UNIVERSIDADE PRESBITERIANA MACKENZIE
FACULDADE DE DIREITO

DANIELE DIMAS RAMOS

PROTEÇÃO DE DADOS PESSOAIS E O PLANO NACIONAL DE INTERNET DAS COISAS (*IOT*) – ANÁLISE DA IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET DAS COISAS E SUA REGULAMENTAÇÃO

São Paulo
2020

DANIELE DIMAS RAMOS

PROTEÇÃO DE DADOS PESSOAIS E O PLANO NACIONAL DE INTERNET DAS COISAS (*IOT*) – ANÁLISE DA IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET DAS COISAS E SUA REGULAMENTAÇÃO

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Universidade Presbiteriana Mackenzie, como requisito parcial para a obtenção do título de bacharel em Direito.

ORIENTADOR: PROF. DR. JOÃO BOSCO COELHO PASIN

São Paulo

2020

DANIELE DIMAS RAMOS

PROTEÇÃO DE DADOS PESSOAIS E O PLANO NACIONAL DE INTERNET DAS COISAS (*IOT*) – ANÁLISE DA IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS NA INTERNET DAS COISAS E SUA REGULAMENTAÇÃO

Trabalho de Conclusão de Curso apresentado ao curso de Direito da Universidade Presbiteriana Mackenzie, como requisito parcial para a obtenção do título de bacharel em Direito.

Aprovado em

BANCA EXAMINADORA

_____

Prof. Dr. João Bosco Coelho Pasin
Universidade Presbiteriana Mackenzie

_____

_____

Aos meus pais, que sempre estiveram ao meu lado; aos meus avós Manoel e Rute, que sempre torceram pelo meu sucesso; à minha avó Rosa, *in memoriam*, que sempre estará presente nos meus pensamentos; ao meu irmão, pela parceria do dia a dia e por ser companhia nessa cidade fria; ao meu amor, Raphael, por acreditar em todo o meu potencial, pelo companheirismo e por nunca me deixar desistir; e principalmente à Deus, pelas oportunidades que Ele apresenta na minha vida.

AGRADECIMENTOS

À Deus, por colocar as oportunidades no meu caminho e dar-me capacidade para que eu faça bom proveito delas e permitir que eu finalizasse mais uma etapa da vida com a entrega deste Trabalho de Conclusão de Curso.

Ao professor Dr. João Bosco Coelho Pasin, a minha gratidão pela dedicação e apoio para o desenvolvimento deste trabalho.

Aos profissionais da saúde, que neste momento tão difícil se mantiveram fortes para que pudéssemos passar pelas dificuldades da pandemia sabendo que eles estão fazendo de tudo para nos manter seguros.

À todos que contribuíram para o sucesso da minha caminhada.

RESUMO

O presente trabalho tem por objetivo tratar dos impactos da proteção de dados e sua regulamentação no Brasil na elaboração do Plano Nacional de Internet das Coisas. Por serem questões extremamente recentes, observa-se uma falta de literatura específica a respeito do tema tratado. Assim, parte-se da análise da importância da proteção de dados pessoais, passando-se pela regulamentação da mesma realizada pela Lei Geral de Proteção de Dados para, por fim, analisar a importância de tal proteção na Internet das Coisas e na criação de sua regulamentação com o Plano Nacional de Internet das Coisas.

Palavras-Chaves: Plano Nacional de Internet das Coisa – Internet das Coisas – Proteção de Dados – Dados Pessoais – Lei Geral de Proteção de Dados

ABSTRACT

The purpose of the present essay is to analyze the impacts of data protection and its regulation in Brazil in the preparation of the National Internet of Things Plan. As they are extremely recent issues, there is a lack of specific literature on the topic addressed. Thus, it starts from the analysis of the importance of the protection of personal data, passing through its regulation carried out by the General Data Protection Law to, finally, analyze the importance of such protection in the Internet of Things and in the creation of its regulation with the National Internet of Things Plan.

Key-words: National Internet of Things Plan – Internet of Things – Data Protection – Personal Data – General Data Protection Law

SUMÁRIO

1. INTRODUÇÃO 9
2. PROTEÇÃO DE DADOS PESSOAIS 11
2.1. ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS 14
2.2. CONCEITO DE DADOS PESSOAIS APRESENTADO PELA LEI 17
2.2.1. Conceito e definição de dados pessoais sensíveis 18
2.3. PRESSUPOSTOS PARA O TRATAMENTO DE DADOS PESSOAIS 19
2.3.1. Coleta, armazenamento e tratamento de dados pessoais 19
2.3.2. Necessidade de base legal para realização do tratamento de dados pessoais 19
2.3.3. Tratamento diferenciado aos dados pessoais sensíveis 21
3. INTERNET DAS COISAS 23
3.1. ASPECTOS GERAIS DA INTERNET DAS COISAS 27
3.2. DISPOSITIVOS PARTE DO SISTEMA DE *IOT* 28
3.2.1. Cidades Inteligentes 29
3.2.2. Wearables 30
4. PLANO NACIONAL DE INTERNET DAS COISAS 32
4.1. REGULAMENTAÇÃO DA INTERNET DAS COISAS NO BRASIL 32
4.2. IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS NA *IOT* 33
4.2.1. Necessidade de criação da Autoridade Nacional de Proteção de Dados Pessoais 35
5. CERTIFICAÇÃO DOS DISPOSITIVOS DE *IOT* PELO INMETRO E ANATEL 36
5.1. ANÁLISE DE COMPLIANCE COM A LGPD E O PLANO NACIONAL DE IOT 37
5.1.1. Proteção contra o vazamento de dados pessoais 38
5.1.2. Necessidade do cumprimento das leis apresentadas 39
6. CONCLUSÃO 41
7. REFERÊNCIAS 42

1. INTRODUÇÃO

Assim como feito por Bruno Bioni em sua obra “Proteção de Dados Pessoais: a função e os limites do consentimento”, utilizaremos da licença poética para apresentar um cenário fictício, porém não muito longe da realidade vivida no presente século XXI. (BIONI, 2018, p. XXII - XXVII)

Imaginem a seguinte situação: é um sábado, e diferente de todos os outros dias da semana o despertador toca às 10 horas da manhã e não às 6:30 horas. Apesar disso, um café quentinho te espera, pronto para ser ingerido e preparado apenas 10 minutos antes pela máquina de café.

Mesmo você tendo acordado 3 horas e meia mais tarde do que de costume, o sistema da máquina de café estava programado de forma correta para preparar o café no horário correto. Isso porque você definiu um horário específico em seu celular para que o despertador tocasse, e, dessa forma, definiu um horário para que o café estivesse pronto.

Isso somente é possível porque seu celular e a máquina de café estão conectadas pela internet e compartilham dados entre si.

Além disso, sua geladeira já enviou uma lista de compras para o mercado mais próximo com todos os alimentos que faltam dentro dela e com aqueles que você definiu que seriam necessários para a próxima semana no seu aplicativo de compras.

Por estar acostumado com o seu estilo de vida e com suas preferências, o mercado te envia diversas propagandas sobre produtos em promoção, além de enviar amostras de produtos que parecem atender aos seus interesses juntamente com a ordem de compra que a geladeira enviou momentos antes.

Isso acontece porque o mercado armazena os dados de todas as suas compras e analisa os seus hábitos não só alimentares, mas de vida, e dessa forma, cria o seu perfil de compras.

É claro que este cenário vai além daquilo que já existe hoje, e o qual ainda demanda muito trabalho para ser alcançado. Entretanto, demonstra o quão importante apresenta-se este tema.

Apesar de não estarmos tão desenvolvidos, já possuímos diversos dispositivos que fazem parte do mundo da Internet das Coisas e do nosso dia a dia. Os *watches* são um ótimo exemplo, em que é possível enxergar um compartilhamento de dados gigantesco,

principalmente dados sobre a saúde do usuário, que ajudam a prevenir e combater doenças antes mesmo de chegarem a um patamar alarmante.

Entretanto, por mais que muitas vezes os dados sejam utilizados para o bem dos usuários, tais dados, na sociedade digital em que vivemos, podem ser vendidos e utilizados como moeda de troca por muitas empresas que trabalham no mundo da *IoT*, ou *Internet of Things.*

O que se tenta evitar com a legislação atual, é que estes dados sejam utilizados de maneira indiscriminada, sem que os seus titulares tenham conhecimento desta utilização.

Por este motivo, o presente trabalho procurar demonstrar a importância da proteção dos dados coletados e armazenados, de forma que a Internet das Coisas seja utilizada de maneira consciente e que seus usuários possuam a proteção adequada para que a *IoT* se expanda no Brasil de maneira segura.

Neste trabalho faremos então uma breve introdução ao direito à proteção de dados pessoais para, após isso, enfrentarmos os pormenores dos impactos causados por este direito na legislação criada no país para a regulamentação da Internet das Coisas.

2. PROTEÇÃO DE DADOS PESSOAIS

O chamado direito à proteção de dados pessoais, apesar de ter tomado conta do debate legislativo atual, remonta um período mais antigo da história, surgindo através do direito à privacidade, como apontado por Hugo Sauaia, a partir da definição sobre a inconstitucionalidade da Lei do Censo Alemã no ano de 1983:

> *"Mais difundido na Europa, o direito à proteção de dados pessoais surgiu fruto de decisão da Corte Constitucional Alemã sobre a inconstitucionalidade da Lei do Censo de 1983, já tendo sido incorporado nas Constituições de diversos países (Portugal, Eslovênia, Rússia, e na Espanha) e na Diretiva 95/46/CE, de 24 de outubro de 1995 da União Europeia (...)."* (SAUAIA, 2018, p. 3-4)

Tal lei continha códigos individuais de identificação que poderiam ser mantidos por um longo período e permitiriam a identificação das famílias que haviam fornecido tais dados, além de seu tratamento por métodos comparativos, o que foi considerado inconstitucional e violador do direito à privacidade pela Corte Constitucional Alemã, além de não contemplar um mecanismo de registro e armazenamento dos dados coletados compatível com a dignidade do homem. (SAUAIA, 2018, p. 106)

Apesar disso, em termos doutrinários, tal direito remonta um período ainda mais antigo da história, com um ponto de partida vindo através de um ensaio publicado nos Estados Unidos da América, conforme apontado por Maldonado:

> *"Em termos doutrinários, o conceito de privacidade tem seu ponto de partida no emblemático ensaio denominado "The right to privacy", de autoria de Samuel D. Warren e Louis D. Brandeis, publicado em* Harvard Law Review*, no ano de 1890" (MALDONADO, 2019, p.12)*

Isso serve para demonstrar que apesar da discussão estar em alta no momento atual em que vivemos, é um assunto tão importante que vem sendo discutido e, acima de tudo, tem tido seus impactos na área jurídica há muito tempo, principalmente a partir da Declaração Universal dos Direitos Humanos, que surgiu no contexto do pós-Segunda Guerra Mundial.

Em meio à discussão acerca dos direitos fundamentais, ficou consignado que todos estariam protegidos contra intromissões arbitrárias em sua própria vida, estabelecendo-se, assim o direito universal à privacidade.

> *"No contexto pós-Segunda Guerra Mundial, o mundo ocidental direcionou-se para o estabelecimento de direitos fundamentais, os quais restaram estabelecidos na Declaração Universal dos Direitos Humanos. No art. 12 foi consignado que "ninguém sofrerá intromissões arbitrárias na sua vida privada, na sua família, no seu domicílio ou na sua correspondência, nem ataques à sua honra e reputação. Contra tais intromissões ou ataques toda a pessoa tem direito à proteção da lei." (MALDONADO, 2019, p.13)*

Após isso, diversos textos legais declararam e protegeram o direito à privacidade, intimidade e proteção da vida privada. Tais como a Convenção Europeia dos Direitos do Homem e das Liberdades Fundamentais de 1950, o Pacto Internacional de Direitos Civis e Políticos de 1966, a Conferência Nórdica sobre o Direito à Intimidade de Estocolmo de 1967 e o Pacto de San Jose da Costa Rica, também conhecida como Convenção Americana sobre Direitos Humanos, de 1969. (MIRANDA, 2018, p. 62 – 66)

Dessa forma, vemos que ao passar dos anos, direitos protetivos à intimidade e proteção de dados foram sendo incluídos nos dispositivos legais de diferentes forças jurídicas, demonstrando a importância de tais direitos no contexto da evolução normativa e aprimoramento da democracia constitucional nos diversos países em que estes dispositivos possuíam força normativa.

Isso porque, como apontado por Sauaia, o direito à proteção de dados pessoais não é só mais um direito privado, mas sim é essencial para tal processo de aprimoramento e desenvolvimento da democracia constitucional. (SAUAIA, 2018, p. XV)

Tal apontamento tem como principal argumento o fato de que o direito à proteção da privacidade e proteção de dados pessoais age como forma de proteção das minorias e salvaguarda dos direitos destes grupos, que tendem a ser os mais prejudicados com o acesso irrestrito a dados pessoais e à esfera íntima dos indivíduos.

Isso acontece porque tais grupos tendem a ser discriminados e afetados negativamente, de forma mais concreta do que para indivíduos que não fazem parte de minorias, com a divulgação de dados sem a sua autorização ou conhecimento.

> *"A proteção à privacidade funciona novamente, neste ponto, como mecanismo de defesa da democracia. Age como mecanismo de salvaguarda das minorias, restringindo o acesso às informações que são da sua esfera mais íntima e cuja utilização desviada poderia permitir a sujeição dessas minorias a diferentes formas de segregação ou preconceito."* (SAUAIA, 2018, p.73-74)

Tudo isso serve para demonstrar que o direito à privacidade e à proteção de dados não é algo novo e de pouco importância, mas sim um direito essencial para a manutenção da democracia.

Trazendo todos esses aspectos para os dias atuais, vemos que, por conta do aumento da utilização da internet na vida cotidiana, a quantidade de dados pessoais de fácil acesso aumenta diariamente.

A revolução tecnológica trazida pela internet fez com que os titulares desses direitos previamente citados compartilhassem ainda mais dados pessoais a todo o momento. Houve, assim, um aumento gigantesco na produção de dados pessoais em um ambiente em que há pouco ou nenhum controle de privacidade e proteção de tais dados.

> *"Trata-se do radical aumento da produção e captação de dados pessoais, fomentada por esta intensa revolução tecnológica pela qual passa a humanidade, nesta quadra inicial do século XXI, e que torna a todos colaboradores e sujeitos deste processo de apropriação do conteúdo informacional."* (SAUAIA, 2018, p.7)

Por esse motivo, sentiu-se a necessidade de voltar às discussões antigas sobre as esferas de privacidade dos indivíduos na sociedade, bem como do compromisso estabelecido com a Declaração dos Direitos Humanos sobre a inviolabilidade da vida privada. (PINHEIRO, 2018, P.17)

Com essa necessidade em vista, e levando em conta o grande fluxo de dados que ocorre na Europa, por ser o polo concentrador dos países desenvolvidos, foi editada a Diretiva nº 95/46, que trazia certo regramento e indicações aos Estados-membros sobre o nível e segurança mínimos para o tratamento de dados pessoais e a segurança da informação.

Para a União Europeia, as Diretivas são quase como orientações para que os próprios Estados-membros legislem a respeito de alguma matéria. Nesse caso, após a edição da Diretiva nº 95/46 cada Estado-membro legislou sobre a proteção de dados de maneira isolada, porém, tal fato, ao passar dos anos e com o surgimento de novos parâmetros pela sociedade, ensejou dificuldades de harmonização, considerando que cada regramento jurídico, apesar de basear-se na mesma Diretiva, possuía suas próprias particularidades. (MALDONADO, 2019, p.14)

Assim, em 2012, anos após a edição da Diretiva citada acima, surgiu a proposta de criação de um Regulamento Geral sobre proteção de dados, que, diferente da Diretiva, teria força vinculativa por si só, não necessitando de qualquer ação por parte dos Estados-membros para que fosse efetivo dentro de suas jurisdições.

Tal Regulamento, após anos de discussões, foi aprovado em 2016, chamado de *General Data Protection Regulation* ("GDPR"), com *vacatio legis* de dois anos, entrando em eficácia apenas no ano de 2018.

O GDPR é, portanto, um regulamento que tem por objetivo estabelecer princípios norteadores para a coleta e tratamento de dados pessoais dentro da Europa e por países que tenham o interesse de fazer negócios com qualquer dos Estados-membros europeus.

Tem como base a necessidade de esclarecimento da importância do tratamento dos dados pessoais e a clareza e transparência referentes a qualquer atividade relacionada com a utilização de dados pessoais. O que demonstra Pohlmann no trecho abaixo:

> *"A GDPR é um regulamento orientado por princípios voltados ao usuário (ou o que chamamos de "titular" dos dados. Entre estes princípios, como referência, se encontram o princípio da necessidade, onde os dados só podem ser coletados mediante comprovação da necessidade dos mesmos; ou o princípio da transparência, onde o usuário têm o direito de saber, com clareza, para quê seus dados serão utilizados, com quem serão intercambiados, etc. O usuário também têm o direito de ser "esquecido", ou seja, solicitar que todos os seus dados sejam completamente deletados do sistema (seja um sistema informático, ou processo manual – papel)."* (POHLMANN, 2019, p. 26)

2.1. ASPECTOS GERAIS DA LEI GERAL DE PROTEÇÃO DE DADOS

Como visto acima, a proteção aos dados pessoais, não é uma novidade no debate jurídico nacional, assim como também não o é no cenário legislativo brasileiro. A Constituição Federal já em 1988 reconheceu direitos e garantias específicas relativos aos dados pessoais como o princípio da dignidade humana, a proteção aos direitos da personalidade, amparando o direito à liberdade de expressão, o direito à informação, a inviolabilidade da vida privada e da intimidade, a garantia do *Habeas Data*, entre várias outras garantias à privacidade e à intimidade.

> *"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;*
>
> *XI - a casa é asilo 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;*
>
> *XII - é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou instrução processual penal;" (BRASIL, 1988)*

Com o surgimento do GDPR e a exigência de que os demais países e as empresas que buscassem manter relações comerciais com a União Europeia adotassem níveis de proteção no mínimo equivalentes àqueles descritos no Regulamento, foi criada no Brasil a Lei Geral de Proteção de Dados Pessoais (LGPD), que, da mesma forma, busca proteger os direitos à privacidade e proteção de dados. (PINHEIRO, 2018, p. 18)

Além disso, ambas as legislações, como afirma Pinheiro "advém da evolução e expansão dos direitos humanos e resulta da atualização/adaptação de documentos internacionais de proteção aos direitos humanos" como amplamente demonstrado acima. PINHEIRO, 2018, p.50)

Publicada como Lei nº 13.709/2018, a princípio, entrará em vigor em maio de 2021[1], tendo suas sanções aplicadas apenas a partir de agosto de 2021[2], e é a legislação brasileira que regula as atividades de tratamento de dados pessoais e que também altera os artigos 7º e 16 do Marco Civil da Internet[3], regulando também a transferência e manipulação de dados pessoais por meio da internet.

A LGPD tem por objetivo garantir a todos a ampla informação sobre como empresas públicas e privadas tratam os dados pessoais de todos os brasileiros e daqueles que estejam em território brasileiro, ou seja, o modo e a qualidade da coleta, como esses dados são armazenados e tratados, por quanto tempo guardam e com quem compartilham.

> *"(...) a lei se aplica a todos aqueles que realizam o tratamento de dados pessoais, sejam organizações públicas ou privadas, pessoas físicas ou jurídicas, que realizam qualquer operação de tratamento de dados pessoais, independentemente do meio, que possa envolver pelo menos um dos seguintes elementos:*
>
> *(i) ocorrer em território nacional;*
> *(ii) que tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional;*
> *(iii) em que os dados tenham sido coletados no território nacional." (PINHEIRO, 2018, p.29)*

Importante salientar, portanto, que a LGPD não se baseia na nacionalidade do indivíduo detentor das informações (dados pessoais), pois, além deles, protege todo e qualquer dado pessoal que seja tratado em território brasileiro, referente a indivíduos localizados no território nacional ou que tenha sido coletado no Brasil.

> *"(...) por tratar de proteção dos dados pessoais dos indivíduos em qualquer relação que envolva o tratamento de informações classificadas como dados pessoais. (...) É uma regulamentação que traz princípios, direitos e obrigações relacionadas ao uso de um dos ativos mais valiosos da sociedade digital, que são as bases de dados relacionados às pessoas."* (PINHEIRO, 2018, p.15)

---

[1] "A princípio", pois a Medida Provisória nº 959/2020 aumentou a *vacatio legis* da LGPD para que a mesma passe a vigorar apenas a partir de 03 de maio de 2021. Entretanto, tal MP precisa ainda passar pelo crivo do Congresso Nacional, para garantir que seja transformada em lei, o que não aconteceu até a finalização deste trabalho. Caso a MP mencionada não seja aprovada pelo Congresso, a LGPD vigoraria a partir de agosto/2020 como estabelecia seu texto antes da publicação da tal Medida Provisória.

[2] As sanções, definidas nos artigos 52, 53 e 54 da LGPD tiveram sua *vacatio legis* prorrogada pela Lei nº 14.010/2020. Sendo assim, só poderão ser aplicadas a partir de agosto/2021.

[3] Lei que regulamenta o uso da Internet no Brasil por meio da previsão de princípios, garantias, direitos e deveres para quem usa a rede, bem como da determinação de diretrizes para a atuação do Estado.

Dessa forma, uma empresa brasileira que colete e trate dados no Brasil, mas que tenha alguma plataforma que permita que seu cliente seja de qualquer cidadania, nacionalidade ou residência, e, portanto, podendo ser um indivíduo europeu ou residente da União Europeia acaba atraindo, em termos de aplicação de leis e jurisdição para a sua operação, não só a regulamentação nacional (LGPD) como também a regulamentação europeia (GDPR). (PINHEIRO, 2018, p.30)

Seu texto determina que todos os dados pessoais (informação relacionada à pessoa natural identificada ou identificável, como nome, idade, estado civil, documentos) necessitam de uma base legal para seu tratamento, do qual trataremos mais adiante, de forma a prezar pela boa-fé e transparência no tratamento de dados pessoais.

> *"O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios (...)"* (PINHEIRO, 2018, p.16)

Basicamente, a lei pretende coibir o uso indiscriminado de dados pessoais coletados pelas empresas e garantir o direito de estar ciente do titular dos dados sobre como será feito o tratamento das informações obtidas de todos os cidadãos e para qual finalidade específica elas serão usadas.

Assim como aponta Patrícia Pinheiro, a lei pretende fortalecer a proteção da privacidade do titular dos dados tratados, bem como tutelar diversos outros direitos garantidos na Constituição Federal:

> *"Portanto, a legislação visa fortalecer a proteção da privacidade do titular dos dados, a liberdade de expressão, de informação, de opinião e de comunicação, a inviolabilidade da intimidade, da honra e da imagem e o desenvolvimento econômico e tecnológico."* (PINHEIRO, 2018, p.31)

A lei determina que qualquer empresa que realize tratamento de dados[4] deve manter um registro do tratamento dos dados pessoais com suas especificações de base legal e necessidade de utilização de tais dados, sendo o tratamento dos dados pessoais pautado em fundamentações claras e legítimas, demonstrando uma grande preocupação com os mecanismos de controle e proteção de tais dados, reunindo um grande número de itens de controle que visam garantir o

[4] "Toda operação realizada com algum tipo de manuseio de dados pessoais: coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, edição, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração". (PINHEIRO, 2018, p.25)

cumprimento das garantias que se fundamentam nos direitos humanos. (PINHEIRO, 2018, p.30)

Além disso, como dito acima, a LGPD preza pela boa-fé daqueles que realizam o tratamento de dados, trazendo em si a possibilidade de aplicação de diversas penalidades, com o intuito de reforçar a importância de seu devido cumprimento.

> *"A LGPD destaca que o tratamento de dados pessoais deve observar a boa-fé e possuir penalidade, limites, prestação de contas, garantir a segurança por meio de técnicas e medidas de segurança, assim como a transparência e a possibilidade de consulta aos titulares."* (PINHEIRO, 2018, p.64)

Assim, levando em conta a possibilidade de aplicação de tais penalidades, a LGPD pressupõe a adoção de medidas de segurança por parte de seus agentes de tratamento.

Uma vez implementadas de maneira correta, tais medidas visam mitigar ao máximo os riscos e vazamentos de dados, sendo, entretanto, impossível garantir com absoluta certeza que tais vazamento não ocorram.

> *"Dessa maneira, para que o tratamento de dados pessoais seja assegurado de maneira eficiente e suficiente, cabe aos agentes responsáveis por esse tratamento a adoção de medidas de segurança técnicas adequadas e específicas para esse tipo de procedimento." (PINHEIRO, 2018, p.103)*

Apesar disso, utilizando-se de medidas de segurança técnicas adequadas e com o cumprimento integral da legislação, torna-se muito mais segura e transparente a realização de qualquer atividade de tratamento de dados pessoais.

2.2. CONCEITO DE DADOS PESSOAIS APRESENTADO PELA LEI

A LGPD define dados pessoais como toda "informação relacionada a pessoa natural identificada ou identificável". Como pode ser visto, essa é uma definição bem ampla de dados pessoais. Entretanto, a LGPD segue os mesmos passos que o GDPR, que define dados pessoais como "*any information relating to an identified or identifiable natural person*" (qualquer informação relativa a uma pessoa natural identificada ou identificável). (UNIÃO EUROPÉIA, 2016)

Assim, observa-se um padrão, iniciado com o GDPR, de apresentar um conceito bastante amplo de dados pessoais, e, dessa forma, abarcar uma grande quantidade de dados sob o chapéu de proteção de suas respectivas legislações.

Como observa Maldonado, ambas as leis, por trazerem uma definição tão aberta de dados pessoais, tornam a análise de enquadramento baseada no caso a caso:

> *"(...) observa-se que nem a LGPD nem o GDPR trazem uma listagem do que poderia constituir um dado pessoal, na medida em que a avaliação deve sempre ser levada a efeito de maneira contextual. Se uma determinada informação potencialmente é capaz de tornar uma pessoa identificável, então ela pode vir a caracterizar-se como dado pessoal naquele específico contexto." (MALDONADO, 2019, p.15)*

Dessa forma, utilizando o exemplo trazido por Pohlmann, a cor do cabelo, a altura de uma pessoa, a cor de sua pele e etc, por si só, não são dados pessoais, pois não identificam uma pessoa. Porém, uma vez trabalhados em conjunto, podem facilmente identificar um indivíduo:

> *"Um dado como a cor do cabelo, sozinho, não é um dado que aponte, precisamente, a uma pessoa. No entanto, em conjunto com outras informações permite uma identificação inequívoca, a uma pessoa "identificável". Assim, a cor do cabelo, em um banco de dados com as informações do exemplo, deve ser tratada, também, como* Dado Pessoal*."* (POHLMANN, 2019, p. 48)

Por esse motivo, não há como apontar com precisão quais classes de dados podem ser considerados dados pessoais, tendo em vista que essa qualificação depende da forma como os dados são relacionados e de sua capacidade ou não de identificar o titular dos dados citados.

> *"No entanto, existirão tabelas com dados que, de forma individual, não apontam especificamente a um indivíduo, mas, em conjunto com outras informações, terminam por oferecer uma identificação única de seu titular." (*POHLMANN, 2019, *p.47)*

2.2.1. Conceito e definição de dados pessoais sensíveis

Diferente do conceito de dados pessoais, o texto da lei demonstra exatamente quais informações são consideradas dados pessoais sensíveis: "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".

De acordo com Pinheiro, dados sensíveis são aqueles que:

> *"[...] estejam relacionados a características da personalidade do indivíduo e suas escolhas pessoais, tais como origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente a saúde ou a vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural*". (PINHEIRO, 2018, p. 26)

A principal premissa da LGPD é a proteção de dados pessoais, sendo que os dados pessoais sensíveis possuem um tratamento diferenciado por serem consideradas informações com potencial discriminativo maior.

> *"Os dados sensíveis merecem tratamento especial porque em algumas situações a sua utilização mostra-se indispensável, porém o cuidado, o respeito e a segurança com tais informações devem ser assegurados, haja vista que – seja por sua natureza, seja por suas características – a sua violação pode implicar riscos significativos em relação aos direitos e às liberdades fundamentais da pessoa."* (PINHEIRO, 2018, p.)

Por possuírem este potencial discriminativo maior do que os dados pessoais no geral, os dados que são caracterizados como sensíveis são aqueles que possuem uma capacidade maior de causar danos aos seus titulares quando divulgados. (POHLMANN, 2019, p.48)

Assim, a LGPD estabelece pressupostos distintos para o tratamento desses dados pessoais sensíveis, por justamente levar em conta este potencial lesivo maior presente naqueles dados classificados como sensíveis.

2.3. PRESSUPOSTOS PARA O TRATAMENTO DE DADOS PESSOAIS

2.3.1. Coleta, armazenamento e tratamento de dados pessoais

Não da mesma forma como feito para a definição de dados pessoais, porém semelhante, a LGPD define tratamento de dados pessoais como "toda operação realizada com dados pessoais" de forma bem abrangente.

Conforme apontado por Maldonado, a definição de tratamento de dados pessoais traz uma infinidade de operações que podem ser realizadas com tais dados:

> *"(tratamento é) assim entendido como toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Note-se que a conceituação é extremamente abrangente e inclui todas as operações relativas aos dados pessoais, desde sua coleta até o término propriamente dito. No mais, é importante destacar que o mero armazenamento está inserido, por definição legal, como atividade de tratamento, de sorte que a simples posse de dados determina, por si só, a observância dos dispositivos legais." (MALDONADO, 2019, p.16)*

Dessa forma, basicamente qualquer atividade envolvendo dados pessoais pode ser considerada tratamento para fins de enquadramento à LGPD, inclusive a própria coleta e armazenamento dos dados, que muitas vezes não são considerados como tratamento.

2.3.2. Necessidade de base legal para realização do tratamento de dados pessoais

O tratamento de dados pessoais não foi proibido pela lei, entretanto, foi estabelecido que tal tratamento deve estar sempre baseado em determinadas situações, o que chamamos de "bases legais" para o tratamento de dados pessoais.

> *"Para o tratamento de dados pessoais, a LGPD estabelece alguns requisitos, ou bases legais, mediante os quais se permite que os dados sejam processados, com a observância dos demais artigos de Lei, em especial, dos princípios de que falamos anteriormente."* (POHLMANN, 2019, p.73)

Assim como no GDPR, a LGPD estabeleceu algumas bases legais, entretanto, aumentou a quantidade de situações em que este tratamento pode acontecer, incluindo situações que o legislador europeu não havia inserido no âmbito de atuação do GDPR. (MALDONADO, 2019, p.20)

Abaixo apresentamos as bases legais definidas pela LGPD para o tratamento de dados pessoais no geral:

> *"Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:*
> *I - mediante o fornecimento de consentimento pelo titular;*
> *II - para o cumprimento de obrigação legal ou regulatória pelo controlador;*
> *III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;*
> *IV - para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;*
> *V - quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;*
> *VI - para o exercício regular de direitos em processo judicial, administrativo ou arbitral, esse último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*
> *VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;*
> *VIII - para a tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária;*
> *IX - quando necessário para atender aos interesses legítimos do controlador ou de terceiro, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou*
> *X - para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente."* (BRASIL, 2018)

Não entraremos no mérito do que significa cada uma das bases legais e como elas podem ser utilizadas, pois esta seria uma análise para outro trabalho. Entretanto, importante ressaltarmos que, diferente do que se tem visto em discussões acerca da LGPD, a base legal chamada de consentimento não é, de forma alguma, tratada pela lei como principal ou "objetivo" a ser alcançado por aqueles que desejam realizar o tratamento de dados pessoais.

O consentimento é, na verdade, apenas mais uma situação em que é possível o tratamento de dados, sendo, por muitas vezes, considerada a base legal mais difícil e não adequada para a maioria das operações de tratamento.

Nesse sentido, Maldonado aponta ainda que, o consentimento pode ser considerado a base legal mais complexa de todas, pois coloca o titular dos dados pessoais em uma posição de controle, competindo a ele a decisão de aceite ou não das condições de tratamento de seus dados:

> *"Ressalte-se, ainda, que, ao contrário de um mito criado, o consentimento não ostenta preponderância sobre as demais bases legais, consistindo ele, aliás, na base mais complexa, pois é a única que de fato aloca na pessoa do titular a possibilidade da existência do tratamento." (MALDONADO, 2019, p.20)*

2.3.3. Tratamento diferenciado aos dados pessoais sensíveis

Conforme dito acima, em relação aos dados pessoais sensíveis a lei estabeleceu um conjunto de bases legais distintas:

> *"Art. 11. O tratamento de dados pessoais sensíveis somente poderá ocorrer nas seguintes hipóteses:*
> *I - quando o titular ou seu responsável legal consentir, de forma específica e destacada, para finalidades específicas;*
> *II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:*
> *a) cumprimento de obrigação legal ou regulatória pelo controlador;*
> *b) tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;*
> *c) realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;*
> *d) exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem) ;*
> *e) proteção da vida ou da incolumidade física do titular ou de terceiro;*
> *f) tutela da saúde, exclusivamente, em procedimento realizado por profissionais de saúde, serviços de saúde ou autoridade sanitária; ou*
> *g) garantia da prevenção à fraude e à segurança do titular, nos processos de identificação e autenticação de cadastro em sistemas eletrônicos, resguardados os direitos mencionados no art. 9º desta Lei e exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais." (BRASIL, 2018)*

Não completamente diferente das bases legais para o tratamento de dados pessoais, porém possível de verificar que o legislador entendeu ser necessário uma cautela maior para o tratamento de dados pessoais sensíveis.

Por esse motivo, o legislador retirou de tais bases legais a possibilidade de tratamento de dados sensíveis puramente quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados.

Isso foi feito justamente por conta do potencial lesivo desses dados, tentando evitar que eles sejam utilizados de maneira irresponsável.

Além disso, conforme apontado por Pinheiro, independentemente da base legal utilizada é necessário que os agentes de tratamento de dados publicizem, ou seja, tornem pública a realização do tratamento de tais dados, bem como sua necessidade. (PINHEIRO, 2018, p.)

Dessa forma, pretende-se manter o titular dos dados ciente da utilização de seus dados pessoais, para que assim possa “garantir” que estes estejam sendo utilizados apenas para a finalidade informada, sem que haja o uso indiscriminado destes dados para finalidades desconhecidas pelos titulares.

3. INTERNET DAS COISAS

Passemos a agora à explicação do conceito de Internet das Coisas ou *IoT* (do inglês *Internet of Things)* e sua apresentação histórica, que, como a proteção de dados, não é um termo recente para que possamos, após, analisar os impactos da proteção dos dados pessoais neste ambiente complexo de *IoT*.

Há muitos anos já se fala em um sistema de comunicações não só entre computadores, mas que também interliga coisas e pessoas.

> "*Há bastantes anos que se antevê a possibilidade de os dispositivos (e não só os computadores) se poderem ligar à Internet e comunicarem em rede. Nos anos 90, a tecnologia Java surgiu como promessa de um mundo de dispositivos diversos ligados em rede, a correr versões próprias daquela tecnologia e a comunicar com servidores ou com pessoas*." (COELHO, 2017, p. 2)

Sabemos que a Internet, por si só, foi inventada na década de 80, com a criação da World Wide Web (www), e desde lá sofreu diversas mudanças juntamente com a evolução da comunicação e conectividade do mundo.

> *"The Internet as we know it today was invented in 1989 when Sir Timothy John Berners-Lee created a system for hyperlinked information—the world wide web—and made the first web browser while at CERN in Switzerland in 1990."* (A Internet como a conhecemos hoje foi inventada em 1989, quando Sir Timothy John Berners-Lee criou um sistema para informações com hiperlink - a rede mundial de computadores - e criou o primeiro navegador da Web no CERN, na Suíça, em 1990.) *(UNEMYR, 2017, posição 173-175)*

Como apontado por Magnus Unemyr, a primeira onda de revolução da internet se apresentou com o aumento dos computadores pessoais. Nesse momento, os computadores começaram a passar de ferramentas somente profissionais para ferramentas pessoais, aumentando, assim, seu alcance.

A segunda onda se deu com a transformação dos desktops, produtos fixos, para produtos móveis (como smartphones e tablets), que aumentou o uso da internet pela sua capacidade de acesso a todo e qualquer momento e em quaisquer situações e lugares.

Atualmente, encontramo-nos na terceira onda de revolução da internet, chamada de Internet das Coisas, em que todas as coisas eletrônicas estão sendo conectadas à internet, o que traz cada vez mais funcionalidades para os produtos eletrônicos que já conhecemos.

Além disso, Unemyr aponta que a quarta onda, pode-se dizer, será a "Internet de Tudo", em que além das coisas, pessoas e animais também estarão conectados ao sistema integrado da internet.

> *"The first wave of the Internet revolution was the growth of personal computers. The second wave was then the Internet came to people using mobile devices. We are now at the third wave, in which all electronic things will become connected. Arguably, the fourth wave will be the Internet of Everything, in which even people and animals will be connected through wearable and surgically implanted sensors."* (A primeira onda da revolução da Internet foi o crescimento de computadores pessoais. A segunda onda foi então a Internet chegou às pessoas que usam dispositivos móveis. Estamos agora na terceira onda, na qual todas as coisas eletrônicas serão conectadas. Indiscutivelmente, a quarta onda será a Internet de Tudo, na qual até pessoas e animais serão conectados através de sensores vestíveis e implantados cirurgicamente.) *(*UNEMYR, 2017, posição 177-180)

Com relação à designação Internet das Coisas, como dito acima, esse não é um termo novo, pelo contrário, foi utilizado pela primeira vez em 1999, com o intuito de designar a internet que começava a conectar não só computadores, mas também objetos físicos.

> *"A designação Internet of Things foi utilizada em 1999 pela primeira vez por Kevin Ashton, um empresário e pioneiro da tecnologia com bastante trabalho realizado na área do RFID (Radio-Frequency IDentification) e dos sensores. O conceito que estava subjacente à designação IoT era o de uma visão da Internet conectada ao mundo físico através de um universo de sensores e atuadores." (COELHO, 2017, p. 8)*

A utilização do sistema RFID nos Estados Unidos para o controle de estoques, no início de 2005, marcou "o início do conceito da Internet das Coisas", como afirmou Kevin Ashton. Isso ocorreu, pois, o Walmart e o Departamento de Defesa dos Estados Unidos exigiram que o RFID fosse inserido nas etiquetas dos paletes de seus produtos para um controle maior da cadeia de abastecimento dos Estados Unidos. (DIAS, 2016, posição 284-290)

No mesmo ano houve a publicação do primeiro relatório pela União de Telecomunicações (ITU) sobre a Internet das Coisas. O relatório sugeria que a Internet das Coisas poderia, como apontado por Dias, "conectar os objetos do mundo, tanto de forma sensorial como inteligente, por meio da combinação de tecnologias, tais como a RFID, para identificação única e exclusiva de cada objeto, sensores e redes de sensores sem fio, sistemas embarcados e nanotecnologia." (DIAS, 2016, posição 290-295)

Assim, ficou claro que a internet havia passado da época em que somente computadores (independentemente de seu tamanho) estavam conectados a ela, passando para o momento em que objetos físicos passavam a integrar a rede complexa da internet.

A internet começou a se estender à um nível que não só pessoas, mas também coisas são conectadas a ela. Dessa forma, vemos que produtos que anteriormente pareciam apenas delírios longínquos de cientistas a frente de seu tempo viram realidade neste mundo em que a informação é valiosíssima.

Neste interim, Sinclair afirma que:

> "À medida que a internet estender seu alcance a objetos físicos e se tornar também a Internet das Coisas, não só a Internet das Pessoas, ela reconfigurará todos os setores que estiverem no percurso. O que é hoje um produto futurista logo será lugar comum. A IoT se converterá em parte integrante de todo empreendimento de negócios e de cada produto de consumo, comercial, industrial e de infraestrutura." (SINCLAIR, 2018, p. 21)

O grande efeito que essa mudança traz é justamente a possibilidade cada vez maior de uso inadequado dos dados coletados no ambiente de internet que todos conhecemos. É muito difícil navegar por 2 ou 3 páginas sem que em ao menos uma delas seja solicitado que você inclua algum dado pessoal (habilitação de cookies, inclusão de e-mail, nome, idade etc).

Neste sentido, considerando a utilização da internet em aparelhos que adquiriram funções diversas da incialmente pensadas para tais objetos, nos deparamos com uma realidade em que os dados coletados por esses aparelhos estão cada vez mais vulneráveis.

Apesar disso, os organismos internacionais ainda abordavam pouquíssimo a tecnologia relacionada à Internet das Coisas, entretanto, esse fato não invalidava o fato de que a cada dia mais e mais objetos físicos conectavam-se à internet. Já em 2009, estimava-se que havia mais objetos conectados à internet do que pessoas no mundo:

> *"Contudo, o facto de os grandes organismos internacionais falarem pouco no conceito não invalidava que cada vez mais dispositivos se fossem ligando à rede. Segundo alguns relatórios de fabricantes em 2009 passou a haver mais "coisas" ligadas à Internet do que pessoas (em 2010 havia um total de 12 500 milhões de objetos conectados à Internet, quase o dobro da população mundial)."* (COELHO, 2017, p. 9)

> *"Em 2009, segundo a Cisco IBSG, Internet Business Solutions Group, havia mais objetos, considerando smartphones, tablets e computadores pessoais, conectados que a própria população mundial. Portanto, este ano foi apontado por muitos autores como o ano de nascimento da Internet das Coisas."* (DIAS, 2016, posição 306-314)

Dessa forma, considerando a proporção em que se encontrava, começou-se a abordar a Internet das Coisas como um ecossistema que ia muito além da comunicação *machine-to-machine,* integrando máquinas, coisas e pessoas:

> *"Mais do que se falar em comunicação entre máquinas, começou a falar-se de um ecossistema mais amplo, que abrange máquinas, pessoas, sistemas e dados unidos pelas redes de comunicação, e utilizou-se a designação IoT para denominar a realidade da miríade de dispositivos que hoje se ligam à Internet, com os objetivos mais diversos."* (COELHO, 2017, p. 3)

Assim, a partir dos anos 2010, justamente pela quantidade de objetos conectados e pelo alcance de seu significado e ecossistema, a Internet das Coisas passou a ser considerada uma das tecnologias mais em voga:

> *"Em 2011 a IoT era considerada pela Gartner uma das tecnologias mais em voga e, em 2014, atingiu mesmo o topo do chamado Peak of inflated expectations, uma das*

> *fases do conhecido indicador Hype cycle da mais famosa empresa de análise de TI do mundo."* (COELHO, 2017, p. 9)

Com tudo isso em mente, e considerando a importância demonstrada acima que a *IoT* adquiriu ao longo dos anos, passamos a nos aprofundar no real significada do termo Internet das Coisas e suas aplicações.

Aponta Coelho que para o empresário Kevin Ashton, quem definiu o conceito de *IoT*, a Internet das Coisas é um sistema capaz de interligar o mundo real e o virtual, "criando um mundo mais inteligente em diferentes segmentos da sociedade". (DIAS, 2016, posição 249-252)

Além disso, interliga dispositivos de computação (computadores, máquinas, pessoas, animais ou objetos) em um sistema capaz de "comunicar e transferir dados sem qualquer intervenção humana." (COELHO, 2017, p. 2)

A Internet das Coisas, portanto, é considerado um sistema que se utiliza da comunicação entre máquinas, sensores e utensílios para a captação de dados a partir da internet, tão disseminada nos dias atuais.

> *"A internet da coisas, à parte maiores rigores semânticos, é um termo que acaba evocando o aumento das comunicação entre máquinas pela internet (M2M, ou machine-to-machine, que recentemente ultrapassou em volume a comunicação interpessoal pela internet), o desenvolvimento de diversos utensílios (desde os prosaicos exemplos das geladeiras ou torradeiras ligadas à internet), além de microdispositivos, como sensores que, dispostos das mais diversas maneiras para captar dados a partir de seu ambiente, tornam-se partes integrantes da internet" (Danilo Doneda, prefácio MAGRINI, p.11)*

Como afirma Magrini, o objetivo central desse sistema é "a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia", justamente por meio da coleta e análise dos dados de seus usuários. (MAGRINI, 2018, p.12)

> *"De maneira geral, pode ser entendido como um ambiente de objetos físicos interconectados com a internet por meio de sensores pequenos e embutidos, criando um ecossistema de computação onipresente (ubíqua), voltado para a facilitação do cotidiano das pessoas, introduzindo soluções funcionais nos processos do dia a dia. O que todas as definições de IoT têm em comum é que elas se concentram em como computadores, sensores e objetos interagem uns com os outros e processam informações/dados em um contexto de hiperconectividade." (MAGRINI, 2018, p.12)*

Em suma, podemos afirmar que a Internet das Coisas é uma rede que conecta objetos físicos, de origens diversas, e que possibilita a troca de informações e dados captados por e entre eles nos dois sentidos, é uma via de mão dupla.

> *"Em termos mais genéricos, pode-se designar a IoT como uma rede de objetos físicos, incluindo dispositivos eletrônicos, sensores, computadores, veículos, edifícios, entre muitos outros objetos, em que os objetos têm eletrônica embebida,*

> *software, sensores e conectividade de rede, possibilitando a troca de informações (nos dois sentidos) entre eles."* (COELHO, 2017, p. 3)

3.1. ASPECTOS GERAIS DA INTERNET DAS COISAS

Apesar de já termos nos adentrado bastante no significado do conceito de Internet das Coisas, passamos agora a aclarar os aspectos gerais de tal sistema e como ele se mostra presente no dia a dia da sociedade atual.

Como aponta Unemyr, o conceito de Internet das Coisas é sobre conectar quase tudo à internet, exemplos típicos seriam os carros, micro-ondas, fechaduras, sistemas de aquecimento etc. que possuem facilidades conectadas à internet que facilitam e ampliam seu uso, de modo a facilitar ainda mais a vida de seus usuários. (UNEMYR, 2017, posição 183-185)

Com isso em mente, Magrini salienta que "a expressão internet das coisas se refere basicamente a objetos que contêm sensores conectados que captam e tratam informações". (MAGRINI, 2018, p.20)

Devemos então considerar que o sistema de Internet das Coisas tem como um de seus principais aspectos o enorme volume de dados coletados e tratados para que as suas funcionalidades atendam ao seu objetivo principal.

Por esse motivo, um dos desafios mais iminentes da tecnologia de Internet das Coisas é justamente a enorme quantidade de dados, em sua maioria dados pessoais, que são gerados pela utilização de tal sistema.

Assim, como afirma Coelho, essa enorme quantidade de dados acaba por potencializar a utilização de tecnologias como o *Big Data,* que facilita a análise e processamento de volumes de dados tais quais os produzidos no ambiente de *IoT*.

> *"A IoT, com os seus muitos milhares de milhões de objetos ligados na rede, vem trazer um mundo de possibilidades novas para os sistemas informáticos, mas há alguns desafios tecnológicos para vencer. Um dos mais significativos resulta da quantidade de dados que os dispositivos podem gerar, inundando os sistemas de dados e dificultando a obtenção de estatísticas analíticas. Isto potencia a utilização de tecnologias modernas como o Big Data, uma tecnologia de processamento de dados que é adequada para grandes volumes de dados."* (COELHO, 2017, p. 7)

Isso significa que a *IoT* se utiliza de uma quantidade massiva de dados para realizar suas evoluções, trazendo resposta para diversos problemas atuais, inclusive, com grande investimento por parte do setor privado.

Dessa forma, é considerada como um interessante ponto de investimento para a procura de soluções para os desafios atuais das gestões públicas, bem como oportunidade de crescimento por parte do setor privado, que vê nela uma grande oportunidade de expansão.

> *"(...) a IoT vem recebendo fortes investimentos do setor privados e surge como possível solução diante dos novos desafios de gestão pública, prometendo, a partir do uso de tecnologias integradas e do processamento massivo de dados, soluções mais eficazes para problemas como poluição, congestionamentos, criminalidade, eficiência produtiva, entre outros."* (MAGRINI, 2018, p.24)

Nesse contexto, já é possível enxergar a utilização da *IoT*, de forma progressiva, em diversos setores da economia, o que deixa cada vez mais clara essa visão de que esse sistema é visto como a grande oportunidade de investimento de um futuro bem próximo.

> *"É a progressiva automatização de setores inteiros da economia e da vida social com base na comunicação máquina-máquina: logística, agricultura, transporte de pessoas, saúde, produção industrial e muitos outros."* (Maximiliano Martinhão, apresentação MAGRINI, 2018, p.15)

3.2. DISPOSITIVOS PARTE DO SISTEMA DE *IOT*

Diante deste contexto, podemos dizer que a cada vez mais, objetos comuns serão incluídos no sistema de Internet das Coisas, adquirindo "*sofisticação tecnológica*" (Danilo Doneda, prefácio MAGRINI, p.12) que os conecta à rede da internet.

Esses objetos são o meio pelo qual a *IoT* se manifesta, e são os, assim chamados, dispositivos que fazem parte do sistema de Internet das Coisas, juntamente com a própria internet.

Como aponta Sinclair, esses produtos vão muito além de um produto inteligente, são produtos que fazem parte de um sistema, e como tanto, trocam informações entre si e entre a internet, explorando, assim, toda sua capacidade tanto como objeto físico como quanto objeto conectado. (SINCLAIR, 2018, p. 31)

Assim, até mesmo os objetos mais comuns podem se transformar em dispositivos parte do sistema de *IoT*, se incluída em sua funcionalidade inicial a possibilidade de este objeto trocar informações com o mundo virtual por meio da internet e, dessa forma, atribuir uma facilidade ainda maior à sua utilização.

Vejamos o exemplo abaixo:

> *"Por exemplo, uma máquina de lavar roupa com um equipamento deste tipo incluído pode ligar-se à Internet, comunicar com um sistema central, informar que a temperatura ou a humanidade estão demasiado elevadas, informar que já terminou de lavar ou ser instruída para começar a lavar." (COELHO, 2017, p. 6)*

Nesse caso, o usuários de tal máquina de lavar, além de utilizar ela em sua funcionalidade principal (lavar a roupa), também poderá, por meio da internet, regular sua temperatura, para que suas roupas tenham uma vida útil maior, ou ser avisado de que a roupa já pode ser retirada, mesmo que não esteja próximo ao objeto.

Entretanto, nem só de funcionalidades interessantes vivem os dispositivos de *IoT*, por esse motivo, divide-se tais objetos em duas categorias: internet das coisas úteis e internet das coisas inúteis.

> *"Com o objetivo de distinguir os produtos da IoT por sua utilidade, alguns estudos vêm sendo desenvolvidos com base na diferenciação entre internet das coisas úteis e internet das coisas inúteis. Produtos incomuns, como garrafas térmicas com sensores, geladeiras com Twitter e persianas conectadas, estariam no rol de coisas que possivelmente se contrapõem à internet das coisas úteis, termo difundido pelo blog de tecnologia MeioBit." (MAGRINI, 2018, p.47)*

Isso significa que alguns objetos são transformados em dispositivos apenas para terem seus valores aumentados, uma vez que suas "funcionalidades *IoT*" não fazem realmente uma diferença e não trazem soluções inteligentes realmente funcionais.

> *"O conceito de internet das coisas inúteis relaciona-se ao posicionamento crítico sobre a adaptação de tecnologia avançadas em objetos sem que haja necessidade para tanto, visto que tornar um objeto apenas inteligente pode complicar seu uso e encarecer o produto, inexistindo um aprimoramento útil. Em diversos casos, o objeto analógico mais simples, sem tecnologia avançada envolvida, atende suficientemente ao consumidor, sem precisar ser algo high tech, podendo custar menos e ter uma utilização facilitada." (MAGRINI, 2018, p.47)*

Abaixo trataremos de dois exemplos, que consideramos os mais próximos à nossa realidade, de como os dispositivos incluídos nesse sistema se apresentam na sociedade e podem ser utilizados por ela.

3.2.1. Cidades Inteligentes

O conceito de cidades inteligentes trazido pela Internet das Coisas abrange a infraestrutura local de uma cidade comum.

Pode-se dizer que a conexão de políticas públicas com a análise de dados coletados por sistemas de segurança ao redor de uma cidade transforma tal sistema em uma cidade inteligente.

A ideia dessa aplicação é se utilizar de tecnologias de informação para coleta e análise de dados para uma gestão de infraestruturas públicas da forma mais inteligente possível, aplicando-se ativos onde mais se mostrar necessário.

> *"O conceito de cidade inteligente (smart city) consiste numa visão de integração entre múltiplas tecnologias de informação, com o objetivo de gerir os ativos das cidades da forma mais inteligente possível. O propósito é utilizar tecnologias de*

> *informação para gerir infraestruturas públicas de forma integrada, sejam elas estradas, parques de estacionamento, escolas, centrais de energia, hospitais, tribunais, esquadras, etc. A ideia é obviamente monitorizar e gerir, abrindo, portanto, um vasto leque de oportunidades para sistemas baseados em IoT." (COELHO, 2017, p. 70)*

Dessa forma, é possível realizar uma análise geral de dados coletados ao redor de uma determinada cidade para designação de pontos e infraestruturas específicas em que seja necessária a inclusão ou adaptação de recursos e equipamentos urbanos para melhoria da qualidade de vida e segurança daquela cidade ou ponto específico, conectando "equipamentos urbanos com os habitantes e com os meios de transporte." (SINCLAIR, 2018, p. 22)

3.2.2. Wearables

Além das cidades inteligentes, um dos exemplos mais fáceis de se encontrar e com mais utilização, no momento atual, de dispositivo parte do sistema de coisas conectadas à internet são os *wearables.*

Mais do que simples peças de roupas e acessórios comuns, os *wearables* são objetos de vestuário conectados à internet que possuem funções de controle de pulsação, análise de gasto calórico, controle de qualidade de sono, análise de ambiente etc.

> *"Os acessórios inteligentes fizeram a sua entrada com grande sucesso no mercado há alguns anos, e rapidamente ganharam o seu espaço de utilidade para um conjunto de funções específicas. Coisas com o controlo de pulsação, tensão arterial ou sono são úteis não só para fins de controlo médico, mas também para desporto ou simples curiosidade dos utilizadores." (COELHO, 2017, p. 73)*

A principal funcionalidade deste tipo de objeto é a análise de dados produzidos por seu usuário, monitorando suas atividades e enviando os dados coletados em tempo real, por meio da internet, para outros dispositivos que, por fim, comparam os dados obtidos entre si.

> *"Essas tecnologias vestíveis consistem em dispositivos que estão conectados uns aos outros produzindo informações sobre os usuários. Entre os principais produtos se destacam pulseiras e tênis que monitoram a atividades fisica do usuário, além de relógios e óculos inteligentes que pretendem prover ao usuário uma experiência de imersão na própria realidade." (MAGRINI, 2018, p.46-47)*

Esse tipo de dispositivo, pode ser apresentado de diversas formas, e é um dos tipos mais fáceis para se incluir funcionalidades ligadas à internet, uma vez que as pessoas já estão acostumadas com o seu uso, sendo que sua funcionalidade *IoT* apenas agrega valor e possibilidades de aplicação ao próprio objeto, como no exemplo abaixo apresentado por Coelho:

> *"Algumas aplicações muito práticas podem ser criadas, apenas balizadas pela imaginação. Por exemplo: um fabricante de fraldas para bebé que colocou sensores*

> *de humanidade na fralda para notificar os pais de que a fralda precisa ser mudada." (COELHO, 2017, p. 74)*

São objetos que podem facilitar o conhecimento do usuário de seu próprio corpo e necessidades, bem como manter o acompanhamento de uma criança, por exemplo, que não possui ainda a capacidade de informar àqueles que são responsáveis por seus cuidados que precisam de uma troca de fralda.

Esses dispositivos já fazem grande sucesso no cenário atual e tendem a ser um dos dispositivos mais disseminados no ambiente de *IoT*. Isso porque são dispositivos que já estamos acostumados a utilizar no dia a dia, apenas com funcionalidades extras que os tornam mais atrativos para o seu público corrente e também para alcançar novos nichos de mercado.

4. PLANO NACIONAL DE INTERNET DAS COISAS

Levando em consideração a importância deste tema e o fato de que a Internet das Coisas está sendo grandemente disseminada e possuir um enorme potencial econômico para o Brasil, o Banco Nacional do Desenvolvimento (BNDES), em parceira com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), realizou um estudo para o diagnóstico e a proposição de um plano de ação estratégico para o país em Internet das Coisas.

Tal estudo culminou com a Regulamentação da Internet das Coisas por meio da publicação do Decreto nº 9.854/2019 que institui o Plano Nacional de Internet das Coisas (Plano Nacional) no Brasil.

Assim, analisaremos abaixo os resultados dos estudos realizados, bem como o impacto destas conclusões na regulamentação e tratamento da *IoT* no Brasil.

4.1. REGULAMENTAÇÃO DA INTERNET DAS COISAS NO BRASIL

Como dito acima, o BNDES, em parceria com o MCTIC, realizou um estudo para o diagnóstico e proposição de um plano estratégico de ação para o Brasil em Internet das Coisas. Tal estudo culminou com a criação do Plano Nacional de Internet das Coisas.

Em seu primeiro artigo, o Plano Nacional define que a *IoT* deve ser implementada e desenvolvida "observadas as diretrizes de segurança da informação e de proteção de dados pessoais."

> *"Art. 1º Fica instituído o Plano Nacional de Internet das Coisas com a finalidade de implementar e desenvolver a Internet das Coisas no País e , com base na livre concorrência e na livre circulação de dados, observadas as diretrizes de segurança da informação e de proteção de dados pessoais." (BRASIL, 2019)*

Essa indicação trazida pela lei demonstra que os estudos trouxeram resultados que apontaram para a importância da proteção de dados pessoais, antes mesmo da publicação da Lei Geral da Proteção de Dados.

Além disso, a privacidade foi inserida como um tema que deverá fazer parte, de acordo com o Plano Nacional, do plano de ação para a viabilização do próprio Plano Nacional, conforme art. 5º, V, trazido a seguir:

> *"Art. 5º Ficam estabelecidos os seguintes temas que integrarão plano de ação destinado a identificar soluções para viabilizar o Plano Nacional de Internet das Coisas*
> *I - ciência, tecnologia e inovação;*
> *II - inserção internacional;*
> *III - educação e capacitação profissional;*

> *IV - infraestrutura de conectividade e interoperabilidade;*
> *V - regulação, segurança e privacidade; e*
> *VI - viabilidade econômica.*
> *Parágrafo único. As ações desenvolvidas no plano de ação de que trata o caput deverão estar alinhadas com as ações estratégicas definidas na Estratégia Brasileira para a Transformação Digital, nos termos do disposto no Decreto nº 9.319, de 21 de março de 2018." (BRASIL, 2019)*

Isso demostra, ainda mais, que o tema foi fortemente tratado nos estudos realizados, bem como que foi considerado de extrema importância e extremamente impactante no tratamento da Internet das Coisas no Brasil, como mostraremos a seguir.

4.2. IMPORTÂNCIA DA PROTEÇÃO DE DADOS PESSOAIS NA *IOT*

Como tratado anteriormente, a enorme quantidade de dados coletados e tratados pelo sistema da Internet das Coisas potencializa a utilização de tecnologias como o *Big Data*. Esse termo é utilizado para descrever a possibilidade de obtenção de informações por meio da análise de grandes volumes de dados, assim como descrito por Magrini. (MAGRINI, 2018, p.22)

Dessa forma, o *Big Data* mostra-se como uma alternativa para a utilização dos diversos dados que a *IoT* acaba por gerar com sua utilização. Isso significa que será possível retirar informações de padrões valiosos por meio da análise realizada com a aplicação desse sistema nos dados coletados.

> *"Big data is about finding valuable and hidden patterns in large amounts of information. Predictive analytics is a method of applying statistical models on that data to predict the most likely future behavior of someone or something."* (Big data é encontrar padrões valiosos e ocultos em grandes quantidades de informações. A análise preditiva é um método de aplicação de modelos estatísticos nesses dados para prever o comportamento futuro mais provável de alguém ou algo.) *(UNEMYR, 2017, posição 215-217)*

É possível afirmar, assim, que o uso de *Big Data* é quase uma certeza para o futuro da *IoT*, o que nos leva a analisar o potencial risco aos dados coletados e à privacidade.

Como o *Big Data* é formado basicamente de bases de dados criadas a partir da coleta de dados, nesse caso, por meio do sistema de Internet das Coisas, isso significa que essas bases de dados podem estar recheadas de dados pessoais, pois, como afirmado no Relatório de Consulta Pública realizada pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações, essa seria uma característica dos dados coletados a partir da *IoT*:

> *"No que tange a privacidade e proteção de dados pessoais, além das vulnerabilidades já mencionadas é importante ter em mente que o ecossistema de M2M/IoT poderá potencializar os negócios com big data, em especial com empresas interessadas em monetizar bases de dados, seja para fins publicitários ou outras destinações. Essas bases de dados podem possuir dados pessoais individualizados ou dados agregados/anonimizados sobre indivíduos." (BRASIL, MCTIC, 2016, p.85)*

Essa característica acaba por potencializar a discussão sobre a privacidade e proteção de dados no ambiente *IoT*. Isso porque ainda não se tem clareza sobre a proteção garantida ou não aos dados tratados, o que gera uma certa incerteza nos usuários e no ambiente regulatório desse sistema.

> *"Não se tem, hoje, clareza do tratamento aos dados. Aspectos sobre a coleta, o compartilhamento e o potencial uso deles por terceiros ainda são desconhecidos pelos consumidores. Isso tem a capacidade de abalar (e, em certo sentido, já abala) a confiança dos usuários nos produtos conectados." (MAGRINI, 2018, p.50)*

Além disso, como aponta Magrini, "questões relacionadas à segurança e proteção de dados pessoais são igualmente importantes para que a *IoT* se consolide como o próximo passo da internet." (MAGRINI, 2018, p.50-51)

Por esse motivo, o estudo comandado pelo BNDES concluiu que os assuntos de privacidade e proteção de dados pessoais no ecossistema de Internet das Coisas deveria contar com especial atenção por parte de sua regulamentação. (BNDES, 2017, p. 24)

Assim, entendeu-se, na época, que além da inclusão da importância da proteção de dados pessoais na regulamentação da *IoT*, também seria necessária a elaboração de norma específica de Proteção de Dados Pessoais, que, no ano seguinte seria publicada.

> *"Nesse cenário, o desenvolvimento de soluções Internet das Coisas perpassa pela edição de normas de proteção de dados pessoais que lide com a complexidade e as nuances dos dados pessoais, e que seja capaz de trazer segurança jurídica à essa nova fronteira da vida em sociedade." (BNDES, 2017, p. 24)*

Esse apontamento deixa ainda mais clara a conclusão em que se chegou com o estudo realizado pelo BNDES: a *IoT*, pela imensa quantidade de dados envolvidos em sua operação, possui um potencial lesivo extremamente grande, por esse motivo, a elaboração e observância de legislação referente à proteção de dados pessoais é de imensa importância para que o ambiente de Internet das Coisas seja seguro aos seus usuários e a seus dados.

Isso tudo porque, além de ser necessário garantir a forma como as empresas utilizarão os dados coletados, é, ainda, necessário prevenir-se de ataques e uso indevido dos dados por terceiros e por empresas que, eventualmente, obtenham acesso a tais dados por meio de seu compartilhamento.

> *"Isto porque, com a proliferação de novos dispositivos conectados à Internet capazes de coletar dados diversos, como é o caso de tecnologias de IoT, mais recorrentes e comprometedores os ataques a data bases e a ocorrência de uso indevido de dados pessoais." (BNDES, 2017, p. 26)*

Por todo o apontado, entendeu o BNDES, por bem, incluir a proteção de dados como um dos pilares basilares do Plano Nacional de Internet das Coisas no Brasil.

4.2.1. Necessidade de criação da Autoridade Nacional de Proteção de Dados Pessoais

Além de tudo o que foi apontado no tópico anterior, uma das principais conclusões a que se chegou no estudo realizado pelo BNDES foi a necessidade e importância da criação e atuação da Autoridade Nacional de Proteção de Dados Pessoais.

Essa necessidade foi "um dos consensos obtidos durante o processo de formulação e consultas públicas relacionadas ao plano nacional de *IoT*", como apontado no Relatório de Estudo do BNDES sobre Internet das Coisas. (BNDES, 2017, p. 25)

Dessa forma, considerou-se que, não só a edição da norma para regulamentação sobre proteção de dados pessoais seria suficiente para a garantia da real proteção desses dados. Além da norma, também seria necessária a criação de uma instância reguladora responsável por garantir o cumprimento do disposto na norma.

> *"Mais do que a edição de norma específica sobre proteção de dados pessoais, também se faz necessária a existência de instância regulatória para lidar com os desafios da atual sociedade da informação, por se fazer necessária a existência de uma autoridade capaz de apresentar opiniões técnicas específicas a este novo ambiente e realizar controle unificado e homogêneo do cumprimento das disposições sobre proteção de dados pessoais." (BNDES, 2017, p. 24-25)*

Essa criação é importante pois somente uma autoridade com alto nível técnico e entendimento aprofundado sobre o tema de proteção de dados pessoais será capaz de emitir opiniões e criar "padrões" de proteção de dados no grau necessário para que a regulamentação seja eficiente.

A Autoridade será o centro da regulamentação, é ela, também, que notificará aqueles que estiverem em discordância com a norma de proteção, bem como é dela que partirão as sanções relacionadas com a quebra de sigilo ou mau uso das informações coletadas.

Nesse sentido, é importante que a Autoridade seja criada observando-se o contexto político-institucional adequado para o tratamento de um sistema ligado ao ambiente dinâmico da internet.

> *"Assim, o desenho da instância reguladora a ser criada deverá levar em conta o contexto político-institucional local e ser adequado à dinamicidade e complexidade técnica da Internet. Além disso, deverá estabelecer reais processos participativos para a tomada de decisões e dispor de capacidades institucionais para fornecer ao mercado parâmetros de conduta e também fiscalizar o cumprimento da legislação relacionada." (BNDES, 2017, p. 28)*

Por fim, destacou-se no estudo do BNDES que o mercado deveria fazer parte do ambiente de regulamentação da *IoT* com o objetivo de ajudar e incentivar parâmetros adequados de conduta e fiscalização entre os próprios integrantes deste mercado.

5. CERTIFICAÇÃO DOS DISPOSITIVOS DE *IOT* PELO INMETRO E ANATEL

Além do exposto anteriormente, vislumbrou-se também a necessidade de certificação dos dispositivos de *IoT* pela Agência Nacional de Telecomunicações – Anatel (Anatel), bem como pelo Instituto Nacional de Metrologia, Qualidade e Tecnologia – Inmetro (Inmetro) em certos casos, com o intuito de garantir o cumprimento das disposições apresentadas, principalmente acerca da proteção de dados. Essa necessidade foi analisada pelo estudo elaborado pelo BNDES e incluída no Plano Nacional, conforme demonstrado abaixo:

> *"Art. 8º Para fins do disposto no art. 38 da Lei nº 12.715, de 17 de setembro de 2012, são considerados sistemas de comunicação máquina a máquina as redes de telecomunicações, incluídos os dispositivos de acesso, para transmitir dados a aplicações remotas com o objetivo de monitorar, de medir e de controlar o próprio dispositivo, o ambiente ao seu redor ou sistemas de dados a ele conectados por meio dessas redes.*
>
> *§ 1º Para fins do disposto no caput, os sistemas de comunicação máquina a máquina não incluem os equipamentos denominados máquinas de cartão de débito e/ou crédito, formalmente considerados terminais de transferência eletrônica de débito e crédito, classificados na posição 8470.50 da Tabela de Incidência do Imposto sobre Produtos Industrializados - TIPI, aprovada pelo Decreto nº 8.950, de 29 de dezembro de 2016.*
>
> *§ 2º Compete à Agência Nacional de Telecomunicações regulamentar e fiscalizar o disposto neste artigo, observadas as normas do Ministério da Ciência, Tecnologia, Inovações e Comunicações." (BRASIL, 2019)*

De acordo com o estudo realizado pelo BNDES previamente citado, entendeu-se que, para que a legislação de proteção de dados e *IoT* fosse devidamente respeitada, seria necessária a certificação de produtos de Internet das Coisas, sob pena de descumprimento das normas citadas.

Tal certificação auxiliaria também na criação de um ambiente de confiança, em que os usuários de tais dispositivos se sentiriam ainda mais protegidos, pois isso incentivaria o compartilhamento de informações sobre segurança de dados, bem como de modelos mais eficazes de segurança da informação. (BNDES, 2017, p. 53)

Dessa forma, além da certificação por parte da Anatel, em alguns casos, conforme citado no estudo realizado pelo BNDES, seria necessário também a certificação por parte do Inmetro, porque ultrapassam o âmbito de atuação da Anatel.

> *"Em ambos os casos citados, exige-se a certificação de produtos que podem ser ligados à Internet das Coisas, sob pena de infração na hipótese de descumprimento. No âmbito do INMETRO, pode ser o caso dos "brinquedos", "equipamentos para consumo de água" e "segurança de aparelhos domésticos e similares". No plano da ANATEL, exige-se a certificação e homologação de produtos para telecomunicação." (BNDES, 2017, p. 53)*

5.1. ANÁLISE DE *COMPLIANCE* COM A LGPD E O PLANO NACIONAL DE *IOT*

Nesse sentido, como dito acima, o objetivo principal com a certificação exigida pelo Plano Nacional, seria o cumprimento das normas estabelecidas pelo próprio Plano Nacional pelos produtos de internet das coisas, bem como com as normas de proteção de dados, consideradas pelo plano tão importantes que foram inseridas em seu artigo 1º, conforme apresentado anteriormente.

Além disso, retornando ao assunto tratado no capítulo anterior, é importante também que a Autoridade Nacional seja estabelecida, pois é com base no que ela estabelecer com relação aos padrões a serem adotados que tanto a Anatel quanto o Inmetro conseguirão fazer uma análise de *compliance* adequada com os parâmetros estabelecidos para o ambiente de *IoT*.

Isso porque, atualmente, as regras relativas à proteção de dados encontram-se estabelecidas em diversas legislações diferentes, o que acaba por tornar tais regramentos objeto de fiscalização por diversos órgãos, e, consequentemente, sem uma uniformidade quanto aos seus parâmetros de aplicação.

> *"Um dos problemas atuais é o fato de que a observância ("enforcement") de normas relativas à privacidade serem objeto de fiscalização e atuação de múltiplas entidades consecutivamente: SENACON (ligada ao Ministério da Justiça), Ministério Público Federal, Ministério Público Estadual e assim por diante. A aprovação de lei específica e a criação de Autoridade de Proteção de Dados Pessoais pode mitigar esse problema. Além disso, pode prevenir abusos na coleta e tratamento de dados pessoais dos usuários de Internet e nos sistemas de Internet das Coisas." (BNDES, 2017, p. 25)*

Dessa forma, conforme apontado pelo estudo realizado pelo BNDES, a implementação de normas de certificação buscaria incentivar a adoção de medidas de segurança e proteção de dados, garantindo, assim, padrões mínimos de infraestrutura de controle do uso e tratamento de dados pessoais.

> *"No âmbito local, faz-se necessário, ainda, encontrar alternativas para incentivar a adoção de medidas protetivas à segurança da informação pela iniciativa privada, seja pela adoção de mecanismos voluntários de certificação de dispositivos ou pelo respeito a critérios mínimos de segurança em infraestruturas críticas." (BNDES, 2017, versão 1.1, p. 40)*

Como alternativa para a certificação obrigatória, pensou-se também na possibilidade de certificações voluntárias, o que seria uma forma de incentivar empresas a manter um alto nível de segurança, além de incentivar os consumidores a procurarem os dispositivos mais seguros, e aqueles que possuem sua infraestrutura analisada e autorizada por um órgão responsável, o que indicaria sua capacidade de proteção dos dados de seus usuários.

> *"Uma alternativa seria a certificação voluntária sobre a segurança de dispositivos ligados à Internet das Coisas. A estruturação de sistema de certificação baseado na auto-avaliação voluntária, sem a imposição de obrigações legais aos aderentes, teria o potencial de criar cultura de transparência na prestação de informações ao usuário e incentivar a adoção de alto padrão de segurança pela iniciativa privada." (BNDES, 2017, versão 1.1, p. 40-41)*

Nesse sentido, o próprio estudo do BNDES admite que essa forma de certificação seria interessante, uma vez que forçaria a iniciativa privada a reconhecer a certificação "não como custo, mas como possibilidade de agregar valor a produtos", pois justamente incentiva os consumidores a dar preferência a equipamentos com alto grau de segurança e devidamente certificados, o que seria "um diferencial competitivo para o mercado." (BNDES, 2017, p. 54)

> *"De forma ilustrativa, deve haver medidas de conscientização que permitam ao consumidor evitar adquirir solução em IoT que possa, por exemplo, causar curto circuito, vazar dados pessoais ou permitir que seus dispositivos domésticos conectados sejam controlados por terceiro não autorizado.[...] Dentre as informações incluídas (na certificação do dispositivo), ressalta-se a importância de temas como: (i) segurança do dispositivo, com informações sobre medidas de segurança adotadas e dados sobre funções e processamento; (ii) credenciais e possibilidade de acesso de usuários; (iii) conectividade; (iv) atualização remota de medidas de segurança." (BNDES, 2017, p.52-56)*

5.2.1. Proteção contra o vazamento de dados pessoais

Como dito, o objetivo dos modelos de certificação apresentados é a proteção dos dados pessoais, por esse motivo, o que a certificação deve buscar encontrar são sistemas adequados que evitem o vazamento/utilização por terceiros não autorizados dos dados pessoais coletados pelos dispositivos *IoT*.

Assim, diversos autores, incluindo Dias, procuraram apresentar modelos de sistemas que seriam adequados para a proteção desses dados. Entre eles, encontra-se a criptografia dos dados coletados. Nesse caso, o próprio sistema de coleta faria a criptografia da informação, para só então enviá-la, de maneira segura, pela internet para sua "central".

Outro modelo seria a utilização de dispositivos que não tratassem os dados, apenas os coletasse. Dessa forma, os dados não seriam armazenados no dispositivo, que seria utilizado apenas para a leitura dos dados, sem gravá-los em seu sistema interno, o que o tornaria mais seguro pelo simples motivo de não possuir dados em sua memória, sem possibilidade assim, de vazamento a partir do mesmo. (DIAS, 2016, posição 2089-2092)

Do mesmo modo, o Relatório de Consulta Pública realizada pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações entendeu que a segurança e a privacidade são blocos essenciais para o funcionamento da Internet das Coisas no Brasil, e que sistemas de controle

devem ser implementados nos dispositivos para evitar falhas/incidentes de segurança da informação a partir de tais objetos.

> *"Desse modo, fica claro que a segurança e a privacidade devem ser blocos essenciais de qualquer modelo de referência para IoT, sendo necessário uma implementação adequada em todas as camadas, do hardware ao software, das aplicações de negócio e de controle. Portanto, é importante que a segurança e a privacidade sejam tratadas em todas as etapas de desenvolvimento de um produto ou serviço comercializado no mercado, incluindo avaliações sobre a segurança do dispositivo, o software, a gestão de identidades e controle de acesso, a comunicação entre dispositivos e sistemas e o monitoramento e tratamento de incidentes de segurança." (BRASIL, MCTIC, 2016, p.82)*

Importante salientar que, segundo Sinclair, a segurança a que nos referimos diante de um cenário de *IoT* é mais ampla que uma segurança simples de TI. Isso acontece porque em um cenário de internet das coisas a proteção é realizada em dados que estejam em repouso e também em movimento, exigindo "conhecimentos de segurança móvel, segurança de rede, segurança de aplicativos, segurança de web e nuvem, e segurança de sistemas." (SINCLAIR, 2018, p. 34)

Isso acontece justamente por conta dos sistemas de proteção apresentados acima, em que dados podem ou não ser tratados no próprio dispositivo de *IoT*, como também podem ser apenas "lidos" por tal objeto e passados adiante para sua "central". Tais sistemas fazem com que não só os dispositivos precisem ser seguros, mas também a rede que fará o transporte de tais dados e a "central" que os receberá.

Tudo isso se mostra importante uma vez que, como os dispositivos trabalham com a coleta e tratamento de dados pessoais, qualquer falha em sua segurança "abre espaço para ataques visando ao acesso às informações geradas pelos próprios dispositivos". Ademais, como aponta Magrini, esses ataques podem significar interferência nos próprios dispositivos, mas também podem acarretar problemas na estrutura de rede da qual o objeto utiliza para realizar sua interconexão pela internet. (MAGRINI, 2018, p.50)

5.2.2. Necessidade do cumprimento das leis apresentadas

Com todos estes aspectos em mente, é possível dizer que não só a formulação das leis foi necessária para a implementação segura da *IoT* no Brasil, mas também seu correto cumprimento e formulação de políticas que incentivem a observância das legislações apresentadas.

Por esse motivo, o estudo realizado pelo BNDES chegou à conclusão de que além da elaboração (o que já ocorreu) de leis necessárias para o ambiente de internet das coisas, como

citado, é também necessário o desenvolvimento de soluções que garantam a segurança dos dados coletados.

> "Nesse cenário, o desenvolvimento de soluções para a comunicação máquina a máquina perpassa pela edição de normas específicas sobre a proteção de dados pessoais que lidem com a complexidade e as nuances dos dados pessoais, e que sejam capazes de trazer segurança jurídica à essa nova fronteira da vida em sociedade, especialmente considerando que a expansão de IoT pode ter o condão de potencializar violações à privacidade dos cidadãos." (BNDES, 2017, p. 26)

Isso porque, não há como realizar o cumprimento da Lei Geral de Proteção de Dados e do Plano Nacional de Internet das Coisas se o ambiente não for seguro o suficiente para garantir que os dados coletados serão tratados da maneira correta.

Da mesma forma, não há como esperar que o ambiente de Internet das Coisas se auto regularize, sem a introdução de normas necessárias para direcionar seus jogadores na direção certa.

Por fim, vale lembrar, que a análise de dados realizada pelos dispositivos integrantes deste sistema pode auxiliar também na formulação de políticas públicas e gestão de órgãos públicos, assim como apontado pelo estudo do BNDES.

> "A formulação de políticas públicas, a gestão eficiente e transparente dos órgãos governamentais e a criação de novos modelos de negócios são diretamente influenciados pelo crescimento exponencial de análises baseadas em grandes volumes de dados." (BNDES, 2017, p. 26)

Com isso em mente, devemos nos perguntar: como seria possível essa análise se não houvesse segurança? É por esses motivos que, além de efetivamente elaborar a lei necessária, é preciso também estabelecer formas para que essa lei seja cumprida pelos atuantes do setor, o que ocorre com a LGPD e o Plano Nacional aqui apresentados.

6. **CONCLUSÃO**

Como demonstrado no presente estudo, ambos os temas tratados não são assuntos que só atualmente entraram no debate jurídico, entretanto apenas recentemente atingiram um patamar de discussão no nível de sua importância.

Assim, a proteção de dados pessoais é um dos principais pontos, e de maior relevância, a ser analisado quando falamos sobre o mundo de Internet das Coisas.

Não há como garantir que os dispositivos de *IoT* são seguros para os dados coletados de seus usuários se não for levado em consideração o fato de que a maioria de tais dados são pessoais, e por este motivo requerem uma atenção especial e um cuidado maior para seu tratamento.

Por fim, além da necessidade de uma legislação adequada ao tratamento de dados pessoais, para que seja garantido aos titulares dos dados tratados seu direito à proteção de dados pessoais é necessário que a Autoridade Nacional seja criada, além da implementação de um sistema de certificação capaz de garantir um ambiente seguro e apropriado para o tráfego de dados pessoais.

7. **REFERÊNCIAS**

BIONI, Bruno Ricardo. *Proteção de Dados Pessoais: a função e os limites do consentimento.* 2. ed. Rio de Janeiro: Editora Forense, 2019.

BNDES. *Relatórios de Estudo sobre Internet das Coisas:* Produto 8: Relatório do Plano de Ação – Capítulo Regulatório. Brasília, 2017. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil. Acesso em: 27 out. 2019.

BNDES. *Relatórios de Estudo sobre Internet das Coisas:* Produto 8: Relatório do Plano de Ação – Iniciativas e Projetos Mobilizadores. Versão 1.1. Brasília, 2017. Disponível em: https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil. Acesso em: 27 out. 2019.

BRASIL. *Lei Federal nº 14.010/2020 (Regime Jurídico Emergencial).* Brasília, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2020/Lei/L14010.htm. Acesso em: 12 jun. 2020.

BRASIL. *Lei Federal nº 13.709/2018 (LGPD)*. Brasília, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em 25 out. 2019.

BRASIL. *Lei Federal nº 12.965/2014 (Marco Civil).* Brasília, 2014. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 25 out. 2019.

BRASIL. *Medida Provisória nº 959/2020.* Brasília, 2020. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2020/mpv/mpv959.htm. Acesso em: 23 mai. 2020.

BRASIL. Ministério da Ciência, Tecnologia, Inovações e Comunicações. *Relatório de Consulta Pública realizada pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações – Câmara IOT:* Identificação dos tópicos de relevância para a viabilização da Internet das Coisas no Brasil. Disponível em: http://www.abinee.org.br/informac/arquivos/aiot.pdf. Acessado em: 27 out. 2019.

COELHO, Pedro. *Internet das Coisas – Introdução Prática.* Lisboa: FCA – Editora de Informática Lda., 2017.

MAGRINI, Eduardo. *A Internet das Coisas*. 2. ed. Rio de Janeiro: Editora FGV, 2019.

PINHEIRO, Peck, P. *Proteção de dados pessoais:* comentários à Lei n. 13.709/2018 LGPD. São Paulo. Saraiva Educação, 2018.

POHLMANN, Sérgio Antônio. *Entendendo e Implementando a Lei Geral de Proteção de dados nas Empresa*. Nova Friburgo: Editora Fross, 2019.

SAUAIA, Hugo Moreira Lima. *A Proteção dos Dados Pessoais no Brasil*. Rio de Janeiro: Editora Lumen Juris, 2018.

SINCLAIR, Bruce. *Como usar a Internet das Coisas para alavancar seus negócios*. Tradução Afonso Celso da Cunha Serra. Editora Autêntica Business, 2018, São Paulo.

UNEMYR, Magnus. *The Internet of Things – The Next Industrial Revolution Has Begun: How IoT, big data, predictive analytics, machine learning and AI will change our lives forever*. 2017. E-book.

UNIÃO EUROPEIA. *Regulamento Geral de Proteção de Dados da União Europeia*. 2016. Disponível em: https://gdpr-info.eu/. Acesso em: 25 out. 2019.

COORDENADORIA DE TRABALHO DE CONCLUSÃO DE CURSO (TCC)

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, Daniele Dimas Ramos

Aluno(a), regularmente matriculado(a), no Curso de Direito, na disciplina do TCC da 10ª etapa, matrícula nº 41510055-2, PeríodoM, TurmaE,

tendo realizado o TCC com o título: Proteção de dados e o Plano Nacional de Internet das Coisas (IOT) - Análise da importância da proteção de dados pessoais na internet das coisas e sua regulamentação.
sob a orientação do(a) professor(a): João Bosco Coelho Pasin

declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 15 de junho de 2020

Assinatura do discente