FACULDADES INTEGRADAS DE RONDONÓPOLIS
CENTRO UNIVERSITÁRIO LEONARDO DA VINCI
CURSO DE DIREITO

EDUARDO JACKSON DE OLIVEIRA BENITES

A LEI GERAL DE PROTEÇÃO DE DADOS COMO UM REFLEXO À ERA DA INFORMAÇÃO: AVANÇOS E PROBLEMÁTICAS

RONDONÓPOLIS

2023

EDUARDO JACKSON DE OLIVEIRA BENITES

A LEI GERAL DE PROTEÇÃO DE DADOS COMO UM REFLEXO À ERA DA INFORMAÇÃO: AVANÇOS E PROBLEMÁTICAS

Trabalho de Conclusão de Curso apresentado como requisito parcial para a aquisição do título de Bacharel em Direito, pelo curso de Direito da Faculdades Integradas de Rondonópolis.

Orientadora: Profª. Esp. Verginia Chinelato.

RONDONÓPOLIS

2023

A LEI GERAL DE PROTEÇÃO DE DADOS COMO UM REFLEXO À ERA DA INFORMAÇÃO: AVANÇOS E PROBLEMÁTICAS

Trabalho de Conclusão de Curso apresentado como requisito parcial para obtenção do título de Bacharel em Direito, pelo Curso de Direito das Faculdades Integradas de Rondonópolis.

Aprovado em: ____/____/_____

BANCA EXAMINADORA

_____

Componente da Banca Examinadora – Nome, titulação, assinatura e instituição a que pertence

_____

Componente da Banca Examinadora – Nome, titulação, assinatura e instituição a que pertence

_____

Componente da Banca Examinadora – Nome, titulação, assinatura e instituição a que pertence

2023

SUMÁRIO

1. INTRODUÇÃO

A sociedade, desde o início de sua formação, está eivada com problemas sociais. Onde existir mais de uma pessoa, existirá desencontro de opiniões que gerarão problemas a serem resolvidos. O Direito surge como um sistema de "soluções" para essas problemáticas que o ser humano gera ao conviver em sociedade. Por isso, o Direto deve acompanhar e servir à sociedade, e de tempos em tempos, atualizar seus conceitos e punições de acordo com a demanda social de sua época.

Após a constante evolução da tecnologia desde o início dos anos 2000, os dados pessoais tornaram-se ativos valiosos para toda a sociedade. Ocorre que os avanços provocados pela era da informação não foram acompanhados, de maneira eficaz, por nosso ordenamento jurídico. Tal cenário desencadeou uma série de acontecimentos benéficos àqueles que coletavam dados pessoais de terceiros e em contrapartida, acontecimentos desfavoráveis aos titulares destes dados.

Proclamado como "o novo petróleo" (REIS, 2021 apud HUMB, 2006), os dados pessoais passaram a ser valorados e começaram a dar retorno financeiro para quem os detinham, a exemplo, algumas das empresas mais ricas e influentes do mundo~~,~~ tais como Facebook e Instagram, que se destacam por manusear, em grande escala, os dados pessoais de seus usuários. (SLYNCHUK, 2021).

Ainda que recentemente o Brasil adotou uma legislação específica para regularizar a coleta, o compartilhamento, o armazenamento e outros atos de tratamento dos dados pessoais do titular, a população brasileira até então, não teve tempo suficiente para se familiarizar, passar a notar e dar valor à privacidade e proteção de seus dados.

Quais os problemas que fizeram necessária a criação de uma legislação específica para dispor sobre dados pessoas e quais os avanços que obtivemos após essa nova percepção de dados pessoais como um ativo de majestoso valor?

Assim como toda novidade, os novos parâmetros para a concessão e utilização de dados pessoais podem causar um estranhamento para quem os conhece em um primeiro momento, nos cidadãos em si, e, também, e principalmente, em empresas que precisam se adequar à legislação.

Com fulcro no direito à liberdade disposto na Constituição Federal, a Lei Geral de Proteção de Dados veio para dar uma maior abrangência e seguridade aos titulares dos dados, haja vista que

na sociedade moderna atual não há de se falar em privacidade sem que haja a devida proteção de dados pessoais.

Porém, presume-se que após o processo de adaptação ao novo método de tratamento dos dados pessoais, a população brasileira começará a ter um senso crítico mais efetivo sobre a concessão de seus dados. Visto que, se a cada ano que se passa, a tecnologia ao nosso alcance avança de maneira exorbitante, é sensato pensarmos que para acompanharmos esse avanço da tecnologia devemos nos atualizar aos novos conceitos trazidos com ela, com destaque aos conceitos virtuais, considerando a modernidade atual.

Ao nos depararmos com situações de constrangimento por violação de dados pessoais, podemos, por ignorância no assunto, deixar que nos reprimam e se beneficiem de má-fé sobre a utilização dos nossos dados pessoais. Vale ressaltar que a nossa privacidade está completamente atrelada aos nossos dados pessoais, logo, devemos olhar atentamente e tomar ciência dos atos despercebidos que praticamos corriqueiramente com nossos dados e evitar que a nossa privacidade seja violada.

Em uma sociedade onde se tem aparelhos eletrônicos à portabilidade da maior parte das pessoas, como no Brasil, onde, em 2019 cerca de 82% dos brasileiros já utilizavam internet (**IBGE EDUCA**, 2019), é evidente que haverá muitas pessoas que tem acesso a celulares, computadores, etc., mas que não têm maturidade suficiente para se prevenirem dos perigos que existem no mundo virtual acerca da proteção de seus dados pessoais.

Dito isso, é totalmente plausível a discussão sobre o tema proposto, tendo em vista que os frutos colhidos de tal assunto tendem a conscientizar o cidadão leigo a se prevenir e utilizar dos seus dados de maneira segura e responsável.

1.1 A era da tecnologia

Desde o fim do século passado e o início do novo século, a internet e os aparelhos eletrônicos começaram a participar cada vez mais do dia a dia das pessoas, de forma que, tudo era novo aos nossos olhos e desde sempre, cedíamos nossos dados sem sequer nos preocuparmos para quem estávamos concedendo esta graça.

Após o fim da Segunda Guerra Mundial, muita tecnologia usada na guerra foi aproveitada e desmiuçada para outro fim que não fosse bélico.

Segundo Kenski (2007, p.16):

> Em muitos casos, é na pesquisa e produção de novos armamentos e equipamentos militares que os órgãos de defesa dos países desenvolvidos descobrem (algumas vezes acidentalmente, mas nem sempre) usos domésticos para os mesmos produtos. Dos centros de pesquisa, essas invenções migram para o uso ampliado em nossas casas e alteram nossas vidas.

Com o avanço tecnológico progredindo com muita rapidez, logo, recursos que eram caros e escassos passaram a ser mais acessíveis aos civis, e com isso, num primeiro momento, computadores e acesso à internet passaram a ingressar como ferramentas no dia a dia dos cidadãos. Isso porque, ao tornar acessível o preço no mercado, empresas começaram a investir em equipamentos mais tecnológicos para agregar em seus negócios, e consequentemente, seus colaboradores passaram a ter contato com mais frequência com esses equipamentos.

Dito isso, conforme os aparelhos iam se atualizando, os funcionários deveriam receber treinamentos para se atualizarem junto, desencadeando assim, cada vez mais familiaridade com o manuseio desses equipamentos que passariam a fazer parte até mesmo do cotidiano social desses funcionários.

A medida em que nos aproximamos dos anos 2000, o mundo foi se virtualizando cada vez mais e as pessoas passaram a consumir internet como não havia consumido antes.

Neste sentido, dispõe Nilton (2011):

> A unificação e comercialização da internet foram encaminhadas a partir de 1993, mas apenas em dois anos ela atingiu seu ápice: a NSFnet deixou de ser a "dona" das redes e todo o tráfego passou a ser público. As universidades, centros de pesquisa e unidades militares não eram mais os únicos locais privilegiados com a rede. Ao mesmo tempo, surgia o domínio de sites comerciais para computador, o ".com", ainda com baixa afiliação de páginas.

Após essa unificação e comercialização da internet passar a ser pública, tudo mudou. O mundo passou a engatinhar para receber de fato a era da tecnologia, e a crescente virtualização de atos e processos físicos começaram a se digitalizar em telas e monitores, criando assim, uma cultura de uso da internet para quase todos os atos da vida civil e corporativa que dificilmente terá um fim.

1.2. As redes sociais

Assim sendo, surgiram as redes sociais, que são as plataformas que atualmente interligam as pessoas a nível global, isto é, pessoas do mundo inteiro usam as redes sociais e se comunicam simultaneamente pelos aplicativos ou sites.

Por mais que hoje em dia temos uma falsa impressão de que as redes sociais é algo que surgiu a pouco tempo, temos datada como rede social, algo que veio antes mesmo do Facebook, que foi a grande massa mundial no que diz respeito à rede social.

Segundo Katia (2022, online):

> Lançado em 1997, o SixDegrees (sixdegrees.com) é considerado a primeira rede social da história da Internet. O site foi pioneiro ao oferecer recursos que são comuns nas plataformas de hoje, como se conectar com outros usuários, criar perfis e organizar grupos. [...]
> Precursor de redes como Orkut, Facebook e Instagram, o SixDegrees chegou a ter cerca de 3,5 milhões de usuários até seu fim, em 1999.

E o número de usuários de aplicativos de redes sociais está em uma constante crescente, para Cris (2022, online):

> Quando falamos em redes sociais, estamos falando de 4,62 bilhões de usuários. Esse número vai crescer ainda mais nos próximos meses e deve chegar a 60% da população global num brevíssimo tempo. Sim, porque essas plataformas recebem cerca de um milhão de novos usuários POR DIA, ou 13,5 POR SEGUNDO.

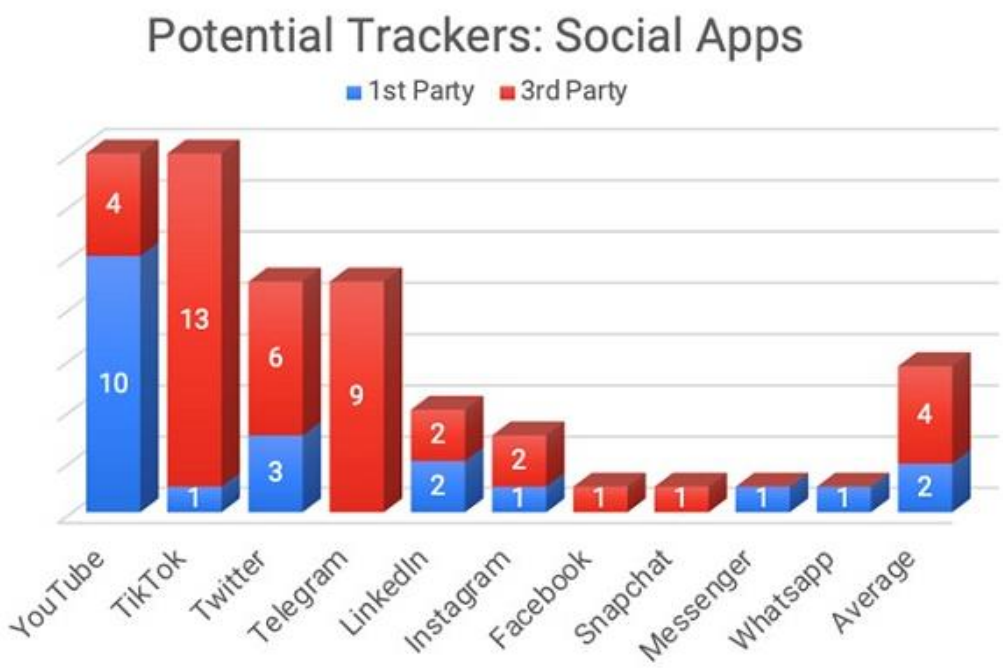
Atualmente, grande parte da população tem alguma rede social e se conecta com outros usuários, mas o que preocupa nesse cenário não é o número de pessoas que acessam, mas sim, a quantidade de dados pessoais que são coletados por esses sites e aplicativos e o que estão fazendo com eles.

Dos aplicativos em alta no momento, o Tik Tok e o Youtube são os que mais coletam dados pessoais de seus usuários, segundo estudo da empresa URL Genius, que foi publicado em janeiro de 2022 (Tudocelular, 2022).

O que preocupa nesse caso é que não fica claro para os usuários o que será feito com esses dados coletados, ou seja, por mais que tenha o termo de política de privacidade, os usuários não sabem com quem os aplicativos compartilham esses dados coletados.

Ainda segundo o site, Tudocelular (2022), a pesquisa URL Genius disponibilizou em gráficos, os aplicativos que mais rastreiam dados pessoais:

Figura 1 – Gráfico de resultado da pesquisa dos aplicativos que mais rastreiam dados pessoais



Fonte: https://www.tudocelular.com/seguranca/noticias/n186054/tiktok-e-youtube-sao-as-plataformas-que-mais-coletam-dados-de-usuarios.html#:~:text=TikTok%20e%20YouTube%20s%C3%A3o%20as%20plataformas%20que%20mais%20coletam%20dados%20dos%20usu%C3%A1rios,-10%20de%20fevereiro

E o site prossegue, dizendo que este relatório verificou que os gerenciadores dos aplicativos, por meio desses rastreadores, conseguem manusear dados mesmo daqueles usuários que já não usam mais os aplicativos (Tudocelular, 2022).

É uma situação alarmante para as pessoas que usam essas redes sociais, pois a grosso modo, não enxergamos nada demais em ceder dados cadastrais para esses aplicativos, já que se levarmos em comparação com os demais atos de nossas vidas, essa prática é corriqueira em várias situações, tais como, preenchimento de ficha médica, curriculum vitae, cadastro em lojas para ter acesso à compra no formato de crediário, cadastro em fichas para concorrer a sorteios, etc.

Todavia, o que temos que sopesar em nossa balança são os motivos, ou melhor dizendo, a fundamentação para a solicitação de alguns dados. Enquanto que, para que o médico realize um

procedimento em um paciente, é crucial que ela saiba de alguns dados do paciente (como tipo sanguíneo, sexo, idade, etc.), para um aplicativo, não é justificável que a pessoa dê a ele, acesso a dados pessoais que não se faz necessário para o uso do aplicativo.

É difícil de imaginarmos, por exemplo, uma justificativa que sustente a solicitação para ter acesso à sua localização, registro de chamadas e contatos para um aplicativo de música, senão para fins pretensiosos. Pode parecer um exemplo esdrúxulo, mas os criadores e/ou gerenciadores dos aplicativos sabem tirar proveito das situações, só precisam de oportunidade ou um pouco de ignorância do seu usuário.

A ideia de conectar pessoas remotamente possibilitando o contato imediato seja ela onde estiver, foi um grande salto na comunicação da sociedade mundial. Ora, assim como um dos motivos da extinção dos Neandertais foi a sua falta de comunicação com outros grupos, os Homo Sapiens progrediram e evoluíram justamente por sua capacidade de comunicação, e novamente, mesmo que em um mundo já globalizado e alfabetizado em vários idiomas, temos um novo avanço na comunicação da raça humana.

Talvez seja esse o motivo dessas novidades chamadas redes sociais nos “cegarem”. A grandeza dos recursos oferecidos pelos sites e plataformas de aplicativos deixam em segundo plano os pontos aos quais deveríamos nos atentarmos.

De certa forma, deixamos de prestar atenção na parte burocrática, como ler o termo de consentimento e/ou políticas de privacidade do serviço oferecido, e apenas aceitamos para contemplarmos um mundo cheio de novidades ao nosso alcance. E é justamente nessa falta de atenção que podemos ser violados sem percebermos.

A proteção da privacidade do cidadão brasileiro vinha sendo defendida por legislações anteriores à vigência da LGPD, inclusive pelo Código de Defesa do Consumidor. Dito isso, teve uma decisão do judiciário que ajudou ainda mais a levantarmos questionamentos acerca do assunto de proteção de dados, em 2019, quando duas empresas grandes e influentes no mercado digital foram multadas por violação da privacidade dos dados pessoais dos brasileiros, onde, segundo Matheus (2019, online):

> O aplicativo de envelhecer rostos FaceApp, que levantou debates sobre privacidade no mês passado, rendeu uma multa milionária para a Google e a Apple no Brasil. A Fundação Procon-SP estipulou que as empresas distribuíram o app no país infringindo regras do Código de Defesa do Consumidor (CDC). A dona do Android recebeu uma penalidade de

> R$ 9.964.615,77, enquanto a empresa responsável pelo iOS tomou uma punição de R$ 7.744.320,00.
>
> Segundo explica o órgão, o motivo para a multa foi a ausência de clareza em documentos como a "Política de Privacidade" e "Termos de Uso" do aplicativo, que não estavam disponíveis em língua portuguesa. Segundo o Procon-SP, a falta de uma versão localizada dos contratos acabou deixando usuários desinformados sobre as possíveis ameaças do FaceApp.

Isso aconteceu porque o aplicativo em questão, por não ter os termos de uso e política da privacidade no idioma do português do Brasil, limitava o entendimento de boa parte dos usuários, visto que, por mais que temos a matéria de estudo do idioma inglês em nossas escolas públicas e privadas, cerca de apenas 5% dos brasileiros sabem o idioma, ainda que, dentre esses 5%, somente 1% falam fluentemente o idioma (LOURENÇO, 2022).

É calorosamente abusiva esta situação, pois o aplicativo condicionava o seu uso ao aceite de seus termos, mas sequer disponibilizava estes termos a todos os idiomas dos países em que o aplicativo alcançava, o que desencadeou esta situação aqui no Brasil.

E o aplicativo foi além, pois, ainda segundo Matheus (2019, online):

> De acordo com o Procon-SP, o FaceApp conta com passagens em seus termos de uso que permitem o compartilhamento de dados do usuário com outras empresas e para outros países. Além disso, as regras do aplicativo também possuem uma cláusula que prevê a resolução de conflitos sem auxílio judicial, mas por meio de um serviço realizado na Califórnia.

Ou seja, ao aceitar os termos de uso do aplicativo, o usuário poderia deleitar-se da ferramenta, (assim com uma grande parte de internautas estavam fazendo na época) mas suas fotos tiradas pelo aplicativos poderiam, e provavelmente, foram comercializadas com outras empresas. Já que, dificilmente esse "compartilhamento" que os termos diziam que poderia ser feito, seriam de maneira não monetizada, fazendo jus à máxima de que se o aplicativo ou programa oferecido para ti é gratuito, então o produto é você.

São fatos como este que destravam a mente de muitas pessoas sobre a importância de serem mais cautelosas quanto ao tratamento de seus dados e logo, começa a fomentar novas indagações acerca do assunto em nossas mentes.

Esta mudança cultural no modus operandi do cidadão brasileiro já está se fazendo por profissionais que estão mais próximos das áreas atingidas pela legislação como por exemplo, advogados e profissionais da Tecnologia da Informação, levando em consideração que esses, a princípio são os que mais têm noção da dimensão e do abrangimento da lei por conta da função que exercem, o profissional de TI pela segurança da informação no exercício da sua função e o advogado por trabalhar com leis.

A Lei Geral de Proteção de Dados surgiu da mesma maneira como corriqueiramente as demais leis surgiram, conciliando e ponderando direito e sociedade e até o momento, é o melhor que temos sobre proteção da privacidade levando em conta o atual cenário tecnológico que o país se encontra, e, logicamente, será aplicada cada vez mais no meio jurídico, abrindo portas para identificarmos possíveis erros, falhas, onde podemos melhorar e/ou aprimorar as normas que já temos e com isso, fazer com que o cidadão brasileiro melhore intelectual e criticamente acerca do assunto.

1.3. A inteligência Artificial

Muito se ouve falar hoje em dia em inteligência artificial. É algo que vem sendo estudado e aplicado a alguns anos, principalmente em empresas, e assim como as demais ferramentas tecnológicas, a inteligência artificial vai se aperfeiçoando cada vez mais ao passar do tempo.

A inteligência artificial trabalha aprimorando-se sozinha. Ela processa uma vastidão de dados e quando identifica algum erro, ela própria procura uma maneira de corrigi-los. É um poderio interessante para auxiliar um profissional no exercício de sua função.

Para UOL (2023, online):

> A inteligência artificial é um campo da ciência da computação que se dedica ao estudo e ao desenvolvimento de máquinas e programas computacionais capazes de reproduzir o comportamento humano na tomada de decisões e na realização de tarefas, desde as mais simples até as mais complexas. É comumente referida pela sigla IA ou AI (em inglês, artificial intelligence).

É uma maneira de agilizar tomada de decisões, com base em dados e com uma eficácia enorme em um curto período de tempo. A inteligência artificial identifica padrões e a partir deles, trabalha para ter um ótimo desempenho para a função que foi programada.

Se pensarmos em inteligência artificial como ferramenta de trabalho no mundo corporativo, temos algo similar à Revolução Industrial à cortesia dos empresários, pois eles podem deixar de investir em conhecimento e competência humana e passar a contar com o auxílio de um produto que pode lhes oferecer uma capacidade de operação de serviço muito maior e com menos probabilidade de erro.

Em relação ao uso da inteligência artificial, expressa Adriano (2022, online):

> Por isso, recursos como a Inteligência Artificial não apenas podem ser utilizados como aliados, como devem; afinal, estão previstos na própria legislação. A LGPD em seu artigo 2, inciso V, descreve como fundamento o desenvolvimento econômico e tecnológico e a inovação. Ou seja, está claro que a tecnologia não é vista como um simples bônus nesse segmento, que pode ser deixado de lado caso a gestão da marca queira. Não, o recurso é um agente fundamental na missão de trazer limites importantes para o uso abusivo dos dados pessoais.

Assim como ele diz, a tecnologia que está no mercado, além de ser uma ótima opção para usarmos nas empresas, são incentivas ao uso até mesmo pela Lei Geral de Proteção de Dados, pois por ser uma lei de 2018 ela já veio eivada de conhecimento do potencial da inteligência artificial, tanto para o malefício (motivo pelo qual a lei foi criada), quanto para o benefício.

E as empresas brasileiras estão investindo bastante no uso da inteligência artificial como instrumento de trabalho.

Segundo Varejo S.A (2022, online):

> Uma pesquisa encomendada pelo SAS revela que o Brasil está em estágio avançado na adoção de Inteligência Artificial (IA), com 63% das companhias que utilizam dados e analytics também utilizando IA, ante uma média de 47% da região.
> [...]
> Segundo o country manager do SAS no Brasil, André Novo, os dados revelam uma maturidade das empresas brasileiras em relação à transformação digital como meio de se tornarem mais competitivas, prevendo os próximos cenários e gerando novas oportunidades de negócios.

Para empresas lojistas, a possibilidade do uso da inteligência artificial para marketing digital é vasta. Se realizada da maneira correta, essas empresas continuam conseguindo usar os dados de seus clientes para criar estratégias de mercado através do cruzamento desses dados.

Ainda segundo Varejo S.A (2022, online):

> Além disso, das empresas brasileiras entrevistadas pelo estudo, 90% investem em dados e analytics com o objetivo principal de identificar tendências e padrões de consumo, percentual superior à média da América Latina, de 60%.
> "A pesquisa mostra que grande parte do mercado nacional já sabe que só conseguirá conhecer melhor seus consumidores por meio de soluções robustas de análise de dados", analisa Novo.
> Em termos técnicos, o principal driver apontado para a adoção de dados e analytics é a confiabilidade e segurança, apontada por 84% dos brasileiros, enquanto na América Latina como um todo, o percentual é menor (73%).
> E, na hora de escolher uma solução, o principal fator levado em conta é um forte sistema de suporte técnico, apontado por 56% dos entrevistados.

Há de se observar também que esse será um processo infinito e que vai somar com os demais existentes em uma empresa, pois assim como a conferência de caixa, conciliação de cartões, emissão de notas fiscais, etc., os procedimentos pertinentes ao cumprimento da Lei Geral de Proteção de Dados também será um processo que terá fiscalização. Logo, é interessante que a empresa a utilize da inteligência artificial para ajudar nesses procedimentos juntamente com profissionais bem qualificados, pois a Autoridade Nacional de Proteção de Dados pode intervir em algum processo de risco e punir a empresa por isso, aplicando severa multa se necessário for.

Ainda sobre a inteligência artificial, continua Adriano (2022, online):

> [...] a forma como uma organização prioriza e leva a sério as questões ligadas à segurança e privacidade de informações é o ponto-chave para definir a integridade das suas plataformas e sistemas.
> Muitas ferramentas usam essa tecnologia para identificar dados considerados pessoais e alertar os administradores sobre como eles são tratados, para que assim possam se adequar à LGPD. Isso ajuda os profissionais encarregados da proteção de informações a controlá-las em um universo extenso de aplicativos, dispositivos, websites, etc. Imagine só a quantidade gigantesca de acessos e dispositivos com esses materiais em empresas de grande porte; é impossível fazer a verificação e o mapeamento de todos esses conteúdos com qualidade por meio de um trabalho manual.

É factível percebemos que esses processos estão ligados a um sistema de precaução de possíveis danos que já existia antes, o processo da segurança da informação, visto que, pode ser algo que complemente ainda mais se juntar aos novos mecanismos da Lei Geral de Proteção de Dados. A própria "política da mesa limpa" agrega muito valor à lei, tendo em vista que ao deixar os documentos com dados pessoais virados para baixo na mesa, o colaborador já está fazendo a sua parte na precaução de vazamento de dados, pois todo cuidado é pouco. O mesmo pode ser aplicado a computadores com senhas para cada colaborador, evitando assim que outra pessoa acesse o computador sem a permissão do usuário. Ambas as sugestões, que aparentam servir perfeitamente

para atender aos cuidados que a Lei Geral de Proteção de Dados, bebem da fonte da segurança da informação, que já está a um bom tempo no ramo das empresas.

1.3.1. Dos algoritmos

É interessante pensarmos em parametrizações (quando se trata de processos em empresa) para diminuir o volume de processos a serem realizados para chegar ao que se destina, por exemplo, criar algum algoritmo de identificação de aceites dos clientes que deram permissão ao lojista, para fazer o uso de seus dados para cadastro, marketing, etc., e o controle dos que não deram aceites também, pois isso diminuiria muito o trabalho de fazer um controle manual, evitando ter que portar todas as folhas de consentimento com a assinatura dos clientes, ter um estoque físico e em condições adequadas para guardá-los, entre outras coisas.

Acerca do conceito de algoritmo, discorre Tallos (2022, online):

> Um algoritmo nada mais é que uma sequência de instruções ou comandos realizados de forma sistemática com a finalidade de resolver um problema ou executar uma determinada tarefa.
> Ou seja, é criado para resolver "problemas", com instruções bastante simples e exatas.
> Os algoritmos se aplicam as tarefas simples do dia a dia a programas computacionais complexos e ferramentas que identificam o comportamento do consumidor na internet.
> [..]
> É fundamental entender que o algoritmo justifica-se no resultado que ele deseja alcançar, logo, deve possuir uma meta específica. Uma sequência de instruções simples poderá tornar-se mais complexa conforme a necessidade de considerar outras situações.

E quando se fala em algoritmos e em parametrizações, o que temos como melhor ferramenta para dar aplicação a esses serviços é a inteligência artificial, que já vem sendo usado a algum tempo no mercado de aplicativos, onde se têm usuários cadastrados como o principal produto.

Sobre o uso do algoritmo aplicado em um sistema de inteligência artificial, continua Tallos (2022, online):

> Nos dias de hoje, muitas das polêmicas estão relacionadas a como as grandes empresas de tecnologia tem utilizado os algoritmos para impactar a vida das pessoas. Um ótimo exemplo e o mais famoso, é o algoritmo do Facebook, que define o que será exibido no feed de notícias de cada usuário.
> Embora seja bastante criticado, pois o algoritmo pode ser alterado para determinados fins, o recurso proporciona uma mediação mais neutra sobre o que é exibido para cada usuário.
> [...]

> Logo, um dos benefícios nos dias de hoje, é que o algoritmo busca fazer essa mediação mais equilibrada entre tudo que está disponível online e filtrá-lo para os mais relevantes a ser exibido.

Não é à toa que as propagandas que aparecem para as pessoas parecem ser as mais assertivas, pois o algoritmo consegue entender o que a pessoa gosta ou gostaria de ter e faz com que isso chegue ao usuário a todo tempo.

2. Dos casos anteriores à Lei Geral de Proteção de Dados

Muitas pessoas já se depararam com a situação de estarem realizando uma compra de medicamentos em uma farmácia e o balconista pedir o seu CPF dizendo que a finalidade dessa solicitação é meramente para dar desconto na compra, pois existem laboratórios ou programas da própria farmácia que dão descontos em compras quando é fornecido o CPF para consulta, todavia, nessa situação não havia nada além da boa-fé do balconista que nos garantissem que essa era de fato a única finalidade do tratamento desse dado.

Advém que, durante anos os dados pessoais dos cidadãos brasileiros foram tratados da maneira como as empresas que os tinham bem entendessem, e muitas vezes as empresas solicitavam os dados de seus clientes com a justificativa de cadastro no sistema ou liberação de desconto, quando a real intenção era de usá-los para marketing ou para a comercialização desses dados sem a anuência do titular. Um exemplo disso é a investigação que o Ministério Público do Distrito Federal abriu contra as farmácias, para investigar se elas estariam vendendo ou repassando dados de seus clientes a planos de saúde, antes mesmo da vigência da Lei Geral de Proteção de Dados, segundo a reportagem de Gabriel Luiz. (2018, online):

> Como o combo “CPF+desconto” é uma prática percebida em todo o país, o MP pretende enviar já na próxima semana essa lista para as dez maiores redes farmacêuticas do Brasil. Elas terão um prazo de dez dias para responder, por escrito. Por ser uma requisição oficial, não há possibilidade de negar esclarecimentos.
> Se as farmácias confirmarem que dados dos clientes estão sendo compartilhados com terceiros, o MP pretende acionar a Justiça para coibir a conduta nacionalmente, com pedido de urgência. Isso porque, ao contrário da Europa ou dos Estados Unidos, ainda não há legislação que trate do assunto.

Essas situações podem causar constrangimento e danos ao detentor dos dados, tendo em vista que regularmente o titular dos dados passa a ser bombardeado com propagandas, emails,

mensagens, ligações com oferecimentos de serviços unicamente por ter passados seus dados pessoais para complementar algum processo de cadastro em algum estabelecimento, e esse assédio é visto como uma violação da privacidade da pessoa pela Lei Geral de Proteção de Dados, podendo até mesmo, ser estendida à violação assegurada na Constituição Federal.

Outro exemplo de violação que hoje se aplicaria a Lei Geral de Proteção de Dados foi o ocorrido com o aplicativo FaceApp. Houve uma época em que os internautas começaram a postar fotos com o rosto envelhecido e caiu na graça do povo. Muitas pessoas baixaram o aplicativo FaceApp para poder ver e se imaginar como seriam suas aptidões físicas daqui alguns anos. De fato, é uma premissa interessante e divertida para os usuários de aplicativos onde se divulgam fotos. O problema é que aqui no Brasil, o termo de consentimento para o uso desse aplicativo estava totalmente em inglês, e ao aceitar os termos, os usuários autorizavam os gerenciadores do aplicativo a terem muitos acessos de dados em seus aparelhos eletrônicos.

Para Thiago (2020, online):

> Dependendo da interpretação, a política de privacidade e os termos de uso dariam à Wireless Lab, empresa russa responsável pelo app, a possibilidade de coletar alguns de seus dados, como:
>
> - As fotos que são escolhidas pelo usuário
> - A banda consumida pelo app
> - O histórico de compras
> - Informações de redes sociais (caso o login seja feito por outra plataforma) O modelo do celular
> - Resolução da tela
> - Tipo de sistema operacional
> - Alguns dados de sua navegação online, como sites que foram visitados.

Esses acessos são muito invasivos, se levarmos em conta o quão íntimo é o aparelho celular de uma pessoa e o que contém nele nos dias atuais, no momento que o usuário dava a permissão (mesmo que sem saber), os gerenciadores do aplicativos estavam “assegurados” pelo princípio do consentimento do titular, a manusearem todos esses dados cedidos, deixando assim, o usuário à mercê de qualquer possível exposição vexatória. Isso porque, ainda segundo Thiago (2020, online):

> Os termos de uso também dão à empresa uma licença livre de royalties para usar as fotos do usuário para fins publicitários, sem pedir autorização. Outra polêmica dos termos é dar à empresa a possibilidade de "processar, armazenar e transferir suas informações para outros países", sem dar mais explicações sobre isso.

Em outras palavras, o aplicativo poderia pegar as fotos que o usuário deu permissão de acesso a ele e usar para vender a empresas de publicidade para usar como marketing ou para algum outro fim, e tudo isso a qualquer momento, sem o dono do rosto da foto saber e/ou receber nada por isso.

Além disso, o aplicativo está rodeado de polêmicas e processos que o envolvem direta ou indiretamente, segundo Thiago (2020, online):

> Em agosto do ano passado, a Fundação Procon de São Paulo multou o Google e a Apple por desrespeitarem o Código de Defesa do Consumidor (CDC) ao fornecer o Faceapp.
> [...]
> O Procon havia notificado as duas empresas em busca de informações sobre como protegiam os dados dos consumidores. O órgão concluiu que elas violaram os direitos do consumidor brasileiro ao permitir que o FaceApp exibisse informações em inglês em sua "Política de Privacidade" e "Termos de Uso.

E no que diz respeito a exposições vexatórias ligadas ao aplicativo, ainda disserta Thiago (2020, online):

> O FaceApp já foi considerado racista. O aplicativo embranqueceu pessoas negras e indianas quando elas usavam um filtro que deveria "embelezá-las". Recentemente, o pesquisador Tarcízio Silva, mestre em comunicação pela UFBA (Universidade Federal da Bahia), lembrou a história em seu Twitter.
> A empresa teria alegado ao jornal The Guardian que o tal branqueamento era "um infeliz efeito colateral da rede neural subjacente causado pelo viés da base de dados para treinamento, não comportamento intencional".
> A Wireless Lab tirou o filtro do ar e pediu desculpas pelo ocorrido.

Casos como este podem acontecer com qualquer aplicativo que usamos, por isso é importante estarmos ligados aos termos de consentimento que aparecem antes do uso de qualquer ferramenta online, e se após os lermos, não estivermos de acordo, que não deixamos com que o prazer do uso do aplicativo nos faça sucumbir ao aceite de condições absurdas apenas para que possamos nos igualar aos demais internautas.

2.1. Da violação a nível global

Por mais claro que seja o risco que corremos aos termos nossos dados acessados por pessoas com más intenções, podemos nos pegar deixando toda essa parte preventiva como segundo plano e apenas seguir cedendo nossos dados para facilitar uso de ferramentas e aplicativos. Entretanto,

houve em 2016 um marco importante para podermos mensurar a grandiosidade dos dados pessoais na era da tecnologia e o quão influente isto pode ser em nossa atual sociedade.

Nas eleições dos Estados Unidos da América em 2016, uma empresa de análise de dados chamada Cambridge Analytica foi contratada pelo pessoal que estava trabalhando na candidatura de Donald Trump, até então, candidato à presidência dos Estados Unidos pelo Partido Republicano, para cuidar do marketing digital da campanha do candidato. Porém, a empresa teve acesso à dados de cidadãos americanos aos quais poderiam influenciar nos votos, e direcionaram a campanha de marketing digital fortemente em cima dessas pessoas identificadas, a modo que, para alguns, influenciou diretamente no resultado das eleições daquele ano.

Segundo a BBC (2018, online):

> O Facebook sofreu um forte abalo no último sábado com a revelação de que as informações de mais de 50 milhões de pessoas foram utilizadas sem o consentimento delas pela empresa americana Cambridge Analytica para fazer propaganda política.
> A empresa teria tido acesso ao volume de dados ao lançar um aplicativo de teste psicológico na rede social. Aqueles usuários do Facebook que participaram do teste acabaram por entregar à Cambridge Analytica não apenas suas informações, mas os dados referentes a todos os amigos do perfil.
> [...]
> A Cambridge Analytica teria comprado acesso a informações pessoais de usuários do Facebook e usado esses dados para criar um sistema que permitiu predizer e influenciar as escolhas dos eleitores nas urnas, segundo a investigação dos jornais The Guardian e The New York Times.

A matéria vai mais a fundo e nos traz a maneira como a Cambridge Analytica comprou esses dados, prossegue BBC (2018, online):

> As informações dos usuários do Facebook foram coletadas por um aplicativo chamado thisisyourdigitallife (essa é sua vida digital, em português), que pagou a centenas de milhares de usuários pequenas quantias para que eles fizessem um teste de personalidade e concordassem em ter seus dados coletados para uso acadêmico.
> Além da óbvia questão de que muitos usuários não leem os longos termos e condições e mal sabem que estão dando suas informações para os desenvolvedores desses testes, o grande problema foi que o aplicativo também coletou as informações dos amigos de Facebook das pessoas que fizeram o teste. Ou seja, se uma pessoa respondesse o quiz, estaria entregando informações privadas não apenas do seu perfil, mas de todos os seus amigos.

Aqui, nota-se como qualquer detalhe que passar despercebido pode causar um grande resultado ao final de tudo, e como as empresas oportunistas sabem tirar proveito das situações.

O aplicativo thiisyourdigitalife veio de maneira despretensiosa, com um atrativo (pagamento de uma quantia) para chamar a atenção dos internautas e perguntava a eles, perguntas “simples” e nada fora do padrão de testes que a própria plataforma do Facebook já não havia oferecido antes.

O que vale destacar é que essa estratégia deles servia para tirar a atenção dos internautas para o que de fato estava em jogo ali; o aceite do usuário para que o aplicativo pudesse usar essas informações e ainda colher informações do seu grupo de amigos na plataforma.

E de fato há uma probabilidade enorme desse desrespeito aos dados do cidadão americano ter interferido nas eleições presidenciais de 2016, já que, ainda segundo a BBC (2018, online):

> Christopher Wylie afirma que, como 270 mil pessoas fizeram o teste de personalidade, por meio do acesso à rede de amigos dessas pessoas, os dados de cerca de 50 milhões de usuários foram coletados, sem autorização. A maioria dos usuários seriam eleitores norte-americanos.
> De acordo com Wylie, os dados vendidos à Cambridge Analytica teriam sido usados para catalogar o perfil das pessoas e, então, direcionar, de forma mais personalizada, materiais pró-Trump e mensagens contrárias à adversária dele, a democrata Hillary Clinton.
> A base de dados coletada é uma ferramenta poderosa porque permite que as campanhas identifiquem pessoas que estão em dúvida e direcionem a elas mensagens com maior probabilidade de convencê-las.

Não obstante com a venda desses dados do aplicativo thisisyourdigitalife para a Cambridge Analytica, a empresa que adquiriu os dados ainda os usou sem o consentimento dos donos, isto é, nem as pessoas que responderam o questionário e nem mesmo os amigos dessas pessoas (que também tiveram seus dados coletados) sabiam desses atos irrisórios.

Não é à toa que em alguns momentos do nosso dia, nossos aparelhos celulares parecem nos ouvir, já que, em muitas situações, quando falamos sobre o interesse de comprar algo, posteriormente nos será direcionada alguma propagando relacionado ao que falamos. Essas gigantes do marketing digital trabalham justamente para isso, para fornecer aos internautas o que elas querem que eles consumam.

Devemos nos atentar ao fato de que em alguns cliques, o aplicativo ao qual os usuários responderam às perguntas, tinha acesso a aproximadamente 50 milhões de dados de civis. É gritante o quão invasivo foi ambas as entidades na privacidade dos usuários americanos para fins políticos. Pode-se considerar uma quebra colossal na privacidade deles, haja vista que tiveram acessos a dados sensíveis.

Em que pese os Estados Unidos, mesmo nos dias atuais não terem se adequado à uma legislação de proteção de dados específica, tal qual a GDPR ou mesmo a nossa LGPD, ainda sim configura invasão na vida privada da pessoa, tanto é que o CEO do Facebook, o Sr. Mark Zuckerberg teve que se explicar para as autoridades.

Ainda segundo BBC (2018, online):

> A empresa também entrou na mira de autoridades nos Estados Unidos e no Reino Unido. O deputado britânico Damian Collins convocou o CEO do Facebook, Mark Zuckerberg, para depor diante de um comitê legislativo. As autoridades também estão trabalhando para conseguir um mandado de busca e apreensão para entrar na sede da Cambridge Analytica e recolher material que ajudem a elucidar o caso.

É congruente que nesse caso as autoridades estão corretas em cobrar explicações da plataforma, tendo em vista que trata de uma responsabilidade solidária. Ora, uma plataforma que garante a segurabilidade dos dados de seu usuário não deveria ter deixado isso acontecer nessas circunstâncias, já que não estamos falando de uma invasão sofrida por eles, mas sim, de um aplicativo que entrou na plataforma atendendo às políticas e normas dela.

Assim como continua BBC (2018, online):

> Posteriormente à revelação do escândalo, alguns executivos da empresa reclamaram no Twitter do uso da palavra "vazamento" no caso envolvendo a Cambridge Analytica, já que na prática a plataforma não foi hackeada. A empresa não precisou "invadir" a rede social para ter acesso às informações – conseguiu os dados de maneira legítima e, depois, desrespeitou as regras do Facebook sobre como poderia usá-los.
> De qualquer forma, milhões de informações de pessoas que não deram seu consentimento acabaram sendo usadas para fins políticos.

Tomando este caso que repercutiu bastante na mídia mundial, dá para ter noção do quão profundo e longevo fica o assunto quando se trata de dados pessoais, ainda mais se levarmos em conta que na era da tecnologia, os algoritmos e máquinas conseguem saber e/ou determinar coisas de nossa personalidade com mais precisão que uma pessoa próxima (CONDLIFFE, 2015), estamos à mercê de um mundo virtual muito perigoso, ao qual devemos estar informados e cautelosos.

3. Do surgimento da lei

3.1. Do Direito à privacidade

É notório o grau de profundidade e importância que devemos fomentar sobre como usam nossos dados e até que ponto não estamos sendo violados com isso. Há de se observar que antes da Lei Geral de Proteção de Dados, o direito à privacidade já era resguardado em nossas legislações.

Como já dito, a privacidade está interligada com a dignidade da pessoa, logo, o princípio da dignidade possui um fortíssimo resguardo, tendo em vista que desde 1988 ele está garantido em nossa Constituição Federal, à qual descreve (Brasil, 1988):

> Art. 1º A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos:
> [...]
> III - a dignidade da pessoa humana;

Em tempos atuais, temos nossa dignidade assimilada com a nossa imagem frente ao povo, isto é, pessoas de reputações ilibadas dificilmente gostariam de serem expostas em suas redes sociais por aplicativos com permissões abusivas ou extraordinárias.

Antes da facilidade ao acesso à internet, acontecia com frequência, principalmente com pessoas famosas, a exposição ao público de momentos de intimidades aos quais não gostariam que fossem compartilhados com outros, e na sociedade atual, em um mundo onde as redes sociais são o que se pode equiparar aos antigos álbuns de fotografias, não queremos que cheguem aos olhos dos demais internautas os nossos momentos ruins ou íntimos, mas sim, nossos momentos de triunfos, escolhidos por nós.

Vivemos em um mundo de uma aparente “perfeição”, onde tudo o que postamos nas redes sociais são os momentos gloriosos, em que estamos felizes e satisfeitos.

Acerca da privacidade da vida e do peso da honra que a nossa imagem carrega, o artigo 5º da Constituição Federal os expressam de maneira mais objetiva que o inciso citado anteriormente, trazendo até a possibilidade de indenização por danos, ao qual dispõe (Brasil, 1988):

> 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:
> [...]

> 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;

Nota-se que desde 1988 o legislador já se preocupava com a inviolabilidade da privacidade do cidadão brasileiro e o amparou de acordo com o momento em que a sociedade vivia, entretanto, fez o uso de palavras abrangentes e que podem ser interpretas até mesmo em situações corriqueiras de hoje em dia.

Atualmente, com o desenvolvimento e o aprimoramento da tecnologia em nossas atividades cotidianas, surgem situações em que lei, doutrina e jurisprudência não dispuseram sobre o assunto ainda, e com isso, faz-se necessário que o Estado deixe de usar da equidade e/ou analogia com outras leis ou deliberações e que se adeque com uma lei específica que atenda a demanda da sociedade, tal qual foi com a Lei Maria da Penha, lei 11.340/06 (Brasil, 2006).

Não somente a Constituição Federal trazia em seu texto uma abordagem da privacidade do cidadão brasileiro antes da LGPD, pois temos também o texto do Código Civil de 2002 que traz em seu artigo 21 um reforço de segurabilidade à proteção da privacidade, o qual expõe (Brasil, 2002):

> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma

Era uma abordagem genérica, pois era onde fundamentávamos todos os atos que entendíamos como violação da nossa privacidade, cabendo ao magistrado, por exemplo, interpretar se compartilhamento de dados pessoais seria ou não uma violação.

E justamente diante dos fatos de violações de dados pessoais ocorridos repetidamente, que a Lei 13.709/2018 surgiu para amparar o cidadão brasileiro e preencher as lacunas deixadas pelas legislações promulgadas anteriormente, porque ela trouxe uma abordagem mais específica e atualizada para nosso regulamento jurídico.

3.2. Da GDPR

Na Europa surgiu a mesma demanda acerca de regulação da utilização dos dados pessoais das pessoas que lá residem e foram os primeiros a criarem uma lei para reger especificamente sobre

a privacidade (Regulamento 2016/679). A General Data Protection Regulation (GDPR) passou a vigorar em toda a União Europeia no dia 25 de maio de 2018 e foi uma forte inspiração e influência para a criação da nossa Lei Geral de Proteção de Dados (LGPD).

A GDPR foi um forte marco na Europa, pois os cidadãos de lá passaram a enraizar a cultura de uma aplicação de política de proteção de dados pessoais, pois para Comissão Europeia (online):

> O pacote de medidas sobre proteção de dados, adotado em maio de 2016, tem por objetivo preparar a Europa para a era digital. Mais de 90% dos europeus querem o mesmo nível de proteção dos dados pessoais em toda a UE, independentemente do lugar onde os dados são tratados.

Assim como os fatos que motivaram a criação da GDPR são semelhantes aos fatos que motivaram a LGPD, o comportamento do cidadão europeu pode refletir no comportamento dos brasileiros, e dessa forma, em alguns anos teríamos uma efetivação da aplicabilidade da lei de forma indireta, isto é, uma mudança no comportamento das pessoas sem que para isso, haja a necessidade movimentar a máquina pública impetrando diversos casos judiciais à serem resolvidos.

3.3. A origem da Lei Geral de Proteção de Dados

Assim como outras leis, a Lei Geral de Proteção de Dados bebeu de fontes externas do país para que fosse instaurada internamente. Foi a junção da necessidade da criação de uma lei que resguardasse a população na era da tecnologia com as referências europeias que findaram na Lei Geral de Proteção de Dados.

Da ficha médica feita em um hospital ou consultório, aos dados no curriculum vitae; há muito tempo, temos o fornecimento de dados pessoais como um pré-requisito para a realização de algum procedimento ou ato da vida cotidiana, afinal, não temos outra escolha, pois são eles que nos identificam.

Naturalmente, com o decorrer do tempo, empresas e organizações perceberam que poderiam aperfeiçoar suas estratégias comerciais a partir do estudo dos dados pessoais cedidos, surgindo assim, uma movimentação de valoração em dados pessoais.

Ora, se combinados, uma clínica médica poderia com facilidade oferecer para o dono de uma farmácia, os dados clínicos de clientes que necessitavam de medicamentos e cobrar por isso. E por outro lado, a farmácia em posse desses dados poderia se organizar e montar uma estratégia

com o fornecedor compras de medicamentos, negociando descontos ou compras em larga escala, haja vista que alguns medicamentos são de uso periódico e o cliente tem que usá-los durante um certo prazo.

Tais negociações não se limitam à área da saúde. Se estendermos nosso olhar um pouco mais longe, podemos perceber outras hipóteses similares, passíveis de ocorrência em áreas como a educação.

Sem a Lei, a população se sujeitava a ver bancos privados, por exemplo, compartilhando de forma indiscriminada, dados pessoais de clientes com bom histórico de pagamento, com outras empresas intencionadas a realizar venda ativa de produtos, sem a autorização ou prévio conhecimento do titular.

As situações exemplificadas revelam o descumprimento de princípios norteadores do direito brasileiro, todavia, antes da vigência da Lei Geral de Proteção de Dados, as empresas que assim agiam, não praticavam ato ilícito, especialmente se a conduta não gerasse dano direto ao titular.

Nem mesmo era entendido com ilícita a coleta excessiva de dados pessoais, ainda que desnecessários ou sem relevância suficiente para sustentar a coleta, já que era praticada culturalmente por empresas que tratavam desses dados de forma a se beneficiarem com o ato. E bons exemplos desse tipo de prática eram as farmácias condicionarem o cliente a passar seu CPF para conseguir gerar desconto em medicamento (ainda que fosse possível gerar o desconto sem o acesso ao CPF do cliente) ou as lojas de roupas que condicionavam a finalização da compra do cliente a um cadastro regado por coleta de dados desnecessários.

Contudo, o avanço exponencial da tecnologia possibilitou cada vez mais ferramentas e meios para coletar dados de pessoas em larga escala. Por conseguinte, criou-se um mercado que passou a fomentar e valorar estes dados pessoais, a ponto de surgir uma demanda social para regulamentar esses atos de coleta e processamento de informação dos dados pessoais do cidadão brasileiro.

Como forma de adequação a legislações de países mais desenvolvidos que o Brasil, cumulados com a prevenção de delitos e/ou danos sobre o assunto, sem que haja lei específica para resolvê-los, restaram na criação da Lei Geral de Proteção de Dados. E dessa maneira, o país se igualou aos países que têm legislação própria acerca do assunto e melhorou até mesmo seus acordos

comerciais, já que as empresas de países europeus passarão a realizar acordos empresariais com países que possam garantir a segurabilidade dos dados pessoais tratados entre eles.

3.3.1. Do artigo 5º da Lei Geral de Proteção de Dados

É importante salientar que a lei brasileira veio para proteger os dados e privacidades da **pessoa natural**, isto é, trata-se de um amparo legal exclusivamente da pessoa física. A pessoa jurídica só se encaixa na lei quando esta estiver relacionada com tratamento de dados de pessoas físicas, logo, o titular dos dados é a pessoa natural de direitos e que é a proprietária dos dados.

Antes de tudo, precisamos entender o que são esses dados pessoais para a lei que os protegem. E a própria lei trouxe a definição, de maneira bem organizada em seus quatro primeiros incisos do artigo 5º, são eles (Brasil. 2018):

> Art. 5º 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 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;
> 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;

É muito interessante que o inciso I tenha divido inicialmente o dado pessoal como identificado ou identificável, pois tem suas diferenças. Um dado **identificado** é algo certo e único de cada pessoa, como por exemplo, o número de CPF, número de RG, número de carteira de trabalho, número de CDI, entre outros registros dos quais necessitamos em nosso cotidiano de cidadão brasileiro. Já o dado **identificável** não é um dado direto e único como o anterior, mas sim, alguma característica que possa identificar uma pessoa, como por exemplo, cor do cabelo, se é do sexo masculino ou feminino, faixa etária de idade, etc.

O dado identificável pode parecer algo que necessite de um grande trabalho e esforço para aplicar, mas se paramos para pensar melhor, com uma simples pesquisa em algum ambiente fica fácil de identificar uma pessoa sem que para isso, necessitamos de seus dados pessoais identificados. Basta imaginarmos que fizemos uma pesquisa em uma empresa na qual foi perguntado o sexo da pessoa, se possui algum veículo, a cor do veículo e a faixa etária de idade, e

com apenas quatro informações, se cruzarmos os dados e verificarmos quem na empresa é homem ou mulher, que possui ou não carro, qual a cor do carro dessa pessoa e em qual faixa etária de idade ela está, é muito provável que possamos identificar muitas pessoas dessa empresa. Só o a pergunta respondida da pessoa ter ou não veículo já poderia identificar alguma pessoa nessa empresa.

Agora, se imaginarmos que essa simples pesquisa foi capaz de identificar muitas pessoas em uma empresa, conseguimos imaginar também que os computadores atuais, com seus algoritmos e inteligências artificiais que trabalham com esses cruzamentos de dados, podem fazer esse serviço em uma larga escala. Quanto maior a capacidade de processamento de uma máquina, mais dados pessoais ela consegue processar, administrar e identificar se preciso for.

O **dado pessoal sensível** pode ser entendido como todo dado pessoal que represente algo íntimo para o titular, como por exemplo, o histórico de compras, juntamente com o nome da pessoa em uma farmácia pode ser compreendido como dado sensível, pois pode ser que essa pessoa seja soro positivo do vírus HIV e precisa comprar medicamentos para se tratar, enquadrando nitidamente no dado referente à saúde que o artigo fala. Podemos imaginar também que uma pessoa que seja gay pode não querer que todos saibam, pois isso pode gerar desconforto a ela a depender do lugar onde ela estiver, sendo este um dado sensível referente à vida sexual dela.

Quando falamos em dados pessoais sensíveis temos que ter em mente que, se vazados, ou usados de maneira incorreta, pode acarretar em danos bem mais catastróficos do que um simples vazamento de dados pessoais identificáveis.

Um dado sensível está inteiramente ligado à intimidade do titular, logo, provavelmente é algo que o titular não quer que seja exposto. Tanto é perigoso a exposição de algo nesse sentido que existem casos de jovens que se suicidam após ter vídeos íntimos vazados pelas redes sociais.

Um exemplo desse tipo de exposição e da consequência que ela pode causar, é a matéria disponível no site da Globo, G1 (2013, online):

> A mãe da garota Júlia Rebeca, de 17 anos, encontrada morta em seu quarto após ter um vídeo íntimo compartilhado na internet, diz que a exposição das imagens da filha configuram uma “violação”. Em entrevista ao Fantástico por telefone, Ivânia Salia diz que não sabia o que estava acontecendo com a filha. “Ela não demonstrou nada, nada. Todo adolescente tem o direito de ser adolescente. Eles são inconsequentes mesmo. Essa exposição toda, do vídeo, da imagem da minha filha, é uma violação.”
> [...]
> O caso de Júlia não é único. Várias mulheres também sofreram com a intimidade exposta na internet. Normalmente, quando um vídeo como esse é disponibilizado na rede perde-se o controle.

Nota-se que a matéria é datada do ano de 2013, e se o acontecido fosse após a promulgação da Lei Geral de Proteção de Dados, o infrator não responderia somente pela violação da intimidade da vítima que está resguardada pela Constituição Federal e pelo Código Civil, como também violaria os princípios estabelecidos na Lei Geral de Proteção de Dados.

Cabe salientar que também devemos nos atentarmos ao contexto da utilização de certos dados e analisarmos a situação. Nesse caso citado, poderia acontecer de ser apenas um vídeo que não mostrasse muito do corpo das pessoas, ou que sequer fossem citados nomes, todavia, uma simples tatuagem exposta no vídeo já poderia ser um dado identificável e que também poderia ser entendido como dado sensível, já que seria uma maneira de identificar a pessoa que estava no vídeo íntimo vazado.

Como **dado anonimizado** temos os dados aos quais não são mais possíveis de identificar a pessoa, isto é, parte da própria semântica da palavra. Um dado anonimizado é aquele que é anônimo, que não se sabe qual a identificação dele, mesmo aquele que já teve uma funcionalidade, a partir do momento que deixar de ser usado como forma de identificação direta, perde a sua funcionalidade, como por exemplo, uma pessoa que teve um cadastro excluído do sistema de uma loja e quando pesquisado o seu antigo código no sistema, não aparece mais nada, ou seja, aquele código que era um dado identificável dela no sistema, já não é mais.

O **banco de dados** é onde se reúnem todos os dados que serão tratados pela pessoa que os detém. Este, em sua maioria, será por meio eletrônico, através de softwares, servidores, computadores, etc., estruturados para aturar a quantidade de informações. Mas também poderá sê-lo feito por meio físico, já que, a depender do volume de dados a serem tratados, pode ser organizado e estruturado para ser mantido em um ambiente com condições apropriadas para isso.

Após a definição do objeto principal que esta lei visa proteger, ela prossegue em suas definições, porém, agora ela nos apresenta não somente a pessoa que tem seus dados protegidos, mas também as pessoas que trabalharão com esses dados.

Elencados em seu artigo 5º, dispõe a lei (Brasil, 2018):

> Art. 5º Para os fins desta Lei, considera-se:
> [...]
> 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 privado, 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);

A lei foi muita objetiva quanto ao titular dos dados, pois não deixou margem de interpretação ao trazer que somente é titular a pessoa natural, isto é, a pessoa física e detentora de direitos e deveres, a qual já foi firmada por entendimento doutrinário a partir do art. 1º do Código Civil (BRASIL, 2002).

É considerável notarmos que as demais figuras dos incisos V, VI e VII do artigo 5º desta lei, podem ser constituídas não somente por pessoa física, mas também por pessoa jurídica, tendo em vista que nos demais polos, independente do cargo, a pessoa o exercerá para dar cumprimento aos procedimentos legais, assim dizendo, será como se fosse uma ferramenta para fazer-se cumprir o que se pede, logo, será um prestador de serviços eivado de responsabilidades, podendo, desta maneira, ser pessoa física ou jurídica assim como em prestações de serviços nos demais âmbitos civis.

O **controlador** é a pessoa física ou jurídica que toma as decisões acerca do tratamento destes dados, ou seja, é quem formaliza processos, estuda e aplica novos meios de abordagem ao cliente, etc. É quem busca ao máximo (juntamente com o encarregado de proteção de dados) diminuir riscos de impactos a vazamentos de dados ou situações constrangedoras com o titular. Em sua maioria, o controlador dos dados figura-se na pessoa do CEO da empresa, pois ele é quem detém o poder econômico para girar os produtos em sua empresa e quer que seja feita de maneira eficiente, logo, ele quem destina os fins a serem concretizados com os dados pessoais de sua clientela.

O **operador**, assim como o próprio inciso expressa, é quem aplica na prática os procedimentos que foram passados a ele, que geralmente veem do controlador. Geralmente, em empresas lojistas, figura-se na persona do vendedor, na pessoa que está diretamente ligada ao contato pessoal com o cliente. Esta pessoa tem que estar muito bem treinada e por dentro da lei, pois é a partir de algum erro dela que pode surgir situações que infringem o dispositivo legal.

É o operador quem pode fazer uma abordagem errada ou não muito clara e que pode desencadear processo contra a empresa, podendo gerar multa e pagamento de indenização por danos morais. É fácil de imaginarmos uma abordagem malfeita por um operador, pois em situações comuns de consumo, ele pode pedir o CPF de algum cliente e dizer que é apenas para verificar desconto ou simular venda, quando na verdade deveria explicar para o cliente que estes dados seriam usados pela empresa e que atendendo a nova legislação vigente no país, o cliente poderia dar o aceite para que a empresa usasse esses dados, mas que poderia a qualquer momento, solicitar a exclusão deles.

Se nessa situação, esse operador cadastrar o CPF do cliente no sistema da empresa, já é o suficiente para que esse cliente possa ser assediado, pois podem começar a surgir mensagens de ofertas dessa empresa, ligações ou emails com liberações de créditos, etc., e isso gera um desconforto enorme em quem está recebendo esse assédio.

Pode acontecer também de o cliente querer se informar sobre a legislação e o operador passar informação errada ou incompleta para o cliente, podendo assim, induzi-lo ao erro ou a dar aceites de uso de seus dados maneira precipitada. Por isso, é importante que as empresas adotem sistemas de treinamento com seus colaboradores para evitar que esse tipo de situação aconteça.

3.3.2. O Encarregado de Proteção de Dados

É necessária uma abordagem mais aprofundada no que concerne ao Encarregado de Proteção de Dados, pois temos muito o que tratar acerca deste cargo. O encarregado é o que se têm como DPO na legislação europeia, ele é encarregado pela proteção dos dados pessoais, isto é, a pessoa a quem tem a maior responsabilidade de proteger os dados que a empresa detém. É um cargo que não existia nas empresas e que teve que ser criado a partir da criação da lei, pois assim como um gerente é responsável pelos acontecimentos em sua administração, aqui, o encarregado de proteção de dados também será, só que com uma carga potencial bem maior do que os outros chefes de setores.

O encarregado é a pessoa física ou jurídica que tem o contato com os dados pessoais desde o início (primeiro contato com o cliente) até o fim a que se destinam esses dados. É ele quem deverá analisar os riscos que a empresa tem em seus procedimentos e sistemas e vai buscar amenizá-los ao máximo. Aqui, ele poderá se estruturar em procedimentos da segurança da informação para criar

os seus processos, pode usar de ferramentas disponíveis no atual mercado (como a inteligência artificial, assim como já dito) para se estruturar. Ele vai exercer uma figura análoga ao Ministério Público, só que na empresa a qual trabalha, isto é, ele será o "órgão fiscalizador" da empresa.

O encarregado pode estar periodicamente fazendo visitas às redes de lojas ou serviços a qual trabalha para verificar a abordagem, os procedimentos dos estabelecimentos no que se refere aos tratamentos dos dados pessoais. Ele pode também, criar os procedimentos (aqui pode ser juntamente com o controlador) a serem adequados a empresa e fiscalizá-los também, no que diz respeito à procedimentos de escritório.

Acerca dos fatos narrados acima, disserta Flowti (2021, online):

> Aqui estamos falando sobre as boas práticas na própria empresa. Tudo o que diz respeito ao tratamento de dados pessoais precisa ser transmitido aos colaboradores, evitando ao máximo incidentes no ambiente digital e também físico.
>
> Com certeza será um profissional de extrema importância na manutenção de um programa de adequação à LGPD e na propagação do tema na empresa. É importante que todos trabalhem em conjunto para manter a privacidade e segurança de todos os dados que circulam na empresa.

O encarregado terá também, contato com o cliente, pois em qualquer caso de dúvida ou de alguma situação esporádica, é o encarregado de proteção de dados quem deve prestar explicações ao detentor dos dados e tentar resolver a situação de maneira mais benéfica para ambas as partes, isto é, sem que o detentor dos dados precise impetrar processo na justiça para resolver a situação.

Neste sentido, discorre Flowti (2021, online):

> Na prática, sempre que houver alguma reclamação ou solicitação por parte do titular de um dado pessoal (um cliente, por exemplo), é o encarregado que a recebe e toma as providências.
>
> Exemplo: Um cidadão deseja revogar um consentimento realizado no passado.

> É o encarregado pelo tratamento dos dados pessoais que aceitará essa solicitação e tomará as providências para resolver a demanda (como, por exemplo, delegar a tarefa ao colaborador específico e se certificar que ela foi feita), prestando todos os esclarecimentos ao titular.

Apesar dessas funções, o encarregado tem ainda outra preocupação para prestar atenção, tal seja a fiscalização da Autoridade Nacional de Proteção de Dados. Ela é citada no próprio inciso VII do artigo 5º e é um órgão que foi criado para fiscalizar a eficácia da aplicação da lei em nosso território brasileiro. Ainda discorrendo sobre o assunto, continua Flowti (2021, online):

> O encarregado também será o mediador entre a empresa e o governo. Ele quem receberá os comunicados da ANPD e adotar as providências.
>
> [...]
>
> Então, na prática, o encarregado precisa ficar atento a normativas emitidas pela autoridade nacional e garantir que elas serão cumpridas pela empresa — quando essas normativas exigirem alguma ação. Caso sejam apenas informativas, ele também é o responsável por manter o empreendimento atualizado.

Um dos encargos importantes na relação do encarregado com a Autoridade Nacional de Proteção de Dados pode ser a geração e apresentação do relatório de impacto, que deve ser apresentado quando solicitado.

Este relatório se faz legal próprio artigo 5º, tal qual dispõe (Brasil, 2018):

> 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;

Por mais que a lei diga que é a documentação do controlador que contenha os processos que podem gerar riscos, na prática pode ser o encarregado quem seja responsável por fazer esse relatório, e por isso, algumas de suas ações devem estar atreladas às decisões do controlador. Aqui,

ambos devem chegar a um consenso de como serão os procedimentos adotados pela empresa e posteriormente, o encarregado deverá listá-los e apresentá-los como mapa de risco, colocando o grau de vulnerabilidade em cada um desses processos e se possível, como agir na situação de ineficácia de algum deles.

Segundo Flowti (2021, online):

> Por fim, a LGPD também atribui ao encarregado pelo tratamento de dados pessoais o recebimento de outras funções determinadas tanto pelo controlador quanto por normas complementares que surgirem.
>
> Isso significa que o encarregado é um subordinado do controlador, ou seja, ele não toma decisões de forma autônoma. Suas decisões precisam passar pela direção da empresa. Por isso, também cabe às empresas determinarem exatamente todas as atribuições do encarregado.

Vale muito ressaltar também que o encarregado de proteção de dados pode responder criminalmente por atos sobre sua gestão.

Sobre este assunto, expõem Ávila, Canterji e Azevedo (2021, online):

> Inicialmente, parece pacífico que, se o encarregado agir com dolo ou culpa grave e em razão disso causar danos (por exemplo, no caso de vazamento intencional de dados pessoais), responderá pelos danos causados perante o empregador e terceiros [2]. A culpa grave passível de responsabilização pode advir tanto de negligência, como de imprudência ou imperícia no exercício das suas atividades. Perante o titular, o controlador é civilmente responsável, mas caberá o direito de regresso contra o DPO faltoso, comprovado o dolo ou a culpa grave.
>
> É importante referir que, em linha de princípio, o DPO não responderá por ato de terceiro e sim por ato próprio, mas temos de atentar a algumas situações que poderão decorrer da interpretação das atividades que a lei lhe reserva, principalmente nos casos de omissão.

O cargo de encarregado de proteção de dados é de muita responsabilidade e necessita de uma escolha certeira da empresa para este profissional, pois além de ser perigoso um profissional não qualificado para essa função, pelo outro lado, se bem escolhido poderá somar muito com o crescimento e segurabilidade dos dados na empresa.

Segundo Varejo (2022, online):

> Hoje, 17,16% das empresas já possuem funcionários responsáveis apenas pelo DPO (Data Protection Officer) – encarregado de tratamento de dados pessoais –; e outras 8,25% contratam serviços especializados. “É um número positivo, e mostra a estruturação da proteção de dados como uma área independente”, afirmou Rony Vainzof, líder do grupo de trabalho de segurança jurídica do Fórum Empresarial LGPD.

O mercado já começou a se movimentar frente à nomeação do funcionário para o cargo de encarregado de proteção de dados, pois a LGPD já está em vigor e a Autoridade Nacional de Proteção de Dados já pode fazer fiscalização nas empresas. Se acontecer da fiscalização chegar até uma empresa que sequer tenha um DPO já nomeado, provavelmente essa empresa terá uma série de problemas na justiça.

Tanto é o grau de efetividade das empresas que já possuem esse profissional atuando, que ainda segundo a Varejo (2022, online):

> Ainda de acordo com a pesquisa, 89,18% das empresas entrevistadas não sofreram acidentes de dados da informação, e as interrupções de serviços e dados pessoais de clientes foram os principais alvos. Já possuem plano de resposta preparado para caso de incidentes 76,19% dos negócios consultados; e 57,14% das firmas possuem seguro cibernéticos.
>
> “São números importantes e a gente espera, com isso, cumprir o papel do Fórum de promover subsídios para as autoridades, conseguindo, assim, um bom encaminhamento da segurança jurídica da Lei Geral de Proteção de Dados”, finalizou Vainzof.

Pelos motivos levantados nesse tópico, é compreensível que inicialmente as empresas estão optando por escolher alguém da área de tecnologia da informação, que pode usar de seu conhecimento para estruturar a empresa no que diz respeito de programas, softwares, gadget, segurança da informação, prevenção de ataques hackers, entre outros, ou uma pessoa da área de formação do Direito, que pode agregar muito na interpretação e aplicabilidade dos procedimentos frente à lei.

3.3.3. Da Agência Nacional de Proteção de Dados

Como já citado anteriormente, temos como entidade fiscalizadora a Autoridade Nacional de Proteção de Dados. Esse é o órgão fiscalizador que os legisladores entenderam como necessário de ser criado para a verificação da eficácia da aplicabilidade da lei no território nacional.

Esta entidade pode e deve aplicar sanções contra as empresas que infringirem os textos dispostos na Lei Geral de Proteção de Dados, e essas sanções poderão ser de multas altíssimas. As sanções que a Autoridade Nacional de Proteção de Dados pode aplicar em uma empresa estão elencadas no artigo 52 da lei, tal qual dispõe (Brasil, 2018):

> 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: (Vigência)
>
> 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;
>
> VI - eliminação dos dados pessoais a que se refere a infração;
>
> VII - (VETADO);
>
> VIII - (VETADO);
>
> IX - (VETADO).
>
> 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; (Incluído pela Lei nº 13.853, de 2019)
>
> 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; (Incluído pela Lei nº 13.853, de 2019)
>
> XII - proibição parcial ou total do exercício de atividades relacionadas a tratamento de dados. (Incluído pela Lei nº 13.853, de 2019)

Aqui destacam-se algumas sanções que podem ser muito ruins ao empresário, ora, dependendo da gravidade da infração, o valor pode chegar a R$ 50.000.000,00 (cinquenta milhões de reais), o que para algumas empresas, pode ser uma perda fatal. Cabe destacar também as sanções dos incisos X, XI e XII, pois, se tratando de uma empresa que trabalha com vendas virtuais, pode

ser uma sanção ainda mais pesada que a aplicação de multa de cinquenta milhões. Ainda que somente aplicaria essa multa em um caso muito extremo ou fecharia os trabalhos frente ao tratamento de dados por mais de seis meses em casos extremos também, cumpre notar o quão sério é a lei, pois traz consigo severas punições aos infratores.

E para suprir a falta de eficácia na aplicabilidade de fiscalização, que poderia ser uma das problemáticas da lei, a lei determinou que a ANPD pode delegar suas competências e se articular com outros órgãos para garantir uma melhor aplicabilidade do cumprimento da lei. Neste sentido, discorre o Ministério da Justiça e Segurança Pública (2023, online):

> [...] A ANPD deve se articular com outras entidades e órgãos públicos a fim de garantir o cumprimento de sua missão institucional, atuando como órgão central de interpretação da LGPD e do estabelecimento de normas e diretrizes para a sua implementação.
>
> A LGPD determina, por exemplo, no art. 55-J, XXIII, que a ANPD e os órgãos e entidades públicos responsáveis pela regulação de setores específicos da atividade econômica e governamental devem coordenar suas atividades, nas correspondentes esferas de atuação, com vistas a assegurar o cumprimento de suas atribuições com maior eficiência e promover o adequado funcionamento dos setores regulados.
>
> [...]
>
> Nesse sentido, a ANPD já celebrou acordos de cooperação técnica com a Secretaria Nacional do Consumidor do Ministério da Justiça e da Segurança Pública, com o Conselho Administrativo de Defesa Econômica - CADE, com o Tribunal Superior Eleitoral – TSE, com a Agência Espanhola de Proteção de Dados e com o NIC.br.

Vale ressaltar que a ANPD pode delegar suas funções para outros órgãos e entidades, mas somente ela quem tem a competência de aplicar as sanções da Lei Geral de Proteção de Dados, evitando assim, que o Procon possa aplicar multa fundada nessa lei, por exemplo. Corroborando com o afirmado, o site do Ministério da Justiça e Segurança Pública (2023, online) continua:

> É importante observar que a aplicação das sanções previstas na LGPD compete exclusivamente à ANPD, e suas competências prevalecerão, no que se refere à proteção de dados pessoais, sobre as competências correlatas de outras entidades ou órgãos da administração pública, conforme o art. 55-K.

Já em relação às atualizações pertinentes à ANDP, houve uma aprovação na câmara recente acerca da autonomia da Autoridade Nacional de Proteção de Dados no território nacional.

Segundo Ananda (2022, online):

> Foi aprovada, no plenário da Câmara dos Deputados, a Medida Provisória (MP) que visa dar independência administrativa e financeira à Autoridade Nacional de Proteção de Dados (ANPD).
>
> A MP 1124/22, agora, precisa ser votada no Senado até o dia 24 de outubro para não perder a validade.
>
> A ANPD é o órgão federal responsável por fiscalizar e aplicar a Lei Geral da Proteção de Dados e a Lei 13.853/19 deu prazo para que o Executivo avaliasse a conveniência de transformar a ANPD em autarquia – o que foi feito pela Medida Provisória 1124/22.
>
> [...]
>
> O relator, deputado Jeronimo Goergen (PP-RS), defendeu a votação do texto original da medida provisória.
>
> "A MP representa mais um passo no fortalecimento da política de proteção de dados em nosso País, promovendo, em resumo, modificações na Autoridade Nacional de Proteção de Dados para compatibilizá-la com outros regimes regulatórios e experiências internacionais exitosas", disse. O relatório foi lido em Plenário pelo deputado Darci de Matos (PSD-SC).

Outro projeto de lei que foi movimentado recentemente na Câmara dos Deputados foi um texto que trata acerca do resguardo da segurança pública e da defesa nacional.

Dispõe Câmara dos Deputados (2022, online):

> O Projeto de Lei 1515/22 trata da aplicação da Lei Geral de Proteção de Dados Pessoais (LGPDP) para fins de segurança do Estado, de defesa nacional, de segurança pública e de investigação e repressão de infrações penais. A proposta tem o objetivo de regular artigo da LGPDP que prevê regra específica para tratamento de dados pessoais nestes casos.
>
> [...]
>
> O projeto, do deputado Coronel Armando (PL-SC), está baseado em três pilares: proteção dos direitos fundamentais de segurança, liberdade e de privacidade; eficiência da atuação dos órgãos responsáveis; e intercâmbio de dados pessoais entre autoridades competentes.
>
> Caberá à Autoridade Nacional de Proteção de Dados (ANPD), que atualmente é responsável pela aplicação da LGPDP, supervisionar a proteção dos dados pessoais nas circunstâncias previstas pelo projeto.

Outra notória e importante decisão da Câmara dos Deputados no que diz respeito à Autoridade Nacional de Proteção de Dados foi a que atribuiu à entidade a competência de autarquia.

Sobre este assunto, discorre Dispõe Câmara dos Deputados (2022, online):

> O presidente do Congresso Nacional, senador Rodrigo Pacheco, promulgou a Lei 14.460/22, que transforma a Autoridade Nacional de Proteção de Dados (ANPD) em uma autarquia.
>
> A nova lei é decorrente da Medida Provisória 1124/22, aprovada neste mês pela Câmara dos Deputados e pelo Senado Federal. O texto foi publicado na edição desta quarta-feira (26) do Diário Oficial da União.
>
> [...]
>
> O objetivo da mudança, segundo a explicação do Poder Executivo, é evitar a descontinuidade administrativa da ANPD e trazer mais confiabilidade ao sistema regulatório de proteção de dados. No novo formato, ele será compatível com outros regimes regulatórios e experiências internacionais, alega o Executivo.

Essas aprovações nos mostram que o assunto é pertinente e atual, pois não foi algo que foi criado para atender a demanda social e deixado de lado posteriormente, mas sim, uma lei que está se moldando a cada dia que se passa, de acordo com os problemas que vão surgindo na aplicação dos parâmetros legais que não poderiam ser previstos como um todo no momento da criação da lei.

3.4. Da não aplicabilidade da LGPD

É de suma importância termos também, o conhecimento de quando a lei não se aplicará ao detentor e controlador dos dados, mesmo tratando dados pessoais, pois existem possibilidades às quais não devem ser interpretadas as exigências legais e a própria Lei Geral de Proteção de Dados nos comunica essas possibilidades em seu artigo 4º.

Dispõe a LGPD (Brasil, 2018):

> Art. 4° Esta Lei não se aplica ao tratamento de dados pessoais:
> I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;
> II - realizado para fins exclusivamente:
> a) jornalístico e artísticos; ou
> b) acadêmicos, aplicando-se a esta hipótese os arts. 7° e 11 desta Lei;
> III - realizado para fins exclusivos de:
> a) segurança pública;
> b) defesa nacional;
> c) segurança do Estado; ou
> d) atividades de investigação e repressão de infrações penais; ou
> IV - provenientes de fora do território nacional e que não sejam objeto de comunicação, uso compartilhado de dados com agentes de tratamento brasileiros ou objeto de transferência internacional de dados com outro país que não o de proveniência, desde que

> o país de proveniência proporcione grau de proteção de dados pessoais adequado ao previsto nesta Lei.

Fundamentalmente, o inciso II e suas alíneas, do artigo 4º da Lei Geral de Proteção de Dados exclui a responsabilidade de quem tratará os dados para fins não lucrativos, isto é, simplesmente pelo motivo de que nesse caso, o objeto principal que fez nascer a lei não estará sendo atingido, pois para o detentor dos dados não haverá retorno financeiro. E tal objetividade faz-se necessário para que a lei não tenha artigos vagos e/ou que fiquem à mercê da interpretação de nossos magistrados, podendo dessa maneira, aplicarem sentenças a pessoas sem que estas tenham obtido algum ganho com os dados, como por exemplo, o acadêmico ou jornalista que está levantando dados para serem aplicados em pesquisas.

Fatos como este poderiam representar um cenário perigoso, pois se acontecesse de uma ou mais decisões fossem proferidas contra essas pessoas, desenlaçaria outros casos com fatos parecidos a abriria margem para jurisprudência, o que, convenhamos, tem uma boa relevância e peso em uma tese de sustentação.

É obviamente certo que, ainda que o inciso II exclua a aplicação da lei para as ocasiões descritas nas alíneas “a” e “b”, esta coleta de dados não pode ser feita sem motivo uma boa fundamentação. Não é sensato, muito menos apoiado em lei, que saiamos por aí pedindo dados de pessoas simplesmente porque queremos saber, aqui, devem ser fundamentados e se possível, que seja colhido o mínimo de dados identificáveis possíveis.

A própria legislação diz como deve ser o procedimento quando se tratar dessas ocasiões, em seu artigo 7º dispõe (Brasil, 2018):

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> [...]
>
> IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

Nessas ocasiões, presume-se que, se pensarmos na total boa-fé objetiva do acadêmico, jornalista ou artista que for precisar dos dados das pessoas, no momento da coleta dos dados que precisarão, eles irão explicar quais os fins que esses dados terão e provavelmente, se as pessoas

concordarem, os cederão. É difícil imaginarmos uma situação em que um cantor ou artista de pintura faça algum trabalho usando o dado totalmente identificável de uma pessoa sem que esta saiba (nome completo ou CPF, por exemplo), e que se sustentará somente no inciso II deste artigo 4º, pois aqui, infringe não somente a legislação de proteção dedos, mas também a intimidade da pessoa assegurada em lei constitucional.

4. Dos exemplos de aplicabilidade da Lei Geral de Proteção de Dados

Presume-se que assim como houveram mudanças na sociedade com o surgimento de novas legislações que foram benéficas aos cidadãos brasileiros no passado, seja de maneira estrita, seja de maneira erga omnes, como por exemplo, as mudanças na cultura das empresas após a promulgação da Consolidação das Leis Trabalhistas (BRASIL, 1943), ou mesmo o artigo 65 do Código de Trânsito Brasileiro (BRASIL, 1997) que passou a ser obrigatório o uso do cinto de segurança no veículo, haverá também mudanças na sociedade brasileira frente à nova legislação de proteção de dados.

À semelhança de que, o Brasil é o segundo país que mais navega na internet durante o ano (**SORTLIST,** 2022, online), estamos em um alto patamar de vulnerabilidade de possíveis violações de nossa privacidade e a partir do momento em que as pessoas passarem a tomar ciência de seus direitos resguardados e da importância que seus dados têm nos dias atuais, presume-se, por conseguinte, que terá uma mudança no comportamento do cidadão.

Após a promulgação de uma lei nova, ficamos à espera dos primeiros casos carregados com embasamentos já sobre ela, e assim como a dinâmica do mundo virtual é rápida, a aplicação da LGPD seguiu essa velocidade. Tanto é que, recentemente houve um caso que foi resolvido de maneira muito interessante, já se fundamentando em parâmetros estabelecidos na LGPD.

Uma advogada usou dos dados pessoais de uma pessoa para que pudesse identificá-la para ajudar sua cliente. Por mais que possa dividir opiniões, para o exercício da profissional, a facilidade das informações e do manuseio da tecnologia a proporcionou algo benéfico.

Segundo Nathália (2022, online):

> Em setembro do ano passado, a advogada cível e trabalhista Mylla Christie, que atua na microrregião de Ilhéus-Itabuna, na Bahia, recebeu um desafio profissional de uma cliente de 34 anos: identificar o homem com quem ela tinha se relacionado, e de quem tinha engravidado, apenas sabendo o primeiro nome dele. A mulher, que trabalha na área da

> Saúde, só tinha o WhatsApp do parceiro — e, quando contou sobre a gravidez, ele a bloqueou do aplicativo de mensagens.
> [...]
> E usou um método pouco provável para encontrá-lo: com o número do celular, conseguiu achar o Pix do homem e, nos dados da transação, o nome completo e CPF dele.

Aqui, para o exercício de sua função, a advogada teve de usar dos dados pessoais da pessoa para o legítimo interesse legal, pois ela precisava citá-lo e não encontrou outro meio senão o que foi feito nessa situação.

Outro fato posterior à promulgação da Lei Geral de Proteção de Dados foi a construtora que foi condenada a pagar indenização a um cliente, por compartilhamento indevido dos dados pessoais dele.

Segundo Valor (2020, online):

> A justiça de São Paulo determinou que a construtora Cyrela pague uma indenização de R$ 10 mil por danos morais a um cliente, em uma das primeiras decisões judiciais por infração à Lei Geral de Proteção de Dados (LGPD), que entrou em vigor no dia 18.
> [...]
> Na ação, o cliente informa que após a aquisição de um imóvel no bairro de Moema, recebeu contatos não autorizados de instituições financeiras, consórcios, empresas de arquitetura e de construção e fornecimento de mobiliário planejado.
> [...]
> A juíza Koroku cita especificamente a infração ao Artigo 2º da LGPD que "prescreve que são fundamentos da disciplina da proteção de dados, dentre outros, o respeito à privacidade, a autodeterminação informativa, a inviolabilidade da intimidade, da honra e da imagem, a defesa do consumidor, os direitos humanos, o livre desenvolvimento da personalidade e a dignidade".
> A sentença determina que a empresa não repasse ou conceda dados pessoais, financeiros ou sensíveis do cliente a terceiros, sob pena de multa de R$ 300 por contato indevido e ao pagamento de indenização de R$ 10 mil por danos morais.

Provavelmente, a aplicação de sentenças como estas implicará na cessão de compartilhamento de dados pessoais de cliente entre empresas para se beneficiarem. Haja vista que, se for condenada, pode ser que a empresa que compartilhe dados com outra tenha que indenizar a vítima em um valor muito acima do que ela receberia pelo compartilhamento com outra empresa.

Temos também, a aplicação da lei para os funcionários de empresa. Aqui não é uma abordagem de clientela, mas sim, de empregado e empregador.

Segundo a revista Consultório Jurídico (2021, online):

> A inserção do número de telefone do empregado no site da empresa, sem prova inequívoca de sua autorização, implica divulgação de dado pessoal, que afronta sua vida privada. Com esse entendimento, amparado na Constituição e na Lei Geral de Proteção de Dados (LGPD — Lei 13.709/2018), o Tribunal Regional do Trabalho da 3ª Região condenou uma empresa a indenizar em R$ 5 mil, por danos morais, uma empregada cujo número de telefone foi divulgado no sítio eletrônico da empregadora.
> A reclamante trabalhava em uma loja de chocolates, que usava o número de celular da ex-empregada como se fosse o contato oficial do estabelecimento. Em primeira instância, a indenização foi fixada em R$ 10 mil. A juíza considerou que número de telefone móvel é dado pessoal, nos termos da LGPD.

Interessante notarmos o peso que cada tipo de dado pessoal pode ter a depender da situação. Aqui, mesmo o número de telefone da colaboradora sendo um dado identificável, ou seja, era algo que a identificava de maneira indireta, foi o suficiente para restar configurada a violação de dados e foi cabível a indenização.

Um ótimo exemplo de caso punitivo ao uso de dado para fins artísticos, mas que foi feito de maneira invasiva, foi a condenação do cantor Gusttavo Lima pela justiça a ter que indenizar um idoso que possui o mesmo número de telefone citado em uma de suas músicas.

Segundo Agência O Globo (2022, online):

> A Justiça de Minas Gerais condenou, na última sexta-feira, o cantor Gusttavo Lima a pagar R$ 10 mil a um idoso, dono de um número de telefone idêntico ao citado na música 'Bloqueado'. Ele relatou à Vara Civil de Pará de Minas que as ligações são tantas que tornaram impossível a utilização do celular.
> A sentença homologada pela juíza Silmara Silva Barros entendeu tratar-se de um caso de violação de privacidade.

Porém, a música cita um número de celular mas não cita o DDD. Então houve mais de uma condenação da justiça para o cantor, pois em mais de uma vez, e em tribunais distintos, foi entendido que houve violação da privacidade dos dados pessoais.

A exemplo da outra condenação da justiça para o cantor, expõe Ane (2022, online):

> O cantor Gusttavo Lima foi condenado a pagar cerca de R$ 48 mil de indenização por danos morais a uma mulher que tem o número de telefone citado na música "Bloqueado". O músico vai recorrer da decisão em primeira instância.
> No processo, ao qual Splash teve acesso, a moradora de Pato Branco (PR) alegou que passou a receber milhares de mensagens e ligações de "uma multidão" de seguidores do artista, o que estava lhe causando "sérios prejuízos psicológicos diante da importunação de sossego vivenciada".

Vale ressaltar que o cantor não é o compositor da música, mas foi condenado pela justiça por mais de uma vez por se tratar de pessoas diferentes. Provavelmente, se mantidas as decisões em segunda instância, o cantor entrará com ação de regresso contra os compositores. Porém, o que é frutífero para nós nesse exemplo é que até mesmo as apresentações artísticas, que estão nas hipóteses de exclusão da aplicabilidade da Lei Geral de Proteção de Dados, são passíveis de violação de dados pessoais se forem feitas de modo invasivo ao titular dos dados.

Há aqueles que estão aproveitando a tecnologia para usar a seu favor. Algumas empresas estão começando a se adequar agora aos parâmetros da Lei Geral de Proteção de Dados e estão buscando as mais diversas consultorias e profissionais do mercado. Aqueles que são mais ligados à área da tecnologia da informação estão começando a juntar-se com o pessoal da área jurídica para criar e disponibilizar no mercado corporativo, consultorias e implementação de sistemas que atendam aos regimentos estabelecidos pela LGPD.

5. Da conclusão

Podemos nos perguntar se somente essa legislação é suficiente para suprir o que temos por violação de dados pessoais. Até porque, a partir dela, surgem desafios para ambos os lados, isto é, se a eficácia da lei atenderá a sociedade como forma preventiva ou punitiva (em caso de violações), e se não exigirá muito do Estado como órgão fiscalizador. Se o Estado realmente conseguirá fazer ser cumprido o que segue no texto, tanto em sua forma de fiscalização, na figura da Autoridade Nacional de Proteção de Dados, quanto na figura do poder judiciário na aplicabilidade de sanções e medidas administrativas cabíveis.

Diante de todas as problemáticas expostas, resta concluído que a Lei Geral de Proteção de Dados é extremamente necessária para atender os anseios da sociedade. Ela surgiu como um reflexo da era da informação e de suas demandas do mundo virtualizado. Sua aplicação já está sendo feita de maneira direta, como nas decisões proferidas do poder judiciário fundamentando-se nessa lei, ou mesmo nas empresas que necessitam de dados pessoais para o seu funcionamento e já estão se implementando aos parâmetros que a lei exige. Até porque, ao ter que implementar-se nos parâmetros da lei, a empresa necessita criar novos cargos, pode ter que contratar consultorias de tecnologia da informação ou consultorias jurídicas, criar novas políticas de atendimento ao cliente, novos procedimentos para o tratamento dos dados pessoais de seus próprios funcionários,

desencadeando uma série de motivos que evitarão que necessite que algo seja levado ao judiciário ou que a Autoridade Nacional de Proteção de Dados tenha que intervir.

De maneira indireta, a aplicabilidade da lei está se dando pela conscientização daqueles que estão tendo contato e conhecimento com o seu texto legal, de modo similar ao que foi feito com a conscientização do povo brasileiro após promulgado o Código de Defesa do Consumidor. Pessoas que não davam importância aos seus dados pessoais passarão à tomar mais cuidado com eles e ficarão mais atentas às situações de violações.

Segundo Sato e Camargo (2022, online):

> O 13º Seminário de Proteção à Privacidade e aos Dados Pessoais promovido pelo Comitê Gestor da Internet no Brasil (CGI.br) e pelo Núcleo de Informação e Coordenação do Ponto BR (NIC.br), ocorrido em agosto, trouxe diversas informações relevantes para os profissionais que atuam com LGPD e Proteção de Dados monitorarem e guiarem suas ações envolvendo a temática.
> [..]
> O documento aponta uma elevada preocupação dos usuários da Internet com riscos relacionados ao tratamento de seus dados pessoais, sendo que, por conta disso, 77% relataram já ter desinstalado algum aplicativo de celular; 69% deixaram de visitar um website; e 56% deixaram de utilizar algum serviço de Internet.
> Quanto às práticas mais adotadas pelos usuários de Internet para proteger seus dados pessoais, estão a verificação da segurança da página (por exemplo, mediante a verificação da existência do cadeado de segurança do navegador); a recusa de permissão de uso de deus dados para publicidade personalizada; e a leitura de políticas de privacidade.

Nota-se que a conscientização dos internautas brasileiros já está mudando quando se trata de seus dados pessoais, e provavelmente, esse número se tornará uma constante crescente. Essa mudança de comportamento é algo inerente à nossa adaptação com novos métodos, nova linguagem, novos conceitos, etc.

Quanto mais temos acesso à informação de direitos que a lei nos resguardam, mais ficamos críticos e evitamos situações de violações justamente por ter conhecimento no assunto. De maneira erga omnes, a lei tem uma eficácia de benefício social, de modo que, no momento em que as pessoas tomam conhecimento de seus direitos, elas cuidam umas das outras para evitar o constrangimento que elas não querem ter.

O tempo de vigência e aplicabilidade da Lei Geral de Proteção de Dados também deve ser levado em consideração, já que, culturalmente, precisamos vê-la surtir seus efeitos para passarmos a "acreditar" na eficácia da lei. Entretanto, se for bem veiculada nos jornais e canais de comunicação, ou até mesmo em grupos de redes sociais, bem como, se for bem acompanhada pelos

cidadãos brasileiros, isto é, se ambas as partes fizerem suas funções sociais, teremos um país com um rígido e cauteloso sistema de tratamento de dados pessoais e cidadãos bem-educados e preparados frente à era da tecnologia, que atualmente, tende ao infinito.

6. REFERÊNCIAS

ALMEIDA, Adriano. Inteligência Artificial une adequação à LGPD ao crescimento dos negócios. **Jornal Estadão Mato Grosso**, 26 out. 2022. Disponível em: < https://www.estadaomatogrosso.com.br/opiniao/inteligencia-artificial-une-adequacao-a-lgpd-ao-crescimento-dos-negocios/63223>. Acesso em: 29 out. 2022.

ARCANGELI, Cris. Redes sociais registram 4,62 bi de usuários - e vão continuar crescendo. **Exame**, 20 abr. 2022. Disponível em: <https://exame.com/colunistas/empreender-liberta/redes-sociais-registram-462-bi-de-usuarios-e-vao-continuar-crescendo/ >. Acesso em: 23 out. 2022

ÁVILA, Ana Paula, AZEVEDO, Rodrigo, CANTERJI, Rafael Braude. Os riscos e as responsabilidades do encarregado de dados. **Consultório Jurídico**, 19 dez. 2021. Disponível em: <https://www.conjur.com.br/2021-dez-19/opiniao-riscos-responsabilidades-encarregado-dados#:~:text=Em%20tal%20hip%C3%B3tese%2C%20o%20DPO,a%C3%A7%C3%A3o%20%C3%A9%20mais%20facilmente%20compreendida.> Acesso em: 30 out. 2022.

A proteção de dados na EU. **Comissão Europeia**, s/d. Disponível em: < https://ec.europa.eu/info/law/law-topic/data-protection/data-protection-eu_pt>. Acesso em: 02 nov. 2022.

BBC. Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades. **G1**, 20 mar. 2018. Disponível em: < https://g1.globo.com/economia/tecnologia/noticia/entenda-o-escandalo-de-uso-politico-de-dados-que-derrubou-valor-do-facebook-e-o-colocou-na-mira-de-autoridades.ghtml>. Acesso em: 25 out. 2022.

BRASIL. [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988**. Brasília, DF: Presidente da República, 2016. Disponível em: <http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm>. Acesso em: 17 jun. 2022.

BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Rio de Janeiro, RJ: Presidente da República, 1943. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm#:~:text=Rio%20de%20Janeiro%2C%201%20de,Independ%C3%AAncia%20e%2055%C2%BA%20da%20Rep%C3%BAblica.>. Acesso em: 03 out. 2022.

BRASIL é o país mais avançado da América Latina no uso de inteligência artificial. **Varejo S.A**, 1 nov. 2022. Disponível em: <https://cndl.org.br/varejosa/brasil-e-o-pais-mais-avancado-da-america-latina-no-uso-de-inteligencia-artificial/>. Acesso em: 02 nov. 2022.

BRASIL. Lei nº 9.503, de 23 de setembro de 1997. Institui o Código de Trânsito Brasileiro. Brasília, DF: Presidente da República, 1997. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l9503compilado.htm>. Acesso em: 30 out. 2022.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil. Diário Oficial da União: seção 1, Brasília, DF, Presidente da República, 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm>. Acesso em: 30 out. 2022.

BRASIL. Lei nº 11.340, de 7 de agosto de 2006. Cria mecanismos para coibir a violência doméstica e familiar contra a mulher. Brasília, DF: Palácio do Planalto, 2006. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2004-2006/2006/lei/l11340.htm>. Acesso em: 17 jun. 2022.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidente da República, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm>. Acesso em: 17 jun. 2022.

CAMARGO, Adriana, SATO, Luisa. Números da Proteção de Dados crescem no país após 4 anos de LGPD. **Olhar Digital**, 21 out. 2022. Disponível em: <

https://olhardigital.com.br/2022/09/21/colunistas/numeros-protecao-de-dados-crescem-apos-4-anos-de-lgpd/>. Acesso em: 03 nov. 2022.

CONDLIFFE, Jamie. Seu computador entende a sua personalidade melhor que seus amigos. **Giz_br**, 13 jan. 2015. Disponível em: <https://gizmodo.uol.com.br/computador-entende-personalidade/>. Acesso em: 25 out. 2022.

EMPRESA divulga celular de empregada em seu site e é condenada com base na LGPD. **Consultório Jurídico**, 26 dez. 2021. Disponível em: <https://www.conjur.com.br/2021-dez-26/empresa-divulga-celular-empregada-condenada-base-lgpd>. Acesso em: 02 nov. 2022.

EMPRESAS brasileiras ainda estão se adequando à LGPD. **Varejo S.A**, 31 jan. 2022. Disponível em: <https://cndl.org.br/varejosa/empresas-brasileiras-ainda-estao-se-adequando-a-lgpd/>. Acesso em: 02 nov. 2022.

G1. Mãe de jovem achada morta após vídeo íntimo reclama de ‘violação’. **G1**, 18 nov. 2013. Disponível em: <https://g1.globo.com/pi/piaui/noticia/2013/11/mae-de-jovem-achada-morta-apos-video-intimo-reclama-de-violacao.html>. Acesso em: 01 nov. 2022.

GERALDO, Nathália. 'Pixbaby': advogada usa dado do Pix de pai e resolve caso de paternidade. **Universa UOL,** São Paulo, 15 jun. 2022. Disponível em: <https://www.uol.com.br/universa/noticias/redacao/2022/06/15/como-advogada-usou-dado-do-pix-em-solucao-de-caso-de-paternidade-pixbaby.htm>. Acesso em: 17 jun. 2022.

GIL, Antonio Carlos. **Métodos e técnicas de pesquisa social**. 6. ed. - São Paulo: Atlas, 2008.

KLEINA, Nilton. A história da Internet: a década de 1990 [infográfico]. **Tecmundo**, 12 mai. 2011. Disponível em: <https://www.tecmundo.com.br/infografico/10054-a-historia-da-internet-a-decada-de-1990-infografico-.htm>. Acesso em: 23 out. 2022.

INTELIGÊNCIA artificial. **UOL**, 2023. Disponível em: <https://brasilescola.uol.com.br/informatica/inteligencia-artificial.htm>. Acesso em: 30 mai. 2023.

LGPD: qual é a função do encarregado pelo tratamento de dados pessoais?. **Flowti**, 2021. Disponível em: <https://flowti.com.br/blog/lgpd-qual-e-a-funcao-do-encarregado-pelo-tratamento-de-dados-pessoais>. Acesso em: 30 mai. 2023.

LOURENÇO, Aline. Apenas 5% da população brasileira fala inglês, aponta pesquisa. **Segs**, 31 mai. 2022. Disponível em: <https://www.segs.com.br/educacao/347834-apenas-5-da-populacao-brasileira-fala-ingles-aponta-pesquisa>. Acesso em: 30 out. 2022.

LUIZ, Gabriel. CPF em troca de desconto: MP investiga venda de dados de clientes por farmácias. **g1.** Disponível em: https://g1.globo.com/df/distrito-federal/noticia/cpf-em-troca-de-desconto-mp-investiga-venda-de-dados-de-clientes-por-farmacias.ghtml. Acesso em: 22 abr. 2022.

MOGNON, Matheus. Google e Apple tomam multa milionária no Brasil por causa do FaceApp. **Tecmundo,** 02 set. 2019. Disponível em: https://www.tecmundo.com.br/software/145468-google-apple-tomam-multa-milionaria-brasil-causa-faceapp.htm. Aceso em: 17 jun. 2022.

MOURA, Kátia de Jesus Zamboni. Qual foi a primeira rede social da história da Internet?. **Techtudo**, 30 jul. 2022. Disponível em: < https://www.techtudo.com.br/noticias/2022/07/qual-foi-a-primeira-rede-social-da-historia-da-internet.ghtml>. Acesso em: 20 out. 2022.

O GLOBO, Agência. Gusttavo Lima é condenado a indenizar idoso por número de celular divulgado na música 'Bloqueado'. **Folha de Pernambuco**, 18 out. 2022. Disponível em: < https://www.folhape.com.br/cultura/gusttavo-lima-e-condenado-a-indenizar-idoso-por-numero-de-celular/243884/>. Acesso em: 03 nov. 2022.

ONLINE, Valor. Cyrela é multada em R$ 10 mil por infração à Lei Geral de Proteção de Dados. **G1**, 30 set. 2020. Disponível em: < https://g1.globo.com/economia/noticia/2020/09/30/cyrela-e-multada-em-r-10-mil-por-infracao-a-lei-geral-de-protecao-de-dados.ghtml>. Acesso em: 02 nov. 2022.

O que é o algoritmo e como ele funciona. **TALLOSblog**, 4 mar. 2022. Disponível em: < https://tallos.com.br/blog/o-que-e-algoritmo-e-como-ele-funciona/#:~:text=Um%20algoritmo%20nada%20mais%20%C3%A9,instru%C3%A7%C3%B5es%20bastante%20simples%20e%20exatas.>. Acesso em: 02 nov. 2022.

PERGUNTAS Frequentes – ANPD. **Ministério da Justiça e Segurança Pública**, 2023. Disponível em: <https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#:~:text=Sim.,diretrizes%20para%20a%20sua%20implementa%C3%A7%C3%A3o.>. Acesso em 30 mai. 2023.

PROJETO altera Lei de Proteção de Dados para resguardar segurança pública e defesa nacional. **Câmara dos Deputados**, 12 ago. 2022. Disponível em: < https://www.camara.leg.br/noticias/893704-projeto-altera-lei-de-protecao-de-dados-para-resguardar-seguranca-publica-e-defesa-nacional/>. Acesso em: 02 nov. 2022.

PROMULGADA lei que transforma Autoridade Nacional de Proteção de Dados em autarquia. **Câmara dos Deputados**, 26 out. 2022. Disponível em: < https://www.camara.leg.br/noticias/915858-promulgada-lei-que-transforma-autoridade-nacional-de-protecao-de-dados-em-autarquia/>. Acesso em: 03 nov. 2022.

REIS, Kleber Vinícius de Abreu. PETRÓLEO DO SÉCULO XXI: DADOS E SUA RIQUEZA INESGOTÁVEL. **Boxnet,** 2021. Disponível em: https://www.boxnet.com.br/insights-tecnologia/petroleo-do-seculo-xxi-dados-e-sua-riqueza-inesgotavel/#:~:text=Ainda%20em%202006%2C%20o%20matem%C3%A1tico,Dados%20s%C3%A3o%20o%20novo%20petr%C3%B3leo%E2%80%9D. Acesso em: 22 abr. 2022.

SANTOS, Ananda. ANPD: Câmara aprova MP que dá autonomia ao órgão de fiscalização da LGPD. **Contábeis**, 15 out. 2022. Disponível em: < https://www.contabeis.com.br/noticias/53343/anpd-camara-aprova-mp-que-da-autonomia-ao-orgao-de-fiscalizacao-da-lgpd/>. Acesso em: 02 nov. 2022.

SLYNCHUCK, Andriy. Big brother brands report: which companies might access our personal data the most?. **Clario**, 2021. Disponível em: https://clario.co/blog/which-company-uses-most-data/. Acesso em: 22 abr. 2022.

TIKTOK e YouTube são as plataformas que mais coletam dados dos usuários. **Tudocelular.com**, 10 fev. 2022. Disponível em: < https://www.tudocelular.com/seguranca/noticias/n186054/tiktok-e-youtube-sao-as-plataformas-que-mais-coletam-dados-de-usuarios.html#:~:text=TikTok%20e%20YouTube%20s%C3%A3o%20as%20plataformas%20que%20mais%20coletam%20dados%20dos%20usu%C3%A1rios,-10%20de%20fevereiro>. Acesso em: 23 out. 2022.

UNIÃO EUROPEIA. Regulamento (EU) 2016/679. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais. União Europeia, 2016. Disponível em: https://www.sg.pcm.gov.pt/media/38093/rgpd_regulamento.pdf. Acesso em: 18 jun. 2022.

USO de internet, televisão e celular no Brasil. **IBGE Educa**, 2019. Disponível em: < https://educa.ibge.gov.br/jovens/materias-especiais/20787-uso-de-internet-televisao-e-celular-no-brasil.html#:~:text=Em%204%2C7%25%20das%20resid%C3%AAncias,m%C3%B3vel%20celular%20para%20uso%20pessoal.> Acesso em: 03 nov. 2022.

VARELLA, Thiago. FaceApp rouba os meus dados? Veja 6 coisas que você devia saber sobre ele. **Tiltuol**, 15 jun. 2020. Disponível em: < https://www.uol.com.br/tilt/noticias/redacao/2020/06/15/faceapp-rouba-os-meus-dados-seis-coisas-que-voce-devia-saber-sobre-ele.htm>. Acesso em: 01 nov. 2022.

URL Genius/Reprodução. **Gráfico de resultado da pesquisa dos aplicativos que mais rastreiam dados pessoais.** Disponível em: < https://www.tudocelular.com/seguranca/noticias/n186054/tiktok-e-youtube-sao-as-plataformas-que-mais-coletam-dados-de-usuarios.html#:~:text=TikTok%20e%20YouTube%20s%C3%A3o%20as%20plataformas%20que%20mais%20coletam%20dados%20dos%20usu%C3%A1rios,-10%20de%20fevereiro>. Acesso em: 23 out. 2022.

YOUR Digital Year Which countries spend the most time on their screens?. **Sortlist**, 2021. Disponível em: https://www.sortlist.com/blog/your-digital-year/. Acesso em: 15 jun. 2022.