16. Salvador: Ed. JusPodivm, 2018.

Construindo caminhos para a justiça de dados no Brasil: o papel das defensorias públicas na proteção de dados pessoais. 1.ed. São Paulo: Associação Data Privacy Brasil de Pesquisa, 2022. PDF.