Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LUCAS DUTRA ROSENDO DA SILVA

O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: PANORAMA, TENDÊNCIAS E DESAFIOS

Assis/SP
2021

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

LUCAS DUTRA ROSENDO DA SILVA

O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: PANORAMA, TENDÊNCIAS E DESAFIOS

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e a Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Lucas Dutra Rosendo da Silva
Orientador(a): Jesualdo Eduardo de Almeida Júnior

Assis/SP
2021

FICHA CATALOGRÁFICA

S586d SILVA, Lucas Dutra Rosendo da

O direito à proteção de dados pessoais: panorama, tendências e desafios / Lucas Dutra Rosendo da Silva. – Assis, 2021.

69p.

Trabalho de conclusão do curso (Direito). – Fundação Educacional do Município de Assis-FEMA

Orientador: Dr. Jesualdo Eduardo de Almeida Júnior

1.Privacidade 2.Proteção-dados 3.Mercado digital

CDD 342.1152

O DIREITO À PROTEÇÃO DE DADOS PESSOAIS: PANORAMA, TENDÊNCIAS E DESAFIOS

LUCAS DUTRA ROSENDO DA SILVA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: Jesualdo Eduardo de Almeida Junior

Examinador: Hilário Vetore Neto

Assis/SP
2021

DEDICATÓRIA

Dedico este trabalho à minha família, aos meus amigos, aos professores e em especial aos que contribuíram para o desenvolvimento do conteúdo.

AGRADECIMENTOS

a Deus e a minha família por todo apoio, suporte e paciência que me cederam durante a realização deste trabalho;

ao professor Dr. Jesualdo Eduardo de Almeida Júnior, pela orientação prestada desde a escolha do tema até a finalização do texto;

a todos os professores da FEMA que não medem esforços para contribuírem com nosso aprendizado;

à professora Dra. Amélia de Jesus Oliveira, por todas as recomendações e orientações de escrita no corpo textual;

à professora Fabiana Williams, pela oportunidade de discussão acerca do tema, pelos conhecimentos e problematizações colocadas;

ao professor Sandro Albertini, pelo suporte prestado nas verificações de traduções de língua estrangeira;

ao Dr. Sando de Cassio Dutra, pelo auxílio acerca do entendimento do tema e sugestões de conteúdo no trabalho;

aos amigos que me apoiaram durante a escrita, propondo questões que problematizassem o tema, além de todo auxílio durante a confecção desta monografia;

Com o avanço tecnológico e o compartilhamento de informações, não há sequer um segundo em que não estamos vulneráveis e à mercê da violação de dados pessoais, a proteção destes elementos é uma garantia fundamental de todos nós.

Josiene Rodrigues Rocha

RESUMO

A evolução da tecnologia da informação nos últimos anos alterou significativamente as relações sociais, em diversos aspectos da atividade humana. Se é verdade que ela gerou muitas facilidades, é certo também que veio acompanhada de desafios e riscos à privacidade dos indivíduos. Para as novas relações estabelecidas, foi necessária uma regulamentação jurídica. Disso trata este trabalho, no qual é apresentada a Lei Geral de Proteção de Dados, com seu regulamento e interferências no cotidiano e no mercado digital. A partir de uma abordagem histórica, que passa pela análise de conceitos, analisa-se a relação de partes envolvidas, as possíveis obrigações aos controladores e operadores e a previsão de aplicação de eventuais responsabilizações. Em referência ao atual modelo de sociedade, são expostos o impacto de determinada legislação no comportamento daqueles que lidam com informações e a perspectiva do mercado digital, diante das novas discussões sobre privacidade, presentes nas empresas de comunicação, e sobre o cumprimento das políticas de privacidade que são observadas num cenário pós GDPR. O objetivo é analisar o impacto da GRPR ao cenário internacional e da LGPD ao cenário nacional, quais foram as suas repercussões e quais as suas atuações perante à economia e a privacidade. Outra finalidade é a dissertação sobre casos que ainda necessitam de maior atenção, frente às novas formas de coleta na internet e a necessidade de auxílio de pessoas de maiores conhecimentos do tema em eventuais legislações futuras. Também tem a mesma disposição, a tentativa de abordar posicionamentos futuros quanto à utilização de dados pessoais no mercado digital, em paralelo ao cumprimento da privacidade de seus titulares. Uma proteção mais vinculada ao tema em questão é de benefício aos titulares e à sociedade em geral, trazendo uma atualização à legislação brasileira, em decorrência de novas modalidades de infrações. Nos embates sobre o tema, constata-se que muitas empresas já visam a necessidade de cumprimento das políticas de privacidade, ao mesmo tempo em que outras utilizam as informações colhidas como forma de troca com interessados, que pagam pelo seu recebimento. As futuras manifestações sobre o assunto ocorrerão de forma mais recorrente e necessária, tendo em vista a procura crescente pela temática da proteção de dados, que requer incessante acompanhamento por parte da legislação brasileira.

Palavras-chave: Proteção de Dados. LGPD. Mercado Digital. Privacidade.

ABSTRACT

The technological evolution of information on recent years has changed meaningfully the social relations in different aspects of human activity. If it is true that it has created many facilities, it is also true that this has come with challenges and risks to individual`s privacy. It was necessary a regulation for the new relations established. This is the subject of this work, in which, the Brazilian General Data Protection Law is presented, with its regulation and interferences in our routine and on digital business. From a historical approach, passing by the analysis of the concept, it is identified the relation between the parts, the possible obligations of the controllers and operators, and the prediction of the application of possible liabilities. In reference to the current model of society, this work exposes the impact of certain laws on the behavior of those who work with information and the perspective of the digital business in the face of new discussions about privacy in communication companies, and about compliance with the privacy policies in a situation after GDPR. The goal is to analyze the implications of GDPR in international cases and of BGDPL (Brazilian General Data Protection Law) in national cases, their repercussions and their actions over economy and privacy. Another purpose is the dissertation about cases that still need more attention in the face of the new forms of collecting data on the internet and the requirement from specialists on the theme to help create future legislations. It is also important the attempts of describing future ideas about the use of personal data in digital business while respecting people's privacy. A protection more linked to the theme discussed is beneficial to people and society in general, updating the Brazilian legislature in consequences of the new types of crimes. The discussions show that many companies have already noticed the importance of following privacy policies, at the same time that others use information gathered as a form of trade-off payments. The upcoming manifestations about these issues will be more constant and necessary considering that the increasing discussion about data protection requires uninterrupted monitoring by the Brazilian laws.

Keywords: Data Protection. BGDPL. Digital Business. Privacy.

LISTA DE ABREVIATURAS E SIGLAS

ANPD	Agência Nacional de Proteção de Dados
ANS	Agencia Nacional de Segurança (Estadunidense)
CDC	Código de Defesa do Consumidor (Lei 8.078/1990)
CLT	Consolidação das Leis do Trabalho (Lei 5452/1943)
CP	Código Penal (Lei 2.848/1940)
EUA	Estados Unidos da América
EU	*European Union*
GDRP	*General Data Protection Regulation*
LGDP	Lei Geral de Proteção de dados (Lei 13.709/2018)
NSA	*National Security Agency*
UE	União Europeia
US	*United States*

SUMÁRIO

1. INTRODUÇÃO

O crescimento do processo de tratamento de dados e informações de titulares é atualmente expressivo, com grande valor e utilização. Muitas dessas informações colhidas são vendidas para empresas, com fins de produção de uma publicidade mais acertada a um determinado usuário, por conter informações acerca de seus hábitos, gostos e preferências de compra.

Durante a pandemia do Covid-19, o assunto se tornou ainda de maior relevância para o país, dado que, nos últimos anos, a quantidade de informações que foram trocadas sem a devida finalidade e legalidade é grande, incluindo escândalos de empresas famosas mundialmente. Tudo isso em decorrência da repentina mudança compulsória para o mundo digital da maioria da população como forma de cumprimento do distanciamento social.

A nova Lei de Proteção de Dados Europeia (GPDR – *General Data Protection Regulation*), sancionada em 2016, veio como modelo de uma legislação específica sobre o tema para diversos países, despertando a necessidade de criação de leis de mesma nivelação sobre o assunto, já que a legislação anterior já não mais acompanhava tamanha enxurrada de coleta de dados e exigia maior aprofundamento no tema.

O presente trabalho tem como objetivo mostrar o que a Lei aborda, quais os direitos do titular, a real necessidade de cessão de seus dados e por que são tão visados pelo mercado. Aborda ainda os temas recorrentes e importantes para a população mundial nessa transferência, a partir do momento em que é possível a troca de informações de diferentes países em menos de segundos, fator impulsionado pela globalização. Por fim, busca evidenciar quais as reais mudanças já visíveis foram trazidas pela Lei e lançar conjecturas sobre o que ainda necessita ser aprimorado.

As motivações para a abordagem do tema estão alicerçadas na sua importância em nível mundial e na necessidade de atenção. Vale lembrar que, para alguns autores, a transferência de dados é vista como o “novo petróleo”, movimentando enormes quantias monetárias ao redor do mundo. A discussão sobre o real consentimento de consulta de informações face à lucratividade é de enorme repercussão e traz uma perspectiva de comportamentos futuros.

No primeiro capítulo, abordamos o histórico do tema (proteção de dados), sua importância e momento inicial de sua valoração aos seus titulares, que passam a requisitar maior privacidade. Abordamos as diferentes tentativas da criação de tratados na Europa em relação à privacidade, o que veio a contribuir para a criação da legislação de tratamento de dados, a GDPR, juntamente com o seu pioneirismo na proteção de dados pessoais. Ganham atenção aqui a origem do documento (GDPR) e a evolução processual e histórica da Lei de Proteção de Dados brasileira (LGPD), na qual é possível detectar uma influência do documento europeu e sua necessidade de criação. Alguns conceitos relevantes no tratamento de dados pessoais, que estão presentes na realização de tais atividades, serão discutidos ainda nessa parte do trabalho.

No segundo capítulo, a lei 13.790/2018 é apresentada com seus princípios, fundamentos e o objetivo de proteger informações extremamente relevantes. Importa mostrar como essa lei realiza essa proteção, externando suas metas por meio da base de sua formulação. Discutimos conceitos importantes entre diferentes tipos de dados, de forma que alguns merecem maior atenção que outros. A relação da legislação brasileira com países estrangeiros na troca de informações, que ultrapassam as fronteiras brasileiras, sua forma de controle e acordo externo são também examinados.

No último capítulo, discorremos sobre a frequência de tratamento de dados, o compartilhamento instantâneo e constante, que os tornam atrativos para empresas que se utilizam dessas informações a fim de produzir uma publicidade mais direcionada a seus consumidores e que gera um enorme mercado digital. Quanto ao mercado, descrevemos as relações de gigantes da tecnologia mundial, seus embates atuais e a perspectiva da posterior relação entre usuário e empresa.

Por fim, são discutidas as questões relevantes pós início da GDPR e a enorme presença de *cookies* nas plataformas on-line, seu conceito e o efetivo cumprimento de suas políticas de privacidade, a partir de análises de pesquisas realizadas em outros países.

2. PROTEÇÃO DE DADOS

2.1. DESENVOLVIMENTO HISTÓRICO

A proteção de dados, ao oposto do que se pensa, é um tema discutido há anos, mesmo antes da expressa utilização da internet. Identifica-se essa proteção quando se tem a preocupação com a proteção da privacidade juntamente com os Direitos Humanos, passo que traz a ideia de que se fazem necessárias normas e princípios que versem sobre determinada matéria, a fim de evitar resultados que possam comprometer o direito alheio.

Inicia-se, por volta do ano de 1950, quando foi esboçada uma convenção internacional para proteger os direitos humanos e políticas de liberdade. A convenção ganha força em setembro de 1953, com o consenso de que qualquer pessoa da União Europeia[1] que sentisse, de qualquer forma, que seus direitos tivessem sido violados, poderia procurar e levar essa questão ao Judiciário. O Comitê de Ministros do Conselho da Europa monitorava as execuções dos julgamentos, analisava o dano para ver a possibilidade de reparação.

Como relata o conselho, por decorrência da convenção[2], a noção de privacidade começa a ganhar um maior sentido e preocupação, tendo cada um o direito de permanecer com suas informações pessoais íntegras e respeitadas. É também o primeiro tratado a estabelecer um órgão supranacional que assegurava que os estados-membros honrassem com seus compromissos.

No início dos anos de 1970, na Alemanha, cria-se a primeira lei relacionada diretamente à proteção de dados pessoais, considerada como *door open*, abridora de portas, nessa linhagem de proteção. O estado de Hesse foi o primeiro da história a adotar essa proteção. Havia na época um avanço da computação e da indústria, incentivando a criação de leis que tratassem da privacidade. A Suécia, um pouco mais adiante, traz a proteção à privacidade a nível nacional, atribuindo grande importância ao tema em discussão. Em sua publicação *Implementing Data Protection in Law*, o sueco Sören Öman (2010, p. 390) aponta:

---

[1] Doravante registrada como UE.

2 Ver: https://www.coe.int/en/web/human-rights-convention/the-convention-in-1950

> A primeira legislação nacional destinada a proteger informações privadas de indivíduos quando seus dados pessoais são processados em computadores, vieram à luz do dia na Suécia em 1973.
>
> O documento, chamado de *The Swedish Data Act*, abordava processos de dados pessoais comuns, registros informatizados. O ato não continha muitas previsões materiais de quando e como os dados deveriam ser processados, ou os princípios gerais de proteção de dados. Ao invés disso, o ato requeria, para cada registro de dados pessoais, uma permissão anterior da nova autoridade de proteção de dados (*Data Inspection Board*). Quando permitido, a autoridade emitia determinadas condições para aquele registro.[3]

Havia uma crescente ideia em prol de uma unificação de normas para que fossem aplicadas em todo território nacional de maneira mais uniforme, não mais como ocorrido na Alemanha, em que a regulamentação focava apenas um estado. Em novembro de 1976, o parlamento alemão aprovou o "Ato de Proteção Contra Usos Indevidos no Processamento de Dados Pessoais." O ato protege o processamento de dados em nível federal e inclusive no setor privado. Outros países também começaram a mostrar interesse nessa regulação. No ano de 1978, França, Noruega, Suécia e Áustria também criaram suas próprias leis. (Cf. NUTGER, 1990).

A preocupação com a privacidade ao utilizar os crescentes serviços informáticos evidencia-se com a criação da "Convenção 108+", como descrita na plataforma digital do Portal Conselho Europeu.

A Convenção foi aberta para assinaturas, em 28 de janeiro de 1981, como o primeiro instrumento legalmente vinculado ao campo da proteção de dados. Sob essa convenção, as partes eram obrigadas a seguirem as devidas etapas em suas legislações locais para aplicar princípios, a fim de estabelecer ordem para garantir respeito em seus territórios pelos direitos humanos fundamentais de todos os indivíduos, considerando o processo de dados pessoais. A Convenção existe até os dias de hoje, contando com a participação de 55 países membros.

---

[3] As citações em língua estrangeira têm tradução nossa. As versões originais estão transcritas em notas de rodapé. A versão original da passagem citada é: *The first national legislation aimed at protecting the informational privacy of individuals when their personal data are processed in computers saw the light of day in Sweden in 1973. The Swedish 1973 Data Act only covered processing of personal data in traditional, computerised registers. The act did not contain many material provisions on when and how the data should be processed, or general data protection principles. Instead, the act required for each computerised personal data register a prior permit from a new data protection authority – the Data Inspection Board. When a permit was given, the Board issued tailor-made conditions for that register.*

2.1.1. Do Safe Harbor ao Privacy Shield

Os continentes começam, então, a estabelecer alguns pactos, regulamentando e facilitando as trocas de informações, no final dos anos de 1990, como explícito pela reportagem feita pelo *Congressional Research Service*[4] a qual detalha que:

> os Estado Unidos e a União Europeia negociaram um acordo chamado de *Safe Harbor* em 2000 para permitir que empresas e organizações norte americanas se adequassem aos requisitos da proteção de dados europeus e permitir a transferência legal de dados pessoais entre membros da União Europeia e os Estados Unidos[5] (WEISS, 2016, p.03).

> Revelações não autorizadas, em junho de 2013, de que a Agência Nacional de Segurança dos Estados Unidos (*National Security Agency*) vigiava programas, e subsequentemente renovadas e exacerbadas alegações de outras atividades de inteligências americana na Europa, preocupavam o bloco europeu sobre os padrões de proteção e privacidade de dados nos EUA. O suposto envolvimento de algumas empresas de telecomunicações e internet nos programas da ANS também elevou as preocupações da Europa sobre como firmas de tecnologias usavam dados pessoais e a extensão do governo norte americano em acessar cada um desses dados. Como resultado, um número de acordos de compartilhamento de dados entre EUA e UE (União Europeia), tanto no comercial, quanto setores de execução, tiveram baixa intensidade de segurança vistos pela Europa.[6]

Devido a todos esses entraves entre os países não havia mais a mesma confiança, principalmente da UE em continuar com o acordo, visto que poderia haver desvio de funções junto dessas operações. No mesmo sentido de desconfiança e entraves, Martin A. Weiss (2016, p.03) descreve o final do acordo denominado como *safe harbor*.

Em outubro de 2015, o Tribunal de Justiça da União Europeia (*Europe Court of Justice*) invalidou o acordo *Safe Harbor*. O tribunal motivou essencialmente que o *Safe Harbor* falhou ao se assemelhar às normas de proteção de

---

[4] Ver: https://fas.org/sgp/crs/misc/R44257.pdf

[5] *In the late 1990s, the United States and the EU negotiated the Safe Harbor Agreement of 2000 to allow U.S. companies and organizations to meet EU data protection requirements and permit the legal transfer of personal data between EU member countries and the United States.*

[6] *The unauthorized disclosures in June 2013 of U.S. National Security Agency (NSA) surveillance programs and subsequent allegations of other U.S. intelligence activities in Europe renewed and exacerbated European concerns about U.S. data privacy and protection standards. The alleged involvement of some U.S. Internet and telecommunications companies in the NSA programs also elevated European worries about how U.S. technology firms use personal data and the extent of U.S. government access to such data. As a result, a number of U.S.-EU data-sharing accords in both the commercial and law enforcement sectors have come under intense scrutiny in Europe.*

dados pessoais Europeias, em grande parte, por conta dos programas de vigilância dos EUA, dado que cerca de 4,500 empresas americanas estavam utilizando o *Safe Harbor* para legitimar a transferência de dados transatlânticos. Oficiais e líderes americanos de negócios foram profundamente desestimulados pela decisão dominante. Empresas que vinham usando o *Safe Harbor* como base legal para a transferência de dados entre EUA-UE foram orientadas a implementar de imediato medidas alternativas. Estudiosos alegam que a decisão do Tribunal criou incertezas legais para diversas companhias que temeram que isso poderia impactar negativamente os laços negociais de EUA-UE.

No dia 02 de fevereiro de 2016, os EUA e UE anunciaram um tratado oficial, a princípio, na revisão do acordo do *Safe Harbor*, sendo conhecido como *Privacy Shield* (Escudo de Privacidade). O texto em sua íntegra foi realizado em 29 de fevereiro de 2016, trazendo as garantias oficiais europeias de que o novo acordo estaria em legitimidade com as preocupações da Corte. Em particular, eles enfatizaram que isso continha proteção forte de privacidade como também a proteção ao acesso de dados pessoais do governo dos EUA.

Em 2014 foi emitido o alerta de que o parlamento europeu deu aval a criação de um regulamento do próprio parlamento e do Conselho relativo à proteção de pessoas no que diz ao tratamento de dados pessoais e à livre circulação desses dados, emitindo como parecer:

> A rápida evolução tecnológica criou novos desafios em matéria de proteção de dados pessoais. A partilha e a recolha de dados registaram um aumento espetacular. As novas tecnologias permitem às empresas privadas e às entidades públicas a utilização de dados pessoais numa escala sem precedentes no exercício das suas atividades. As pessoas disponibilizam cada vez mais as suas informações pessoais de uma forma pública e global. As novas tecnologias transformaram a economia e a vida social, trazendo uma maior facilidade na livre circulação de dados na União, na transferência para países terceiros e organizações internacionais, devendo ser assegurado simultaneamente um elevado nível de proteção dos dados pessoais (POSIÇÃO DO PARLEMENTO EUROPEU (2014).

Esta evolução exige o estabelecimento de um quadro de proteção de dados sólido e mais coerente na União Europeia, apoiado por uma aplicação rigorosa das regras, pois é importante gerar confiança para permitir o desenvolvimento da economia digital no conjunto do mercado interno. As pessoas singulares devem ter autonomia de controlar a utilização

dos seus dados pessoais. Nesse momento a necessidade está em um grau bastante elevado e essas relações necessitam cada vez mais de uma regulamentação para que não houvesse a utilização desses dados com diferentes objetivos.

O bloco também afirmava ser necessário que todos os Estados-membros deveriam adotar essas medidas, a fim de assegurar um nível de proteção coerente e elevado. Solicitando a necessidade do conjunto da União à aplicação coerente e homogenia das regras de proteção de liberdade e dos direitos fundamenteis das pessoas singulares no que diz respeito ao tratamento de dados pessoais.

Em 2016 se consolidou a promulgação do Regulamento de Proteção de Dados Pessoais Europeu, aprovado em abril. “Tinha como objetivo abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão *free data flow.”* Como cita a autora Patrícia Peck em sua obra *Proteção de Dados Pessoais* (PINHEIRO, 2020, p. 17).

A previsão para adequação era até 25 de maio de 2018, quando se iniciariam os efeitos das penalidades. A influência da criação dessa norma foi extremamente forte, ao passo que, a partir deste momento, a UE começa a exigir uma legislação ao mesmo nível da GPDR (*General Protection Data Regulation*), fazendo com que empresas e países também adotassem essa modificação em seus regramentos.

O Estado que não possuísse o mesmo nível de segurança quanto à transferência de dados poderia passar a sofrer algum tipo de barreira econômica ou dificuldade de fazer negócios com países-membros da UE. Considerando a necessidade de muitos países que dependiam de comércios e relações com a UE, ocorreu a necessidade de adequação.

> A regulamentação destaca a proteção de pessoas físicas, tendo vista que pertence ao ramo dos direitos fundamentais. A norma padronizou o que seriam os atributos qualitativos da proteção de dados pessoais sem a presença dos quais haveria penalidades. Os efeitos trazidos pela GDPR são principalmente econômicos, sociais e políticos (PINHEIRO, 2020, p. 18).

Em 2020 o Tribunal de Justiça Europeu[7] derrubou o *Privacy Shield*, que assegurava a troca de dados de forma irrestrita entre os EUA-UE, afirmando a possibilidade de não

[7] Ver: https://www.privacyshield.gov/Program-Overview

garantir adequado nível de proteção desses dados transferidos entre os dois polos, quando comparados à nova lei sancionada (GDPR).

A decisão fez com que houvesse a necessidade de adequação dos controladores para terem acesso aos dados. Os que não passavam por essa modificação seriam suspensos quanto à transferência de dados com o Bloco Europeu. Eram também suspensos nos casos em que o bloco reconhecia uma proteção ineficaz, tendo como base a nova legislação.

A nova lei de proteção de dados europeia é, nos dias atuais, modelo a ser seguido, possuindo enorme influência exterior e já exercendo suas penalidades. A responsabilização de diversas empresas já está sendo feita, trazendo um direcionamento de adequação empresarial para evitar penalidades e cumprir efetivamente as regras.

2.1.2. A proteção de Dados Pessoais no Brasil

Tratando-se de “privacidade”, esse é um conceito que está amparado aos cidadãos brasileiros desde bem antes da criação da Lei Geral de Proteção de Dados. Consta como um princípio de origem constitucional como relatado no artigo 5º da Constituição Federal de 1988: Art 5: “são invioláveis a intimidade da vida privada, a honra e a imagem das pessoas, assegurando o direito a indenização pelo dano material ou moral decorrente de sua violação.”

No ano de 1993 o Código de Defesa do Consumidor (Lei 8.078/90) traz uma proteção ainda mais específica. Com sua chegada, uma nova ideia foi trazida, ao passo de carregar garantias essenciais aos consumidores, agora tratados como hipossuficientes. Com uma maior vulnerabilidade em relação a uma empresa, a legislação trouxe maior segurança nas relações consumeristas.

Foi possível identificar o anteparo aos dados de clientes de forma que as empresas necessitassem de adequação. A exemplo de proteção, está descrita em seu artigo 43 que trata de banco de dados e cadastros de consumidores, proteção maior aos dados cedidos por consumidores em suas relações:

> Art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1° Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> § 2° A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3° O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
>
> § 4° Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.
>
> § 5° Consumada a prescrição relativa à cobrança de débitos do consumidor, não serão fornecidas, pelos respectivos Sistemas de Proteção ao Crédito, quaisquer informações que possam impedir ou dificultar novo acesso ao crédito junto aos fornecedores.
>
> § 6º Todas as informações de que trata o **caput** deste artigo devem ser disponibilizadas em formatos acessíveis, inclusive para a pessoa com deficiência, mediante solicitação do consumidor (BRASIL, 1990, art. 43).

Tornam-se públicos os princípios de recolhimentos de dados com uma finalidade específica: direito de acesso por parte do consumidor e a responsabilidade das empresas sobre a segurança das informações armazenadas.

Em 2013 a lei 12.737, popularmente conhecida por Lei Carolina Dieckmann, impacta o direito penal, acrescentando os artigos 154-A e 154-B ao Código Penal Brasileiro. Altera também a redação dos artigos 266 e 298. A lei recebe o nome da atriz por conta dela ter sido vítima de um crime quando teve seu computador invadido por um hacker e suas fotos íntimas publicadas na rede. Desperta-se uma nova modalidade de crimes que necessitam de punição, momento em que o modelo da infração penal possui ligação com a atualidade, envolvendo recursos tecnológicos mais modernos.

Bruno Bioni, em sua obra: *Proteção de Dados pessoais (2019,* p. 05) afirma que: “Os relacionamentos sociais foram energizados por um fluxo informacional que não encontram mais obstáculos físicos distanciais.” Exemplifica uma visão de mudança comportamental na utilização das redes quando afirma:

> com as manifestações de junho de 2013 foi possível enxergar que o exercício da cidadania foi revitalizado por um fluxo informacional – em especial das redes sociais – que conectou seus manifestantes, facilitando a organização a e disseminação dos protestos. Verificou-se um novo instrumento de engajamento social. Por isso, a

> informação avoca um papel central e adjetivante da sociedade: Sociedade da Informação. (...) Sendo a informação o (novo) elemento estruturante que (re)organiza a sociedade, tal como fizeram a terra, as máquinas a vapor, a eletricidade (BIONI, 2019, p. 05).

Os bancos de dados eletrônicos mudaram o formato da economia e do capitalismo, o que é capaz de gerar efeitos sobre o cidadão. O autor também observa a relação dos dados com a economia atual, dizendo:

> ao passo da inteligência gerada pela ciência mercadológica, especialmente quanto à segmentação dos bens de consumo (marketing) e a sua promoção (publicidade), os dados pessoais dos cidadãos convertem-se em um fator vital para a engrenagem da economia da informação.
>
> E, com a possibilidade de organizar tais dados de maneira mais escalável (e.g., Big Data), criou-se um novo mercado cuja base de sustentação é a sua extração e modificação. Há uma "economia de vigilância" que tende a posicionar o cidadão como mero expectador das suas informações (BIONI, 2019, p. 12).

A vigilância ocorre pela observação feita pelos sistemas, ao identificar seus gostos e preferências, através de comportamentos digitais, como nos casos em que são computados o tempo em que a pessoa permanece focada na tela de seu Smartphone, significando que aprova determinado conteúdo, como demonstrado no documentário "O dilema das redes" (2020), adquirindo um resultado (dados) que poderá ser vendido a uma empresa que deseja saber quem são seus consumidores, intensificando os anúncios publicitários para tal indivíduo.

Crescem as citações relacionadas à proteção de dados na legislação brasileira, ao se encontrar na Seção II – Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas – da lei 12.965/2014 (Marco Civil da Internet), regulamentação sobre o uso da internet no Brasil. Nesse ponto, a ideia de proteção aos dados é mais amadurecida, vistas a vontade e a necessidade em aprovações de legislações específicas. As ações ocorridas nesta plataforma no território nacional possuem uma crescente utilização, sendo considerada pelos autores Cintia Rosa Pereira de Lima e Kelvin Peroli (2019, p. 82) como um microssistema de proteção de dados pessoais, a partir do art. 3º, inciso III e artigo 7º, incisos VIII – X. Eles apontam, em seguida, que o Marco Civil da Internet estabeleceu o âmbito de aplicação da proteção dos dados pessoais já no intuito de implementar a conformidade da proteção no Brasil à instituída na UE que foi revogada pela GDPR.

Em outro ponto era possível observar a questão ainda, muitas vezes, reconhecida de forma difusa e sem objetividade no tocante aos critérios que seriam considerados adequados para determinar se houve ou não guarda, manuseio e descarte dentro dos padrões mínimos de segurança condizente, como afirma Patrícia Peck (2020, p. 18) em sua obra *Proteção de dados pessoais.*

No ano de 2016, a regulamentação de proteção de dados da UE vem à tona. Revoga-se sua Diretriz 95/46 anteriormente aprovada, a medida dessa nova aprovação se tratar de uma maior cautela na utilização das informações. O bloco europeu, ao sancionar a lei, objetiva incentivar outros países a também ratificar uma legislação com a mesma intensidade da GDPR, exigem que todas as empresas e países, com quem possuem relações deveriam se adequar.

Com o Estado brasileiro, esse impacto não foi diferente. Por possuir quantitativas relações comerciais e transferência de dados, os legisladores viram-se obrigados a criar uma regulamentação mais específica quanto a esse tema, a fim de evitar barreiras que poderiam ser criadas com o bloco europeu. Trazem a ideia de comprometimento com a proteção de dados levado a um cenário mundial, não se omitindo diante dessas relações comerciais.

Cria-se a lei 13.709/2018 - Lei Geral de Proteção de Dados. Inspirada na lei de proteção de dados europeia (GDPR), a lei brasileira tem por objetivo proteger dados de pessoas naturais, ou seja, pessoas físicas. Não tem por escopo a proteção de dados de empresas, mas sim todos os dados que uma empresa possui de pessoas físicas. Houve veto quanto à criação da Agencia Nacional de Proteção de Dados e entraria em pleno vigor 18 meses após sua publicação. Existem diversos pedidos de adiamento da *vacatio legis,* como observados em seu trâmite, disposto no site do Senado Federal:

> No final de 2018, o presidente da república Michel Temer promulga a Medida Provisória número 869/2019 que autoriza a criação da Autoridade nacional de Proteção de Dados e aumenta o prazo de vacância da lei para 24 meses (agosto de 2020).
>
> No mês de outubro de 2018 foi criado um projeto de lei sugerindo a prorrogação da entrada em vigor da lei para 15 de agosto de 2022. Em março do seguinte ano outro projeto de lei sugere a prorrogação da entrada em vigor da LGPD para 16 de fevereiro de 2022. Ambos os projetos foram acatados.
>
> O Projeto de Lei 1179/2020 é sancionado e convertido na lei nº 14.010/2020 que mantém a vigência da LGPD para agosto de 2020, mas a condição de que as multas

> e sanções só começariam a valer a partir de 1º de agosto de 2021 foi acrescida (Câmara Federal 2018).

2.2. ALGUNS CONCEITOS RELEVANTES NA DISCUSSÃO SOBRE A PROTEÇÃO DE DADOS

Ao conversarmos sobre a troca de dados e a sua proteção, primeiro precisamos compreender a ideia do termo “dados”, a quem dizem respeito e qual a intenção de tutela da legislação vigente na proteção da privacidade e comprometimento com os direitos da personalidade.

A personalidade faz parte desse conceito de dados, sendo descrita como insuficiente para descrever os dados em sua totalidade como descrito por Bruno Bioni onde define a personalidade como:

> características ou o conjunto de características que distingue uma pessoa da outra (nome, integridade física e psíquica seriam um desses atributos). Dada a ipseidade que difere o ser humano dos outros entes e entre seus próprios pares, a ciência jurídica o protege das agressões que afetem a sua individualidade (BIONI, 2019, p. 54).

Os dados se inserem na categoria da personalidade, como afirma Bruno Bioni (2019, p.56): “um dado atrelado à esfera de uma pessoa, pode se inserir dentre os direitos da personalidade. Para tanto deve ser adjetivado como pessoal, caracterizando-se como uma projeção, extensão ou dimensão do seu titular.”

Trata-se de um novo tipo de identidade que pode diferenciar indivíduos movimentando e orientando a economia que se utiliza norteando-se quanto as características. Portando, o autor afirma: “Seria contra procedente e até mesmo incoerente pensar a proteção de dados pessoais somente sob as lentes do direito à privacidade.” (BIONI, 2019, p. 56)

De início, cabe destacar que dados e informação não se equivalem, ainda que sejam recorrentemente tratados como sinônimos e tenham sido utilizados de maneira intercambiável. O doutrinador dá sua definição:

> O dado é o estado primitivo da informação, pois não é algo *per se* que se acresce conhecimento. Dados são fatos brutos que, quando processados e organizados, se convertem em algo inteligível, podendo ser deles extraída uma informação (BIONI, 2019, p.31).

Segundo Wolfgang Hoffmann-Riem,Ne

> os dados na literatura teórica são entendidos como sinais ou símbolos para mensagens que podem ser formalizadas e (aleatoriamente) reproduzidas e facilmente transportadas por meio de meios técnicos adequados. Os dados, enquanto tais, não têm significado. No entanto, podem ser portadores de informação, nomeadamente “informação codificada”. O significado é-lhes atribuído quando estão envolvidos num processo de comunicação de informação por um remetente e de geração e informação pelo destinatário, ou seja, quando se tornam objeto de comunicação. Esta comunicação pode ocorrer entre humanos, mas também entre humanos e máquinas ou entre máquinas (HOFFMANN-RIEM, 2018, p.16).

Thomas Vesting assim define “dados”:

> são “sinais”, “símbolos” não interpretados, que, assim como os números, têm natureza formalizada, podendo ser reproduzidos e transmitidos mediante determinados procedimentos - razão pela qual computadores leem dados -, de sorte que dados dependem de um meio técnico, portanto, físico, e não apenas assumem forma semântica, que se distingue da informação por eles processada (VESTING, 2018, p. 09).

A legislação especial de tratamento de dados em seu Art. 5º, I da define dados pessoais: “art. 5º, I: dado pessoal: dado relacionado à pessoa natural identificada ou identificável”.

Já informações, de acordo com Marion Albers, são

> elementos de sentido obtidos em determinado contexto social, mediante observações, comunicações ou dados e para posterior utilização, sempre dependentes (ou associados) a um processo de interpretação, visto que envolvem uma atribuição de sentido. Assim, embora informações sejam contidas e veiculadas mediante dados, com estes não se confundem, porquanto dependem (daí não terem natureza puramente formal como os dados) do contexto de sua utilização (ALBERS, p. 116-117).

2.2.1. Banco de dados

A Lei Geral de Proteção de Dados define “banco de dados” em seu artigo 5º, inciso IV:

> Art. 5º Para os fins desta Lei, considera-se:
>
> (...)
>
> IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; (BRASIL, 2018, art. 5º inciso IV).

É a coleção organizada de dados, armazenados em meio eletrônico e que se relacionam de alguma forma, permitindo efetuar consultas que retornam os dados armazenados, de diversas maneiras e combinações distintas. É também o armazenamento do considerado “novo petróleo” por diferentes doutrinadores, sendo grande fonte de poder econômico, social e político.

> Os dados pessoais têm sido utilizados por governos e grandes *players* econômicos para a criação de um *one way mirror,* (espelho unilateral) possibilitando que tais agentes saibam tudo dos cidadãos, enquanto estes nada sabem dos primeiros. (PASQUALE, 2015, P. 09).

Nesse contexto, observa-se ainda mais a necessidade de controle e de armazenamento desses dados, de forma que o banco de dados deve estar de acordo com a lei, para que estes não sejam levados a outras atividades. São de tamanha importância, que Yuval Harari (2018) afirma que é talvez a questão política mais importante da nossa era e que, se não formos capazes de dar respostas para esse problema, nosso sistema sociopolítico poderá entrar em colapso.

A dinâmica do banco de dados envolve entrada (input) e processamento de dados e a saída (output) de uma informação. É imprescindível o gerenciamento manual ou automatizado de um banco de dados, para que dele seja extraído algum conhecimento, conforme Bioni (2019, p.32), que, ao analisar o assunto, afirma:

> a informática e a tecnologia da informação foram cruciais, pois foi com os softwares que se automatizou, ainda que parcialmente, a gestão desses bancos de dados,

> havendo, por conseguinte, uma guinada de ordem qualitativa no processamento de tais informações brutas. Fala-se em automatização parcial, pois tais softwares não eliminaram a etapa prévia, conduzida por um ser humano, de estruturação de dados.
>
> O chamado banco de dados operacional, é o local onde é possível emitir faturas de cobrança, relatórios dos clientes inadimplentes etc. Os chamados *data warehouses*, permitem por exemplo identificar um fator que será determinante para adoção ou não de uma ação de marketing, como a classificação daqueles clientes que tem maior probabilidade de serem seduzidos por uma "mala direta", ou, por outro tipo de abordagem publicitária.
>
> O banco de dados deve ser atrelado à ideia de um sistema de informação, cuja dinâmica explicita, sequencialmente, um processo que se inicia pala coleta e estruturação dos dados, perpassa a extração de uma informação que, por fim, agrega conhecimento.

Os bancos de dados servem como uma ferramenta que possibilita a descoberta da tomada de decisões efetivadas, levando a organização dessa ideia de forma mais segura e padronizada, o que traz uma enorme valorização dessas informações visadas; decisões

> que vão desde a concepção de um bem de consumo ao direcionamento da mensagem publicitária. Possibilita-se identificar e precisar o perfil do potencial consumidor, seus hábitos e outras "informações necessárias para a tomada de decisões táticas e estratégicas. Conhecido como mineração de dados ou data mining (BIONI, 2019, p. 33).

Trata da dinâmica de um sistema de informação, que é o que permite a um manancial de fatos (dados) ser estruturado, organizado e gerenciado para produzir um conhecimento que possa ser revertido para tomada de uma decisão.

2.2.2. Big Data

O *Big Data* é uma tecnologia que permite que um volume descomunal de dados seja estruturado e analisado para uma gama indeterminada de finalidades. Conforme Doug Laney (2014):

> o *big data* é comummente associado a 3 (três) "Vs": Volume e Variedade, porque ele excede a capacidade das tecnológicas "tradicionais" de processamento, conseguindo organizar quantidades antes inimagináveis, em diversos formatos (textos, fotos, vídeos) e tudo isso em alta Velocidade." Outros doutrinadores ainda acrescentam mais dois "Vs": Veracidade e Valor.

Os dados passaram a ser analisados não mais em pequenas quantidades ou por amostras, mas em toda sua extensão. Há um grande aumento quanto ao número de dados processados, sendo possível relacionar uma série de fatos. Conforme aponta Bruno Bioni (2019, p. 36) o *big data* não é um sistema inteligente. Não se trata de ensinar o computador a pensar como ser humano, trata-se apenas de uma nova metodologia para que tal ferramental processe e organize dados para inferir a (re)ocorrência de acontecimentos. Conclui que o *Big Data* não se preocupa com a causalidade de um evento, mas tão somente com a probabilidade de sua ocorrência. Em vez de questionar por que algo acontece, procura-se diagnosticar o que está acontecendo. Não se está preocupado com a análise de razões que geram uma cadeia de eventos, mas tão somente, com o seu desencadeamento.

> Dados precisam ser processados e trabalhados para que possam gerar valor. Se tal constatação não afasta a importância dos dados isolados ou "crus", tem o papel fundamental de realçar o fato de que o mero acesso a dados, sem a possibilidade efetiva e eficiente de transformá-los em informações, pode ser insuficiente para resolver diversos problemas competitivos.
>
> Daí a progressiva relevância que se dá ao *Big analytics*, ou seja, a possibilidade de extrair, a partir dos dados, correlações, diagnósticos, padrões, inferências e associações que possam ser consideradas informações (FRAZÃO, 2020, p. 542).

Como afirma a doutrina, deve haver um trabalho com esses dados, de modo que se fossem trazidos sozinhos, não continham determinadas informações obtidas, sendo possível organizá-los para que possam gerar valor. O autor cita a "Competitividade", que deve ser regulada para que não haja uma exploração por parte das empresas a fim de obter conhecimento de quais materiais oferecer a determinada pessoa, a partir de dados gerados.

Representam um novo momento da sociedade, quando a mutação tecnológica ganha força, com uma enorme produção de dados. Carlos Barbieri, em *governança de Dados* (2019, p.107), aponta que o "*big data*" representa um novo estado das tecnologias existentes, algumas agora evoluídas e outras relativamente novas, tudo em função deste novo momento. Fenômenos como a internet, redes sociais, portabilidade, *devices* mais inteligentes (*smart devices*), suas respectivas produções de dados e novas formas de tratá-los (como Inteligência Artificial com aprendizado de máquina) compuseram esse mosaico de fatores do que hoje é chamado simplificadamente de *Big Data*.

3. LEI GERAL DE PROTEÇÃO DE DADOS

3.1. PRINCÍPIOS E FUNDAMENTOS

Os princípios em uma legislação são extremamente importantes, ao passo que se caracterizam por ser a base de todo ordenamento, possuem um maior grau de abstração que contempla toda uma ideia sobre a legislação, tendo os artigos interpretações voltadas aos princípios. O seu não cumprimento pode levar a um vício processual e contratual. Dentre eles a LGPD conta com os seguintes:

1) Princípio da Boa Fé: Princípio previsto em diversas áreas do direito, tratando-se de contratos em que inicialmente, quando celebrados, devem conter sempre boas intenções, sem o propósito de obter determinada vantagem indevida. Dessa forma proíbem-se o abuso, a mentira, falta de consideração e falta de comportamento, devendo manter a confiança existente no momento do ato.

2) Finalidade: O princípio da finalidade versa sobre a motivação e intenção do operador ao obter determinados dados de seus titulares, afim de haver uma boa justificativa para essa aquisição. Devem ser usados para determinado objetivo anunciado no momento da coleta o que limita de usufruí-los indevidamente. O artigo 6º em seu inciso I da lei, descreve: “a realização no tratamento de dados para propósitos legítimos, específicos, explícitos e informações ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades.”

3) Necessidade: Esse princípio descreve a necessidade da obtenção de determinados dados, devendo não ocorrer apenas por mero armazenamento, porém ser preciso para determinada atividade. O artigo 6º da LGPD em seu inciso III prescreve: “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.”

4) Transparência: este contém a ideia de total transparência dos dados coletados, diante de seu titular, podendo solicitar ao operador de seus dados o que está sendo coletado e o que possui em seu armazenamento. Definido na Lei em seu artigo 6º em seu inciso VI: “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."

5) Não discriminação: A discriminação também é repudiada na coleta de informações, sendo proibida, principalmente quando os dados foram sensíveis e relatarem informações pessoais de grande importância ao titular. Não podendo ser utilizado para discriminar alguém por possuir acesso a determinado dado. Ana Paula Moraes, Patrícia Peck e Marcelo Crespo, em *LGPD Aplicada* tratam do princípio diante dos dados sensíveis:

> o princípio da não discriminação deve ser refletido em todas as circunstâncias em que o uso de dados, sejam sensíveis ou não, gere algum tipo de desvalor ou introdução a resultados que seriam equitativos, devendo, portanto, esse princípio servir como base de sustentação de tutela de dados sensíveis, especialmente quando diante do exercício democrático e de direitos sociais, tais como o direito ao trabalho, sem discriminação, saúde e moradia (PINHEIRO, 2020, p.33).

Presente no artigo 6º da LGPD em seu inciso IX: "impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos."

6) Adequação: A adequação faz-se necessária ao passo que a coletânea deve ocorrer de maneira adequada, de maneira prevista em lei. O artigo 6º inciso II da LGPD relata: "compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento."

7) Prevenção: Zela-se pela prevenção ao tratamento dessas informações, devendo evitar de todas as maneiras que sejam desviados de suas finalidades, ou vazadas de forma com que comprometam o titular. Disposta também no artigo 6º em seu inciso VIII: "adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais."

8) Qualidade dos dados: a qualidade dos dados informados deve ser de boa legibilidade de forma que seja possível identificá-los facilmente e com clareza, sempre armazenados de forma atualizada e conforme sua necessidade. Em sua legalidade, disposta no artigo 6º da lei (LGPD), em seu inciso V descreve: "garantia, aos titulares, de exatidão, clareza, relevância a atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento."

9) Segurança: O armazenamento dessas informações deve ter segurança, tratando de informações que pertencem a um titular; deve proteger esse banco de dados

com o objetivo de assegurar o seu acesso, sua clareza e sua inicial motivação. O artigo 6 inciso VII da LGPD traz: “utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acesso não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.”

10) Livre acesso: pode ser analisado com o princípio da transparência, por trazer ao titular o direito de acesso aos seus dados informados, de forma que pode reivindicá-los a qualquer momento, não podendo ser utilizados de maneira omissa. Descrito no artigo 6º da LGPD em seu artigo IV: “garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;”

11) Responsabilização e prestação de contas: por fim, o princípio da prestação de contas tem como finalidade fazer com que o agente que armazena os dados demonstre os cuidados e obediências as normas ordenadas e a real eficácia da tomada dessas medidas. Prevista no último inciso (X) do artigo 6º da LGPD: “demonstração pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.”

Os fundamentos dessa lei estão descritos em seu artigo 2º e tratam das direções que devem ser tomadas ao interpretar a lei perante processos que envolvem a coletânea de dados. Os doutrinadores ressaltam que:

> a lei deixa claro que não estão sujeitos a ela os dados tratados por uma pessoa sem qualquer finalidade econômica, aqueles utilizados para fins artísticos, jornalísticos e acadêmicos. Ou, ainda, para fins de segurança pública, defesa nacional, segurança do estado e atividades de investigação e repressão a infrações penais – nesses casos, haverá legislação específica sobre o assunto e o banco de dados não poderá ser utilizado por empresa privada.
>
> Ela também exclui os dados que tenham origem fora do território nacional, desde que não haja compartilhamento, tratamento ou transferência no Brasil (GARCIA et al., 2020, p.17).

O respeito à privacidade, ao assegurar os direitos fundamentais de inviolabilidade, da honra, da imagem e da vida privada está previsto na Constituição Federal em seu artigo 5º:

> 5º: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; as relações que contém troca de dados detêm o fundamento de respeito ao indivíduo como um todo. (BRASIL, 1989, art. 5º inciso X).

Entretanto, doutrinadores destacam sobre a não semelhança com a proteção abordada na Carta Magna, ao versar sobre esse direito:

> a privacidade e proteção de dados são questões diferentes. Por exemplo, se uma pessoa publicar um dado e sua página pessoal numa rede social, ele se torna público. Entretanto, isso não significa que esse dado pode ser utilizado indiscriminadamente. Aquele que vier a utilizá-lo, deve respeitar os direitos do titular do dado, previstos na LGPD. Tais dados, portanto, não estão sob a égide do princípio constitucional da privacidade, mas sim sob o escopo da proteção de dados (GARCIA et al., 2020, p. 17).

O segundo fundamento é o da autodeterminação informativa. Define-se por:

> garantir que o titular tenha o direito de decidir o que será feito com a sua informação, em saber quais dados as organizações possuem, como elas os utilizam e se ele quer que seu dado esteja com elas, quer seja utilizado ou não. Em outras palavras, de acordo com esse fundamento, cada pessoa natural determina como sua informação pode (e se vai ser) utilizada (GARCIA, 2020, p. 18).

O doutrinador discorre que o fundamento não deve ter apenas olhares para com as pessoas de modo exclusivamente individual, apresentando dupla dimensão: individual e coletiva:

> Não é apenas (embora possa ser, como direito subjetivo individual, o mais importante) a possibilidade de cada um decidir sobre o acesso, uso e difusão de seus dados pessoais, mas também - e aqui a dimensão metaindividual (coletiva) - se trata de destacar que a autodeterminação informativa constitui precondição para uma ordem comunicacional livre e democrática, distanciando-se, nessa medida, de uma concepção de privacidade individualista e mesmo isolacionista à feição de um direito a estar só (*right to be alone*) (BIONI, 2020, p. 51).

Outro tema central, é a liberdade de expressão, de comunicação e de opinião que tem seu fundamento na carta Magna em seu artigo 5º inciso IX que prescreve:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> (...)
>
> IX - é livre a expressão da atividade intelectual, artística, científica e de comunicação, independentemente de censura ou licença; (BRASIL, 1989, art. 5 inciso IX).

A Inviolabilidade da intimidade, da honra e da imagem versa sobre a seguridade em que cada um deve ter de sua imagem, honra e da intimidade e nada mais do que nossos dados para exteriorizar essas informações. Dessa maneira, a lei traz em um de seus fundamentos um direcionamento de controle de dados de forma que não atinja um desses pilares.

O direito ao livre desenvolvimento econômico tecnológico vem como fundamento para esclarecer que a lei não veio para proibir nada, nem mesmo é contra o desenvolvimento da tecnologia e da economia, de modo que ela regula as maneiras em que podem ser coletados esses dados, sem com que ocorra uma atribuição monetária a eles.

A livre iniciativa, a livre concorrência e a defesa do consumidor, nascem com a ideia presente na Constituição Federal (1989), a qual descreve esses direitos de forma que qualquer um do povo poderá participar do mercado, sem a autorização do Estado, juntamente com a possibilidade de ter uma concorrência ampla e legal e por fim a presença da defesa do consumidor, com todos os seus princípios:

> Art. 170. A ordem econômica, fundada na valorização do trabalho humano e na livre iniciativa, tem por fim assegurar a todos existência digna, conforme os ditames da justiça social, observados os seguintes princípios:
>
> I - soberania nacional;
>
> II - propriedade privada;
>
> III - função social da propriedade;
>
> IV - livre concorrência;

> V - defesa do consumidor; (...) (BRASIL, 1989, art. 170).

3.2. DADOS ANÔNIMOS

Os dados anônimos conceituam-se como a oposição do que seria um dado identificável, como afirma o doutrinador:

> antítese de dado pessoal seria um dado anônimo, ou seja, aquele que é incapaz de revelar a identidade de uma pessoa. Diante do próprio significado do termo, anônimo seria aquele que não tem nome nem rosto. Essa inaptidão pode ser fruto de um processo pelo qual é quebrado o vínculo entre o(s) dado(s) e seu(s) respectivo(s) titular(es), o que é chamado de anonimização (...)
>
> Dados anônimos não são dados relacionados a uma pessoa identificada, demandando a reversão do processo de anonimização para se chegar aos respectivos titulares, sendo a sua identificabilidade remota (identificável) e não imediata (identificada) (BIONI, 2018, p.61).

A lei 13.709/2018 (LGPD), em seu 5º artigo, classifica um dado anonimizado como:

> Art. 5º Para os fins desta lei, considera-se:
>
> (...)
>
> III – dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento;

Patrícia Peck (2020) define os dados anonimizados: “são relativos a um titular que não poderia ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião do seu tratamento.”

A anonimização é a caracterização de um dado que perde a possibilidade de associação, direta ou indireta a um indivíduo, porém qualquer dado pessoal anonimizado detém o risco inerente de se transmudar em um dado pessoal. Bruno Bioni (2018, p. 65) classifica que pode gerar o efeito mosaico onde a agregação de diversos “pedaços” de informações (dados) pode revelar (identificar) a imagem (sujeito) do quebra-cabeça, imagem que era, até então, desfigurada (anônima).

Preocupa-se com essa facilidade de conversão de dados anonimizados em dados identificados, feita por terceiros, de maneira que a característica de “anônimo” na cessão desses dados pode ser comprometida. Daniel Bittencourt Guariento e Ricardo Maffeis Martins (2020), compartilham da ideia da não efetiva anonimização de dados, que facilmente pode ser descaracterizada como tal, passando a ser identificada pelo seu titular. Em suas palavras:

> independentemente de qualquer regulamentação pela ANPD (Agência Nacional de Proteção de Dados), levando em consideração o ritmo atual de evolução tecnológica, parece que teremos cada vez mais dificuldade em garantir a efetiva anonimização de dados pessoais, exigindo, a nosso ver, que essa anonimização seja feita por empresa independentemente (e não internamente pelo controlador) e mediante a utilização continuada de técnicas de última geração, que sejam constantemente atualizadas, mantendo o estado da arte (GUARIENTO e MARTINS, 2020).

Os autores citam ainda pesquisas realizadas em outros países que identificam essa fácil “desanonimização”:

> o primeiro desses estudos denominado *Unique in the crowd: the privacy bounds of human mobility*, realizado em 2013 pelas universidades de Harvard, nos Estados Unidos, e Louvain, na Bélgica, bem como pelo Massachusetts Institute of Technology, também nos Estados Unidos, e publicado na *Scientific Reports*, chegou-se à conclusão de que pessoas podem ser rastreadas e identificadas a partir de bancos de dados contendo informações em princípio consideradas anonimizadas.
>
> A pesquisa realizada por 15 meses com base em dados de telefones móveis de cerca de 1,5 milhão de indivíduos, demonstrou que, quando a informação do indivíduo foi disponibilizada em base horária pelas antenas de celulares, apenas quatro pontos de dados foram necessários para reidentificar a pessoa. Isso se mostrou verdade em 95% dos casos, sendo levado à conclusão de que os movimentos de seres humanos são altamente idiossincráticos, apresentando traços únicos que podem ser analisados com precisão. (GUARIENTO e MARTINS, 2020).

Um segundo estudo mais recente, de 2019, denominado *Estimating the success of reidentifications in complete datasets using generative models*, realizado mais uma vez pela Universidade de Louvains, em conjunto com a *Imperial College of Science*, *Technology and Medicine*, em Londres, publicados na *Nature Communications*, estimou, com a ajuda de *machine learning*, a probabilidade de um indivíduo especifico ser reidentificado a partir de banco de dados anonimizados, ainda que incompletos.

“Nesta pesquisa, chegou-se à conclusão de que 99,98% dos americanos podem ser corretamente reidentificados a partir de qualquer banco de dados, utilizando 15 atributos demográficos - idade, gênero, estado civil etc. (...)”

Aos titulares, a falta de crédito e confiança é válida, ao passo que gerando algumas informações, estas podem ser facilmente reconhecidas e individualizadas em banco de dados. A regulamentação mais específica sobre este assunto, faz-se necessária, a fim de formalizar os processos de anonimização, suas técnicas e padrões legais, de modo que a atualização da norma deve ocorrer com a mesma paridade tecnológica à desanonimização.

3.3. DADOS SENSÍVEIS

Uma outra subclassificação de dados existe, visto a sua necessidade, comparada às demais. Patrícia Peck classifica dados sensíveis caracterizando-os como:

> são dados da personalidade do indivíduo e suas escolhas pessoais, tais como 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. (PINHEIRO, 2020, p.35).

Na LGPD lemos:

> “Art. 5º Para os fins desta Lei, considera-se:
>
> (...)
>
> II - dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural; (BRASIL, 2018, art. 5 inciso II).

Bruno Bioni (2021, p.152) descreve a possibilidade de enquadramento nos casos em que esses dados abordam matéria de origem racial ou étnica, convicção religiosa, opinião política e filiação a sindicato ou a organização de caráter religioso, filosófico ou político. São

também sensíveis aqueles referentes à saúde, à vida sexual e a dados genéticos ou biométricos. Acerca de sua determinação,

> entende-se que essencial para se determinar se um dado é sensível ou não é verificar o contexto de sua utilização, além das relações que podem ser restabelecidas com as demais informações disponíveis e a potencialidade de seu tratamento servir como instrumento de estigmatização ou discriminação. (BIONI, 2021, p.153).

Destaca a doutrina: “(...) deve-se admitir que certos dados, ainda que não tenham, a princípio, essa natureza especial, venham a ser considerados como tal, a depender do uso que deles é feito no tratamento de dados”. (MULHOLLAND, 2019, p. 49).

O doutrinador ainda acrescenta a característica da possibilidade de discriminação: “os dados sensíveis correspondem a uma tipologia diferente em razão de o seu conteúdo oferecer uma especial vulnerabilidade: discriminação.” (BIONI, 2021, p. 158). O autor acrescenta ter uma umbilical relação com a dignidade da pessoa humana e os direitos de personalidade. Faz total atribuição ao princípio da Não Descriminalização.

Surge aí a preocupação em haver distinção ou diferenciação de uma pessoa por conta de tais aspectos da sua personalidade. Leis de proteção de dados pessoais, inclusive a brasileira, dedicam um regime jurídico mais protetivo em relação a dados sensíveis com o intuito de frear práticas discriminatórias.

Em sua Seção II, a lei 13.709/2018 descreve em seu artigo 11, casos possíveis de tratamento de dados pessoais sensíveis:

> Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:
>
> I – quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;
>
> II – sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:
>
> a) cumprimento de obrigação legal ou regulatória pelo controlador;
>
> b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

> c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
>
> d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei de Arbitragem;
>
> e) proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou
>
> g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais (BRASIL, 2018, art. 11).

Determinados dados merecem uma maior atenção, pois tratam de informações que dizem estritamente a respeito de escolhas, condições e características. As instituições que os armazenarem, necessitarão mantê-los seguros, com um padrão ainda mais rigoroso de proteção, a exemplo dos dados biométricos, que recebem essa maior atenção por ser um reconhecimento, imutável, duradouro e singular perante aos demais.

A lei faz menção a duas vertentes: (1) com o consentimento do titular ou responsável legal e (2) nas hipóteses em que for indispensável para determinadas atividades trazidas pelo artigo, não devendo haver uma separação entre elas, muito menos uma maior valoração de uma em contraposição da outra, como afirma a doutrina:

> tanto na hipótese de tratamento de dados sensíveis por meio do consentimento do titular quanto naquelas que se referem às demais situações que impedem desta manifestação de autonomia, previstos nos incisos I e II do art. 11 da LGPD, reconhece-se na técnica legislativa utilizada uma posição de igualdade entre essas hipóteses, e não a de prevalência do consentimento (MULHOLLAND, 2019, p. 52).

É necessário que o consentimento para a utilização de seus dados seja caracterizado de forma específica e destacada:

> específico deve ser compreendido com um consentimento manifestado em relação a propósitos concretos e claramente determinados pelo controlador e antes do tratamento dos dados, havendo também aqui, e com ênfase, as obrigações de granularidade.
>
> Destacado pode ser interpretado no sentido de que é importante que o titular tenha pleno acesso ao documento que informará todos os fatos relevantes sobre o tratamento, devendo tais disposições vir destacadas para que a expressão do

> consentimento também o seja. Além de se referir a dados determinados e haver declaração de vontade que esteja ligada a objetivo específico, a manifestação de vontade deverá vir em destaque no instrumento de declaração que autoriza o tratamento (BIONI, 2021, p. 156).

De acordo com Rodotà, reconhece-se que o consentimento do titular de dados sensíveis deve ser qualificado, na medida em que estamos diante de um “contratante vulnerável”, caracterizado justamente pela ausência de liberdade substancial no momento da determinação da vontade, e pela natureza do objeto do tratamento, quais sejam, interesses de natureza personalíssima (RODOTÀ, 2008, p.90).

O artigo, 11, II, “g” trouxe uma possibilidade de seu armazenamento nos casos em que estes são utilizados para fins de identificação e proteção ao acesso de maiores valores. A exemplo de agências bancárias que utilizam do armazenamento de biometrias, a fim de trazer maior agilidade e segurança no momento de acesso as contas bancárias pessoais, de forma a prevenir fraudes contra seus clientes. O mesmo artigo em seu parágrafo 5º, especifica:

> § 5º É vedado às operadoras de planos privados de assistência à saúde o tratamento de dados de saúde para a prática de seleção de riscos na contratação de qualquer modalidade, assim como na contratação e exclusão de beneficiários. (BRASIL, 2018, art. 11, § 5º).

Tratando-se de dados sensíveis que dizem respeito a características das pessoas, inclusive se possuir alguma doença mental, física, ou se necessita de remédios, impossibilita que planos de saúde se utilizem dessas informações para diferenciação ou até mesmo maior valoração nos preços mensais do plano de saúde e diferenciação no momento da contratação ou exclusão de beneficiários.

3.4. TRANSFERÊNCIA INTERNACIONAL DE DADOS

A transferência de dados pessoais de forma que ultrapassa as fronteiras brasileiras, estão em constante aumento. O processo de Globalização, criou ferramentas que facilitaram a comunicação entre diversos polos do planeta, como no caso de uma mensagem que, enviada do Brasil, chega instantaneamente ao outro lado do mundo. As

compras virtuais de outros países também se tornaram parte da rotina humana. Essas atividades envolvem troca de dados e ainda com a participação de mais de dois países. Como controlar isso, a fim de que essas informações sejam seguramente armazenadas em um outro território?

A própria LGPD traz em seu artigo 33, limitações quanto a essa transferência:

> Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:
>
> I - para países ou organismos internacionais que proporcionem grau de proteção de dados pessoais adequado ao previsto nesta Lei;
>
> II - quando o controlador oferecer e comprovar garantias de cumprimento dos princípios, dos direitos do titular e do regime de proteção de dados previstos nesta Lei, na forma de:
>
> a) cláusulas contratuais específicas para determinada transferência;
>
> b) cláusulas-padrão contratuais;
>
> c) normas corporativas globais;
>
> d) selos, certificados e códigos de conduta regularmente emitidos;
>
> III - quando a transferência for necessária para a cooperação jurídica internacional entre órgãos públicos de inteligência, de investigação e de persecução, de acordo com os instrumentos de direito internacional;
>
> IV - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;
>
> V - quando a autoridade nacional autorizar a transferência;
>
> VI - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;
>
> VII - quando a transferência for necessária para a execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do inciso I do caput do art. 23 desta Lei;
>
> VIII - quando o titular tiver fornecido o seu consentimento específico e em destaque para a transferência, com informação prévia sobre o caráter internacional da operação, distinguindo claramente esta de outras finalidades; ou
>
> IX - quando necessário para atender as hipóteses previstas nos incisos II, V e VI do art. 7º desta Lei.
>
> Parágrafo único. Para os fins do inciso I deste artigo, as pessoas jurídicas de direito público referidas no parágrafo único do art. 1º da Lei nº 12.527, de 18 de novembro de 2011 (Lei de Acesso à Informação), no âmbito de suas competências legais, e responsáveis, no âmbito de suas atividades, poderão requerer à autoridade nacional a avaliação do nível de proteção a dados pessoais conferido por país ou organismo internacional. (BRASIL, 2018, art. 33).

A doutrinadora Patrícia Peck Pinheiro (2020, p. 111) afirma que o Brasil segue o movimento europeu de padronização internacional do fluxo de dados, assim como de proteção dessas informações, de maneira a garantir que o desenvolvimento tecnológico e

econômico possa continuar seu acelerado e complexo processo, sem que, com isso, direitos e garantias fundamentais sejam relativizados ou violados. A autora aponta, por fim, a existência de uma padronização do modelo de cláusulas contratuais que deve ser observada pelas instituições em suas relações corporativas globais ou em seus códigos internos e, ainda, que os países que se envolverem nessa relação contratual devem oferecer a garantia da proteção dos dados pessoais em mesmo grau que a LGPD prevê.

O artigo 34 da mesma lei define que o nível de proteção de dados do país estrangeiro ou do organismo internacional será avaliado pela Autoridade Nacional. As Autoridades Nacionais acima citadas são: "órgão da administração pública indireta responsável por zelar, implementar e fiscalizar o cumprimento desta lei." Esta deverá levar em consideração para análise, como citado no artigo 34 da LGPD,: (i) as normas gerais e setoriais em vigor no país ou organismo internacional; (II) a natureza dos dados; (III) a observância de princípios gerais de proteção de dados e direitos dos titulares; (IV) a adoção de medidas de segurança; (V) a existência de garantias judiciais e institucionais para o respeito aos direitos de proteção de dados; e (VI) outras circunstâncias específicas que forem relevantes para a transferência, Portanto, adequando-se às exigências de determinado país, qualquer pessoa poderá transferir dados livremente.

O artigo 44 da GDPR[8], dentro de seu capítulo 5, que trata da transferência de dados para países terceiros ou organizações internacionais, afirma ser de extrema necessidade que territórios estrangeiros cumpram os requisitos impostos pela legislação europeia e um nível adequado de proteção, a fim de que não haja descumprimento da legislação, tampouco a queda na qualidade de proteção de dados. Em seu artigo 45[9], a GDPR trata da necessidade do nível de proteção dos titulares localizados na União Europeia, sendo condicionados à Comissão Europeia sobre o nível de proteção em países terceiros, territórios estrangeiros ou organizações internacionais. Com a observação da grande

[8] *[1]Any transfer of personal data which are undergoing processing or are intended for processing after transfer to a third country or to an international organisation shall take place only if, subject to the other provisions of this Regulation, the conditions laid down in this Chapter are complied with by the controller and processor, including for onward transfers of personal data from the third country or an international organisation to another third country or to another international organisation. [2]All provisions in this Chapter shall be applied in order to ensure that the level of protection of natural persons guaranteed by this Regulation is not undermined.*

[9] *[1]A transfer of personal data to a third country or an international organisation may take place where the Commission has decided that the third country, a territory or one or more specified sectors within that third country, or the international organisation in question ensures an adequate level of protection. 2Such a transfer shall not require any specific authorisation.*

interferência europeia na aceitação ou não quanto à transferência de dados pessoais, Cintia Rosa Pereira e Kelvin Peroli (2019, p. 80) afirmam tratar-se da “europeização”. Em virtude da incessante regulação em busca de determinada proteção, instaurou-se uma corrida pelo alcance do nível protetivo adequado aos padrões da UE, em razão de que os dados relativos aos titulares localizados na UE podem apenas ser tratados por aqueles que as autoridades garantistas da UE afirmem possuir o nível protetivo requerido. Caso contrário, o tratamento dos dados por agentes de tratamento estrangeiros, realizado por intermédio da circulação internacional dos dados, pode ser bloqueado.

Nada mais caracterizado do que um modelo a ser seguido por outros países e por influência, na maioria das vezes necessidade de contato com o grupo econômico, demais territórios alteram e adequam suas legislações, como no caso do Brasil.

Marcel Leonardi em contrapartida a intensivos cumprimentos de requisitos para a troca de dados, alerta esperar que a Autoridade Nacional adote modelos flexíveis para viabilizar, de modo prático, rápido e eficaz, a transferência internacional de dados pessoais.

> Um modelo restritivo cria barreiras comerciais que podem limitar a inovação, a produção de conhecimento e o acesso à informação no território brasileiro e contraria o estado da arte da economia, uma vez que a lógica de adequação não é mais aplicável à natureza global e atual dos fluxos de dados pessoais, principalmente em um país em desenvolvimento como o Brasil, que não tem o mesmo peso da União Europeia para impor esse modelo ao resto do mundo. (2020, p. 309).

Importante ressaltar que a proteção à privacidade e aos dados é o grande objetivo da Lei. Deixar de olhar para os requisitos necessários ao transferir dados além das fronteiras do país, pode fazer com que estes sejam corrompidos e utilizados para outras finalidades, por atualmente possuírem enorme valor, “novo petróleo”, devem haver termos e condições para essas atividades. Com equiparação ao Bloco Europeu, faz-se necessário o cumprimento de modo que as relações entre Brasil e União Europeia são inúmeras, de grande importância e ainda mais por motivos de o bloco possuir tamanha bagagem em sua história, pioneiro na proteção de dados.

3.5. RESPONSABILIZAÇÕES E RESPECTIVAS SANÇÕES NO ÂMBITO DAS TRÊS ÁREAS DE RESPONSABILIZAÇÃO DO DIREITO (PENAL, CIVIL E ADMINISTRATIVO)

Na tentativa de frear o compartilhamento do uso de dados pessoais de maneira excessiva e ilegal, são criadas leis, com objetivo de responsabilização e punição. Áreas do direito trazem essa possibilidade, de maneira que o Estado possa punir o infrator da mesma forma em que o ofendido pode pedir ressarcimento pelos danos sofridos. Um grande avanço no controle de informações utilizadas pelos controladores e operadores que indiretamente detém maior atenção na segurança e legalidade de suas atividades.

A responsabilidade civil vem como ferramenta com fins de concretizar o ressarcimento de danos causados por aqueles que tratam os dados de titulares de maneira irregular, tendo a função de assegurar o respeito aos direitos de terceiros. São obrigações impostas aos que violam direito de titular regulamentado em lei.

> É o instituto cuja finalidade é aplicar medidas que obriguem alguém a reparar dano patrimonial e/ou extrapatrimonial (moral) causado a outra pessoa, buscando assim reequilibrar a situação das partes, bem como inibir outros atos transgressores.
>
> (...)
>
> O exame da responsabilidade civil pode ser visto, basicamente, em duas situações. A primeira, pela questão do não cumprimento contratual (inadimplemento), em que está presente a responsabilidade extracontratual. Alguns consideram superada esta divisão de regimes em contratual e aquiliana, preferindo falar em responsabilidade legal (derivada da lei). (LIMA, 2020, p.300).

Os controladores descritos no capítulo 3 da LGPD, devem garantir que os deveres e responsabilidades descritos em lei sejam respeitados. É definido pela lei 13.709/2018, em seu art. 5º, VI como: “VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;”

Em outra classificação podemos ver o controlador como aquele que recepciona os dados pessoais dos titulares de dados por meio do consentimento ou por hipóteses de exceção (PINHEIRO, 2018, p.36). Possui enorme reponsabilidade perante a tutela e manejo desses dados.

No caso do operador, é também definido pela lei em seu art. 5º inciso VII: “VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;”. “O operador é aquele que realiza algum

tratamento de dados pessoais motivado por contrato ou obrigação legal.” (PINHEIRO, 2018, p. 36).

Em regra, seguindo o artigo 42[10] da LGPD, o controlador e operador respondem individualmente, pelos danos causados ao titular de dados, ficando os bens do agente responsável pela reparação dos danos causados pelo ato ilícito, no caso de pessoa jurídica de sociedade limitada, esta responde até o valor de seu patrimônio social. Na reparação desses danos, devem ser levados em conta a reabilitação em lucros cessantes, dano patrimonial e extrapatrimonial e danos emergentes.

> A LGPD mandou bem ao mencionar expressamente as diferentes espécies de danos que podem resultar do tratamento de dados pessoais, evitando dúvidas quanto à ampla proteção reservada não apenas aos titulares de dados pessoais, mas também a terceiros. (...) A LGPD amplia expressamente essa esfera de proteção, de modo a abranger não apenas interesses outros daquele mesmo titular (interesses econômicos, por exemplo), mas também interesses transindividuais que possam ter sido lesados pelo referido tratamento (SCHREIBER, 2020, p. 330).

A obrigação é solidária no caso de descumprimento da lei, seguindo o artigo 42 § 1º, que deixa claro que poderá ocorrer a responsabilização tanto do operador quanto do controlador de forma solidária, existindo entre eles algo que faça com que os prejudicados sejam ressarcidos independentes da discussão de culpa.

> O inc. I do §1º do art. 42[11] dispõe que o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados; ou quando não tiver seguido as instruções lícitas do controlador (à luz do art.39). Neste caso, operador fica equiparado a controlador (exceto quanto às exclusões previstas no art. 43) (LIMA, 2020, p. 315).

---

[10] Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo.

[11] § 1º A fim de assegurar a efetiva indenização ao titular dos dados:
I - o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador equipara-se ao controlador, salvo nos casos de exclusão previstos no art. 43 desta Lei;
II - os controladores que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados respondem solidariamente, salvo nos casos de exclusão previstos no art. 43 desta Lei.

Salienta-se que nesse caso a importância do contrato firmado entre controlador e operador de forma bem detalhada, sendo através deste possível identificar as instruções informadas pelo controlador ao operador, a qual explica a possibilidade de regresso a depender do que estava previsto anteriormente.

> Ainda, visando concretizar a indenização ao titular, o inc. II do § 1º do art. 420 da LGPD descreve que, havendo dois ou mais controladores, os que estiverem diretamente envolvidos no tratamento do qual decorreram danos ao titular dos dados responderão solidariamente (salvo excludentes do art, 43) (LIMA, 2020, p. 316).

Aquele que pagar a indenização tem a possibilidade de regresso em desfavor de quem pagou a obrigação, como assegura o artigo 42 da lei em seu parágrafo 4º: "§4º Aquele que reparar o dano ao titular tem direito de regresso contra os demais responsáveis, na medida de sua participação no evento danoso."

As excludentes de responsabilidade que estão prescritas no art. 43 da LGPD tratam de três hipóteses em que é possível o afastamento da responsabilização: "quando não realizarem o tratamento de dados pessoais que lhes é atribuído; não houve violação à legislação de proteção de dados; ou o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiros".

Nos casos em que houver culpa concorrente, de modo que a responsabilidade não fica de modo exclusivo do controlador ou operador, tendo o titular parte, não afasta a responsabilidade do controlador ou do operador, de modo que atenua-se o valor cobrado para fins indenizatórios, seguindo neste caso o artigo 945[12] do Código Civil.

Já a culpa exclusiva do titular dos dados afasta a responsabilidade do operador ou controlador em arcar com danos advindos de certa ação ou omissão que tem por responsabilidade exclusiva o próprio titular. Exemplifica-se no caso em que o titular dos dados pessoais os divulga publicamente em plataformas digitais; ou armazena seus dados de forma insegura em um *pendrive*, o qual é esquecido negligentemente em local público. (LIMA, 2020, p. 318).

[12] Art. 945. Se a vítima tiver concorrido culposamente para o evento danoso, a sua indenização será fixada tendo-se em conta a gravidade de sua culpa em confronto com a do autor do dano.

Por fim, quanto à exclusão perante a responsabilidade por culpa exclusiva de terceiro:

> Para a sua aplicação este terceiro não pode ser alguém que mantenha qualquer tipo de relação com o fornecedor (como comerciantes-intermediários, agentes, funcionários, prepostos em geral etc). Terceiro é uma pessoa que não se identifique com o controlador ou o operador (fornecedor), nem com o titular dos dados (consumidor).
>
> (...)
>
> Ressalte-se que quando se pensa na excludente da culpa exclusiva de terceiros, e tratamento ilícito de dados, não é possível alegar a hipótese de corrompimento de sistema (invasão de *hackers*, por exemplo) se ficar comprovado que as medidas de segurança adotadas pelo agente de tratamento não seguiam os padrões estabelecidos no art. 44 da LGPD (LIMA, 2020, p. 318).

Muitos autores sustentam a ideia de que a responsabilização se dá de forma subjetiva, de forma que seria responsabilizada caso houvesse a culpa do agente:

> Em versões anteriores ao Projeto de Lei que deu origem à Lei Geral de Proteção de Dados, chegou a se incluir disposições que conceituavam a atividade de tratamento de dados pessoais como atividade de risco, expressamente, as quais, no entanto, foram retiradas da proposição no decorrer do processo legislativo. Por conta disso, é possível sustentar que a regra geral da Lei é a da responsabilidade civil subjetiva, na qual o elemento da culpa deverá ser demonstrado, admitida em algumas hipóteses específicas, a responsabilidade civil objetiva, de acordo com a natureza do tratamento de dados pessoais, que realmente possa se enquadrar como atividade de risco (BLUM, 2019, p.323).

Defendendo a mesma corrente de que a LGPD se enquadraria em seu modo de responsabilização subjetiva, defensores da corrente afirmam que por seguir os parâmetros da GDPR (art.82, inciso I), apontam violação a esse regulamento, que no continente Europeu se tem defendido essa ideia: “Art. 82 Qualquer pessoa que sofrer danos materiais ou imateriais devido a uma violação do presente Regulamento tem o direito de receber uma indenização do responsável pelo tratamento ou do subcontratante pelos danos sofridos.”[13]

Em outra ponta, doutrinadores afirmam não causar espanto a responsabilidade objetiva no âmbito da LGPD, fazendo ligação ao Código de Defesa do Consumidor que

---

[13] *(82) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*

permite a matéria da responsabilidade sem culpa. No mesmo posicionamento houve um parecer da Comissão Especial constituída pela Câmara dos Deputados em 25 de outubro de 2016 que expressa:

> A atividade de tratamento de dados pessoais constitui atividade de risco, o que atrai a incidência da responsabilidade objetiva ao agente de tratamento, ou seja, aquela segundo a qual não há necessidade de perquirir a existência de culpa para obrigar o causador do dano a repará-lo. Esta já é a regra geral do direito brasileiro para toda e qualquer atividade de risco, conforme previsto no parágrafo único do artigo 927 do Código Civil, como também constitui base da responsabilização dos fornecedores nas relações de consumo[14] (POSICIONAMENTO DA COMISSÃO ESPECIAL, 2016).

A inversão do ônus da prova presente em outras leis como o Código de Defesa do Consumidor, instituto em que trata a produção de provas, pertencentes à acusação, faz com que a parte acusada deva provar que não praticou determinado vício, de modo que poderão ocorrer de acordo com o art. 42[15] da LGPD em seu parágrafo 2º em três ocasiões que podem ser destacados: I- For verossímil a alegação; II- houver hipossuficiência para fins de produção de provas; ou III- A produção de prova pelo titular resultar-lhe excessivamente onerosa.

> Entende-se por verossimilhança a plausibilidade da narrativa fática apresentada pelo autor da demanda, muitas vezes confirmada pelas regras de experiência. Seu reconhecimento vincula-se, comumente, à produção, ao menos, de “prova indiciária, que possibilita ao juiz realizar uma associação entre dois fatos: um comprovado (o fato indiciário) e outro apenas alegado (o fato constitutivo do direito do consumidor). (BIONI, 2020, p. 345).

É também justificada sua utilização pelo fato de que os agentes de tratamento de dados estarão em posse das provas necessárias à instrução do processo. Já a hipossuficiência do titular de dados em relação a quem os trata, de modo que a sua posição em relação aos outros é de muita desvantagem sem acesso ao sistema de armazenamento de dados de forma fácil e direta e muitas vezes sem o necessário conhecimento de comprovação de eventual irregularidade:

---

[14] Ver: https://www.camara.leg.br/proposicoesWeb/prop_mostrarintegra?codteor=1663305&filename=

[15] § 2º O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

> A hipossuficiência do titular de dados se torna facilmente constatável quando se tem uma sociedade permeada pela cultura do *Big Data*, em que há uma coleta massiva de dados, muitas vezes até desnecessária. Diante dessa realidade, o titular de dados se encontra em uma posição claramente desfavorável, em que beira o impossível saber quais de seus dados estão sendo tratados, de forma que isso tem sido feito e que, seriam os agentes de tratamento (LIMA, 2020, p. 323).

O reconhecimento de hipossuficiência é um importante instrumento, que traz com clareza a base do Código de Defesa do Consumidor, onde o consumidor é visto como hipossuficiente, tendo como maiores garantias em seu código, como a exemplo o instituto da inversão do ônus da prova. Ressalta-se sua importância em casos geralmente vistos na exposição indevida de dados pessoais, em que mesmo por meio de investigações policiais fica difícil a descoberta da fonte originária de tal ilegalidade.

> A fonte originária de dados pessoais expostos indevidamente nem sempre é passível de identificação (*trackable*) e o caminho percorrido pelos dados pessoais frequentemente restará demonstrado mais a título de efetiva probabilidade que de certeza matemática. Aqui, desempenha papel relevante o mecanismo de inversão do ônus da prova (BIONI, 2020, p.340).

A aplicação da lei em seu ramo administrativo encontra-se a partir de seu artigo 52, trazendo as possíveis sanções aos agentes que tratam dados de maneira infracional em desacordo com a lei, estimulando ao agente maior atenção e investimento em segurança digital e proteção ao banco de dados.

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
>
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
>
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração;
>
> III - multa diária, observado o limite total a que se refere o inciso II;

IV - publicização da infração após devidamente apurada e confirmada a sua ocorrência;

V - bloqueio dos dados pessoais a que se refere a infração até a sua regularização;

VI - eliminação dos dados pessoais a que se refere a infração;

(...)

X - suspensão parcial do funcionamento do banco de dados a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador;

XI - suspensão do exercício da atividade de tratamento dos dados pessoais a que se refere a infração pelo período máximo de 6 (seis) meses, prorrogável por igual período;

XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados.

§ 1º As sanções serão aplicadas após procedimento administrativo que possibilite a oportunidade da ampla defesa, de forma gradativa, isolada ou cumulativa, de acordo com as peculiaridades do caso concreto e considerados os seguintes parâmetros e critérios:

I - a gravidade e a natureza das infrações e dos direitos pessoais afetados;

II - a boa-fé do infrator;

III - a vantagem auferida ou pretendida pelo infrator;

IV - a condição econômica do infrator;

V - a reincidência;

VI - o grau do dano;

VII - a cooperação do infrator;

VIII - a adoção reiterada e demonstrada de mecanismos e procedimentos internos capazes de minimizar o dano, voltados ao tratamento seguro e adequado de dados, em consonância com o disposto no inciso II do § 2º do art. 48 desta Lei;

IX - a adoção de política de boas práticas e governança;

X - a pronta adoção de medidas corretivas; e

XI - a proporcionalidade entre a gravidade da falta e a intensidade da sanção.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas na Lei nº 8.078, de 11 de setembro de 1990, e em legislação específica.

§ 3º O disposto nos incisos I, IV, V, VI, X, XI e XII do caput deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº

> 8.112, de 11 de dezembro de 1990, na Lei nº 8.429, de 2 de junho de 1992, e na Lei nº 12.527, de 18 de novembro de 2011.
>
> § 4º No cálculo do valor da multa de que trata o inciso II do caput deste artigo, a autoridade nacional poderá considerar o faturamento total da empresa ou grupo de empresas, quando não dispuser do valor do faturamento no ramo de atividade empresarial em que ocorreu a infração, definido pela autoridade nacional, ou quando o valor for apresentado de forma incompleta ou não for demonstrado de forma inequívoca e idônea.
>
> § 5º O produto da arrecadação das multas aplicadas pela ANPD, inscritas ou não em dívida ativa, será destinado ao Fundo de Defesa de Direitos Difusos de que tratam o art. 13 da Lei nº 7.347, de 24 de julho de 1985, e a Lei nº 9.008, de 21 de março de 1995.
>
> § 6º As sanções previstas nos incisos X, XI e XII do caput deste artigo serão aplicadas:
>
> I - somente após já ter sido imposta ao menos 1 (uma) das sanções de que tratam os incisos II, III, IV, V e VI do caput deste artigo para o mesmo caso concreto; e
>
> II - em caso de controladores submetidos a outros órgãos e entidades com competências sancionatórias, ouvidos esses órgãos.
>
> § 7º Os vazamentos individuais ou os acessos não autorizados de que trata o caput do art. 46 desta Lei poderão ser objeto de conciliação direta entre controlador e titular e, caso não haja acordo, o controlador estará sujeito à aplicação das penalidades de que trata este artigo (BRASIL, 2018, art. 52).

A fiscalização e aplicação de determinadas sanções fica de responsabilidade da Agencia Nacional de Proteção de Dados (ANPD), porém a fiscalização e vigilância da lei podem ser feitas também pelo Ministério Público.

> A imputação das sanções deve sempre observar a proporcionalidade como um critério para prevenir e inibir possíveis abusos do poder estatal no momento do exercício de suas funções.
>
> (...)
>
> Há de se considerar uma dosagem na aplicação das punições, sob pena de inviabilizar a pequena empresa ou mesmo os projetos de maior inovação que tendem a assumir mais riscos operacionais. (PINHEIRO, 2020, p. 132).

A proporcionalidade é necessária, a fim do não cometimento de injustiças e uma melhor análise geral (citado no parágrafo 1º do artigo 52 da LGPD), através de incisos que trazem itens necessários de serem avaliados para enfim gerar uma real sanção,

proporcional à empresa, de modo que deve ser sempre respeitada a ampla defesa no procedimento administrativo.

> As sanções administrativas seguem uma gradação:
>
> - Advertência
> - Multa simples
> - Multa diária
> - Bloqueio dos dados
> - Eliminação dos dados
> - Suspensão do funcionamento do banco de dados
> - Suspensão do tratamento de dados
> - Proibição parcial ou total do exercício de atividades que se relacionem com o tratamento de dados.
>
> Além dessas sanções, há também a possibilidade de dar ampla publicidade à infração, e, em todos os casos, é preciso notificar o motivo do problema e as medidas corretivas planejadas e executadas. (GARCIA, FERNANDES, GONÇALVES, BARRETO, 2020, p. 24-25).

Apesar da ordem descrita pela doutrina, o legislador declara que não há necessidade de observância dessa ordem para a aplicação de sanções administrativas, podem elas ser aplicadas de forma isolada ou cumulativamente. A ampla publicidade, faz com que determinada empresa seja autuada e demonstrada a outras que se assim também agirem, terão as mesmas consequências. De forma indireta, também perde determinada credibilidade perante aos seus consumidores, que se sentem com a privacidade ameaçada. A UE possui um site[16], especificando as sanções que são impostas pela Agência Regulamentadora Europeia, demonstrando exorbitantes preços que são pagos por pessoas jurídicas por não cumprirem determinadas ordens.

Devem ser observados o princípio da proporcionalidade, presente no Direito Administrativo de modo que a ANPD como agência reguladora, deverá seguir tal descrição. Em comparação a GDPR, que traz em seu artigo 83, a necessidade de adoção dos critérios e proporcionalidade a momento da aplicação de conduta, reforça a ideia da lei em trazer determinado instituto a fim de não prejudicar em exagerado tal empresa por eventuais tratamentos errôneos de dados. “Art. 83 As autoridades de controlo deverão prestar-se

[16] Ver: https://www.enforcementtracker.com/

mutuamente assistência no exercício das suas atribuições, por forma a assegurar a execução e aplicação coerentes das disposições adotadas por força da presente diretiva."[17]

Vale dizer que as sanções são ferramentas que visam a prevenção da utilização irregular de dados, de modo que haverá prejuízos casos sejam desobedecidos, trazendo multas de até 2% do faturamento da empresa, não podendo ultrapassar R$ 50.000.000,00 (cinquenta milhões de reais) por cada ato. Vista por outro lado, a lei leva sempre em consideração o sistema utilizado por cada empresa, no armazenamento de seus dados e de que forma trabalha para sua segurança.

Em específico, a LGPD não traz em sua escrita, a responsabilização penal, porém não é impedida que se utilize de outros códigos para que determinadas condutas sejam passíveis de responsabilização perante outros códigos como a exemplo do CDC e CP.

O artigo 154-A[18] do Código Penal descreve casos em que ocorre a invasão informática com o fim de obter dados, alterá-los ou destruí-los sem autorização do usuário, podendo incorrer em pena de 1 a 4 anos e multa. Observa-se que a intenção do legislador com o artigo é evitar a violação de privacidade e quando isso é feito mediante valoração, como para venda ou repasse desses dados, há um agravante na pena.

> O e-mail tornou-se uma forma padrão de enviar informes e mensagens a profissionais e particulares, seja para fins comerciais, seja para outras finalidades, as mais diversas possíveis. As redes sociais criaram, também, mecanismos de comunicação, com dispositivos próprios de transmissão de mensagens. Torna-se cada vez mais rara a utilização de cartas e outras bases físicas, suportando escritos, para a comunicação de dados e informes. Diante disso, criou-se novel figura típica incriminadora, buscando punir quem viole não apenas a comunicação telemática, mas também os dispositivos informáticos, que mantém dados relevantes do seu proprietário (NUCCI, 2020, p. 292).

A doutrina também afirma que faz menção da internet, porém não é necessário que o dispositivo esteja conectado, sendo o principal objetivo a proteção de informações e

[17] (83) The supervisory authorities should assist one another in performing their tasks and provide mutual assistance, so as to ensure the consistent application and enforcement of the provisions adopted pursuant to this Directive.

[18] Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita.

dados pessoais, mesmo que de forma *offline*, quando uma pessoa instala um programa o dispositivo que a facilitará em colher informações futuras.

> É indiferente haver conexão ou não. E está correta tal medida, pois o agente pode invadir computadores desconectados de redes, conseguindo obter dados, adulterar ou destruir informes ali constantes. Pode, ainda, instalar vulnerabilidades, que somente se manifestarão quando houver conexão futura à rede (NUCCI, 2020, p. 293).

O artigo, por ter a intenção de evitar a invasão à privacidade do sujeito, a descreve desde o seu processo preparatório para a ocorrência do crime, de forma que o principal objetivo é o de evitar que informações de titulares sejam veiculadas de maneira errônea.

> A figura da equiparação, em verdade, tem a finalidade de punir os atos preparatórios do crime de invasão de dispositivo informático. Para que a violação se concretize, torna-se fundamental existir mecanismo apto a viabilizá-la. Portanto, os verbos do tipo são: produzir (dar origem a algo, criar, fabricar); oferecer (apresentar algo a alguém para que seja aceito); distribuir (entregar a várias pessoas); vender (alienar mediante a entrega de certo preço); difundir (tornar algo conhecido, propagar) (NUCCI, 2020, p. 293).

Outros dois artigos que podem também ser impostas sanções no âmbito penal, encontram-se no Código de Defesa do Consumidor, que mesmo antes da LGPD já descrevia sobre cuidados em que empresas deveriam ter com dados de seus consumidores de forma que poderiam incorrer em sanções penais. Os titulares devem tem seus dados protegidos de maneira que possam solicitá-los quando quiserem e também atentar-se para eventuais erros em suas informações.

> Art. 72. Impedir ou dificultar o acesso do consumidor às informações que sobre ele constem em cadastros, banco de dados, fichas e registros:
>
> Pena Detenção de seis meses a um ano ou multa.
>
> Art. 73. Deixar de corrigir imediatamente informação sobre consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata:
>
> Pena Detenção de um a seis meses ou multa (BRASIL, 1990, arts. 72 e 73).

O acesso ao consumidor aos arquivos de consumo é faculdade imprescritível para evitar, ou fazer cessar, ofensa a direitos da personalidade. É aspecto fundamental do direito à privacidade no que diz respeito à proteção de dados pessoais.

(...)

O art. 73 do CDC apresenta o segundo tipo penal relativo às atividades dos bancos de dados e cadastros de consumo. Com sanção mais branda (detenção de um a seis meses ou multa), apena-se a conduta consistente em “deixar de corrigir imediatamente informação sobre o consumidor constante de cadastro, banco de dados, fichas ou registros que sabe ou deveria saber ser inexata” (BESSA, 2021, p. 454).

4. VALORIZAÇÃO DOS DADOS, O IMPACTO DA LGPD AO TITULAR E AS SUAS REPERCUSSÕES

4.1. PUBLICIDADE DIRECIONADA, COMPARTILHAMENTO DE DADOS E O PREDOMINANTE MERCADO DIGITAL

Um dos maiores e crescentes mercados da economia digital se dá pelo compartilhamento de dados, a partir da geolocalização por aparelhos celulares, sendo possível a identificação de lugares que são frequentados por determinada pessoa e através deles descobrir seus gostos e preferências. O jornal estadunidense *The New York Times* em uma de suas reportagens aponta que a partir de 800 pontos de localização dentro de uma sala de aula foram ligados à identidade de uma professora, ao quais foram obtidos por meio de vários aplicativos. A reportagem[19] conta ainda que mais de 1.000 aplicativos populares contém código-fonte, um comando para que seja enviada a geolocalização dos usuários para empresas parceiras. De acordo com dados de 2018 da *MightySignal*, companhia de análise móvel, aponta que o Android (sistema do Google) foi encontrado tendo cerca de 1.200 aplicativos com tal código, comparado a cerca de 200 no sistema iOS, da Apple. A grande parte dessas informações são vendidas às empresas que se beneficiam com a publicidade direcionada. A matéria ainda conta que a companhia mais produtiva foi a Reveal Mobile, situada no estado da Carolina do Norte, a qual tinha o código de colheita de localizações em mais de 500 aplicativos, incluindo alguns que proporcionavam notícias locais. O porta-voz da empresa (Reveal Mobile) afirma que a popularidade de seus códigos mostrou que isso ajudou os desenvolvedores de aplicativos a lucrarem através de anúncios e os consumidores a possibilidade de utilização de serviços grátis[20] (Cf, FILHO, 2021 p.213-214).

---

[19] More than 1,000 popular apps contain location-sharing code from such companies, according to 2018 data from MightySignal, a mobile analysis firm. Google's Android system was found to have about 1,200 apps with such code, compared with about 200 on Apple's iOS.

[20] The most prolific company was Reveal Mobile, based in North Carolina, which had location-gathering code in more than 500 apps, including many that provide local news. A Reveal spokesman said that the popularity of its code showed that it helped app developers make ad money and consumers get free services.

Muitas empresas de tecnologia utilizam a localização a fim de obter informações que serão lucrativas e posteriormente salvam-se na motivação de gratuidade em seus aplicativos como forma de “moeda de troca” por ter acesso aos dados de usuários. A mídia progmática está presente principalmente em aplicativos gratuitos, os quais encontram a possibilidade de enorme valoração a partir de diversas informações sobre determinadas pessoas que podem muitas vezes ser grandemente lucrativas.

> Trata-se da veiculação automatizada de anúncios com base no perfil do usuário que acessa o aplicativo. Em milésimos de segundos, a requisição é enviada para o ecossistema de mídia progmática, retornando ao usuário um anúncio.
>
> (...)
>
> Os agentes do mercado de publicidade online relacionado aos aplicativos de celular não se interessam economicamente apenas em dados de geolocalização dos usuários, mas também em qualquer conjunto de dados que possa revelar hábitos dos consumidores e facilitar o seu mapeamento comportamental. O entrecruzamento de dados identificadores obtidos a partir de diferentes aplicativos e enviados a terceiros agregadores permite a formação de um perfil comportamental ainda mais completo dos usuários (FILHO, 2021, p. 213).

A privacidade é questão que sempre foi recorrente e de extrema importância, de modo que os sistemas operacionais móveis vão introduzindo, aos poucos, políticas que devem ser respeitadas, muitas em nível que não agradam e tampouco dão credibilidade ao seu titular. Duas gigantes nesse mercado são o sistema iOS e Android.

> Algumas empresas de localização afirmam que quando usuários habilitam os serviços de rastreio, seus dados são corretamente utilizados. Porém, o jornal descobriu que as explicações que as pessoas veem quando solicitadas a dar permissão costumam ser incompletas ou enganosas. Um aplicativo pode dizer aos usuários que ao garantir acesso a suas localizações, poderá ajudá-lo a obter informações sobre o trânsito em sua área, porém não mencionam que os dados serão compartilhados e vendidos. Isso revela um soterramento causado por uma política de privacidade vaga[21].

[21] *Many location companies say that when phone users enable location services, their data is fair game. But, The Times found, the explanations people see when prompted to give permission are often incomplete or misleading. An app may tell users that granting access to their location will help them get traffic information, but not mention that the data will be shared and sold. That disclosure is often buried in a vague privacy policy.*

Um documento bastante importante na orientação quanto a medidas de privacidade é aquele emitido pela autoridade estadunidense FTC (*Federal Trade Commission*). Este reconhece que os dois maiores sistema de celulares, tem enorme responsabilidade “com uma única posição que elas ocupam, as plataformas poderiam ser colocadas como ótimas ênfases a privacidade do consumidor, em suas relações com desenvolvedores do aplicativo.”[22]

Vale destacar que o sistema operacional tem influência direta na quantidade de dados pessoais coletados e transmitidos, seja pelo próprio sistema operacional, seja pelos aplicativos instalados. A doutrina afirma que os sistemas operacionais (Apple e Google) estão assentados em premissas diferentes. Isso porque o primeiro tem maior parte de suas receitas obtidas na venda de hardware (iPhone), enquanto o último, em propaganda online, não analisando individualmente se todas as permissões solicitadas são estritamente necessárias para cada aplicativo funcionar (Cf, FILHO, 2021, p. 218).

> Atualmente, consolidou-se de que o sistema operacional deve adotar o Princípio do Menor Privilégio segundo o qual um aplicativo deve possuir somente as mínimas permissões necessárias para desempenhar suas tarefas. Além disso, os desenvolvedores devem declarar de antemão as permissões que necessitam, e os usuários devem ter a oportunidade de analisar e decidir se essas permissões parecem adequadas antes de instalar um aplicativo (FILHO, 2021, p.218).

Nesse contexto que surge um desacordo entre gigantes da tecnologia (Apple e Facebook), mobilizando vários mercados e trazendo um reforço à privacidade tecnológica. A primeira das empresas, afirma que sempre zelou pela privacidade, tendo como um de suas principais publicidades a fim de atrair mais consumidores da marca, desde o primeiro iPhone lançado no ano de 2008. E uma de suas falas no ano de 2010, Steve Jobs frisa a respeito da atenção à privacidade que é tida na empresa

> Acredito que as pessoas são inteligentes e que algumas querem compartilhar mais dados do que outras. Pergunte a elas. Pergunte sempre. Faça-as dizer para você parar de perguntar, se elas se cansarem de tantas perguntas. Diga a elas exatamente o que vai fazer com seus dados. (JOBS, 2010).

[22] With the unique position they occupy, platforms could be placing a greater emphasis on consumer privacy in their relationship with app developers.

Em 2011 Tim Cook assumiu o cargo de CEO da gigante e passou a ter como referencial da empresa o tema da “Privacidade”. Em uma reportagem feita pelo Jornal Uol, Carlos Affonso aponta que a Apple confere um certificado para que empresas possam desenvolver aplicativos de uso interno e que rodem em iPhones. A empresa passa a revogar o certificado emitido para o Facebook em 2019, após o caso em que a empresa estaria disponibilizando um App de pesquisa de comportamento online do usuário em troca do pagamento mensal de 20 dólares. Cerca de 5% desses usuários eram adolescentes. A partir daí, foi necessária a análise da Apple na entrada de qualquer dos aplicativos do Facebook na App Store.

Foi então que em 2021, a empresa traz em sua atualização do iOS 14.5 a possibilidade de permitir ou não o acesso as nossas informações, abrindo uma nova aba, a partir da nova atualização, a qual pergunta sobre a autorização e consentimento para que seus dados sejam rastreados para além de determinado app instalado.

> Nós acreditamos que os usuários deveriam ter a escolha sobre os seus dados que estão sendo coletados sobre eles e como são utilizados. O Facebook pode continuar monitorando seus usuários através dos Apps e sites como antes, o *App Tracking Transparency* no iOS 14 apenas irá requerer que pergunte pela permissão primeiro[23] (COOK, 2020).

> Com efeito, desde a coleta exagerada e o monitoramento injustificado do comportamento alheio até exposição de informações altamente relevantes são várias as possibilidades de violação a direitos durante a atividade dos agentes de tratamento. Nesse sentido, o potencial para que eventuais falhas afetem de forma lesiva o patrimônio ou os direitos da personalidade dos sujeitos envolvidos é enorme. Sigilo profissional, livre concorrência, segredo industrial, honra, imagem e intimidade são apenas alguns dos fatores que fazem parte dessa complexa equação (FILHO, 2021, p.227).

Em contrapartida o Facebook defende que as informações coletadas durante a navegação, não são prejudiciais ao titular, devendo salientar que a principal fone de renda do aplicativo é através dos anúncios progmáticos. A empresa ainda defende que pode ser

---

[23] *We believe users should have choice over the data that is being collected about them and how it’s used. Facebook can continue to track users across apps and websites as before, App Tracking Transparency in iOS 14 will just require that they ask for your permission first.*

que conforme as coisas ocorram e as receitas despenquem, possa ser cobrada uma taxa ao instalar o App, sendo extremamente prejudiciais ao mercado de publicidade online. Criticam também o modo em que a Apple posicionou a autorização, sendo de forma simplista, fazendo com que o usuário simplesmente recuse o rastreamento, sem saber como isso poderia afetar os seus serviços.

Outra afirmação da gigante das redes sociais, é que a Apple teria todo interesse em reduzir o número de aplicativos grátis e extremamente populares na sua loja, como redes sociais, e fomentar uma cultura de apps que sejam pagos, nem que seja uma quantia pequena para serem baixados ou que contenham algum plano de assinatura, já que a empresa adquire um percentual do valor cobrado para a instalação, feita pelo usuário (Cf, WAKEFIELD in BBC *News,* 2021).

Com todo esse conflito de interesses, é possível enxergar a crescente preocupação com a privacidade, de modo que, juntamente com a lei de proteção de dados pessoais, continue a crescente procura por tecnologia, porém de modo em que seus usuários se sintam seguros quanto ao tratamento de suas informações.

Os ataques a essas plataformas (sites e aplicativos) é uma realidade, quanto menos informações possuírem, aos usuários poderão causar uma menor lesão e aos responsáveis pelo tratamento um menor prejuízo. Observa-se que as medidas muitas vezes sugeridas pelo aplicativo prometem um melhor desempenho, porém muitas outras informações são obtidas de forma desnecessária.

> O uso do hardware dos dispositivos, condição necessária para que a funcionalidade das aplicações sejam desempenhadas, também não pode ser desconsiderado. Câmeras, microfones, leitores de impressão digital e GPSs fazem parte do rol de mecanismos que viabilizam a coleta de dados e potencializa a exposição do usuário aos perigos próprios do mundo digital. Nesse sentido, são diversos casos de vazamento ou mesmo obtenção deliberada de imagens, vídeos, gravações de voz, localização, dentre outros, a partir da fragilidade de segurança das aplicações e plataformas que fazem uso do *hardware* dos dispositivos eletrônicos (FILHO, 2021, p. 230).

Um vazamento que ocorreu em janeiro de 2020 e teve como vítima a empresa francesa Next Motion, que atua no ramo de dermatologia e procedimentos estéticos, a qual fornecia ferramentas de fotografia e vídeo digitais para 170 clínicas em 35 países. O banco de dados exposto continha quase 900.000 (novecentos mil) arquivos individuais que

traziam, dentre outras informações altamente sensíveis como tratamentos estéticos, arquivos de vídeo (*scans* em 360 graus de rosto e corpo dos pacientes).

> No caso da responsabilização dos desenvolvedores de aplicativos e plataformas digitais, o enfoque abrange os termos e condições de uso, políticas de privacidade, termos de consentimento, entre outros instrumentos particulares, bem como as disposições legais pertinentes, em especial a LGPD e os diplomas que com ela dialogam, como por exemplo o CDC (FILHO, 2021, p. 231).

Portanto as atividades ligadas ao mercado de consumo permanecem sujeitas as regras do Código de Defesa do consumidor, em específico aos arts. 12 e seguintes.

4.2. UTILIZAÇÃO DE COOKIES E O REAL CUMPRIMENTO DAS POLÍTICAS DE PRIVACIDADE

Qualquer pessoa hoje está sujeita a um fluxo de cookies em seus procedimentos na internet. As tarefas mais básicas, como a de ler uma reportagem cotidiana, até as mais complexas, como a de pesquisar dados mais complexos, exige do usuário uma série de desvios para cookies, assim definidos por Ruiz:

> Os cookies são o nome genérico para os pequenos arquivos de dados deixados nos nossos computadores quando visitamos algum site. Os cookies foram projetados para serem um repositório confiável para armazenamento de dados de operações que realizamos na web. Por exemplo, os cookies podem armazenar nosso login, os itens de um "carrinho virtual de compras", nossa preferência pelo idioma de um site, entre outros. Na navegação web os cookies são muito úteis como, por exemplo, em sites de serviços como os da Google. Se estamos usando o Gmail, por exemplo, e optamos por criar uma planilha usando o serviço Planilhas Google (Google Sheets), não precisamos entrar com a senha novamente. Para isso os cookies lembram nossos nomes de usuário e nossas senhas (RUIZ, 2021).

Com a Lei Geral de Proteção de Dados, os Cookies ficaram mais visíveis, ao passo que o cenário pós GDPR já indicava essa mudança, de modo que os sites que lá operavam ou que trocavam dados com a UE, já estariam sujeitos a essa mudança. Muitos deles fizeram a adaptação, a fim de que não sofressem nenhuma barreira pelo Grupo europeu. Diversas vezes as mensagens vêm assim descritas: “este site utiliza *cookies* e tecnologias semelhantes para recomendar conteúdo e publicidade”, juntamente trazem uma informação

de que se aceitos os *cookies,* o usuário terá uma melhor experiência com determinado site, trazendo a opção ao lado de consulta de Políticas de Privacidade.

Muitos dos usuários não têm tamanha informação sobre eles e acabam aceitando de forma que acreditam ter essa “vantagem” ao acessar determinado site. Na maioria das vezes, com pressa e guiado pelo desejo ou pela necessidade da informação, o usuário acaba aceitando as condições, sem conhecê-las adequadamente, e mais importante, sem ter ideia das consequências. Porém concordam com a utilização de seus dados com fins de consulta de informações. São chamados de *Cookies* de autenticação.

> Estes servem para melhorar a experiência de navegação do usuário e, como toda informação armazenada e utilizada pelo serviço, essa também deveria obter o consentimento livre e esclarecido do usuário. Procedimento que raramente vemos nos websites brasileiros (RUIZ, 2021).

Os *cookies* de personalização podem armazenar todo tipo de escolha e preferência do usuário, como nos produtos que tem a intenção de compra, o modelo, a marca, o preço, informações que são colhidas e que após são direcionadas a publicidade específica para determinada pessoa (Cf, RUIZ, 2021).

Uma pesquisa feita pela Universidade de Stanford e Carnegie Mellon[24] demonstra a ciência dos usuários quanto a utilização de seus dados em plataformas online e se consentem com tal política.

> Os usuários não têm um conhecimento técnico para autodeterminar os seus dados pessoais no plano da sua coleta. Apenas 23% dos usuários usam o modo de navegação privada - aquele que bloqueia a coleta dos dados pessoais -, enquanto 50% dos usuários não usam tal ferramenta e 27% não têm certeza. Além disso, somente 17% deletam cookies, 23% não tem certeza, e, por fim, 60% não deletam essa ferramenta de coleta de dados pessoais (CRANOR, MCDONALD, 2012).

Um número curioso demonstrado pela pesquisa foi o resultado de que 70% dos entrevistados afirmam que levariam em consideração se o *website* compartilharia os seus dados com parceiros, cuja atividade estaria relacionada ao ramo publicitário. A

[24] Ver: http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092

preocupação com os dados pessoais se vê elevada ao passo de que 64% dos entrevistados consideram ser invasiva a vigilância sobre as suas atividades online.

> Essa contradição é sublinhada na última parte da pesquisa empírica, quando os entrevistados são divididos em dois grupos: i) se pagariam U$ 1,00 (um dólar) para evitar que os provedores de Internet coletassem suas informações pessoais, ou, alternativamente; ii) se aceitariam o desconto de U$ 1,00 (um dólar) em troca da permissão para que os provedores de Internet coletassem seus dados pessoais (Cf. BIONI, 2020).

Bruno Bioni afirma ainda que juntando os dois subgrupos da pesquisa, houve o consenso de 69% dos entrevistados de que a privacidade é um direito, de modo que eles não deveriam ser obrigados a apagar uma quantia monetária para evitar que as empresas a violassem. Nesse sentido, 61% dos entrevistados afirmaram, categoricamente, que tal tipo de pagamento consistiria em uma extorsão. (BIONI, 2020, p.143)

Voltando ao tema de embates entre Apple e Facebook: se a decisão tomada pela Apple futuramente prejudicar o Facebook em suas receitas e assim eles tivessem que começar a cobrar pelo aplicativo, as pessoas pagariam para o instalar ou aceitariam o *trade-off* (câmbio troca) de dados pela gratuidade ou benefícios no App? Muitos dos usuários, como relatado na pesquisa, consideram o pagamento para a segurança de seus dados uma extorsão. Qual seria a valoração para a coleta de dados no Brasil? As pessoas consentiriam em ceder suas informações ao invés de efetuar o pagamento para a utilização de tal ferramenta? De qualquer forma a proteção total de dados no universo da Internet não é das mais fáceis. Conforme a tecnologia avança diariamente, as leis precisam acompanhá-las.

Um estudo feito nos EUA relata o surgimento de novas tecnologias de rastreamento que convivem muitas vezes com os *cookies*, substituem ou dificulta que os usuários as deletem ou as bloqueiem. Perpassando *E-tags, flash cookies, HTML, Web storage, evercookie, fingerprinting*, são exemplos delas. A utilização de tais *trackers* (rastreadores), é conclusiva de que essas novas tecnologias tornam a coleta de dados ubíqua, robusta e redundante.

As tecnologias citadas são mais difíceis de serem bloqueadas, pois são armazenadas de forma incomum em pastas locais do sistema computacional. Elas têm capacidade de reviver, isso porque, mesmo que sejam deletadas, a execução de um programa pode reativá-las automaticamente, sem o consentimento do usuário. Por estes

motivos é que a coleta de dados pessoais é quase que perene. Por exemplo, se o usuário deleta *cookies*, ele ainda poderá ser rastreado por outros inúmeros *trackers* – *flash cookies*, *E-tags* e assim por diante. (Cf. BIONI, 2020, p. 147).

Outra pesquisa, feita pela Universidade de Bochum (Alemanha), percebeu um aumento de 45% na adoção de cookies após a implantação da GDPR. Foram então realizados os estudos em que consideram respectivamente: a) a posição na qual o aviso era exibido na plataforma; b) se aos usuários eram franqueadas opções para decidir como seus dados poderiam ser utilizados pela plataforma e, ainda, como tais preferências poderiam ser exercidas; c) por fim, a linguagem de tais avisos. Com relação a primeiro estudo constatou-se que em 91,8% das vezes o conteúdo era disponibilizado no topo ou ao final da plataforma, não sendo de fácil visualização.

Em segundo constatou que tal tecnologia não causava interação do usuário, porque na maior parte das vezes não lhe franqueava qualquer tipo de opção senão a aceitação do uso dos seus dados. Muitas vezes quando havia a possibilidade de escolha, aplicavam opções pré-marcadas, de modo que por padrão, o usuário autorizava o processamento de seus dados. As opções de não aceitação não eram destacadas e muitas vezes não tinham cores que as realçassem.

Outro teste considerou que é desafiador a construção de um vocabulário de fácil compreensão, sendo que alguns entrevistados não compreendem as implicações das suas escolhas, como, por exemplo, acreditando que recusar um cookie os impediria de acessar o site ou significaria o aparecimento de menos anúncios. (Cf. BIONI, 2020)

Dessa forma fica evidente muitas vezes a difícil escolha do usuário, de forma que na maioria das vezes muitos deles não sabem sobre a sua finalidade e até mesmo não exercem a leitura do que estão aceitando nos termos de privacidade. Alguns *websites* não emitem a opção de não aceitação e quando previstas e escolhidas a não coleta de cookies, simplesmente não podem ter acesso a determinada matéria.

> A ideia é arquitetar sistemas (estratégias reguladoras) que facilitem o processo de tomada de decisão para que o sujeito, tido como vulnerável, supere a sua debilidade para empreender decisões genuínas.
>
> (...)

> Demonstrada a (hiper)vulnerabilidade do cidadão em meio a uma economia de dados. A partir dessa orientação, pretende-se não só verificar como se poderia (re)pensar a estrutura normativa de proteção de dados pessoais, mas, igualmente, projetar a sua aplicação-interpretação - seja das leis setoriais ou geral de proteção de dados pessoais no Brasil. (BIONI, 2020, p. 161).

A falta de conhecimento a respeito de dados é marca evidente, tratando-se de internet em que a maioria dos brasileiros a utiliza para diversas finalidades, de forma que em analogia ao autor, podemos comparar a vulnerabilidade do consumidor no momento da elaboração de seu código e também a CLT que trata assim os seus empregados. As legislações descritas tem a intenção de produzir uma plataforma igualitária onde suas partes possam dialogar sem desvantagens, o que afirma o autor que ainda é falha na aplicação na Lei de Dados.

> Hoje, como usuários da web e como cidadãos resta-nos alertar que cabe ao usuário da web o domínio sobre seus dados. Cabe ao usuário permitir ou não o uso de cookies, cabe a ele ser informado sobre a real utilidade e finalidade desses cookies como qualquer outro dado armazenado em seu computador ou em outro dispositivo. Cabe saber por quanto tempo ele é armazenado e como o usuário pode apagar esses dados. Cabe a ele a ciência se esses dados são compartilhados, quais são os dados compartilhados e com quem são compartilhados, como também cabe ao usuário ter o controle desse compartilhamento. Raramente vemos Termos de Uso e funcionalidades nos sites que permitem todas essas prerrogativas da lei. Somos todos cientes que o combustível da web são os dados pessoais, mas, como usuários, devemos escolher quais tanques vamos encher (RUIZ, 2021).

Muitas ferramentas ainda precisam de ajustes para ficarem dentro dos conformes da lei, principalmente quando envolvidos dados processados na Internet, onde possuem um maior valor na economia digital, movimentando enormes quantias de dinheiro em torno do mundo inteiro. Aos seus usuários mais segurança de suas informações e privacidade, pois com apenas alguns cliques e aceites são identificados pelas plataformas, juntamente com suas preferências e gostos, hábitos de consumo e até mesmo a sua localização.

A história do Direito tem mostrado que, para novas relações de direitos e deveres, são necessárias novas leis. As leis que versam sobre proteção de dados precisam ser incessantemente renovadas. Se já há algumas décadas, inovações em sites, aplicativos etc. vinham tendo um avanço significativo, esse avanço condensou-se de forma radical com o advento da pandemia e a consequente nova demanda que atingiu todos os níveis da existência: laboral, social, financeira, cultural etc. É importante lembrar ainda que,

usualmente, e em grau crescente, o usuário não tem real conhecimento do funcionamento das ferramentas de informática de que se utiliza.

A renovação de leis faz com que o legislador exerça essa observação de necessidade de inovação. Dessa forma é aconselhável que esteja em constate conhecimento e até mesmo na busca de auxílio com a consulta doutrinadores e legislações internacionais do tema, indagando sobre as possíveis alterações que podem ser feitas para a melhor garantia de direitos. A participação de especialistas da área de processamento de dados também facilita a alteração de modo que fugindo do meio jurídico e entrando na prática e conceitos informáticos, pode-se ter maior conhecimento dos problemas enfrentados e a ciência da dificuldade para real proteção pessoal.

Na velocidade em que as plataformas em que os dados circulam e sua enorme valoração crescem (novo petróleo), fica mais evidente a necessidade de controle e proteção da privacidade do usuário que na maioria das vezes não possuem tamanho conhecimento do objetivo da coleta de suas informações e como isso pode afetar a sua privacidade. Desse modo, a atenção a políticas de necessidade de informações mais acessíveis e de fácil interpretação, de modo que o real motivo da coleta de dados seja passado ao seu titular e que possa ter a possibilidade de negá-las facilmente.

5. CONSIDERAÇÕES FINAIS

Neste trabalho percorremos as diversas áreas de atuação na vertente da proteção de dados pessoais, todo o seu histórico e princípios desde as primeiras tentativas e preocupações de resguardar uma maior privacidade que se iniciam no continente europeu, até mesmo nos dias atuais em que vem à tona a Lei Geral de Proteção de Dados brasileira, trazendo uma regulamentação ainda mais específica sobre o tema. Os principais desafios de implantação e o impacto que a lei trouxe à economia e às relações que tratam dados também fazem parte do presente texto. Na busca de maiores informações para a real pesquisa, fizeram-se necessárias consultas a bibliografias que dizem respeito sobre a LGPD e a pioneira internacional GDPR, de maneira que podem ser destacados os pontos de maior importância e relevância dentre elas. Artigos internacionais que abordam o atual mercado digital e suas influências na vida cotidiana, juntamente com a consulta de pesquisas que relatam ainda uma dificuldade no controle de determinada matéria, também se agruparam ao conteúdo.

A política de implementação de legislações na tentativa de abranger uma maior proteção ao tratamento de informações é observada no momento em que surge um crescimento da preocupação e real valoração à privacidade individual, acarretando diversos tratados internacionais sobre o tema. Dessa forma, com a incessante busca pelo zelo da vida privada dos titulares, resolve-se avançar ainda mais nessa questão.

A partir do surgimento da GDPR, o cenário mundial passa a ter uma outra concepção do tema tratado, de forma que, a fim de evitar barreiras comerciais com o gigante mercado europeu, outros países veem a necessidade de acordo e alteração de suas legislações próprias acerca do tema. Este é um ponto de muita atenção, de forma que, mesmo que de maneira não voluntária para a criação de uma legislação mais específica para determinado país, passam a também versar sobre o assunto. No caso brasileiro em questão, a visão de necessidade de criação de legislação específica para o tratamento de dados é adquirida após a criação da legislação europeia, de certa forma que, se assim não fossem pressionados, uma Lei com mesmo padrão de proteção na troca de dados não seria aprovada em tempo curto, de tal forma que o seu período de *Vacatio Legis* e real aplicação de sanções poderia ser postergado ainda mais. De qualquer forma, sendo guiada pela

GDPR, a LGPD traz uma boa visão de que o sistema legislativo tende a estar mais atualizado com os novos conflitos e crimes.

Com o advento da LGPD, é gerada a ideia de anonimização, a qual é definida em seu corpo. Ocorre nos casos em que os dados não são possíveis de serem referidos ou ligados a uma determinada pessoa, fazendo com que muitos dos que tratam dados alegassem a utilização desse modelo, utilizando os dados sem que fosse possível saber a quem pertencia determinada informação. Alguns doutrinadores e pesquisas em contrapartida, apontam que, para que uma pessoa seja identificada por dados anonimizados não é uma tarefa de tamanha dificuldade, como no caso em que, com a habilitação para a localização de dispositivos, é possível ver uma trajetória única. Além da localização, o tempo em que a pessoa permanece em cada página, seus gostos e preferências já são capazes de informar o sexo, idade etc.

A internet e aplicativos são enormes plataformas de troca de dados pessoais, o que torna ainda maior a dificuldade de real controle da coleta de informações feita. Diferentes visões de empresas colocam em discussões temas relevantes ao futuro do mercado digital, como a difusão de ideias entre empresas que apontam que a coleta de dados é completamente legal (desde que os usuários concordem) e sem prejuízos aos seus titulares. Em contrapartida, há outras que mencionam a falta de informações sobre os reais dados coletados e que os mesmos são repassados a terceiros com efeitos lucrativos, sem prévio aviso. Na visão geral a ideia de privacidade é algo que parece ter um custo, como ocorre quando empresas indicam ser possível a cobrança de dinheiro ao se obter um app, caso não se permita que seus dados sejam repassados a terceiros. Em específico, no Brasil, caso isso ocorresse, as pessoas optariam por fazer o trade-off (permitir o repasse de dados a terceiros em troca da gratuidade do aplicativo) ou pagariam para efetuar a instalação em troca do não repasse informacional.

Tão repleto é o assunto que jornalistas norte-americanas relatam em uma obra (*An Ugly Truth,* 2021) a ligação do Facebook e a eleição de candidatos à presidência dos Estados Unidos como uma real troca de dados. Explicam que muitas pessoas eram dirigidas à determinadas matérias, aprimorando ainda mais o fanatismo político, com o exemplo de estadunidenses que se interessariam por determinado candidato e que, depois de acesso ao seu vídeo nas redes sociais, os seguintes conteúdos seriam de mesma base ideológica e mesmas opiniões. Vale lembrar que apontam que essas ocorrências não ocorrem apenas em áreas políticas, mas também em outros campos de ideias. Por fim,

dizem não ser algo positivo, já que faz com que o fanatismo cresça e não dê mais espaço aos debates.

Ainda com relação aos padrões da rede mundial de computadores, é visual o crescimento de *cookies* no cenário pós GDPR e pandêmico, em que sites se utilizam dessas ferramentas a fim de capturar dados e informações dos usuários. Com a lei, a utilização de barras de aviso de uso de cookies foi regulamentada, com intenção de tornar possível a advertência ao usuário a fim de que a utilização de dados fosse permitida por seus titulares. Pesquisas apontam que a maioria das pessoas se importam com a proteção de sua privacidade, e, se a elas fossem relatados os modos com que seus dados são utilizados, não consentiriam com tal atividade. Fica evidente que muitos dos usuários não sabem o que estão aceitando e nem mesmo leem os termos de privacidade. Outros *websites* apresentam esses termos em locais de difícil acesso e na maioria das vezes não dão a oportunidade de negar a utilização dos *cookies*. Quando agem dessa forma deixam em marcado (pré-selecionado) a opção de salvar ou aceitar, de modo a induzir o usuário a concordar como se fosse a mais segura opção ou de maior confiança. A visão de hipossuficiência do usuário nessa relação é clara, fazendo com que os artigos dispostos em determinada lei, busquem uma igualdade entre controladores, operadores e titulares. Ela se dá de forma que a maioria dos titulares não possuem nenhum conhecimento das políticas de privacidade e cookies gerados, sendo de dever da LGPD dar maior suporte a eles.

Por fim resta a observância na busca por uma maior responsabilização de pessoas que se utilizam de dados com intenções que fogem de sua finalidade inicial de coleta, de maneira que anteriormente não era comumente vista. Uma legislação tão específica na tentativa de frear esse tipo de crime era necessária, não apenas no cenário nacional, mas também no exterior, como no caso da UE que, ao ver essa necessidade, traz um modelo a ser seguido, perspectiva de futuro e políticas de dados em empresas, dispositivos e na internet. Quanto ao legislador, este é de melhor ordem que conte com o apoio de especialistas na área, a fim de conseguir acompanhar os mais novos tipos de crimes envolvendo dados e as necessárias modificações para melhor resultado da Lei. O cenário que se tem é de otimismo, estando longe do total controle de tratamento. Porém, é o início de uma maior preocupação e cautela com nossa privacidade e com nossas informações que movem o mercado mundial.

6. REFERÊNCIAS

BRASIL. Lei 8.078 de 1990. **Código de Defesa do Consumidor** São Paulo: Planalto 1990.

BRASIL. Lei 2.848 de 1940 **Código Penal**. São Paulo: Planalto, 1940.

BRASIL. Constituição (1998). **Constituição da República Federativa do Brasil**: promulgada em 5 de outubro de 1988.

BRASIL. Lei 13.709 de 2018. **Lei Geral de Proteção de Dados (LGPD)**. São Paulo: Planalto, 2018.

BARBIERI, C.; **Governança de Dados**: Práticas, Conceitos e Novos Caminhos. 1. ed. Rio de Janeiro: Alta Books, 2019.

BIONI, B.; **Proteção de Dados Pessoais:** a função e os limites do consentimento. 2. ed. Rio de Janeiro: Forense, 2020.

CAPANEMA, Valter Aranha. **A responsabilidade civil na Lei Geral de Proteção de Dados**. Cadernos Políticos da Escola Paulista de Magistratura. Disponível em< https://www.tjsp.jus.br/download/EPM/Publicacoes/CadernosJuridicos/ii_6_a_responsabilidade_civil.pdf?d=637250347559005712>. Acesso em: 15 de jun. 2021.

CRANOR, Lorrie Faith; MCDONALD, Aleecia M. Beliefs and Behaviors: ***Internet Users' Understanding of Behavioral Advertising***, p. 1. Disponível em: <http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1989092>. Acesso 25 mai. 2021.

COUNCIL OF EUROPE. ***Convention 108 and Protocols***. Disponível em: <https://www.coe.int/en/web/data-protection/convention108-and-protocol>. Acesso em: 08 abr. 2021.

COUNCIL OF EUROPE. ***The Convention in 1950.*** Disponível em: <https://www.coe.int/en/web/human-rights-convention/the-convention-in-1950>. Acesso em: 5 abr. 2021.

DONEDA, D. (Org.) et al. **Tratado de Proteção de Dados Pessoais**. Rio de Janeiro: Forense, 2021.

FILHO, E. (Org.). **A Lei Geral de Proteção de Dados Brasileira:** Análise setorial (Volume 1), 1. ed. São Paulo: Almedina, 2021.

GARCIA, L., et al. **Lei Geral de Proteção de Dados Pessoais (LGPD):** guia de implantação. 5. ed. São Paulo: Edgard Blücher, 2020.

GOLDSCHMIDT, R.; BEZERRA, E.; PASSOS, E. **Data Mining**. Conceitos, técnicas, algoritmos, orientações e aplicações. Rio de Janeiro: Elsevier, 2015.

GUARIENTO, Daniel Bittencourt; MARTINS, Ricardo Maffeis. **Impressões Digitais.** Migalhas. Disponível em: <https://www.migalhas.com.br/coluna/impressoes-digitais/319519/a-efetividade-da-anonimizacao-de-dados-pessoais>. Acesso em: 14 abr. 2021.

HARARI, Y.; **21 Lições para o Século 21**. 1. Ed. Companhia das Letras, 2018.

HOFFMANNRIEM,Wolfgang. **Rechtliche Rahmenbedingungen für und regulative Hera usforderungen durch Big Data**. In: HOFFMANN-RIEM, Wolfgang (coord.). Big Data – Regulative Herausforderungen. Baden-Baden: Nomos, 2018. p. 16.

LANEY, Doug. *3D data management:* ***Controlling data volume, velocity and variety*****.** Disponível em: <http://blogs.gartner.com/doug-laney/files/2012/01/ad949-3D-Data-Management-Controlling-Data-Volume-Velocity-and-Variety.pdf>. Acesso em: 8 mar. 2021.

Lima, A.; CRESPO, M.; PINHEIRO, P. **LGPD Aplicada.** São Paulo: Atlas, 2021.

LIMA, C. (Org.). **Comentários à Lei Geral de Proteção de Dados.** Lei n. 13.709/2018, com alteração da Lei n. 13.853/2019. São Paulo: Almeida Brasil, 2020.

LIMA, Cintia Rosa Pereira. ***Cookies*****: Doces ou travessuras**. Migalhas. 29 jan. 2021. Disponpível em: <https://www.migalhas.com.br/coluna/migalhas-de-protecao-de-dados/339601/cookies-doces-ou-travessuras-na-lgpd>. Acesso em: 03 jul. 2021.

NUCCI, G.; **Curso de Direito Penal:** parte especial: arts 121 a 212 do código penal. 4. ed. Rio de Janeiro: Forense, 2021.

NUTGER, A. C. M. ***Transborder Flow of Personal Data within the EC***, Springer, Olanda, 1990. Disponível em: <https://pdpecho.com/2012/08/10/dp-history-which-was-the-first-country-to-adopt-a-data-protection-law/>. Acesso em 18 mar. 2021.

O DILEMA das Redes. Jeff Orlowsk. *Exposure Labs,* 2020. Netflix.

ÖMAN, Sören. ***Implementing Data Protection in Law****, 20*10 Disponível em: <https://www.scandinavianlaw.se/pdf/47-18.pdf>. Acesso em 18 mar 2021.

PARLAMENTO EUROPEU. **Resolução P7 TC1-COD(2012)0011 de 12 de Março de 2014**. Disponível em: <https://www.europarl.europa.eu/doceo/document/TA-7-2014-0212_PT.html>. Acesso em: 03 jun. 2021.

PASQUALE, F. **The black box society:** The secret Algorithms Control Money and Information. Reprint ed. London: Harvard University Press, 2015.

PINHEIRO, P. **Proteção de Dados Pessoais**: comentários à Lei n. 13.709/2018 (LGPD). 2. ed. São Paulo: Saraiva Educação, 2020.

PRIVACY SHIELD FRAMEWORK. ***Privacy Shield Overview****.* Disponível em: <https://www.privacyshield.gov/Program-Overview>. Acesso em 25 mar. 2021.

PROCURA-SE. **O 14.5 da APPLE chegou: como terminar de se preparar de se preparar de se preparar e o que está mudando.** *Facebook for Business,* 2021. Disponível em: <https://www.facebook.com/business/news/how-to-prepare-for-changes-to-facebook-ads-from-ios-14-update>. Acesso em: 19 abr. 2021.

PROCURA-SE. ***SCHREMS II and the Privacy Shield | 2021 EU SCCs (standard contractual clauses) for safe data transfers. Cookiebot***. 26 jul. 2021. Disponível em: <https://www.cookiebot.com/en/schrems-ii-privacy-shield>. Acesso em: 26 mar. 2021.

RODOTÀ, Stefano. A vida na sociedade da vigilância: a privacidade hoje. Tradução Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008. P. 15.

UNIÃO EUROPEIA. Lei 679/2016. ***General Data Protection Regulation***. UE, 2018.

WAKEFIELD, Jane. **Ferramenta do iPhone que acirra disputa das gigantes da tecnologia**. BBC *News* Brasil. 27abr. 2021. Disponível em: <https://www.bbc.com/portuguese/geral-56905209>.

WEISS, Martin A.; ARCHICK, Kristin. **US-EU Data Privacy: From Safe Harbor to Privacy Shield**. In: Congressional Research Service. 7-5700, 2016. Disponível em: https://fas.org/sgp/crs/misc/R44257.pdf. Acesso em: 13 mar. 2021.