A PROTEÇÃO DA PRIVACIDADE PELA LEI GERAL DE PROTEÇÃO DE DADOS (LGPD) NA ERA DA INTERNET DAS COISAS (IOT) | *PRIVACY PROTECTION UNDER THE GENERAL DATA PROTECTION LAW (LGPD) IN THE ERA OF THE INTERNET OF THINGS (IOT)*

DIEGO BIANCHI DE OLIVEIRA
GUSTAVO CONSALTER MIEREZ VEGA

RESUMO | Este artigo explora a evolução da Internet até a ascensão da Internet das Coisas (IoT), destacando seu impacto na coleta e tratamento de dados pessoais e sensíveis. A disseminação dessas informações levantou preocupações sobre seu uso por empresas e indivíduos para influenciar hábitos de consumo e opiniões públicas. Em resposta, a Lei Geral de Proteção de Dados (LGPD) foi promulgada em 2018 para regular a coleta e tratamento de dados no Brasil. Contudo, a implementação da LGPD suscita questões sobre sua eficácia, concluindo que, embora represente um avanço significativo, sua eficácia social depende da colaboração entre governos, empresas e sociedade civil.

PALAVRAS-CHAVE | Dados Pessoais; Dados Sensíveis; Direitos Fundamentais; Tecnologia; Vulnerabilidade.

ABSTRACT | *This article explores the evolution of the Internet leading up to the emergence of the Internet of Things (IoT), emphasizing its impact on the collection and processing of personal and sensitive data. The dissemination of this information has raised concerns about its use by companies and individuals to influence consumer habits and public opinions. In response, the General Data Protection Law (LGPD) was enacted in 2018 to regulate the collection and processing of data in Brazil. However, the implementation of the LGPD raises questions about its effectiveness, leading to the conclusion that, while it represents a significant advancement, its social effectiveness depends on collaboration among governments, businesses, and civil society.*

KEYWORDS | Personal Data; Sensitive Data; Fundamental Rights; Technology; Vulnerability.

1. INTRODUÇÃO

A Internet cresceu, e ainda cresce, extraordinariamente tornando-se uma ferramenta de alcance mundial que conecta homens e máquinas. Apesar dos diversos benefícios alcançados por meio dessa tecnologia, também trouxe à luz questões elementares como, por exemplo, a privacidade dos dados de usuários da rede.

O surgimento da Internet das Coisas (IoT, do inglês Internet of Things) revolucionou a maneira como os indivíduos interagem com os dispositivos e como os dados gerados por essa interação são geridos. Em termos gerais, a IoT refere-se a dispositivos que podem se conectar à internet e interagir tanto com os usuários quanto entre si. Esses dispositivos variam desde os mais simples, como aqueles utilizados em casas inteligentes, até sistemas industriais complexos que podem identificar falhas em linhas de produção antes que sejam detectadas por operadores humanos. Com a crescente presença da interconectividade em nosso cotidiano e a diversidade de dispositivos envolvidos, surgem preocupações quanto aos limites da privacidade e à possível invasão dos dados dos usuários.

Sendo assim, a proteção da privacidade vem à tona como uma preocupação basilar. A privacidade diz respeito a manter os dados pessoais e sensíveis seguros, bem como garantir autonomia e dignidade dos usuários em um mundo cada vez mais virtual. Nessa seara, o Direito tem papel essencial em defesa da proteção dos dados de usuários da internet e das IoT.

A Constituição Federal de 1988, bem como o Código Civil, já previam algumas medidas em relação a preservação da intimidade e privacidade dos cidadãos, mas é apenas em 2018 que a Lei Geral de Proteção de Dados (LGPD) é aprovada. A LGPD inaugura uma nova era na manipulação de dados de usuários da rede pois determina todos os processos que os controladores, ou seja, quem coleta esses dados, devem seguir para garantir a proteção das informações colhidas.

O escândalo envolvendo o *Facebook* e a *Cambridge Analytica* é um lembrete categórico a respeito dos riscos que os usuários enfrentam ao fornecer seus dados indiscriminadamente. A esse respeito, os dados abrangem um leque maior e não dizem respeito apenas a nome, endereço e documentos pessoais, mas também se referem à pegada digital deixada em redes sociais, por exemplo. As informações coletadas por controladores podem ser utilizadas para manipular a opinião pública em relação a situações de suma importância, como pleitos eleitorais. Esse episódio acendeu um alerta mundial a respeito do tratamento de dados e impulsionou a aprovação da LGPD no Brasil.

Demonstra-se neste artigo a abrangência das IoT, bem como seus usos no mundo atual. Da mesma maneira, aponta-se como os dados sensíveis e pessoais de usuários são tratados para diversos fins, desde atividades voltadas ao *marketing* de produtos até na manipulação da opinião pública.

Diante desse cenário, analisam-se a origem da LGPD e os mecanismos que a Lei disponibiliza para preservar a intimidade e a privacidade dos usuários em um mundo cada vez mais digital. Objetiva-se verificar, através do método dedutivo, se tais mecanismos fornecidos pela referida lei mostram-se suficientes para a proteção dos dados dos usuários frente a esse novo cenário.

2. SURGIMENTO DA INTERNET DAS COISAS (IOT) E VULNERABILIDADE DOS DADOS PESSOAIS

A Internet originou-se durante a Guerra Fria, confronto político ideológico protagonizado pelos Estados Unidos e a União Soviética entre os anos de 1947 a 1989. O Exército estadunidense investigava uma maneira de compartilhar dados e informações entre as bases militares de maneira rápida e segura, sem a necessidade de estar conectada a uma base central. Dessa maneira, caso um bombardeio atingisse uma das bases, os documentos não seriam perdidos já que essas informações estavam armazenadas também em outros pontos. Assim nasceu a ARPAnet (ARPA: *Advanced Research Projects*

Agency), um projeto de rede que interligava quatro pontos: UCLA – *University of Califórnia at Los Angeles*; SRI – *Stanford Research Institute*; UC Santa Bárbara e a Universidade de Utah. A nomenclatura internet surgiria apenas em 1981, quando cientistas e acadêmicos começaram a utilizar a tecnologia, sendo que em 1987 a rede difundiu-se também no âmbito comercial (Matos, 2005).

Nesse momento, a internet limitava-se não apenas a um grupo social específico, mas também era difícil de acessar. Ao ligar o computador, por exemplo, que era um equipamento robusto, o operador tinha acesso a uma tela preta cheia de códigos, sem imagens ou sons. A interface e o design não eram atrativos e limitavam muito o entendimento da tecnologia bem como as informações que podiam ser compartilhadas.

A Internet, atualmente, pode ser definida como uma rede global capaz de conectar computadores possibilitando a comunicação entre pontos diferentes bem como a troca de informações rapidamente e de forma nunca antes vista na história (Matos, 2005). O impacto gerado na comunicação entre indivíduos, propiciado pela Internet, é tão expressivo que novas formas de se relacionar foram estabelecidas gerando novos paradigmas e questões, entre elas, a privacidade.

Atualmente a Internet ainda cumpre o papel para o qual foi idealizada, mas ultrapassa em muitos aspectos seu objetivo inicial. A troca de informações na rede mundial de computadores ainda acontece, mas através dela também é possível acessar vídeos, sons e imagens, bem como realizar venda e compra de diversos tipos de produtos e serviços, controlar finanças pelo acesso a contas bancárias entre outros (Matos, 2005). Em termos históricos, conforme pontua Patrícia Peck Pinheiro (2016), advogada especialista em Direito Digital, a Internet evoluiu para o atual estágio muito rapidamente, algo positivo em termos tecnológicos, mas também perigoso, já que as consequências dessa transformação ainda estão sendo compreendidas e amadurecidas. Considerando os problemas causados por essa transformação tecnológica protagonizada pela Internet, o Direito desempenha papel importante ao lidar com questões como a privacidade, por exemplo.

A Internet é mais que um simples meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de Indivíduos. Indivíduos com letra maiúscula, porque estão inseridos em um conceito mais amplo, que abrange uma individualização não só de pessoas físicas como também de empresas, instituições e governos (Pinheiro, 2016. p. 47).

A preocupação com a privacidade de pessoas físicas, empresas, governos e demais agentes que utilizam a internet como uma ferramenta diária independente da finalidade é basilar. Atualmente, a web não opera apenas através de computadores, mas também através de uma infinidade de dispositivos, situação que gerou até mesmo um novo nome: Internet das Coisas (Matos, 2005). A amálgama entre os setores industrial computacional, das telecomunicações e a ciência da computação transformou a IoT em uma realidade capaz de conectar pessoas às máquinas, assim como intercambiar a comunicação entre objetos (Paz et al., 2023).

O primeiro dispositivo IoT foi criado por John Romkey e apresentado na INTEROP ‘89 *Conference*, em 1990. Romkey criou uma torradeira que podia ser ligada e desligada pela Internet através da conexão entre a torradeira e um computador com rede TCP/IP. Entretanto, a nomenclatura IoT só seria cunhada em 1999 por Kevin Ashton, cofundador e diretor executivo do Auto - ID *Center*. Durante sua palestra no Procter & Gamble, Ashton demonstrou a ideia de utilizar etiquetas eletrônicas em produtos a fim de facilitar a logística da cadeia de produção que encontraria o produto desejado por meio de identificadores e radiofrequência (Matos, 2005).

Na literatura, é possível encontrar algumas definições, e discordâncias, a respeito do conceito de internet das coisas. Para Minerva et al. (2015, p. 19) a IoT é uma infraestrutura global que viabiliza a conexão física e virtual de objetos enquanto Faccioni Filho (2016, p. 32) entende que a IoT não é uma tecnologia em si e sim um conceito que “abrange várias plataformas, tecnologias e modelos de negócio”. De acordo com Atzori (et al., 2010) a IoT na atualidade pode ser definida como uma variedade de coisas ou objetos como celulares e sensores que interagem e cooperam entre si compartilhando

informações e executando comandos. A conexão entre as IoT precisa convergir em três pontos: middleware, ou seja, orientado para a internet; orientado para as coisas através de sensores e atuadores; e a capacidade de representar e armazenar as informações adquiridas e trocadas entre dispositivos. Eduardo Magrani (2018, p. 20), por outro lado, argumenta que apesar das divergências em relação ao conceito, as definições apontam para um ecossistema de "objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente".

A aplicabilidade da Internet das Coisas é imensa e abrange desde o ambiente doméstico até setores complexos como indústrias e agricultura. No quadro abaixo, é possível visualizar algumas das aplicabilidades das IoT:

Tabela 1 – Aplicações das IoT

Smartphones, gadgets para automatização de casas (*smarthouse*) como fechaduras automáticas e geladeiras conectadas a internet que informa falta de mantimentos e faz lista de compras, câmeras Wi-fI, *smart speaker*, tomada inteligente, interruptor *smart*, *smart-car*, *smartTV* e *wearables* (acessórios de vestuário como relógios e óculos conectados à internet).	Produtos *Smart*
Transporte Inteligente Aplicativos de monitoramento de tráfego e GPS como *Waze* e *Moovit*, por exemplo, e sinais de desvio ou avisos em estradas.	Transporte Inteligente
Logística *Smart* *E-commerce*, tecnologias de rastreamento e gerenciamento de estoque.	Logística *Smart*
Indústria Segurança de processos como controle de qualidade e monitoramento de erros e/ou defeitos de produção.	Indústria
Monitoramento ambiental (sensores para medir temperatura e umidade, por exemplo), segurança e rastreabilidade de produtos.	Agricultura de Precisão
Monitoramento por vídeo, gerenciamento de controle de incêndio.	Segurança
Detecção de níveis de lixo em pontos de descarte e otimização da rota de coleta.	Gestão de resíduos

Fonte: Baseada em CHICARINO, Vanessa R. L; ROCHA, Antonio (2017)

A IoT possibilita a redução na taxa de erros operacionais relacionados a distração ou esquecimento, por exemplo, apesar de ser impossível eliminar a

probabilidade de erros em 100%. A grande questão é que, apesar da drástica diminuição na proporção de equívocos, quando eles ocorrem a tendência é que o impacto seja muito grande. Um exemplo prático e didático é pensar na fabricação de turbinas de avião da *Rolls Royce*, uma marca conceituada no mercado, que possui uma tecnologia que permite monitorar em tempo real se todas as turbinas fabricadas pela empresa estão funcionando ou não e em que parte do globo terrestre elas estão. Em uma situação hipotética, imagine que um hacker consegue invadir esse sistema e desligar todas as turbinas em funcionamento. Um acidente catastrófico aconteceria (Camargo; Kadow, 2016).

> Enquanto elas removem os fatores humanos das tomadas de decisões como julgamentos errados, ela introduz um novo problema que é trocar acidentes menores por outros em maior escala. É o chamado paradoxo da automação. Enquanto as chances de acidentes diminuem, as consequências aumentam exponencialmente (Camargo; Kadow, 2016, p. 156).

Outro problema, dessa vez mais prático e palpável, é a perda da privacidade diante da IoT. Os dispositivos conectados à internet são capazes captar diversos dados das mais variadas naturezas e ser usados pelas empresas donas desses dispositivos para fins específicos (Camargo; Kadow, 2016). Nesse ponto é importante esclarecer a diferença de dado e informação: dados são números, estatísticas e gráficos que, após analisados e processados, transformam-se em informações, essas sim capazes de demonstrar os hábitos e interesses de um grupo ou até mesmo o perfil de pessoas específicas. Os dados, por sua vez, se dividem em dados pessoais, sensíveis e anônimos. Conforme a própria Lei de Proteção de Dados, LGPD, que será abordada nesse trabalho, explica: dados pessoais são aqueles capazes de identificar uma pessoa como, por exemplo, número de documentos, nome completo e endereço; dados sensíveis são aqueles relacionados a posicionamento político e ideológico, religião, sexualidade e até mesmo informações relacionadas à saúde; o último, dados anônimos, são informações onde a identidade é protegida e portanto não estão sujeitos a tutela jurídica (Oliveira, 2017; Brasil, 2018). Assim, os dados sensíveis, como o

nome sugere, são aqueles que necessitam de maior proteção devido a seu conteúdo passível de exposição de identidade e a possibilidade aumentada de ofender os direitos fundamentais caso sua privacidade seja desrespeitada. A coleta e armazenagem desses dados, que pode se apresentar em diversos formatos como texto, imagens e sons, constitui os bancos de dados que nada mais é do que um registro eletrônico, um grande arquivo que armazena e organiza, conforme a necessidade de quem o detém, os dados recolhidos, transformando, a partir disso, os dados em informações (Sobrinho, 2019; Oliveira, 2018).

A todo momento as pessoas inserem conteúdos a respeito de seu dia a dia em canais digitais gerando uma quantidade gigantesca de dados. Entre eles os dados sensíveis ou pessoais caracterizados por toda e qualquer informação capaz de identificar ou tornar alguém identificável como, por exemplo, nome completo, número de documentos, endereço, foto entre outros. Essas informações são armazenadas em servidores dos respectivos sites ou aplicativos que as coletaram.

A capacidade de coleta de dados na Internet, principalmente no contexto das IoT, é ampliada infinitamente requerendo, portanto, a necessidade de políticas e ações rígidas e assertivas no que diz respeito à proteção das informações coletadas. Além disso, os usuários necessitam compreender como o funcionamento de dispositivos conectados à internet pode impactar negativamente seu dia a dia, objetivo que por vezes não é alcançado (Paz et al., 2023).

Para exemplificar essa situação imagine a interação humano máquina que um dispositivo de imersão como o *Kinect*, *gadget* do videogame *Xbox One* da Microsoft é capaz de provocar (Camargo; Kadow, 2016). O *Kinect* é um dispositivo que quando conectado ao videogame escaneia o jogador e todo o ambiente em que ele se encontra para criar um avatar do *player* e permitir que o mesmo controle as funções do jogo através de movimentos. Basicamente o *Kinect* substitui o *joystick*, ou controle, entregando todos os comandos, literalmente, na mão do jogador. Esse dispositivo consegue realizar essa tarefa através de uma série de sensores como câmeras e microfones. Isso significa

que o *Kinect* é capaz de coletar dados menos complexos como sexo, altura e idade, além de prever os padrões de consumo com base no ambiente em que o jogador está inserido bem como o seu padrão de vestimenta. Através da coleta desses dados, as empresas fabricantes mapeiam seus consumidores constante e profundamente a fim de manipular seus desejos de consumo e assim vender mais produtos.

Outra aplicabilidade desse tipo de tecnologia é a espionagem para fins governamentais. A preocupação com essa situação é tão real que a *Microsoft*, empresa responsável pelo *Kinect*, expressou-se publicamente, em 2013, e garantiu que não compartilha os dados coletados através de seus dispositivos com nenhuma outra empresa ou com o governo estadunidense (Camargo; Kadow, 2016).

Diante da operabilidade das IoT, uma questão importante é levantada: o Direito e a proteção à privacidade dos usuários. Os *Personally Identifiable Information,* ou PII, são dados coletados pelas IoT capazes de traçar um perfil preciso sobre seus usuários informando características como peso, idade e sexo, por exemplo (Matos, 2005). De acordo com Matos (2005) as PII são tão importantes que analistas de mercado têm utilizado a quantidade de informações sobre clientes armazenadas por umas empresas como determinante de seu valor de mercado, ou seja, quanto mais PII, mais caro as ações na Bolsa de Valores. A obtenção dessas informações permite com que os investimentos sejam direcionados diminuindo o risco de perda e aumentando a taxa de sucesso das vendas, além de prever quais produtos seriam atrativos para o consumidor. Assim, quanto maior o volume e mais exatas as PIIs que são coletadas, menor será o risco de investimento de determinada empresa.

Como demonstrado anteriormente, algumas IoT acessam dados de Identificação Pessoal (PII) como parte de suas funções operacionais, como é o caso do dispositivo *Kinect*. No entanto, existem diversas formas, frequentemente desconhecidas pelo público devido à falta de compreensão sobre o funcionamento tecnológico e inteligente desses equipamentos, de reconhecer e construir perfis dos usuários. Uma dessas formas envolve o

preenchimento de formulários. Muitas empresas oferecem prêmios ou bônus para os usuários que se cadastram em seus sites, solicitando informações que muitas vezes são irrelevantes para o serviço prestado, como *e-mail*, nome, estado civil e interesses pessoais, entre outras. Nessa situação, o usuário fornece dados espontaneamente, mesmo que não saiba qual a destinação das PIIs fornecidas (Matos, 2005).

Outra maneira de coletar dados são os *cookies*, que adversos aos formulários, coletam dados sem o consentimento ou ciência do usuário. Os *cookies* são "arquivos de informações lançados pelos sites visitados, dentro do computador do visitante, e ficam armazenados no respectivo disco rígido para, enquanto houver navegação na web, serem utilizados pela memória RAM" (Matos, 2005, p. 9).

Há dois tipos de *cookies*: aqueles que armazenam dados relacionados ao site acessado e facilitam um carregamento mais rápido em visitas subsequentes, e aqueles que apenas coletam informações sobre quem acessou a página. Nessas ocasiões, uma ampla gama de dados de Identificação Pessoal (PII) pode ser coletada, incluindo o navegador utilizado, o sistema operacional, o horário e a quantidade de acessos, o número de IP do computador e até mesmo a localização geográfica. Embora essas informações possam ser úteis para identificar criminosos virtuais, elas também expõem usuários legítimos a riscos de vazamento de dados, uma vez que a localização pode revelar até mesmo o endereço preciso e o número de telefone do usuário. (Matos, 2005).

Dados recentes demonstram que o Brasil lidera o *ranking* de vazamentos de dados da NordVPN, empresa global de cibersegurança. De acordo com o levantamento, cerca de 2 bilhões de dados como e-mail, senha, nome e telefone de usuários foram vazados no país sendo que grande parte desses dados são adquiridos através de *cookies*. Entre os sites com maior volume de vazamentos constam *Google* (2,5 bilhões) e *YouTube* (692 milhões) (Felix, 2024).

Ao público geral é muito conhecida a figura dos *hackers* e *crackers*. Enquanto os primeiros são motivados a navegar por sistemas a fim de encontrar falhas computacionais e corrigi-las, os segundos utilizam essas fragilidades para cometer crimes. Portanto, um dos perigos relacionados a imensa quantidade de PIIs disponível nos mais variados bancos de dados na rede é que crackers os acessem e utilizem para cometer crimes ou até mesmo venda essas informações (Matos, 2005).

Outro fato importante a ser considerado é o fenômeno da "virtualização" dos dados, ou seja, dados que anteriormente pertenciam a bancos de dados de instituições específicas como colégios e universidades, consultórios médicos e bancos, e informações sobre pessoas físicas pertencentes a órgão como INSS ou Serasa, agora já estão disponíveis na Grande Rede. Por óbvio que tais dados são protegidos com diversos recursos como senhas, por exemplo, mas uma vez *online*, ainda que o sistema seja seguro, a chance de vazamento existe (Matos, 2005).

A situação apresentada coloca o usuário em uma situação de vulnerabilidade em relação a grandes empresas potencialmente interessadas na manipulação de dados a fim de maximizar os lucros, bem como perante possíveis criminosos. Além do mais, os indivíduos têm direito à privacidade, à intimidade e ao resguardo de suas informações, assunto que será explorado nas próximas páginas. No que diz respeito à vulnerabilidade, é interessante pontuar que essa conjuntura se refere a uma condição desfavorável, ou seja, uma situação de inferioridade em relação a algo (Merabet et al, 2021). Considerando o contexto em análise, os usuários, portanto, encontram-se em uma situação de desfavor, de vulnerabilidade diante das inúmeras maneiras de captação de dados na web e através das IoT. Diante dessa circunstância, o Direito tem papel importante em garantir que a balança seja equilibrada contribuindo não apenas para a regulação de Leis e dispositivos que protejam os dados dos usuários das redes diante das novas tecnologias, mas também na educação dos cidadãos a respeito do assunto.

3. A PRIVACIDADE COMO DIREITO FUNDAMENTAL

Privacidade é um termo que pode ser definido através de preceitos diferentes. Sem grande rigor, o termo pode referir-se a alguém que controla o acesso à informação que outros detém sobre si mesmos. Considerando, portanto, a vulnerabilidade dos dados pessoais nas redes, especialmente no contexto das IoT, a privacidade torna-se um tema tão relevante que cabe ao Direito garantir sua preservação.

Conforme Chabridon (et al., 2014) pontua a privacidade pode ser dividida em três categorias:

> a) confidencialidade: é a forma mais básica da privacidade já que seu objetivo primário é garantir que dados pessoais não sejam divulgados ou acessados por pessoas não autorizadas. Essa característica preocupa-se em garantir soluções tecnológicas que preservem o anonimato dos usuários e de suas comunicações, ou seja, garantir que as informações trocadas não sejam vazadas. O *Whatsapp*, por exemplo, um dos aplicativos de mensagens mais populares da atualidade, utiliza a tecnologia de criptografia de ponta a ponta para proteger o conteúdo das conversas e, segundo a empresa afirma em seu blog, "Ninguém verá o conteúdo dessa mensagem. Nenhum cibercriminoso. Nenhum hacker. Nenhum regime opressivo. Nem mesmo nós. A criptografia de ponta a ponta ajuda a tornar a comunicação via WhatsApp privada, como se você estivesse conversando pessoalmente" (*Whatsapp*, 2016 - online). Os dispositivos legais, como as Leis, portanto regulam os termos do que é considerado secreto além de punir casos em que essa característica seja violada.
> b) controle: esse aspecto diz respeito a capacidade de moderar como os dados pessoais são tratados a fim de evitar abusos que requer a aplicação de políticas de privacidade rígidas na rede e na IoT.
> c) transparência: é, como o nome sugere, a cristalinidade entre a maneira como os dados são coletados e tratados e o usuário, a fim de que o dono das informações saiba exatamente o que acontece com o que ele forneceu. No contexto da IoT isso se torna ainda mais complexo já que a questão dos dados fornecidos não diz respeito apenas aos equipamentos que cada indivíduo possui, mas também aos dispositivos conectados a internet que coletam dados sem que o usuário se dê conta como, por exemplo, câmeras e sensores em locais como shoppings centers.

A privacidade ainda pode ser dividida em duas esferas: a pública e a privada. Em ambos os casos é regulado pela Lei, diferindo-se pela maneira como se materializa. No âmbito privado, a privacidade diz respeito ao limite que regulamenta até que ponto alguém ou o próprio governo pode invadir o espaço

alheio, enquanto no espaço público “privacidade é vista mais no sentido de “vigilância”, pois é o ambiente onde o indivíduo exerce relações sociais e atividades que são públicas” (Dias, 2017 p. 243). Nessa situação, em tese, o indivíduo renuncia ao seu direito à privacidade, pois quando realiza suas atividades rotineiras como ir ao supermercado ou ao trabalho, outras pessoas conseguem monitorar suas atividades e, portanto, não é algo privado (Dias, 2017).

O direito à privacidade, embora essencial, é paradoxal, já que pode ser negado diante de ameaça ao bem público ou em casos de investigação com devida autorização judicial. Ademais, alguns dados considerados privados podem ser importantes para tratar de questões sociais como, por exemplo, os coletados por órgãos como o IBGE (Instituto Brasileiro de Geografia e Estatística). Embora o Instituto em questão jamais personalize os dados e informações coletadas e divulgadas periodicamente sobre a população, é importante considerar que estes provêm da privacidade de cada cidadão. Entretanto, os números indicados por tais informações são essenciais para a construção de políticas sociais importantes para a melhora da qualidade de vida dos brasileiros e que promovam a cidadania.

> Contudo, a liberdade das práticas de vigilância pública ou privada é fundamental para a prática de informação e reflexão da cidadania. Ou seja, nos dias de hoje, as tecnologias das informações têm permitido o monitoramento das atividades das pessoas para que as empresas e/ou governo manipulem as informações disponíveis ao público por meio da utilização de ferramentas de pesquisas, filtros, plataformas sociais e propagandas. Isto quer dizer, se a cidadania envolve votar, participar de debates públicos e opinar; estes direitos somente são exercidos de forma plena quando as informações disponíveis ao público não são manipuladas de acordo com determinado interesse público ou privado. Privacidade é uma característica estrutural indispensável dos sistemas político democrático liberal (Dias, 2017 p. 244).

No Brasil, a história da proteção de dados inicia-se com a Constituição Federal (CF), que elenca a dignidade humana como um dos direitos fundamentais. Em seu Artigo 5º inciso X “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas”. Já o inciso XI determina que o domicílio é local “inviolável do indivíduo, ninguém nela podendo penetrar sem

consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial" enquanto o inciso XII diz "é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas" salvo casos de ordem judicial (Brasil, 1988). A dignidade, substância citada na CF, é compreendida como uma atribuição humana inegociável que dota os sujeitos de direito e deveres, bem como lhes assegura uma vida saudável, sem constrangimentos e plena. Portanto, o direito de ter a intimidade preservada e a não exposição de dados sensíveis enquadra-se dentro dessa garantia constitucional.

Além da CF, o Código Civil também aponta, em seu artigo 21 do Capítulo IV que "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" (Brasil, 2002).

É importante citar a Lei Nº 12.965 de 2014, conhecida como Marco Civil da Internet, que tem por função garantir o exercício da cidadania nas redes, a liberdade de expressão e a proteção de dados. O artigo 7º da referida Lei esclarece que ao usuário deve ser garantida a "I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação; II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet" e "III - inviolabilidade e sigilo de suas comunicações privadas armazenadas" (Brasil, 2014) sendo que os dois últimos incisos podem ser violados apenas sob ordem judicial. Dessa forma, dados como data, hora, duração de um acesso e endereço de IP são informações sensíveis que devem ser protegidas pelas empresas que gerem esse fluxo (Bruno, 2019). Além disso, o art. 8 da referida Lei 12.965 ainda pontua que são nulas cláusulas contratuais nas comunicações que violem os direitos de privacidade estabelecidos (Brasil, 2014). Nota-se que nesse contexto respeita-se o direito fundamental em relação à privacidade e a informação, existe

> [...] uma proporcionalidade entre ambos, no qual evite a intromissão nas informações que não sejam do interesse social, ou que possam ocasionar algum prejuízo ao próprio titular, preservando, desta maneira, a vida e a intimidade privada de cada sujeito (Bruno, 2019, p.20)

Tendo em mente o novo cenário de hiperconectividade e a vulnerabilidade na qual os sujeitos foram inseridos diante das IoT, a capacidade dos algoritmos e da Inteligência Artificial (AI) de processar e direcionar informações, foi criada em 2018 a Lei n. 13.709/2018 - Lei Geral de Proteção de Dados também conhecida como LGPD que será discutida mais profundamente no capítulo 3.

Para ilustrar como a internet e as IoT podem violar o direito à privacidade dos usuários, analisamos brevemente o escândalo protagonizado pelo *Facebook* e a *Cambridge Analytics* (CA) que exerceu influência sobre o resultado da eleição presidencial em 2016 nos Estados Unidos dando a vitória a Donald Trump.

O *Facebook* é a rede social mais popular do mundo e registrou o número de 2,11 bilhão de usuários no final de 2023. Operando através de um perfil criado pelos usuários em sua plataforma, o *Facebook* é conhecido por mostrar os conteúdos postados em uma linha do tempo denominada feed que informa postagens realizadas por amigos, amigos de amigos, empresas e anunciantes, por exemplo. Isso acontece porque os algoritmos da plataforma são capazes de identificar, através das curtidas e localização, por exemplo, quais os interesses do usuário direcionando anúncios específicos para cada perfil. É possível se conectar ao Facebook utilizando muitos dispositivos como o computador, o celular e *smarTV*, por exemplo. Além disso, é possível *logar* em diversos sites através do Facebook, estratégia utilizada por outras empresas como o Google, ampliando o leque de vigilância da plataforma e a disponibilidade de dados (BBC News Brasil, 2018; 2021).

Diante disso, em meados de 2014, circulou no Facebook um aplicativo denominado *thisisyourdigitallife* que pagou pequenas quantias em dinheiro a milhares de usuários para que eles respondessem a um teste de personalidade. As informações obtidas neste aplicativo foram combinadas com diversos dados coletados pelo *Facebook*, inclusive curtidas e dados relacionados a amigos dos usuários, e com o auxílio da *Cambridge Analytica*, empresa dirigida na época por Steve Bannon, assistente de Donald Trump em sua campanha presidencial de 2016, um modelo matemático, ou seja, um

algoritmo foi criado para direcionar anúncio, com base em perfis muito precisos traçados pela tecnologia, capazes de influenciar a opinião pública sobre assuntos relacionados às pautas favoráveis a Trump. Nessa situação, grande parte dos dados coletados eram referentes a cidadãos estadunidenses, mas não apenas, já que dados de usuários brasileiros também foram coletados. Por exemplo, uma das bandeiras levantadas pelo ex-presidente dos Estados Unidos referia-se ao porte de armas de fogo. Portanto, se o algoritmo identificar uma pessoa que gosta de viajar e conhecer novas culturas, ele poderia indicar que a posse de uma arma de fogo é um bem imprescindível para sua proteção individual diante dessa característica (BBC News, 2018; BBC News Brasil, 2021; PIAIA, Thami C. et al., 2019; The New York Time, 2018).

Além do *Facebook*, o *WhatsApp* também foi utilizado para esse propósito. Embora o aplicativo de mensagens não possua anúncios, números de telefone foram vazados de dentro do Facebook permitindo que os usuários fossem colocados dentro de grupos ou incluídos em lista de malas diretas para o mesmo fim explicitado no parágrafo anterior (BBC News Brasil, 2021).

A proporção do escândalo é tão grande porque demonstra que os usuários não têm o direito à privacidade garantido, já que seus dados são vendidos e manipulados por empresas capazes de traçar perfis tão precisos de cada sujeito a ponto de prever seus comportamentos e tendências políticas e influenciar desonestamente a opinião política por meios escusos.

Em 2018, durante a corrida presidencial no Brasil, os métodos do *Facebook* no que diz respeito a propagação de propagandas demandaram que o Tribunal Superior Eleitoral (TSE) obrigasse o *Facebook* a retirar alguns anúncios que se enquadram como *Fake News* e, portanto, influenciam a opinião pública de maneira errônea a respeito de um ou outro candidato (CONJUR, 2018).

4. A PROTEÇÃO DA PRIVACIDADE NA LGPD

Em um breve retrocesso histórico, é possível traçar a linha do tempo até a concretização da LGPD. Em 2012 tramitava no Congresso Nacional o Projeto de Lei (PL) 4060 que argumentava sobre o tratamento de dados pessoais (Brasil, 2012). Em 2016, antes do afastamento da então presidente da república Dilma Rousseff, encaminhou a Câmara dos Deputados o anteprojeto que se tornaria o PL 5276 que dispunha sobre o "tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural" (Brasil, 2016). No mesmo ano formou-se uma Comissão Especial constituída pelo deputado Orlando Silva (PCdoB/SP), como relator, presidência da Deputada Bruna Furlan (PSDB/SP) e vice-presidência pelos deputados André Figueiredo (PDT/CE), Alessandro Molon (REDE/RJ) e Milton Monti (PR/SP) que tinha como objetivo analisar os dois PLs citados anteriormente que resultou em onze audiências públicas e um seminário internacional entre 2016 e 2017. Entretanto, diante de tribulações envolvendo a figura de Michel Temer, então presidente da república, o relatório final da Comissão foi adiado para o próximo ano. Em 2019 é redigido o Plano Nacional de Internet das Coisas que se tornaria, no ano seguinte, o Decreto Nº 9.854 (Brasil, 2018; Sobrinho, 2019). Nesse sentido, torna-se urgente a constituição de um marco regulatório no que diz respeito à proteção da privacidade dos usuários da Internet.

O caso demonstrado no capítulo anterior envolvendo o *Facebook* e a *Cambridge Analytica* acendeu um alerta em todo mundo a respeito da necessidade de políticas específicas e rígidas a respeito da privacidade na internet. No Brasil, essa situação impulsionou a aprovação da Lei Nº 13.709/2018 doravante denominada Lei Geral de Proteção de Dados ou LGPD que se baseia na lei europeia denominada Regulamento Geral de Proteção de Dados (GDPR) (Paz et al., 2023; Sobrinho, 2019). No ano seguinte, 2019, foi criada pela Lei n. 13.853 a Autoridade Nacional de Proteção de Dados (ANPD), que tem a função de cobrar a aplicação da LGPD fiscalizando e aplicando sanções quando necessário (Brasil, 2024).

Em linhas gerais, entre os 65 artigos que estruturam a Lei, a LGPD

> dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Fundamentando-se nos seguintes princípios:

> I - o respeito à privacidade;
> II - a autodeterminação informativa;
> III - a liberdade de expressão, de informação, de comunicação e de opinião;
> IV - a inviolabilidade da intimidade, da honra e da imagem;
> V - o desenvolvimento econômico e tecnológico e a inovação;
> VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

A Lei explica que a proteção se estende a pessoas jurídicas de direito público ou privado, ou seja, engloba também empresas, ainda que estas sejam sujeitos de deveres e não de direitos. Além disso, o artigo 1° explica que as normas criadas pela LGPD são de interesse nacional, ou seja, no que diz respeito ao tratamento de dados, ela deve ser seguida por pessoas físicas, jurídicas assim como pela União, Estados, Distrito Federal e Municípios.

É interessante pontuar também que a Lei é clara ao dizer que a proteção da LGPD se estende apenas a pessoas naturais, ou seja, pessoas vivas. Isso significa que os dados de pessoas falecidas não são defendidos pela LGPD. Esse aspecto pode ser considerado uma falha no ato da redação da Lei já que os dados de pessoas falecidas são manipulados no ato do óbito como, por exemplo, para realização do enterro, de cerimônias religiosas, para averiguação de bens e encerramento de contas bancárias. Em alguns casos, quando há necessidade de realizar inventários, os dados de pessoas falecidas podem ser tratados por anos a depender de quanto tempo o processo tramitará na Justiça. Além disso, dados de pessoas falecidas também podem ser utilizados para cometer crimes (Mori; Rezende, 2023).

A coleta e o compartilhamento dos dados por parte das empresas devem ser realizados de maneira gratuita e clara ao titular, entretanto, Leme

(2019) aponta que 91% da população confirma os termos de privacidades em sites e aplicativos em geral sem ao menos ler. A complexidade e extensão dos termos pode ser um dos fatores que assusta o usuário, mas a ingenuidade acerca dos dados que pode estar entregando ao acessar determinado serviço também contribui para o desequilíbrio dessa equação (Sobrinho, 2019).

A LGPD tem como uma de suas bases o consentimento conforme expressa no art. 7º , que em seu inciso I estabelece que o tratamento de dados pessoais somente poderá ser realizado mediante o fornecimento de consentimento pelo titular. Portanto, Sobrinho (2019) afirma que para que o usuário concorde conscientemente com os termos de uso ao qual é exposto diariamente, as empresas devem pensar em estratégias para diminuir a robustez dos documentos e simplificar a linguagem.

Outro princípio importante da LGPD é o da necessidade, ou seja, as empresas apenas podem coletar dados que sejam realmente necessários para a finalidade pretendida. Da mesma forma, no caso de compartilhamento de dados entre empresas, o titular dos mesmos deve ser comunicado.

> Art. 5º Para os fins desta Lei, considera-se: [...]III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados […].
> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses: [...] § 5º O controlador [...] que necessitar comunicar ou compartilhar dados pessoais com outros controladores deverá obter consentimento específico do titular para esse fim [...]. (Brasil, 2018).

Em seu artigo 5º a LGPD define algumas nomenclaturas utilizadas em sua redação entre elas as expostas nos incisos IV e V que dissertam sobre o titular e controlador, respectivamente. O controlador é a “pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais”; enquanto o operador é a “pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador” (Brasil, 2018). Sendo assim, a estes dois agentes compete a função de fazer saber violações no tratamento de

dados aos órgãos competentes além de criar mecanismos para a sua proteção. Entretanto, a responsabilidade do operador é limitada a suas obrigações expressas em contrato transferindo o poder ao titular, que por sua vez é a quem os dados pessoais tratados se referem, dos dados que pode exigir ao controlador um dossiê sobre o tratamento de suas informações bem como pedir a exclusão dos mesmos de sua base de informações (salvo em algumas exceções expostas no Art 16).

> Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses: I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários [...] II - fim do período de tratamento; III - comunicação do titular, inclusive no exercício de seu direito de revogação do consentimento [...] ou IV - determinação da autoridade nacional (Brasil, 2018).

No que diz respeito ao tratamento pessoal de dados pessoais e/ou sensíveis de crianças e adolescentes, é importante levar em consideração o que a CF aponta em seu Art. 227:

> Art. 227. É dever da família, da sociedade e do Estado assegurar à criança, ao adolescente e ao jovem, com absoluta prioridade, o direito à vida, à saúde, à alimentação, à educação, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária, além de colocá-los a salvo de toda forma de negligência, discriminação, exploração, violência, crueldade e opressão.

No contexto da hiperconectividade e da exposição em redes sociais de crianças e adolescentes, é importante considerar que, ao explicitar que é dever da família garantir a dignidade, colocando menores de idade longe de qualquer tipo de violação física ou psicológica, é possível interpretar que a Lei também engloba a internet.

Nesse sentido, a própria LGPD prevê providências para essa situação em seu Art. 14. Conforme inciso 1 do artigo supracitado, o tratamento de dados de crianças e adolescentes deve ser realizado apenas com o consentimento de pelo menos um dos responsáveis legais ou país. Os controladores, por sua

vez, devem seguir as mesmas regras a respeito do tipo de dados coletados no que diz respeito a informar por que e para que a coleta de determinado dado é necessária. A coleta de dados de crianças e adolescentes somente será permitida sem a autorização dos pais ou responsáveis, conforme inciso 3 quando a coleta "for necessária para contatar os pais ou o responsável legal, utilizados uma única vez e sem armazenamento, ou para sua proteção, e em nenhum caso poderão ser repassados a terceiro sem o consentimento" (Brasil, 2018). O inciso 6 ainda apregoa que a linguagem utilizada para informar o usuário sobre a coleta de dados deve ser compatível com a sua idade, ou seja,

> [...] de maneira simples, clara e acessível, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, com uso de recursos audiovisuais quando adequado, de forma a proporcionar a informação necessária aos pais ou ao responsável legal e adequada ao entendimento da criança (Brasil, 2018).

Esse inciso reforça a necessidade da transparência na comunicação feita entre usuário e portador, entretanto não deixa claro se se aplica a crianças e adolescentes ou apenas aos dois. É interessante considerar que crianças muito novas já têm familiaridade com IoT devido ao nível de exposição e, portanto, sabem operar diversos equipamentos como tablets e celulares. Sendo assim, ao acessar alguns aplicativos como *Youtube* ou até mesmo jogos, a criança pode conceder autorização para que os mesmos acessem dados, seja do portador do celular ou delas próprias. Ainda no caso dos adolescentes, mesmo que eles possuam as faculdades intelectuais necessárias para compreender termos de uso de aplicativos e sites, o discernimento sobre a questão deve partir dos responsáveis legais já que a eles compete a obrigação de garantir a segurança, online ou física, dos filhos. Sendo assim, é sensato apontar que os pais ou responsáveis por crianças e adolescentes devem vistoriar além de educar esse público-alvo a respeito desse assunto.

Outro ponto que merece destaque é referente aos vazamentos, roubo dos dados do controlador ou acessos não autorizados. Em casos como esse, o

controlador deve informar, em um prazo razoável, a ANPD a respeito do incidente e fornecer algumas informações estipuladas na Lei conforme explicita o Art. 46 a 48 e seus incisos. Assim a ANPD será capaz de avaliar o que causou o incidente e como o controlador deverá ser responsabilizado.

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares. 1º A comunicação será feita em prazo razoável, conforme definido pela autoridade nacional, e deverá mencionar, no mínimo: I - a descrição da natureza dos dados pessoais afetados; II - as informações sobre os titulares envolvidos; V - os riscos relacionados ao incidente; V - os motivos da demora, no caso de a comunicação não ter sido imediata; e VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos do prejuízo (Brasil, 2018).

Após concluídas as investigações da ANPD, os responsáveis podem receber advertências, multas, bloqueio de dados pessoais que se referem a multa ou até mesmo eliminação desses mesmos dados conforme explica o Art. 52 da LGPD.

No caso de empresas que possuem filiais em outros países, a LGPD possui alcance extraterritorial e, portanto, deve ser respeitada ainda que fora do território brasileiro. Também estabeleceu 24 meses, a contar da sua sanção, para que as empresas se adequem às suas exigências com incidência de multa e punições no caso de descumprimento (Sobrinho, 2019).

A LGPD é uma lei processual, ou seja, ela demonstra os caminhos que os controladores devem seguir para adequar as empresas às recomendações da LGPD. A eficiência da LGPD portanto depende do cumprimento dessas recomendações bem como da fiscalização por parte da ANPD. Além disso, é preciso educar os usuários de maneira simples e objetiva a respeito dos riscos de fornecer dados online e a dispositivos conectados à internet bem como seus direitos, em relação a LGPD, e deveres como, por exemplo, atentar-se aos termos de uso.

Em 2023, três anos após o início da vigência da LGPD, a ANPD registrou cerca de 636 incidentes relacionados à segurança de dados na rede.

Os casos mais comuns envolvem sequestro de dados, exploração de vulnerabilidades, acesso ilegal a sistema de informática e roubo de credenciais demonstrando a falta de segurança dos sistemas e expondo os usuários a criminosos e golpistas (CISI, 2023).

A regulação para dosimetria e aplicação das sanções administrativas aplicadas pela ANPD só foi oficializada em fevereiro de 2023, sendo que a primeira multa aplicada pela Autoridade aconteceu apenas em julho de 2023 (Vital, 2023).

Observa-se que os avanços e a consequente eficácia da LGPD ainda são tímidos além de recentes, o que torna difícil avaliar sua eficácia. Entretanto, é possível prever algumas medidas essenciais para garantir o sucesso da LGPD na matéria que se propõe.

Em primeiro lugar, a ANPD precisa fiscalizar e garantir que as empresas estão se adequando a LGPD, tarefa árdua visto que a Lei se aplica a qualquer empresa, independentemente de seu tamanho, que trate dados pessoais de usuários. Para que as empresas estejam aptas a essa adequação, uma série de procedimentos também precisam ser seguidos como, por exemplo, a contratação de especialistas em segurança e tratamento de dados, avaliação para realizar os devidos ajustes a respeito da gestão de arquivos, elaboração de um plano de contingência em caso de para casos de incidentes.

Além disso, é importante também a conscientização e educação do usuário a respeito dos riscos e dos tratamentos que seus dados recebem nas redes, bem como a ciência a respeito da LGPD e dos mecanismos criados pela Lei para protegê-lo.

5. CONCLUSÃO

A proteção da privacidade, e por consequência dos dados pessoais e sensíveis, das pessoas diante dos avanços tecnológicos possibilitados pela internet é uma questão complexa, urgente e em constante movimento. Diante

da proporção de grandes vazamentos de dados e a manipulação por terceiros dessas informações, como foi o caso do *Facebook* e da *Cambridge Analytica*. A LGPD, inspirada no Regulamento Geral de Proteção de Dados (GDPR) europeu, surge em 2018 como uma tentativa de mitigar os efeitos danosos que o tratamento de dados de maneira maliciosa pode causar. Entretanto, a eficácia da LGPD é uma questão que ainda está sendo debatida e analisada assim como sua implementação e impactos.

Em vias de avaliar a importância da LGPD, é imprescindível analisar alguns aspectos, entre eles os obstáculos enfrentados na sua implementação e fiscalização a ser realizada por meio da Autoridade Nacional de Proteção de Dados (ANPD). Além disso, também é importante considerar os impactos que a adequação a Lei pode causar nas empresas e nos usuários.

Em relação à implementação, sendo uma Lei processual, a LGPD demonstra claramente como os controladores devem tratar dados pessoais exigindo, inclusive, o consentimento do titular dos dados. Ademais, os controladores devem notificar a ANPD sempre que algum incidente relacionado ao vazamento, roubo ou acesso não autorizado dos dados acontecer.

Apesar da clareza da Legislação, alguns controladores, especialmente os provenientes de empresas ou negócios de menor porte, podem enfrentar problemas de ordem orçamentária quando da implementação das regras. Isso se deve ao fato de que é necessário promover uma reestruturação importante no tratamento de dados e garantir que uma equipe de informática seja alocada exclusivamente para implementar tecnologias que tratem os dados conforme a Lei indica e, sobretudo, os protejam. No que diz respeito aos dados de crianças e adolescentes, a questão se complexifica visto que cabe aos pais e responsáveis legais controlar a disponibilidade desses dados. Portanto, a Lei carece ainda de esclarecimentos a respeito de como tais dados devem ser tratados.

Além disso, a LGPD ainda não explicita como os dados de pessoas falecidas devem ser tratados. Essa questão é de suma importância visto que a manipulação desses dados para fins maliciosos pode acontecer além de que

também podem ser utilizados para expor e causar constrangimento a pessoa morta, situação que enquadra crime de ofensa à memória de pessoa falecida conforme artigo 185.º do Código Penal além de outros possíveis crimes.

A ANPD também tem um papel importante em garantir a eficácia da LGPD, pois é através dela que os controladores serão fiscalizados e punidos, quando necessário. A ANPD é a Autoridade responsável por fiscalizar e inspecionar o cumprimento da legislação, bem como administrar e investigar os incidentes relacionados à segurança de dados.

Para a ANPD o cumprimento da LGPD bem como a sua melhoria e inclusão de situações que ainda não foram tratadas é fundamental e, para tanto, é preciso capital humano e intelectual para refinar os mecanismos já expressos na Lei. Além disso, a ANPD deve focar, em um primeiro momento, em empresas de grande porte e que manipulam grande quantidade de dados por uma questão de análise de risco. O vazamento de dados em grande volume é mais prejudicial para o interesse público do que um vazamento menor. Entenda que os dois casos são importantes, entretanto, diante de um cenário de adequação e início das fiscalizações e sanções, é preciso elencar por quais alvos começar.

Situações como a que ocorreu com o *Facebook* e a *Cambridge Analytica* devem ser reduzidas a zero e não podem ser toleradas. As proporções perigosas e danosas que situações como essa podem causar ao interesse público são imensas e, portanto, a rigorosidade da Lei na fiscalização e punição dessas empresas também deve ser inflexível e intransigente.

Para que a ANPD funcione de maneira eficiente, é preciso o investimento máximo em capital humano visto que a fiscalização que deverá ser promovida para averiguar se os controladores se enquadram na LGPD precisa ser volumosa. Alguns aspectos, no entanto, preocupam no que tange a eficácia da Lei como, por exemplo, a demora na regulamentação da dosimetria e como isso pode ter afetado a punição de incidentes.

Apesar de alguns impasses, a LGPD é um avanço importantíssimo e sem precedentes na Legislação brasileira em relação à temática que se

propõe. A Legislação é clara no que diz respeito aos processos de tratamento de dados incentivando práticas de responsabilidade e transparência nos operadores. Por outro lado, os usuários também devem ser contemplados com campanhas educativas a respeito da importância e da razão de ser da LGPD a fim de que compreendam melhor a importância de proteger seus dados e se tornem indivíduos mais cautelosos. Essa ação por si só ajudaria na eficácia da Lei pois sujeitos atentos certamente pensariam melhor antes de compartilhar seus dados pessoais e sensíveis diminuindo também o volume de incidentes.

Conclui-se que a desenvoltura da LGPD depende de um esforço conjunto entre governos, empresas e sociedade civil. Apenas envolvendo, conscientizando e educando os agentes envolvidos nessa equação é que será possível criar um ambiente digital seguro, respeitoso, honesto e que garanta, acima de qualquer circunstância, a integridade e privacidade dos dados de seus usuários.

REFERÊNCIAS

BBC News Brasil. **Como o Facebook mudou a internet, o comércio e até a política | 21 notícias que marcaram o século 21**. Youtube, 11 jul. 2021. Disponível em: https://www.youtube.com/watch?v=XTMGETyc6G4. Acesso em: 30 mar. 2024.

BBC NEWS. **Entenda o escândalo de uso político de dados que derrubou valor do Facebook e o colocou na mira de autoridades**. 2018. Disponível em: https://www.bbc.com/portuguese/internacional-43461751. Acesso em: 15 jan. 2024.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 15 jan. 2024.

BRASIL. **Decreto-Lei n. 2.848, De 7 De Dezembro De 1940.** Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 jan. 2024.

BRASIL. **Lei nº 10.406, de 10 de janeiro de 2002.** Código Civil. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/2002/l10406compilada.htm. Acesso em: 15 jan. 2024.

BRASIL. **Lei nº 12.965, de 23 de abril de 2014**. Marco Civil da Internet. Disponível em: https://www.planalto.gov.br/CCIVIL_03/_Ato2011-2014/2014/Lei/L12965.htm#art32. Acesso em: 15 jan. 2024.

BRASIL. **LEI nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: 2018. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 15 mar. 2024.

BRASIL. **Perguntas Frequentes – ANPD.** 2024. Disponível em: https://www.gov.br/anpd/pt-br/acesso-a-informacao/perguntas-frequentes-2013-anpd#:~:text=Cabe%20%C3%A0%20ANPD%20fiscalizar%20e,com%20contradit%C3%B3rio%20e%20ampla%20defesa. Acesso em: 20 mar. 2024.

BRASIL. **PL 4060/2012.** Projeto de Lei que dispõe sobre o tratamento de dados pessoais, e dá outras providências. 2012. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=548066. Acesso em: 15 mar. 2024.

BRASIL. **PL 5276/2016**. Projeto de lei que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. 2016. Disponível em: https://www.camara.leg.br/proposicoesWeb/fichadetramitacao?idProposicao=2084378#:~:text=PL%205276%2F2016%20Inteiro%20teor,Projeto%20de%20Lei&text=Disp%C3%B5e%20sobre%20o%20tratamento%20de,da%20dignidade%20da%20pessoa%20natural. Acesso em: 15. mar. 2024.

BRUNO, Giovana Pizzato. **A Proteção de Dados Pessoais na Internet no Brasil: Regime Jurídico e Responsabilidade dos Agentes Sob a Ótica da Lei Nº 13.709 de 14 de Agosto De 2018**. Monografia (Graduação em Direito). Centro Universitário Antônio Eufrásio De Toledo De Presidente Prudente, Presidente Prudente, SP. 2019. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/Direito/article/view/8327. Accesso em: 15 fev. 2024.

CHABRIDON, Sophie; et al. A survey on addressing privacy together with quality of context for context management in the Internet of Things. **Annals of Telecommunications**, v. 69, n. 1-2, p. 47-62. Disponível em: https://hal.science/hal-01285786/document. Acesso em: 10 jan. 2024.

CHICARINO, Vanessa R. L; ROCHA, Antonio. Uso de Blockchain para Privacidade e Segurança em Internet das Coisas. In: NUNES, Raul Cereta et al. **Minicursos do XVII Simpósio Brasileiro de Segurança da Informação e de Sistemas Computacionais**. Brasília: Sociedade Brasileira de Computação,

2017. Disponível em: https://books-sol.sbc.org.br/index.php/sbc/catalog/view/84/371/635. Acesso em: 30 jan. 2024.

CISI, Luz. Três anos de LGPD: mais de 600 casos já foram registrados na Agência Nacional de Proteção de Dados. **CNN Brasil**. 2023. Disponível em: https://www.cnnbrasil.com.br/nacional/tres-anos-de-lgpd-mais-de-600-casos-ja-foram-registrados-na-agencia-nacional-de-protecao-de-dados/. Acesso em: 10 mar. 2024.

DIAS, Patricia Yurie. Regulação da internet como administração da privacidade. **Revista de Direito Setorial e Regulatório**, Brasília, v. 3, n. 1, p. 239-254, maio de 2017. Disponível em: https://periodicos.unb.br/index.php/rdsr/article/view/19206. Acesso em: 05 fev. 2024.

FACCIONI FILHO, Mauro. Designing “things” for the Internet of Things. In: I Congresso Internacional e VII Workshop Design & Materiais, 2016, São Paulo, **Anais** [...] São Paulo: Universidade Anhembi Morumbi, 2016, p. 502-509. Disponível em: https://www.researchgate.net/publication/319881659_Internet_das_Coisas_Internet_of_Things. Acesso em: 10 abr. 2024.

FELIX, Diego. **Brasil lidera em vazamento de dados na internet.** 2024. Disponível em: https://www1.folha.uol.com.br/colunas/painelsa/2024/04/brasil-lidera-em-vazamento-de-dados-na-internet.shtml. Acesso em: 10 jan. 2024.

KADOW, André; CAMARGO, Carlos Eduardo Pires. Internet Das Coisas: Vulnerabilidade, Privacidade e Pontos de Segurança. **Revista Competência**. Porto Alegre, RS, v.9, n.1, p. 153-161, Jan/jul. 2016. Disponível em: https://www.researchgate.net/publication/320315070_INTERNET_DAS_COISAS_VULNERABILIDADE_PRIVACIDADE_E_PONTOS_DE_SEGURANCA. Acesso em: 25 fev. 2024.

LEME, Carolina da Silva. Proteção e tratamento de dados sob o prisma da legislação vigente. **Revista Fronteiras Interdisciplinares do Direito**, [s.l.], v. 1, n. 1, p.178- 197, 9 maio 2019. Disponível em: https://revistas.pucsp.br/index.php/fid/article/view/41960/28471. Acesso em: 15 mar. 2024.

MATOS, Tiago Faria. **Comércio de dados pessoais, privacidade e Internet. Revista de Doutrina da 4ª Região**, n. 7, 18 jul. 2005. Disponível em: https://revistadoutrina.trf4.jus.br/index.htm?https://revistadoutrina.trf4.jus.br/artigos/edicao007/tiago_matos.htm. Acesso em: 12 fev. 2024.

MERABET, Daniel de Oliveira Barata; et al. Uma discussão necessária sobre a vulnerabilidade do consumidor: avanços, lacunas e novas perspectivas. **Cad. EBAPE.BR**, v. 19, nº 1, Rio de Janeiro, Jan./Mar. 2021. Disponível em:

https://www.scielo.br/j/cebape/a/TqJ8X8WvJysZ3TKDJm5PwnB/#. Acesso em: 22 jan. 2024.

MINERVA, Roberto, et al. Towards a definition of the Internet of Things (IoT). **IEEE Internet Initiative**, v. 1, n. 1, p. 1-86, 2015. Disponível em: https://www.researchgate.net/publication/317588072_Towards_a_definition_of_the_Internet_of_Things_IoT. Acesso em: 20 fev. 2024.

MORI, Jennifer Mayumi; REZENDE, Laura Wihby. Dados pessoais de falecidos: privacidade diante da inaplicabilidade da LGPD. **Conjur**, 2023. Disponível em: https://www.conjur.com.br/2023-jun-27/morie-rezende-dados-pessoais-pessoas-falecidas/. Acesso em: 20 mar. 2024.

OLIVEIRA, Tassyara Onofre de. **Gestão de dados pessoais: uma análise de casos concretos a partir do ordenamento jurídico brasileiro.** 2017. 109 f. Dissertação (Mestrado em Gestão nas organizações aprendentes) – Curso de Pós Graduação em Gestão nas organizações aprendentes, Universidade Federal da 50 Paraíba, João Pessoa, 2017. Disponível em: https://repositorio.ufpb.br/jspui/handle/tede/9770?locale=pt_BR. Acesso em: 10 jan. 2024.

PAZ, Herlane Chaves, et al. Internet das coisas: a vulnerabilidade do consumidor no compartilhamento de dados. **Revista de Tecnologia Aplicada (RTA)** v.12, n.1, jan./abr., 2023, p. 68-85. Disponível em: https://www.cc.faccamp.br/ojs-2.4.8-2/index.php/RTA/article/view/1965. Acesso em: 12 jan. 2024.

PIAI, Thami Covatti, et al. Quarta Revolução Industrial e a Proteção do indivíduo na Sociedade Digital: Desafios para o Direito. **Revista Paradigma**, Ribeirão Preto-SP, a. XXIV, v. 28, n. 1, p. 122-140, jan./abr. 2019. Disponível em: https://revistas.unaerp.br/paradigma/article/view/1444. Acesso em: 10 fev. 2024.

PINHEIRO, Patricia Peck. **Direito Digital**. 6. ed. São Paulo: Saraiva, 2016.

SOBRINHO, Nayara da Silveira. **A Proteção De Dados Pessoais No E-Commerce: Análise Da Aplicação Da Lgpd Diante Da Vulnerabilidade Do Consumidor.** 2019. Monografia (Graduação em Direito). Centro Universitário - Unifacig. Manhuaçu, Minas Gerais, 2019. Disponível em: https://pensaracademico.unifacig.edu.br/index.php/repositoriotcc/article/view/1745. Acesso em: 18 mar. 2024.

THE NEW YORK TIMES. **How Cambridge Analytica Exploited the Facebook Data of Millions | NYT**. Youtube, 9 abr. 2018. Disponível em: https://www.youtube.com/watch?v=mrnXv-g4yKU. Acesso em: 30 mar. 2024.

OLIVEIRA, Mariana. TSE usa conceito de fake news para mandar Facebook retirar postagens do ar. **Conjur**, 2018. Disponível em:

https://www.conjur.com.br/2018-jun-07/tse-manda-facebook-retirar-post-fake-news-ar/. Acesso em: 15 jan. 2024.

VITAL, Danilo. Em 5 anos, LGPD tem impacto regulatório, mas efeito prático é duvidoso. **Conjur**, 2023. Disponível em: https://www.conjur.com.br/2023-ago-14/anos-lgpd-muda-cultura-abre-horizonte-regulatorio/. Acesso em: 10 mar. 2024.

WHATSAPP BLOG. **Criptografia de ponta a ponta.** 2016. Disponível em: https://blog.whatsapp.com/end-to-end-encryption. Acesso em: 01 abr. 2024.

SUBMETIDO | *SUBMITTED* | *SOMETIDO* | 22/07/2024
APROVADO | *APPROVED* | *APROBADO* | 02/10/2024

REVISÃO DE LÍNGUA | *LANGUAGE REVIEW* | *REVISIÓN DE LENGUAJE*
Claudinei José De Oliveira

SOBRE OS AUTORES | *ABOUT THE AUTHORS* | *SOBRE LOS AUTORES*

DIEGO BIANCHI DE OLIVEIRA
Universidade Paranaense, Umuarama, Paraná, Brasil.
Doutor em Direito pela Universidade de Marília. Mestre em Direito Processual e Cidadania pela Universidade Paranaense (UNIPAR). Especialista em Direito Imobiliário pela Universidade Cândido Mendes e em Metodologia do Ensino Superior pelo Instituto Facuminas. Bacharel em Direito pela Universidade Estadual de Mato Grosso do Sul e em Administração pela Universidade Anhanguera-Uniderp. Professor da UNIPAR e da Universidade Estadual de Mato Grosso do Sul. Advogado. E-mail: odiegobianchi@gmail.com. ORCID: https://orcid.org/0000-0002-1456-9666

GUSTAVO CONSALTER MIEREZ VEGA
Universidade Estadual de Mato Grosso do Sul, Dourados, Mato Grosso do Sul, Brasil.
Bacharel em Direito pela Universidade Estadual de Mato Grosso do Sul. E-mail: gusconmv@gmail.com.