UNIVERSIDADE FEDERAL DA PARAÍBA – UFPB
CENTRO DE CIÊNCIAS JURÍDICAS – CCJ
COORDENAÇÃO DO CURSO DE DIREITO – CAMPUS JOÃO PESSOA
COORDENAÇÃO DE MONOGRAFIA

YURI HENRIQUE COSTA SILVA

A INFLUÊNCIA DA RGPD NA LGPD: APROXIMAÇÕES LEGISLATIVAS

JOÃO PESSOA
2022

YURI HENRIQUE COSTA SILVA

A INFLUÊNCIA DA RGPD NA LGPD: APROXIMAÇÕES LEGISLATIVAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientadora: Ms. Juliana Coelho Tavares Marques

JOÃO PESSOA
2022

Catalogação na publicação
Seção de Catalogação e Classificação

S586i Silva, Yuri Henrique Costa.
A influência da RGPD na LGPD: aproximações legislativas / Yuri Henrique Costa Silva. - João Pessoa, 2022.
41 f.

Orientação: Juliana Coelho Tavares Marques.
Monografia (Graduação) - UFPB/CCJ.

1. LGPD. 2. Dados Pessoais. 3. MASCs. I. Marques, Juliana Coelho Tavares. II. Título.

UFPB/CCJ CDU 34

Elaborado por Lucimário Dias dos Santos - CRB-15/645

YURI HENRIQUE COSTA SILVA

A INFLUÊNCIA DA RGPD NA LGPD: APROXIMAÇÕES LEGISLATIVAS

Trabalho de Conclusão de Curso apresentado ao Curso de Graduação em Direito de João Pessoa do Centro de Ciências Jurídicas da Universidade Federal da Paraíba como requisito parcial da obtenção do grau de Bacharel em Direito.

Orientadora: Ms.ª Juliana Coelho Tavares Marques

DATA DA APROVAÇÃO: 01 DE JULHO DE 2022

BANCA EXAMINADORA:

Prof.ª Ms.ª JULIANA COELHO TAVARES MARQUES
(ORIENTADORA)

Prof. Ms. HECTOR RUSLAN RODRIGUES MOTA
(AVALIADOR)

Prof. ª Dr.ª MÁRCIA GLEBYANE MACIEL QUIRINO
(AVALIADORA)

RESUMO

A era digital é fruto de grandes avanços tecnológicos, o advento da internet provocou grandes mudanças na sociedade. A globalização conecta todos e a troca de informações se tornou instantânea, através de aparelhos como computadores e celulares. Nesse contexto, a informação adquiriu grande relevância nessa nova dinâmica, e com ela, uma nova necessidade de proteção de dados pessoais. Desta forma, o Direito enquanto ciência precisou adaptar-se e conceber instrumentos capazes de garantir o mínimo de tutela desse direito fundamental. Tal fenômeno se concretizou com a criação da Lei Geral de Proteção de Dados Pessoais, que visou regular o poder de entidades e garantir a privacidade e a transparência como direito. Porém, mesmo sendo uma legislação recente, ela já encontra desafios na efetivação de seus preceitos. Assim, ressalta-se a importância de analisar o comportamento de regulamentações semelhantes no intuito de descobrir quais passos podem ser adotados para sanar essas dificuldades. Dito isso, o uso de métodos adequados de solução de conflitos surge como uma grande opção no contexto da LGPD, atuando como um aliado na materialização da proteção de dados.

Palavras-chave: LGPD. Dados Pessoais. MASCs.

ABSTRACT

The digital age is the result of great technological advances, the advent of the internet has brought about great changes in society. Globalization connects everyone and the exchange of information has become instantaneous, through devices such as computers and cell phones. In this context, information has acquired great relevance in this new dynamic, and with it, a new need to protect personal data. In this way, Law as a science needed to adapt and devise instruments capable of guaranteeing the minimum protection of this fundamental right. This phenomenon materialized with the creation of the General Personal Data Protection Law, which aimed to regulate the power of entities and to guarantee privacy and transparency as a right. However, even though it is a recent legislation, it already faces challenges in the implementation of its precepts. Thus, it is important to analyze the behavior of similar regulations in order to discover what steps can be taken to solve these difficulties. That said, the use of alternative dispute resolutions emerges as a great option in the context of LGPD, acting as an ally in the materialization of data protection.

Key-words: LGPD. Personal Data. ADR.

SUMÁRIO

1 INTRODUÇÃO

Segundo a pesquisa Tecnologias de Informação e Comunicação(TIC) Domicílios – realizada pelo Centro Regional de Estudos para o Desenvolvimento da Sociedade da Informação (Cetic.br) do Núcleo de Informação e Coordenação do Ponto BR (Nic.br), 82% das residências dispõem de conexão de internet, representando 59,5 milhões de domicílios em 2021.

Além disso, no Brasil, segundo o estudo "Digital 2022: Global Overview Report" realizado pelo site Datareportal, cerca de 34,4% dos internautas utilizam as redes sociais para atividades profissionais, com uma taxa muito acima da média mundial, que é de 23%.

Todavia, mesmo sendo um setor que apresenta um crescimento significativo e de grande importância na economia do país, a legislação sobre a proteção de dados do país, a Lei Geral de Proteção de Dados Pessoais, ainda encontra desafios na sua implementação concreta.

Tal temática se faz pertinente por se tratar de assunto cada vez mais importante para a sociedade em um contexto de avanços tecnológicos, globalização e proteção de dados como um direito fundamental.

Portanto, questiona-se: a aplicação da LGPD no presente estado é suficiente para promover uma defesa plena dos direitos pertinentes a proteção de dados pessoais?

Então, o objetivo geral da presente pesquisa é analisar regulamentos internacionais através do contexto histórico e estrutural; explorar os preceitos da LGPD e os reflexos do Regulamento Geral de Proteção de Dados da União Europeia na sua redação; e estudar a aplicação da LGPD em seus períodos iniciais e atualmente para determinar uma possível melhoria no regulamento, através da utilização de Métodos Adequados de Resolução de Conflitos.

Parte-se da hipótese de que mesmo referindo-se a uma legislação recente, ela encontra-se carecendo de sensibilidade quanto a realidade brasileira, ignorando o histórico contencioso do país e negligenciando mecanismos diversos para resolução de conflitos, possibilitando assim uma ineficiência na sua implementação.

Nesse contexto, o Sistema Multiportas possui o poder de conferir vias de menor resistência ou melhor adequação, implicando na diminuição da participação direta do Estado no desfecho das divergências originadas pela aplicação da LGPD.

Assim, para viabilizar o teste da hipótese, realiza-se uma pesquisa das origens da proteção de dados, analisando a trajetória desse direito, e do contexto internacional, destacando a aplicação de métodos alternativos de resolução de conflittos em legislações distintas, bem como investigando os períodos iniciais da vigência da LGPD e seu cumprimento pós aplicação

das sanções no intuito de avaliar o impacto do vacatio legis e como a utilização de meios alternativos de solução de divergências na complementação da aplicação da LGPD.

2 CONTEXTO HISTÓRICO DA PROTEÇÃO DE DADOS EM ÂMBITO INTERNACIONAL

As ideias e princípios que fundamentariam os regulamentos de proteção de dados podem ser datados desde meio século passado, e são importantes para compreensão do curso trilhado pelos códigos jurídicos ao redor do mundo, tanto de suas formações como progressões.

Como resultado dessa trajetória, surgiram normas pelo globo preocupadas em tutelar sobre a proteção de dados, cada uma possuindo semelhanças entre si, porém com distintas soluções para mesmos problemas enfrentados.

2.1 Surgimento da necessidade de Proteção de Dados Pessoais

Dado o caráter tecnológico na internet, da proteção de dados de informações, enfatizado em razão da sua recente popularidade, é possível concluir erroneamente que a sua tutela tenha iniciado apenas recentemente, porém os princípios e pensamentos relativos tiveram seu início muito antes.

Tais princípios podem ser datados desde meados de 1960, através do discurso do até então presidente John F. Kennedy que, apesar de popularmente conhecido marco do Direito do Consumidor, propôs reflexões sobre os direitos fundamentais de todo consumidor, tendo em vista a aceleração do consumo no panorama capitalista.

O presidente apontou 4 direitos inerentes do consumidor na Mensagem Especial ao Congresso Sobre a Proteção do Interesse do Consumidor em 15 de março de 1962:

> (1) O direito à segurança – de ser protegido contra a comercialização de produtos prejudiciais à saúde ou à vida.
> (2) O direito de ser informado – de ser protegido contra a informação, publicidade, rotulagem ou outras práticas que sejam fraudulentas, enganosas, ou grosseiramente falaciosas, e que sejam a ele dadas todas as informações das quais precisa para fazer uma escolha adequada.
> (3) O direito de escolher – ser assegurado, sempre que possível, o acesso a uma variedade de produtos e serviços a preços competitivos; e nas indústrias em que a concorrência não é viável que a regulamentação governamental seja efetiva, deve também haver garantia de qualidade e serviço satisfatórios a preços justos.
> (4) O direito de ser ouvido – para se ter a certeza de que os interesses dos consumidores receberão consideração completa e favorável na formulação das políticas de Governo, e também tratamento justo e rápido em seus tribunais administrativos.

A relação do discurso presidencial com a proteção de dados se faz através do tratamento da informação veiculada ao consumidor, na dinâmica da Revolução-Técnico-Científico-Informacional, em que os dados dos usuários são usados e as propagandas são orientadas no intuito de maximização do lucro. Portanto, atualmente, a capacidade de escolha do consumidor é perturbada pelo paradoxo de excesso de informações superficiais e escassez de escolha pelo direcionamento de propagandas.

O que o dirigente procurou defender foram princípios fundamentais, invioláveis, capazes de guiar as normas referentes ao consumo regular, refletindo-se posteriormente também na proteção de dados, e pode ser considerado como umas das bases para a elaboração das leis, reforçando preceitos já trazidos pela Declaração Universal de Direitos Humanos da ONU, de 1948, que destacou a privacidade como direito fundamental quando previu que "Ninguém será sujeito à interferência na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataque à sua honra e reputação. Todo ser humano tem direito à proteção da lei contra tais interferências ou ataques" (ONU, 1948, Art. 12).

Então, na década de 70, devido ao avanço da indústria e da computação nos países desenvolvidos, verificou-se a necessidade de criação de uma legislação capaz de proteger os dados dos cidadãos, e foi na cidade de Hesse, na Alemanha, que foi elaborada e aprovada a "Hessiches Datenschutzgesetz", o Ato de Proteção de Dados de Hesse. É justo destacar os 7 comandos dessa legislação que seriam os princípios regentes da sua fundamentação:

> 1) Proibir a não ser por permissão: O recolhimento, armazenamento e utilização de dados pessoais é, em princípio, proibida, a menos que seja permitida por uma disposição legal ou o consentimento do titular dos dados.
> 2) Coleta direta: os dados podem ser coletados apenas do próprio titular. A lei prevê exceções, por exemplo, se essa coleta for muito complicada ou se outra lei permitir coleta.
> 3) Economia de dados: os dados não devem ser mantidos por muito tempo e devem ser excluídos após um período apropriado.
> 4) Minimiação de dados: o mínimo de dados possível deve ser coletado e processado.
> 5) Limitação de finalidade: o processamento de dados e permitido somente para um propósito específico, previamente definido, a menos que o titular consente em outro arranjo.
> 6) Transparência: o indivíduo afetado (titular dos dados) deve saber que os dados estão sendo coletados, que tipo de dados são, por que está sendo gravado e por quanto tempo ele será armazenado.
> 7) Necessidade: a coleta dos dados dever ser necessária; só é permitida se não houver outros meios disponíveis.

Após, por influência da norma alemã, houve a criação do “Sw. Datalagen”, Ato de Dados Sueco, de 1973, que procurou regular, apesar da maneira pouco detalhada ou objetiva, a proteção de dados em nível nacional. Tal fenômeno seguiu-se de discussões em outra nações europeias, como a França, Dinamarca e Noruega sobre a movimentação para a proteção de dados, culminando, em 1979, na elaboração de legislações específicas desses países, apenas seis anos depois da legislação sueca, porém, possuindo limitações semelhantes a mesma.

Nesse mesmo contexto histórico europeu, e como resultado das discussões prévias, houve a inclusão do direito à privacidade nas próprias Constituições de países como Portugal, que ao preocupar-se com a privacidade como direito fundamental, preveu em sua carta magna sobre a relação de dados pessoais e a sistema de rede de computadores, apontando inclusive sobre dados sensíveis:

> Art. 26º Outros direitos pessoais:
> […]
> 2. A lei estabelecerá garantias efetivas contra a obtenção e utilização abusivas, ou contrárias à dignidade humana, de informações relativas às pessoas e famílias.
>
> Art. 35. Utilização da informática:
> 1. Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua retificação e atualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.
> 2. A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao tratamento automatizado, conexão, transmissão e utilização, e garante a sua proteção, designadamente através de entidade administrativa independente.
> 3. A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis
> 4. É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcioais previstos em lei. (PORTUGAL, 1976)

Bem como na constituição da Espanha, que estabeleceu os limites do tratamento de dados como manifestação do direito à privacidade. Atestando a incorporação dos princípios da ONU e a importância da inclusão não apenas em legislação específica do país:

> Seção 18
> 1. É garantido o direito à honra, à privacidade pessoal e familiar e à própria imagem.
> […]

> 4. A lei restringirá o uso do tratamento de dados para garantir a honra e a privacidade pessoal e familiar dos cidadãos e o pleno exercício dos seus direitos. (ESPANHA, 1978)

Demonstrando-se assim claramente a inclusão do tratamento do direito à privacidade e concretizando as ideias levantadas pela DUDH como direito inerente do ser humano.

Posteriormente, houve a aprovação da Convenção 108 do Conselho da Europa que evoluiu os debates para o tópico da proteção dos dados de caráter pessoal de indivíduos com o propósito de expandir a cobertura dos direitos e das liberdades basilares das pessoas, dado o crescimento do fluxo de informações e tratamento automatizado que tais dados de caráter sensível, tornando-os suscetíveis à abusos.

A Convenção estabeleceu esse instrumento jurídico que vincularia os países signatários – como também outros na condição de observadores, qualidade do Brasil desde 2018 – a se reunirem duas vezes ao ano, a partir de 28 de janeiro de 1981, e discutirem o "Tratamento Automatizado de Dados Pessoais" desde então.

Adiante, com a aprovação do Tratado de Maastricht em 1992, o continente europeu presenciou sua maior transformação com a criação da União Europeia, o seu bloco unificado. Por meio do bloco, promulgou-se a Diretiva 95/46/CE em 1995, que inovou no tratamento da defesa dos dados pessoais bem como da relação livre da livre circulação de dados.

Através da Diretiva, ocorreu a unificação do tratamento de dados e dos direitos dos usuários entre países pertencentes ao bloco, oferecendo princípios sobre o tema e medidas específicas e pormenorizadas. Essa legislação exibiu o detalhamento que as anteriores careciam.

A partir dela também que surgiram os princípios da necessidade, da transparência, da adequação, da licitude do tratamento, da limitação dos propósitos, além de outros, que norteiam-na e serviriam de base para elaboração das próximas leis semelhantes dada a sua influência.

2.2 Panorama mundial da regulamentação sobre a proteção de dados

Recentemente, vários países elaboraram suas próprias legislações no tocante da proteção digital como uma resposta para a mudança da dinâmica entre instituições e indivíduos. Vale destacar que apesar de ser uma realidade relativamente moderna, o número de casos

relacionados tende a aumentar gradativamente, tanto pelo número total de casos quanto pela conscientização da população sobre seus direitos.

Dito isto, a elaboração de legislações específicas buscou sanar problemas substanciais que sua vacância poderia desencadear mas também incorreu em uma nova preocupação, que faz parte de vários países mas especialmente aflige o judiciário brasileiro: a sobrecarga do judiciário, que provoca um congestionamento e que viola o direito de cidadãos consequentemente. Afinal, ao discriminar sobre a proteção de dados, as legislações invariavelmente criam outra via que demanda resolução, geralmente promovida pelo Judiciário.

Neste tocante, é importante analisar não só a RGPD e as normas específicas dos países integrantes, mas também distinguir três legislações que buscaram solucionar o problema do aumento de demandas através de métodos alternativos: as leis de proteção de dados da Austrália, Singapura, e da Nova Zelândia.

O RGPD, como norma de proteção de dados da União Europeia desde 2018, procurou elucidar sobre os direitos dos titulares de dados e deveres dos agentes de tratamento, além de conceituar os termos mais comuns desse ambiente, estabelecendo mecanismos de fiscalização, prevenção e sanção. Apesar disso, a RGPD não prevê procedimentos não judiciais para resolução de conflitos, o que acarreta em um acúmulo de ambas, denúncias e investigações, interpostas pelas autoridades de proteção de dados que contudo não alcançam seu desfecho.

O regulamento dedica-se a individualização do tratamento pelos países, encarregando as autoridades de proteção no tratamento de casos que envolvam dados pessoais. Isto é, as autoridades de proteção de dados possuem prerrogativas para investigar e aplicar sanções quando assim cabíveis, dando uma maior autonomia para os países e deslocando o RGPD para seu papel maior de referência, através de suas diretrizes.

Dito isso, alguns países integrantes da União Europeia utilizam-se do "Ombudsman", como é o caso da República Tcheca e da Itália, que é a uma espécie de defensor público, em essência, trabalhando como ouvidor de queixas e mediando a relação entre titulares e controladores.

Quanto a Austrália, sua legislação é digna de avaliação por apresentar sistemas distintos de resolução de disputas através de soluções não judiciais, mesmo que não aplicada diretamente pela agência de proteção de dados nacional, "Office of the Australian Information Comissioner, o OAIC, e sim a partir de uma cooperação entre o órgão e agências estaduais de proteção de dados.

A resolução de conflitos pode então ser firmada através da delegação para entidades externas, como órgão regulatórios, também chamado de External Dispute Resolution, e deve

ser estabelecido e regulado pelos agentes de proteção de dados, desempenhando assim um papel de supervisão do processo. Além disso, é obrigação dessas entidades garantir a acessibilidade, eficiência e transparência dos mecanismos estabelecidos, bem como de manter os agentes informados sobre o andamento e os procedimentos utilizados nesses métodos de resolução alternativas.

Em síntese, a norma australiana apresenta a autoridade de proteção de dados como órgão de supervisionamento da resolução de disputas, encarregando outros entes para proposição, organização e gerência de processos semelhantes a arbitragem, desenvolvendo assim uma multiplicidade de mecanismos capazes de sanar os conflitos.

Já em Singapura, a "Personal Data Protection Act", PDPA, é a legislação vigente do país para proteção de dados pessoais. Promulgada em outubro de 2012, mas entrando em vigor somente em 2014, a norma é aplicável somente em relação aos dados pessoais tratados pelo setor privado.

Como outras legislações, a PDPA estabelece uma autoridade de proteção de dados, o "Personal Data Protection Comission", nomeado pelo governo. Entre as atribuições da Comissão está a análise de controvérsias e orientação para o método mais adequado de solução, havendo a possibilidade de submissão do conflito para mediação sob o entendimento de ambas as partes, titulares e agentes de tratamento. Isso demonstra a previsão expressa dos métodos alternativos de solução de conflitos sobre a proteção de dados no próprio regulamento singapurense.

A resolução não judicial instituída pela Comissão também não é realizada por ação própria da mesma, ela encaminha os casos de controvérsia para câmaras de mediação autorizadas pela entidade, que disponibilizam os mecanismos e plataformas necessários para o processo.

Por fim, a Nova Zelândia, através do Privacy Act de 1993, a legislação relacionada de proteção de dados, de modo similar à Austrália, também apresenta o modelo de meio externo de resolução de conflitos.

Nesse sentido, a autoridade de proteção de dados neozelandeza, o Privacy Comissioner, analisa as reclamações e busca uma conciliação entre titulares e agentes de tratamento, e caso não haja algum acordo, possui a autoridade de remeter a controvérsia para ser resolvida no tribunal de direitos humanos nacional.

Portanto, a figura do Privacy Comissioner é a de intermediário, zelando por uma maior dinâmica na solução de conflitos, os meios alternativos de resolução de controvérsias

então atua como um plano sucessor, certamente em atenção para um descongestionamento da vias jurídicas e uma proporção maior de decisões relacionadas a proteção de dados..

Como pode ser observado por alguns exemplos, o panorama internacional da regulamentação sobre a proteção de dados é relativamente recente, mas a evolução do papel das autoridades de proteção de dados converge numa mesma direção de expansão de suas funções para além de mero ente de fiscalização ou sancionatório, mas como órgão ativo capaz de garantir o pleno direito de titulares.

3 QUADRO DA PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

Apesar da importância de uma legislação unificada tratando da proteção de dados pessoais no país, o Brasil só implementou uma legislação dedicada na segunda década do século 21, seguindo uma tendência mundial que enfim atentou-se para a importância das informações e a vulnerabilidade dos usuários de serviços na internet.

Surgiu assim a Lei Geral de Proteção de Dados, LGPD, que é a consolidação de esforços na área jurídica para uma mais eficiente proteção de dados, estabelecendo regras para empresas e organizações sobre a coleta, uso, armazenamento e compartilhamento de dados pessoais, além de prever multas e sanções.

A LGPD é resultado da evolução das normas relacionadas nacionalmente mas deve muito de sua inspiração para o Regulamento Geral de Proteção de Dados , o RGPD, que é o regulamento de proteção de dados da União Europeia, sendo possível traçar paralelos direitos entre dispositivos de ambas as legislações.

3.1 Lei nº 13.709, a Lei Geral de Proteção de Dados Pessoais

A Lei nº 13.709, Lei Geral de Proteção de Dados, foi sancionada desde agosto de 2018 mas apenas entrou em vigor em agosto de 2020 e possui o objetivo de regular o tratamento de dados pessoais, visando proteger a privacidade, intimidade e os direitos fundamentais como os de imagem e dignidade dos indivíduos residentes no território brasileiro dos quais os dados pessoais sejam coletados.

Ela surge em um contexto de grande evolução tecnológica através da globalização, onde surge a necessidade de criação de leis mais robustas e específicas para proteção de dados pessoais, que agora restavam-se vulneráveis ao aproveitamento ilegítimo de órgãos, sejam eles governantes ou empresários, capazes de obter vantagens através dessa nova “moeda” da qual valorizava-se em um ritmo acelerado: a informação.

A LGPD então busca criar normas que devem ser seguidas por empresas e Estados, e conceitua termos típicos da atividade de proteção de dados, aspirando a criação de um cenário de segurança jurídica ao padronizar as práticas. A regulamentação desdobrou-se através de mecanismos de proteção de dados para os vulneráveis dessa equação, aqueles que utilizavam-se de serviços pela rede mundial de computadores e tinham seus dados pessoais coletados para finalidades diversas.

Pode-se qualificar a LGPD como expressão dos direitos humanos acumulados pelos diversos tratados internacionais, tendo sua maior influência o Regulamento Geral Sobre a Proteção de Dados, a RGPD, que é a lei europeia análoga, atuante nos países da União Europeia e que substituiu a Diretiva da União Europeia n. 95/46/CE, antiga responsável pela proteção de dados da região.

Além do regulamento, a LGPD, de modo tautócrono, recebeu influências fortes do próprio Código de Defesa do Consumidor, que em seu art. 43 prevê sobre o acesso pelo consumidor de suas próprias informações coletadas pelas empresas, os parâmetros de coleta etc:

> 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.
> [...]
> § 6° 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, 2018)

Neste artigo, é possível identificar princípios como transparência, pela exigência de informações claras e de fácil assimilação, bem como de consentimento, ao demandar a comunicação ao consumidor do uso de seus dados pessoais, que são alguns dos pilares da LGPD.

Ademais, evidentemente que a lei que trata da proteção de dados pessoais teria influência em seu texto da Lei nº 12.965/14, o Marco Civil da Internet. No art. 7º, a norma trata dos direitos dos usuários que acessam o ciberespaço, trazendo temas como intimidade, privacidade, e, como o Código de Defesa do Consumidor, alguns parâmetros para extração e tratamento de dados pessoais:

> Art. 7° O acesso à internet é essencial ao exercício da cidadania, e ao usuário são as-segurados os seguintes direitos:
> I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; [...]
> III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial; [...]
> VII – não fornecimento a terceiros de seus dados pessoais, inclu-sive registros de conexão, e de acesso a aplicações de internet, salvo mediante consen-timento livre, expresso e informado ou nas hipóteses previstas em lei;
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
> a) justifiquem sua coleta;
> b) não sejam vedadas pela legislação; e
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;
> XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet; […] (BRASIL, 2014)

Não apenas, o art. 11 do Marco Civil da Internet também busca tratar sobre o assunto, expandindo sobre o tratamento adequado, , e estabelecendo diretrizes:

> Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
> § 1° O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
> § 2° O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil. (BRASIL, 2014)

Então, é claro que a LGPD procurou de ambas as fontes: legislações internacionais, com destaque para a RGPD, que operaram como precedente dada a maior experiência no tratamento do assunto; e em legislações nacionais, já que o processo de criação de legislações deve preocupar-se em conformar-se à realidade brasileira, e é proveitoso o estudo dos efeitos de normas similares.

Em seu art. 2º, a LGPD manifestou sua preocupação em defender direitos fundamentais, intrinsecamente relacionados com o uso da internet como plataforma de troca de dados:

> Art. 2° A disciplina da proteção de dados pessoais tem como fundamentos:
> I – o respeito à privacidade;
> II – a autodeterminação informativa;
> III – a liberdade de expressão, de informação, de comunicação e de opinião;
> IV – a inviolabilidade da intimidade, da honra e da imagem;
> V – o desenvolvimento econômico e tecnológico e a inovação;
> VI – a livre-iniciativa, a livre concorrência e a defesa do consumidor; e
> VII – os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2018)

Então este artigo empenha-se no comprometimento da norma em critérios basilares já defendidos até mesmo pela CF/88, porém no ambiente digital, apresentando uma maior especificidade no assunto.

O artigo seguinte, o art 3º dedica-se a delimitação da territorialidade, isto é, do alcance do tratamento da legislação, discorre:

> Art. 3° Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I – a operação de tratamento seja realizada no território nacional;
> II – a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;
> III – os dados pessoais objeto do tratamento tenham sido coletados no território nacional.
> § 1° Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2° Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4° desta Lei. (BRASIL, 2018)

Destaca-se então que o critério para determinar a aplicabilidade da lei envolve dois casos: dados coletados no Brasil ou aqueles dos quais o objeto de transação, seja ele oferta de bens e/ou serviços, tenha sido efetuado no território nacional. O primeiro parágrafo também reforça a ideia de que os dados pessoais a que se referem a norma como sendo daqueles titulares presentes no território nacional no momento de coleta.

Já o art. 5º é importantíssimo dado que ele especifica os termos a serem utilizados no tratamento de dados pessoais:

> Art. 5° Para os fins desta Lei, considera-se:
> I – dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II – dado pessoal sensível: dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organiza-ção de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural;
> 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;
> IV – banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico;
> V – titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI – controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII – operador: pessoa natural ou jurídica, de direito público ou pri-vado, que realiza o tratamento de dados pessoais em nome do controlador;
> VIII – encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD);
> IX – agentes de tratamento: o controlador e o operador;
> X – tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utiliza-ção, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
> XI – anonimização: utilização de meios técnicos razoáveis e disponí-veis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;
> XII – consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;
> XIII – bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados;
> XIV – eliminação: exclusão de dado ou de conjunto de dados arma-zenados em banco de dados, independentemente do procedimento empregado;
> XV – transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro;
> XVI – uso compartilhado de dados: comunicação, difusão, transferên-cia internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados;
> XVII – relatório de impacto à proteção de dados pessoais: documen-tação do controlador que contém a descrição dos processos de tra-tamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco;
> XVIII – órgão de pesquisa: órgão ou entidade da administração pú-blica direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua

> missão institucional ou em seu obje-tivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e
> XIX – autoridade nacional: órgão da administração pública responsá-vel por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional. (BRASIL, 2018)

A conceituação foi essencial para categorização dos elementos tratados, além dos processos, técnicas e procedimentos relativos, afunilando os elementos-chave e discernindo daqueles que não são alvo da proteção advinda da legislação.

Por fim, o art. 6 apresenta os princípios norteadores que garantem a proteção dos direitos dos titulares quanto aos dados pessoais:

> Art. 6° As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I – finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II – adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III – necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinen-tes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV – livre acesso: garantia, aos titulares, de consulta facilitada e gratui-ta sobre a forma e a duração do tratamento, bem como sobre a in-tegralidade de seus dados pessoais;
> V – qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI – transparência: garantia, aos titulares, de informações claras, pre-cisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII – segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
> VIII – prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX – não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X – responsabilização e prestação de contas: 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. (BRASIL, 2018)

De certo modo, os princípios agem na delimitação da ação do tratamento de dados pelos agentes, já que estes devem ser feitos segundo continências estabelecidas, evitando qualquer transgressão que extrapole os direitos fundamentais.

3.2 Influências do Regulamento Geral de Proteção de Dados sobre a Lei Geral de Proteção de Dados Pessoais

O Regulamento Geral sobre a Proteção de Dados, a RGPD UE 2016/679, é a mais recente legislação de proteção da privacidade e de dados pessoais do direito europeu coletivo, e incorre grande influência na legislação brasileira pela sua expressiva configuração, além do papel de vanguarda que empenha como legislação unificada.

Criada em 04 de maio de 2016, e apenas promulgada em 25 de maio de 2018, a RGPD preocupou-se com a regularização do direito à proteção de dados e da livre circulação, não sendo o primeiro dispositivo que trata da questão no bloco unificado, como já era o objetivo da Diretiva Comunitária nº 46 de 1995, que exigia diversos parâmetros aos membros da UE, como a existência de agência ou comissário de proteção de dados, e também a edição de leis sobre o processamento de dados pessoais.

Desde seu vigor, o objetivo do regulamento foi proteger o direito fundamental à proteção de dados, já instaurado pelo art. 8 da Carta Europeia de Direitos Humanos, ao tratar dos arquivos automatizados que contém dados pessoais.

A LGPD se assemelhou a RGPD quando procurou definir e distinguir, como dito anteriormente, os dados pessoais e sensíveis, conceituando assim os direitos e informações a serem protegidas pela legislação, com os dado pessoal como a "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018, Art. 5º, I).

E os sensíveis contendo dados capazes de gerar discriminação sobre o titular e, consequentemente, capazes de gerar efeitos bastante nocivos se permitido seu abuso:

> Art. 5º [...]
> 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)

Adotando princípios e conceitos semelhantes em natureza com os da RGPD, que, além disso, também pontuou considerações sobre dados genéticos, biométricos e relativos à saúde:

> Art. 4º Para efeitos do presente regulamento, entende-se por: [...]
> 13) «Dados genéticos», os dados pessoais relativos às características genéticas, hereditárias ou adquiridas, de uma pessoa singular que deem informações únicas sobre a fisiologia ou a saúde dessa pessoa singular e que resulta designadamente de uma análise de uma amostra biológica proveniente da pessoa singular em causa;
> 14) Dados biométricos, dados pessoais resultantes de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam ou confirmem a identificação única dessa pessoa singular, nomeadamente imagens faciais ou dados dactiloscópicos;
> 15) Dados relativos à saúde, dados pessoais relacionados com a saúde física ou mental de uma pessoa singular, incluindo a prestação de serviços de saúde, que revelem informações sobre o seu estado de saúde. (UNIÃO EUROPEIA, 2016)

Sobre o consentimento, a lei brasileira além de exigir a "manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada. (BRASIL, 2018, Art. 5º, XII)" para a coleta de dados, também dispõe sobre os quesitos que devem ser apontados pelo agente nessas funções, como a finalidade certa, garantida e justificável ao tratamento do dado e o uso exclusivo para tal finalidade:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios: [...]
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades. (BRASIL, 2018)

Na RGPD, além desses pontos, também prevê exceções para o tratamento por razões de segurança, saúde ou interesse público.

Outro ponto em que a LGPD recebeu influência da RGPD foi na distinção entre o titular e o responsável pelo tratamento de dados, definindo-os, delimitando suas atribuições e responsabilidades, ambas as legislações definem a figura do titular como "pessoa natural a quem se referem os dados pessoais que são objeto de tratamento. (BRASIL, 2018, art. 5, V)".

O regulamento europeu também importou-se em discernir o sujeito do titular através da conceituação dos dados pessoais "informação relativa a uma pessoa singular identificada ou identificável (titular dos dados) […]" (UNIÃO EUROPEIA, 2016, Art. 4º, 1).

Já o responsável, segundo a LGPD, é a pessoa física ou jurídica, de direito público ou privado, que efetua decisões sobre tais dados, sendo que os agentes são divididos em controlador e operador:

> Art. 5º […]
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador. (BRASIL, 2018)

A diferença é que na RGPD o agente responsável é dividido em controlador, responsável pela decisão a respeito do tratamento de dados, como previsto no art. 7 do regulamento:

> 7) Responsável pelo tratamento, a pessoa singular ou coletiva, a autoridade pública, a agência ou outro organismo que, individualmente ou em conjunto com outras, determina as finalidades e os meios de tratamento de dados pessoais; sempre que as finalidades e os meios desse tratamento sejam determinados pelo direito da União ou de um Estado-Membro, o responsável pelo tratamento ou os critérios específicos aplicáveis à sua nomeação podem ser previstos pelo direito da União ou de um Estado-Membro. (UNIÃO EUROPEIA, 2016)

E o processador de dados concernindo quem efetua o tratamento de dados, como exposto a seguir denominado como subcontratante que é “uma pessoa singular ou coletiva, a autoridade pública, agência ou outro organismo que trate os dados pessoais por conta do responsável pelo tratamento destes” (UNIÃO EUROPEIA, 2016, Art. 7, 8).

A RGPD também estabeleceu no seu texto a figura de um encarregado, distinguindo-se dos agentes, que estaria encarregado pela comunicação entre os sujeitos da relação do tratamento de dados, atuando como canal entre agentes, titulares e órgãos competentes para informações relevantes, na lesgislação europeia configurando-se na forma do “Data Protection Officer” (DPO):

> 1. O encarregado da proteção de dados tem, pelo menos, as seguintes funções:

> a) Informa e aconselha o responsável pelo tratamento ou o subcontratante, bem como os trabalhadores que tratem os dados, a respeito das suas obrigações nos termos do presente regulamento e de outras disposições de proteção de dados da União ou dos Estados-Membros;
> b) Controla a conformidade com o presente regulamento, com outras disposições de proteção de dados da União ou dos Estados-Membros e com as políticas do responsável pelo tratamento ou do subcontratante relativas à proteção de dados pessoais, incluindo a repartição de responsabilidades, a sensibilização e formação do pessoal implicado nas operações de tratamento de dados, e as auditorias correspondentes;
> c) Presta aconselhamento, quando tal lhe for solicitado, no que respeita à avaliação de impacto sobre a proteção de dados e controla a sua realização nos termos do artigo 35.o;
> d) Coopera com a autoridade de controlo;
> e) Ponto de contacto para a autoridade de controlo sobre questões relacionadas com o tratamento, incluindo a consulta prévia a que se refere o artigo 36.o, e consulta, sendo caso disso, esta autoridade sobre qualquer outro assunto. (UNIÃO EUROPEIA, 2016)

E, seguindo a mesma linha, na LGPD com a indicação do Agente de Proteção de Dados:

> Art. 5º […]
> VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD). (BRASIL)

Como expressão do princípio da transparência e também preconizado no RGPD, a LGPD preocupou-se em aplicar mecanismos que facilitassem o acesso à informação pelos usuários:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
> I - finalidade específica do tratamento;
> II - forma e duração do tratamento, observados os segredos comercial e industrial;
> III - identificação do controlador;
> IV - informações de contato do controlador;
> V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade;
> VI - responsabilidades dos agentes que realizarão o tratamento; e
> VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei. (BRASIL)

Compreendendo-se assim práticas relativas ao consentimento e informações sobre o processo de tratamento, como o método de arrecadação, uso e término no manuseio dos dados; e o consentimento, que deve claro e de livre vontade, pode ser revogado a qualquer momento.

Ainda nesse sentido, com precedente do RGPD, o tratamento dos dados deve, segundo a LGPD, possibilitar a alteração e exclusão dos dados, tanto por vontade do usuário com a revogação do consentimento quanto pelo cumprimento da função a que estavam destinados os dados coletados:

> Art. 18. O titular dos dados pessoais tem direito a obter do controlador, em relação aos dados do titular por ele tratados, a qualquer momento e mediante requisição: […] VI - eliminação dos dados pessoais tratados com o consentimento do titular, exceto nas hipóteses previstas no art. 16 desta Lei. (BRASIL)

Além disso, a LGPD, como o RGPD, assegurou a aplicação de medidas de segurança, como a anonimização, que é a técnica de desassociação entre informações e os indivíduos as quais são referentes:

> Art. 5º [...]
> XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; (BRASIL, 2018)

Uma outra medida é a encriptação de dados, que é o processo de codificação de mensagens ou arquivos, onde a informação necessita de uma chave específica para acesso. Mesmo que essa disposição não esteja expressamente citada na legislação, o art. 48 menciona condutas que afetam a natureza dos dados pessoais, dificultando sua identificação, e é especialmente indicada para dados sensíveis. Tal dispositivo atua assim em caráter preventivo, vejamos:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. § 3º No juízo de gravidade do incidente, será avaliada

> eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis, no âmbito e nos limites técnicos de seus serviços, para terceiros não autorizados a acessá-los. (BRASIL, 2018)

No mesmo dispositivo também apresenta-se o dever de reportar, que é a obrigação da organização responsável de notificar as autoridades imediatamente após o conhecimento de qualquer incidente que comprometa os dados coletados.

Outro traço herdado relacionado que a LGPD contém é sobre a possibilidade de alteração e exclusão dos dados pessoais, que deve ser permitida a qualquer momento, salvo em casos previstos em lei:

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:
> I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;
> II - fim do período de tratamento;
> III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento conforme disposto no § 5º do art. 8º desta Lei, resguardado o interesse público; ou
> IV - determinação da autoridade nacional, quando houver violação ao disposto nesta Lei. (BRASIL, 2018)

Assim, com o cessamento do tratamento dos dados – por finalidade ou revogação da concessão – as informações do usuário devem ser apagadas pelo agente que as coletou.

Quanto a aplicação de sanções, o RGPD estipula penas gradativas bem como também multas administrativas, no limite de 20 milhões de euros ou 4% do faturamento anual da empresa. De modo análogo, a LGPD também prevê a variação de sanções:

> 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 (BRASIL, 2018)

Baseando na gravidade e natureza do caso, como critérios de reincidência, condição econômica, entre outros, e modalizam-se entre multas simples ou diárias, restringindo-se a 2% do faturamento da organização responśavel, podendo chegar a R$ 50 milhões por cada infração.

Por fim, o RGPD formou um órgão de controle e fiscalização de proteção de dados pessoais para cada estado, denominados APD:

> Art. 51 Autoridade de Controle:
> 1. Os Estados-Membros estabelecem que cabe a uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização da aplicação do presente regulamento, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União (autoridade de controle).
> 2. As autoridades de controlo contribuem para a aplicação coerente do presente regulamento em toda a União. Para esse efeito, as autoridades de controlo cooperam entre si e com a Comissão, nos termos do capítulo VII. (UNIÃO EUROPEIA, 2016)

Do mesmo modo, a LGPD determinou a criação da ANPD, a Autoridade Nacional de Proteção de Dados Pessoais,

> Art. 55-A. Fica criada a Autoridade Nacional de Proteção de Dados - ANPD, autarquia de natureza especial, dotada de autonomia técnica e decisória, com patrimônio próprio e com sede e foro no Distrito Federal. (BRASIL, 2018)

Bem como atentou-se para as responsabilidades da ANPD, ao listar no art. 55-J as competências do órgão, que possui como atribuições principais a tutela e supervisionamento do tratamento de dados:

> Art. 55-J. Compete à ANPD:
> I - zelar pela proteção dos dados pessoais, nos termos da legislação;
> II - zelar pela observância dos segredos comercial e industrial, observada a proteção de dados pessoais e do sigilo das informações quando protegido por lei ou quando a quebra do sigilo violar os fundamentos do art. 2º desta Lei;
> III - elaborar diretrizes para a Política Nacional de Proteção de Dados Pessoais e da Privacidade;
> IV - fiscalizar e aplicar sanções em caso de tratamento de dados realizado em descumprimento à legislação, mediante processo administrativo que assegure o contraditório, a ampla defesa e o direito de recurso. (BRASIL, 2018)

O art. 55 aufere um grande valor ao analisar-se o papel das autoridades de proteção de dados em legislações de outros países, o órgão possui a capacidade, similarmente, de desempenhar funções até além do que LGPD prevê, como poderá ser visto adiante.

Essas possíveis atribuições ganham um significado ainda mais especial devido a recente transformação do órgão em autarquia de natureza especial, através da Medida Provisória nº 1.124, de 13 de junho de 2022:

> Art. 1º Fica a Autoridade Nacional de Proteção de Dados - ANPD transformada em autarquia de natureza especial, mantidas a estrutura organizacional e as competências e observados os demais dispositivos da Lei nº 13.709, de 14 de agosto de 2018. (BRASIL, 2022).

A medida altera a natureza da ANPD, conferindo-a uma autonomia administrativa e orçamentária, e faz parte do plano elaborado pelo texto original da lei, o antigo art. 55 previa:

> Art. 55 [...]
> § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República.
> § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. (BRASIL, 2019)

Apesar de depender de sancionamento, a independência de gestão mediante conversão do órgão em autarquia de natureza especial possibilitaria o tornar equivalente aos APD do regulamento europeu, capacitando-o para determinação de seus melhores interesses e evolução de suas práticas.

4 RELAÇÃO DA IMPLEMENTAÇÃO DA LGPD NOS PERÍODOS ANTERIORES E POSTERIORES À APLICAÇÃO DE SANÇÕES

O período da vacatio legis da LGPD foi de questionável tutela sobre os dados pessoais no Brasil, com o dilatamento da fase de adaptação das empresas ao regulamento e adiamento da aplicação de sanções, o país foi cenário de casos atípicos em que há margem para a impunidade mas a legislação é utilizada como referência em momento anterior a sua efetivação.

Posteriormente, mesmo com a aplicação de sanções em funcionamento, novos desafios estavam fadados a surgir, refletindo uma realidade comum a outros ramos do Direito, o grande contingente de casos sobrecarregando o sistema, fruto de uma Cultura de Litigância somada a imprópria abordagem do problema.

4.1 A aplicação da proteção de dados durante a vacatio legis da LGPD: os casos da Netshoes e Vivo

Inicialmente, a LGPD teria seu período de adaptação programado para 18 (dezoito) meses após a sua publicação, isto é, a lei, que fora promulgada em agosto de 2018, teria sua vigência apenas em setembro de 2020, após um conturbado processo de emancipação dada as discussões no que tange o reduzido período para adaptação das empresas e órgãos públicos.

Além disso, houve uma pressão para prorrogação desse período em consequência do panorama de pandemia que acometeu o Brasil, justificando uma narrativa de que a implementação custaria recursos que os pretensos responsáveis não poderiam arcar, resultando em mais 6 (seis) meses de prorrogação, totalizando 2 (dois) anos de vacatio legis.

Ainda, por meio da lei 14.010/2020, as sanções estariam planejadas apenas para surtir efeitos em agosto de 2021, ou seja, a LGPD contemplava-se em um limbo legal que fora agravado pela Medida Provisória n. 959/2020, esta buscava estender o vacatio legis antes estabelecido para maio de 2021 apenas para ter esta previsão excluída na sua conversão na lei 14.058/20, resultando no seu vigor em setembro de 2020 mas suas sanções administrativas pospostas para 1º de agosto de 2021.

Diante disso, é possível reconhecer que o período de vacatio-legis prolongado da LGPD instituiu certas crises, tal qual o quesito de acúmulo de processos, como ressaltado pelos autores Celso Monteiro e Patrícia Helena em matéria do “Valor Econômico”, visto que o

Superior Tribunal de Justiça (STJ) antecipou que “a LGPD, logo em seu primeiro ano de vigência, já poderia ser o objeto de mais de 20 mil processos judiciais”.

Tal declaração baseava-se na ideia de que mesmo não estando ainda em vigência quanto as sanções administrativas, a LGPD trouxe uma conscientização dos direitos sobre a proteção de dados, não apenas refletindo em demandas de interesse difuso e coletivo, mas também individuais, assim, a LGPD tornou-se base para processos judiciais, sendo citada como base jurídica de vários processos mesmo no período de vacância.

Para ilustrar a aplicação no vacatio legis, pode-se mencionar dois casos em que MPDFT, Ministério Público do Distrito Federal e Territórios, tratou sobre a proteção de dados nessa fase: o termo de ajustamento de conduta da Netshoes e o inquérito contra a plataforma Vivo Ads.

O primeiro caso tratou-se, como citado anteriormente, no ajustamento de conduta em que a empresa Netshoes passou a se comprometer em práticas mais responsáveis em relação a proteção de dados, quer dizer, o termo firmado citou a LGPD mesmo antes de sua integral implementação referindo-se a mesma como norma norteadora de suas ações “Considerando, a título de diretriz, que a Lei n. 13.709/18 prevê a necessidade […]” para justificar o uso de tal recurso pela autoridade responsável. Tal atitude foi influenciada pelos casos de 2017 e 2018.

No qual, como mencionado, houve um vazamento de informações de cerca de 2 milhões dos clientes da loja, em que a empresa precisou pagar R$ 500.000,00 de indenização pelos danos morais coletivos ocasionados.

A indenização refere-se ao episódio em que a empresa Netshoes, entre o fim de 2017 e começo de 2018, teve informações de sua lista de credenciais vazadas, cerca de 1.999.704 usuários foram afetados. Entre as informações vazadas estavam dados como nome completo dos usuários, e-mails, cadastros de pessoa física e produtos comprados.

Para agravar a situação, a Netshoes lidou com a situação somente através de um e-mail genérico, informando para alguns usuários que seus dados poderiam estar comprometidos, e foi apenas após pressão do Ministério Público que a empresa entrou em contato mediante ligações para os quase 2 milhões de afetados

Foi através da colaboração da empresa com o Ministério Público durante a investigação que a mesma conseguiu fechar um acordo judicial para evitar uma ação coletiva a ser interposta pela instituição. No acordo a Netshoes se comprometeu a pagar 5 parcelas a título de indenização pelos danos morais cometidos, que deveriam ser depositados no Fundo de Defesa de Direitos Difusos, o FDD. Além disso, como mencionado, a empresa teve que

implementar medidas adicionais ao seu Programa de Proteção de Dados, adequando-se assim às políticas de segurança cibernéticas previstas na LGPD.

Já no segundo caso relevante, o MPDFT exigiu um relatório prescrito na própria LGPD para a empresa Vivo, o Relatório de Impacto à Proteção de Dados Pessoais, RIPD, que é um quadro geral do qual a empresa demonstra como os dados são coletados, tratados, usados, compartilhados e quais tipos de medidas serão implementadas para diminuir os riscos que possam afetar os titulares, presente no art. 5º, inciso XVII:

> Art. 5º Para os fins desta Lei, considera-se: […]
> XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco. (BRASIL, 2018)

Em concordância com o art. 38 da mesma lei, em que prevê a autorização para tal requerimento:

> Art. 38. A autoridade nacional poderá determinar ao controlador que elabore relatório de impacto à proteção de dados pessoais, inclusive de dados sensíveis, referente a suas operações de tratamento de dados, nos termos de regulamento, observados os segredos comercial e industrial.
> Parágrafo único. Observado o disposto no caput deste artigo, o relatório deverá conter, no mínimo, a descrição dos tipos de dados coletados, a metodologia utilizada para a coleta e para a garantia da segurança das informações e a análise do controlador com relação a medidas, salvaguardas e mecanismos de mitigação de risco adotados. (BRASIL, 2018)

Tal evento ocorreu para apuração da plataforma “Vivo Ads” sobre o uso de dados para publicidade pela mesma, e foi ajuizada em 30 de julho de 2019 através de uma Ação Civil Pública. O desenvolvimento do caso estendeu-se até em pedido de suspensão do serviço de mídia geolocalizada, em que o MPDFT pediu pelo cessamento da comercialização da plataforma contra a Telefônica Brasil, sucessora por incorporação da Vivo, sob a justificativa de que o serviço “ADS” permitiria, além da publicidade baseada no perfil e localização do usuário, o uso dos dados de geolocalização para extração de informações sensíveis dos clientes,

que, ao serem repassados comercialmente e sem o devido controle, provocam grandes consequências aos consumidores.

O pedido foi julgado improcedente e em sua defesa a Vivo assumiu uma postura de que a publicidade decorrente dos dados de localização coletas pela plataforma possuem somente como alvo aqueles consumidores que consentiram para o uso dos dados. Em especial, para o momento, o relatório do Impacto à Proteção de Dados foi entendido como desnecessário pela empresa, que alegou que a ANDP, a Autoridade Nacional de Proteção de Dados, ainda não havia detalhado como deveria ser feito o parecer, carecendo de regulamentação.

Ambos os casos sintetizam a imediata relevância da legislação, em que a LGPD, apesar de suas limitações, foi citada em casos mesmo antes de sua implementação de fato, mas também apontou para uma demanda forte mesmo inicialmente, e do tipo problemas que o período de vacatio-legis acarretou.

4.2 Situação atual da proteção de dados no contexto da LGPD

De acordo com o exposto anteriormente, a LGPD teve a implementação de sanções administrativas desde de agosto de 2021, após amplo período de suposta adaptação pelas empresas, agravado por várias prorrogações que estenderam por mais do que o previsto na sua criação. Foi só a partir desse momento que a Autoridade Nacional de Proteção de Dados pôde exercer a função de aplicação de penalidades.

Mesmo assim, o prolongamento do tempo não foi o suficiente para garantir uma implementação ampla e eficiente das políticas previstas na legislação pela empresas, com crescente número de casos que se acumulam e não alcançam um desfecho.

O período caótico da pandemia do coronavírus justificou a alegação de vulnerabilidade das empresas, porém, apenas serviu para demonstrar uma incongruência em que empresas não eram compelidas a respeitar os dados pessoais de titulares num período de exponencial crescimento do uso de serviços pela internet.

Nesse cenário, evidentemente, a dinâmica social e de consumo sofreu grandes mudanças e uma nova realidade exigiu uma adaptação por parte de empresas, com muitas migrando seus negócios para o ambiente digital de modo exclusivo, não obstante, a análise de dados para compreensão de hábitos e comportamentos no comércio atingiu um grau de importância ainda maior e com isso um aumento de episódios de vazamentos, manipulação e violações de dados, intensificando o cenário de desamparo jurídico.

A própria ANPD divulgou dados alarmantes já em 2021, segundo o órgão, somente entre janeiro e outubro, foram 2.930 demandas que alcançaram a Ouvidoria, com 547 denúncias de titulares. No mês de agosto ,quando entraram em vigor as sanções, foram 627 demandas, como expôs a diretora Miriam Wimmer durante seminário promovido pelo Tribunal de Contas da União.

Isso demonstra uma maior conscientização sobre os direitos previstos na LGPD mas escancara uma predisposição já bastante comum para o Judiciário brasileiro: o acúmulo de casos, que congestionam o sistema jurídico e prejudica a reinvidicação de direitos dos indivíduos.

4.3 Possibilidade de desenvolvimento da legislação

Como visto no estudo, um dos maiores desafios encontrados pela LGPD para a proteção de dados pessoais está relacionado com o tema central de acesso à justiça: os titulares devem possuir canais de à infomações e a métodos alternativos de resolução de conflitos.

A precária realidade brasileira quanto aos litígios é sempre evidente, apesar de grandes avanços ao longo dos anos, o país enfrenta um grande histórico de ineficiência do judiciário, com alto número de demandas e morosidade processual exacerbada.

É importante então reconhecer a necessidade de meios facilitadores como forma de diminuir a sobrecarga judiciária. Uma das formas possíveis é a implementação de sistemas de métodos alternativos de resolução de conflitos.

A própria ideia de uma disposição multifacetada de soluções não é estranha para o ordenamento jurídico brasileiro e teve como grande marco as mudanças trazidas pelo Código de Processo Civil de 2015, através do disposto no art. 3º, §§ 2º e 3º:

> Art. 3º Não se excluirá da apreciação jurisdicional ameaça ou lesão a direito.
> § 2º O Estado promoverá, sempre que possível, a solução consensual dos conflitos.
> § 3º A conciliação, a mediação e outros métodos de solução consensual de conflitos deverão ser estimulados por juízes, advogados, defensores públicos e membros do Ministério Público, inclusive no curso do processo judicial. (BRASIL, 2015)

Bem como também a Resolução nº 125 de 29 de novembro de 2010, que dispõe sobre a Política Judiciária Nacional de tratamento adequado dos conflitos de interesse no âmbito do Poder Judiciário, buscando esclarecer e aplicar diretrizes para contrapor a cultura do litígio brasileira. Sobre o assunto, dispõe Cahali (2014):

> Coloca a disposição da sociedade, alternativas variadas para se buscar a solução mais adequada de controvérsias, especialmente valorizados os mecanismos de pacificação (meios consesuais), e não mais restrita a oferta ao processo clássico de decisão imposta pela sentença judicial, cada uma das opções (mediação, conciliação, orientação a própria ação judicial contenciosa, etc.), representa uma porta, a ser utilizada de acordo com a conveniência do interessado, na perspectiva de se ter a maneira mais apropriada de administração e resolução do conflito. (CAHALI, 2014)

Tais métodos então almejam facilitar e ampliar a efetivação de direitos, sem prejuízo da tutela de direitos convencionais, apresentando uma justiça preocupada na coexistência e maior participação das partes.

Os MESCS, meio extrajudiciais de solução de conflitos, são geralmente divididos em arbitragem, negociação, conciliação e mediação, e podem ser aplicados na realidade dos conflitos originários da aplicação da LGPD mediante certas adaptações.

Como primeiro exemplo dos MESCS, pode-se falar da arbitragem, que é um dos métodos heterocompositivos para resolução de conflitos, onde as partes concordam um autorizado, geralmente especialista no tipo de caso, que proferirá julgamento com poder de decisão.

A ideia desse método é encaminhar os casos para autoridades previamente estabelecidas pela legislação - como é exemplo das normas de internacionais vistas anteriormente - onde as partes encontram-se sob o método adversarial, isto é, representam-se e posicionam-se como oponentes, havendo um choque de interesses e resultando na vitória de uma das partes.

As legislações internacionais demonstraram ser possível a aplicação da arbitragem no conflitos originados pela tutela dos dados pessoais, mesmo que de diferentes formas, seja a semi-institucionalização de Singapura, seja pela delegação de entidades externas como são os casos da Austrália e Nova Zelândia.

Porém, a arbitragem ainda possui desafios intrísecos, afinal, ainda consiste em uma disputa entre indivíduos ou grupos de indivíduos e empresas; uma relação desigual entre o

hipossuficiente, na forma do titular dos dados pessoais, e do hipersuficiente, do responsável pelo tratamento dos dados.

Já a negociação, conciliação e mediação configuram os métodos autocompositivos de resolução de conflitos, isto é, quando ambos as partes trabalham juntos buscando a solução do desacordo, e também são uma alternativa viável para servir como resposta ao aumento de demandas do Judiciário, e, paralelamente, no conflitos da implementação da LGPD.

A negociação e a conciliação se assemelham ao compreenderem, respectivamente, a autocomposição sem auxílio de terceiros e com a intervenção de terceiro desinteressado, na figura do conciliador, que auxilia através de sugestões para solucionar a divergência.

Já a mediação, apesar de também possuir um terceiro imparcial, tem sua condução feita pelo mediador, que aufere uma comunicação mais eficiente entre as partes, atuando no descalonamento do conflito e negociação de soluções entre as partes.

Diferentemente da arbitragem, nos métodos autocompositivos às partes não são impostas decisões sobre o conflito, cabendo a elas decidir se acatam ao que for acordado em sessão. Esse tipo de composição possui vantagens ao trabalhar com o esgotamento de recursos até as vias judiciais, isto é, as partes podem conduzir seus litígios por diferentes mecanismos, no intuito de atingir aquele mais adequado.

Quanto a aplicação e fiscalização dessas vias, o passo mais lógico seria a da expansão do papel da ANPD, aumentando o seu rol de funções para enquadrar o órgão como intermediário entre titulares, agentes e entes autorizados, na arbitragem, ou a própria institucionalização dos métodos autocompositivos, como a criação de centros especializados do governo para conflitos gerados no âmbito de proteção de dados pessoais.

5 CONSIDERAÇÕES FINAIS

Este trabalho se propôs a analisar a Lei Geral de Proteção de Dados e traçar um paralelo entre a legislação e a possibilidade de implementação de mudanças capazes de sanar parte dos desafios encontrados pela mesma mediante meios alternativos de solução de conflitos.

Ao analisar sobre legislações diversas, foi possível traçar uma linha lógica geral do desenvolvimento da proteção de dados, desde seus primórdios, bem como estudar diferentes métodos utilizados

Como explorado, a morosidade da Justiça e a cultura da Judicialização são adversários na resolução de demandas sociais, e como abordado, também presentes no contexto da proteção de dados pessoais, que mesmo sendo uma legislação recente já enfrenta um número substancial de casos e, consequentemente, acúmulo de processos.

Para suprimir essas adversidades há a necessidade de se seguir o caminho aparentemente dicotômico de institucionalização de métodos extrajudiciais e/ou adequados de solução de conflitos justamente para aliviar o Judiciário.

Insere-se na questão a expansão das funções da ANPD, que pode atuar como figura intermediária entre os envolvidos e garantidora do cumprimento das normas, como é o caso das autoridade de proteção de dados de países como Singapura, Austrália e Nova Zelândia.

A LGPD dispõe de valores de empoderamento do titular dos dados, preceituando sobre independência e capacidade, essas concepções possuem uma grande afinidade com os métodos heterocompositivos e autocompositivos.

Isto é, ao promover tais métodos, a LGPD estaria proporcionando uma justiça mais eficiente, prática e, especialmente, participativa. O titular gozaria assim de uma maior gama de escolhas de promover a resolução de sua divergência e não inviabilizando o uso dos métodos tradicionais, ao mesmo tempo que diminuiria a sobrecarga da Justiça que aflige os diferentes ramos do Direito.

REFERÊNCIAS

ANPD participa da 41 Reunião Plenária da Convenção 108. Portal Único do Governo, Brasília, 01 de julho de 2021. Disponível em: https://www.gov.br/anpd/pt-br/assuntos/noticias/anpd-participa-da-41a-reuniao-plenaria-da-convencao-108. Acesso em: 03 jan. 2022.

ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS. Declaração Universal dos Direitos Humanos, 10 de dezembro de 1948. Disponível em: https://www.unicef.org/brazil/declaracao-universal-dos-direitos-humanos. Acesso em: 01 jan. 2022.

BRASIL. [Constituição (1988)]. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/ Constituiçao.htm. Acesso em: 21 out. 2021.

BRASIL. Lei nº 12.965, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Brasília, DF: Presidência da República, [2021]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm . Acesso em: 22 out. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 22 out. 2021.

BRASIL. Lei nº 13.853, de julho de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá providências. Brasília, DF: Presidência da República, [2019]. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/lei/l13853.htm. Acesso em: 22 out. 2021.

BRASIL. Medida Provisória nº 1.124, de 13 de junho de 2022. Altera a Lei nº 13.709, de 14 de agosto de 2018 – Lei Geral de Proteção de Dados Pessoais, transforma a Autoridade Nacional de Proteçã de Dados em autarquia de natureza especial e transforma cargos em comissão. Brasília, DF: Presidência da República, [2022]. Disponível em: https://www.in.gov.br/en/web/dou/-/medida-provisoria-n-1.124-de-13-de-junho-de-2022-407804608. Acesso em: 29 jun. 2022.

COSTA JR., Paulo José da. O direito a estar só: tutela penal da intimidade. São Paulo: RT, 1970, p. 31, citando HENKEL, Der Strafschutz des Privatlebens. Em sentido contrário, não reconhecendo a Teoria das Esferas, DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar: 2006, p. 108-109.

GROSSMANN. Luis Osvaldo. ANPD: notificações de incidentes disparam em agosto e ano já tem 116 casos. Portal Convergência Digital, 2021. Disponível em: https://www.convergenciadigital.com.br/Governo/Legislacao/ANPD%3A-Notificacoes-de-incidentes-disparam-em-agosto-e-ano-ja-tem-116-casos-58541.html?UserActiveTemplate=mobile. Acesso em: 28 jun. 2022.

KEMP, Simon. Digital 2022: Global Overview Report. Datareportal, 2022. Disponível em: https://datareportal.com/reports/digital-2022-global-overview-report. Acesso em: 28 jun. 2022.

MONTANGER, Camila. Sua cidade, seus dados, 2017. Histórico pelo Mundo: Alemanha. Disponível em: http://dadospessoais.lavits.org/historico-pelo-mundo/. Acesso em 03 jan. 2022.

MPDTF, TAC nº 01/2019 – ESPEC Termo de Ajustamento de Conduta firmado pela Netshoes (Ns2.Com Internet S.A.) com o Ministério Público do Distrito Federal e Territórios, para pagamento de indenização por danos morais coletivos causados pelo incidente de segurança que gerou o comprometivmento de dados pessoais de clientes. Disponível em: https://www.mpdft.mp.br/portal/pdf/tacs/espec/TAC_Espec_2019_001.pdf. Acesso em: 13 jun. 2022.

MUNDO se aproxima da marca de 5 bilhões de usuaários de internet, 63% da população. Insper, 2022. Disponível em: https://www.insper.edu.br/noticias/mundo-se-aproxima-da-marca-de-5-bilhoes-de-usuarios-de-internet-63-da-populacao/. Acesso em: 28 jun. 2022.

OLIVEIRA, Icaro Aron Paulino Soares de Oliveira. Constituição da Espanha de 1978 (revisada em 2011). Jus, 2022. Disponível em: https://jus.com.br/artigos/98127/constituicao-da-espanha-de-1978-revisada-em-2011. Acesso em: 28 jun. 2022.

PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. Diretiva 46/95/CE. Relativa à proteção das pessoas singulares no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados, 24 de outubro de 1995. Disponível em: https://eur-lex.europa.eu/legal-content/PT/LSU/?uri=celex%3A31995L0046. Acesso em: 22 out. 2021.

PARLAMENTO EUROPEU E O CONSELHO DA UNIÃO EUROPEIA. Regulamento (UE) 2016/679. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados, 27 de abril de 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/?uri=celex%3A32016R0679. Acesso em: 22 out. 2021.

PECK, Patrícia. Proteção de dados pessoais. São Paulo: Editora Saraiva, 2020. 9788553613625. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788553613625/. Acesso em: 30 mai. 2022.

PORTUGAL. Constituição da República Portuguesa de 1976. Defende a independência nacional, garante os direitos fundamentais dos cidadãos, estabelece os princípios basilares da

democracia e assegura o primado do Estado de Direito democrático. Disponível em: https://www.parlamento.pt/ArquivoDocumentacao/Documents/CRPVIIrevisao.pdf. Acesso em: 28 jun. 2022.

RIQUITO, Ana Luísa. [et al.]. Carta de Direitos Fundamentais da União Europeia. Coimbra: Coimbra Editora, 2001.

SPECIAL message to congress on protecting consumer interest. John F. Kennedy Presidential Library and Museum. Disponível em : http://www.jfklibrary.org/Asset-Viewer/Archives/JFKPOF-037-028.aspx. Acesso em: 01 jan. 2022.

USO da internet avança em áreas rurais durante a pandemia, revela nova edição da TIC Domicílios. Centro Regional de Estudos para Desenvolvimento da Sociedade da Informação, 2022. Disponível em: https://www.cetic.br/pt/noticia/uso-da-internet-avanca-em-areas-rurais-durante-a-pandemia-revela-nova-edicao-da-tic-domicilios/. Acesso em: 28 jun. 2022.

VENTURA, Felipe. Netshoes paga R$ 500 MIL em danos morais após vazamento de dados, Tecnoblog, fevereiro de 2019. Disponível em: https://tecnoblog.net/277594/netshoes-acordo-mpdft-vazamento-dados/. Acesso em: 13 jun. 2022.