UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ

DIRETORIA DE PESQUISA E PÓS-GRADUAÇÃO

DEPARTAMENTO ACADÊMICO DE ELETRÔNICA

CURSO DE ESPECIALIZAÇÃO EM REDES DE COMPUTADORES E TELEINFORMÁTICA

DIOGO VINÍCIUS MARTINS DA CRUZ

DESAFIOS PARA A IMPLEMENTAÇÃO DO ECOSSISTEMA DE INTERNET DAS COISAS NO COTIDIANO BRASILEIRO

MONOGRAFIA DE ESPECIALIZAÇÃO

CURITIBA

2018

DIOGO VINÍCIUS MARTINS DA CRUZ

DESAFIOS PARA A IMPLEMENTAÇÃO DO ECOSSISTEMA DE INTERNET DAS COISAS NO COTIDIANO BRASILEIRO

Monografia de Especialização, apresentada ao Curso de Especialização em Redes de Computadores e Teleinformática, do Departamento Acadêmico de Eletrônica – DAELN, da Universidade Tecnológica Federal do Paraná – UTFPR, como requisito parcial para obtenção do título de Especialista.

Orientadora: Profa. Dra. Tânia Lúcia Monteiro

CURITIBA

2018

Ministério da Educação
Universidade Tecnológica Federal do Paraná
Câmpus Curitiba

Diretoria de Pesquisa e Pós-Graduação
Departamento Acadêmico de Eletrônica
Curso de Especialização em Redes de Computadores e Teleinformática

TERMO DE APROVAÇÃO

DESAFIOS PARA A IMPLEMENTAÇÃO DO ECOSSISTEMA DE INTERNET DAS COISAS NO COTIDIANO BRASILEIRO

por

DIOGO VINÍCIUS MARTINS DA CRUZ

Esta monografia foi apresentada em 12 de Dezembro de 2017 como requisito parcial para a obtenção do título de Especialista em Redes de Computadores e Teleinformática. O candidato foi arguido pela Banca Examinadora composta pelos professores abaixo assinados. Após deliberação, a Banca Examinadora considerou o trabalho aprovado.

_____
Profa. Dra. Tânia Lucia Monteiro
Orientadora

_____
Prof. Dr. Kleber Kendy Horikawa Nabas
Membro titular

_____
Prof. M.Sc. Danillo Leal Belmonte
Membro titular

- O Termo de Aprovação assinado encontra-se na Coordenação do Curso -

Dedico este trabalho sobretudo a Deus, que me capacitou a esse momento de desafio. À minha família, que mesmo distante sempre me apoiou, dando-me forças nos momentos difíceis. Bem como à Caroline do Rocio, pessoa que amo e que abriu meus horizontes educacionais e pedagógicos, tornando-me quem sou hoje na esfera cognitiva.

O primeiro dever do pregador do Evangelho é declarar a lei de Deus para mostrar a natureza do pecado. Pois é melhor ter alguma dificuldade em ouvir falar de Deus, do que não ter qualquer dificuldade em ouvir falar do que está bem longe Dele. (LUTERO, Martinho, 1517)

RESUMO

CRUZ, Diogo Vinícius Martins da. **Desafios para a implementação do ecossistema de internet das coisas no cotidiano brasileiro**. 2017. 62 f. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

Vive-se vivendo uma nova realidade. A tecnologia da informação, através de seus diversos dispositivos vem proporcionando à sociedade uma nova maneira de conduzir sua forma de viver, melhorando em diversos aspectos a qualidade de vida a qualidade de vida das pessoas e fazendo com que se acostumem com o novo. Nesta nova e constante caminhada a um futuro conectado, advêm uma nova maneira de utilização de dispositivos outrora comuns no dia a dia. Carros, geladeiras, micro-ondas, uma simples lâmpada, até mesmo uma casa[1], ou seja, "coisas" diversas, farão parte desta nova realidade tecnológica. Não como coadjuvantes, como estamos acostumados, mas sim, como personagens principais de uma nova "onda" tecnológica. Com o advento da Internet das Coisas (IoT), do inglês *"Internet of Things",* tudo pode passar a ser inteligente, responsável e conectado, vindo a facilitar a vida dos cidadãos[2]. Entretanto, para isso, muitos desafios precisam ser entendidos, debatidos, estudados e superados. Uns mais, outros menos complicados, mas que, juntos, dificultam ou inviabilizam a implantação da Internet das Coisas em larga escala em no cotidiano das pessoas, sobretudo à grande massa da população. Neste trabalho destacam-se barreiras de implantação, tais como: limite entre o que é privado e público, e como as leis regem acerca deste assunto, quais políticas públicas estão sendo adotadas com esse viés. Bem como, a real e maciça implantação do protocolo IPv6 nas redes domésticas, já que este protocolo é fundamental à utilização e popularização da IoT. Essas intemperes observadas acima, não findam este assunto, o qual ainda requer muita atenção, sobretudo do usuário final, da indústria como um todo, da sociedade civil organizada, bem como do poder público em suas diversas instâncias.

Palavras-chave: Internet das Coisas (IoT). Desafios em IoT. IPv6. Redes de sensores sem fio. Privacidade.

ABSTRACT

CRUZ, Diogo Vinícius Martins da. **Challenges for the implementation of the internet ecosystem of things in brazilian daily life**. 2017. 62 f. Monografia de Especialização em Redes de Computadores e Teleinformática, Departamento Acadêmico de Eletrônica, Universidade Tecnológica Federal do Paraná. Curitiba, 2017.

Live a new reality. Information technology, through its various devices, has provided society with a new way of conducting its way of life, improving the quality of life and quality of life of people and making them accustomed to the new. In this new and constant walk to a connected future, advance a new way of using external devices in our day to day. Cars, refrigerators, microwaves, a simple lamp, even a house[1], that is, various "things", will be part of this new technological reality. Not as secondary, as they are accustomed, but rather, as main characters of a new technological "wave". With the advent of the Internet of Things (IoT), make English the "Internet of Things", everything can become an intelligent, responsible and connected being, making life easier for citizens[2]. In all cases, many challenges are successful, debated, studied and overcome. Some more, others less complicated, but which, together, make difficult or impossible a deployment of the Internet of Things with more ownership and large scale in our daily lives, especially in large mass of the population. In this work we highlight the implementation barriers, such as the border between what is private and public, and as our rights reserved for the subject, what public policies are being adopted with this bias. As well as, a real implementation of IPv6 protocol in home networks, since this protocol is fundamental to the use and popularization of IoT. These difficulties observed above, not found at the moment, which still have a lot of attention, mainly of the user, of the industry as a whole, of organized civil society, as well as of the public power in its various instances.

Keywords: Internet of Things (IoT). Challenges in IoT. IPv6. Wireless Sensor Networks. Privacy.

LISTA DE FIGURAS

LISTA DE TABELAS

LISTA DE SIGLAS

BNDES	Banco Nacional do Desenvolvimento Econômico e Social
CGI.br	Comitê Gestor da Internet
CIDR	*Inter-Domain Routing*
DHCP	*Dynamic Host Configuration Protocol Classes*
DOU	Diário Oficial da União
EUA	Estados Unidos da América
IANA	*Internet Assigned Numbers Authority*
ICTs	Instituições Científicas e Tecnológicas
IoE	*Internet of Everythings*
IoT	*Internet of Things*
IPv4	*Internet Protocol version 4*
IPv6	*Internet Protocol version 6*
ITCs	Instituição de Pesquisa Científica Tecnologia
LACNIC	*Latin America and Caribbean Network Information Centre*
M2M	*Machine to Machine*
M2P	*Machine to Person*
MCTIC	Ministério da Ciência, Tecnologia, Inovações e Comunicações
MTU	*Maximum Transmission Unit*
NAT	*Network Adress Translation*
NFC	*Near Field Communication*
NIC.br	Núcleo de Informação e Coordenação do Ponto BR
P2P	*Person to Person*
PL	Projeto de Lei
RFID	*Radio Frequency-Identification*
SD-RJ	Partido Solidariedade do Rio de Janeiro
TI	Tecnologia da Informação
UE	União Europeia

SUMÁRIO

1 INTRODUÇÃO

Esta etapa do trabalho, será mostrado de forma sucinta ao leitor duas das grandes dificuldades de popularização dos dispositivos munidos com internet das coisas. Para isso serão apresentadas as dificuldades abordadas, objetivos gerais e específicos, justificativa e organização do conteúdo.

1.1 DIFICULDADES ABORDADAS

Ao comprar um dispositivo com acesso à internet, nem sempre o usuário lê ou ao menos se dá conta das políticas de segurança da informação relacionadas ao dispositivo. Bem como, simples acesso a um "*web site",* pode conter informações de privacidade de um usuário, seja por falta de atenção do mesmo ou má fé da de administradores do site acessado.

Que tipo de política as empresas adotam para o uso dos dados coletados, até que ponto os consumidores estão cientes e se preocupam ao fornecer informações pessoais[2], e, até onde os termos de uso estabelecidos no momento da adesão estão, de fato, sendo cumpridos.

Ainda sobre este tema, observa-se como se apresenta o ordenamento jurídico do país, trazendo trechos de portarias, decretos e leis diversas, as quais abordam o tema e dão respaldo a procedimentos legais. Entretanto não se esgotam, sendo necessário ainda um debate mais amplo sobre a privacidade do usuário final.

Uma outra visão sobre esse novo ecossistema proveniente da Internet das Coisas, ou Internet de Todas as Coisas (*Internet of Everythings*: IoE)[3], é a concreta utilização do protocolo IPv6 nas redes.

Com o crescimento populacional e consecutivamente a adesão a novos dispositivos conectados, chegou-se ao esgotamento do protocolo IPv4[4]. Um exemplo disto é o Brasil que possui cerca de 207 milhões de habitantes[5], e possuirá até o fim deste ano um smartphone per capita[6]. Isto sem falar nos outros dispositivos pessoais conectados à internet que necessitam de um endereço IP para navegarem.

Os diversos dispositivos já vêm habilitados à utilização do novo protocolo de endereçamento IP, o IPv6. Contudo técnicas de aproveitamento de endereçamento

do IPv4 vêm tardando a completa migração para o novo protocolo de endereçamento. Logo este é outro limitador do uso da Internet das Coisas, já que o IPv6 é indispensável a sua utilização.

1.2 OBJETIVOS

1.2.1 Objetivos Gerais

Levar ao questionamento, e debates às consequências de uma política de privacidade de dados individuais, margeadas por interesses comerciais, em detrimento à individualidade soberana do cidadão, em um cenário com inúmeros dispositivos conectados. Bem como fomentar a migração do protocolo de endereçamento de rede, quando da potencialidade do IPv6 sobre sua versão anterior, tendo em vista ser esta uma condição indispensável para a implantação do ecossistema da Internet das Coisas.

1.2.2 Objetivos Específicos

Para atender ao objetivo geral neste trabalho de conclusão de curso os seguintes objetivos específicos serão abordados:

- Alertar ao cidadão comum sobre os perigos de um mundo conectado.
- Apresentar e debater sobre o ordenamento jurídico brasileiro acerca da privacidade dos dados, e da individualidade do usuário.
- Entender que ferramentas e práticas que tardam a adoção real e prática do protocolo IPv6, interferem sobremaneira nas funcionalidades advindas da Internet das Coisas.
- Demonstrar que o mercado de IPv6 ainda tem muito a crescer e demandará capacitação de profissionais habilitados.

1.3 JUSTIFICATIVA

Estes são alguns dos principais assuntos abordados quando se fala em IoT: Introdução de novos dispositivos no mercado; novas tecnologias; topologias de redes de sensores sem fio; consumo de energia, entre outros. Representam

igualmente, temas intrinsecamente ligados a essa nova realidade de conectividade das coisas. Contudo, sem antes possibilitar o seu acesso em massa e, cuidar da privacidade de quem realmente consumirá estes produtos, deve-se abordar temas de caráter secundários e que podem ser vistos como melhorias contínuas de iterações futuras, à temas primordiais de debate público.

1.4 ORGANIZAÇÃO

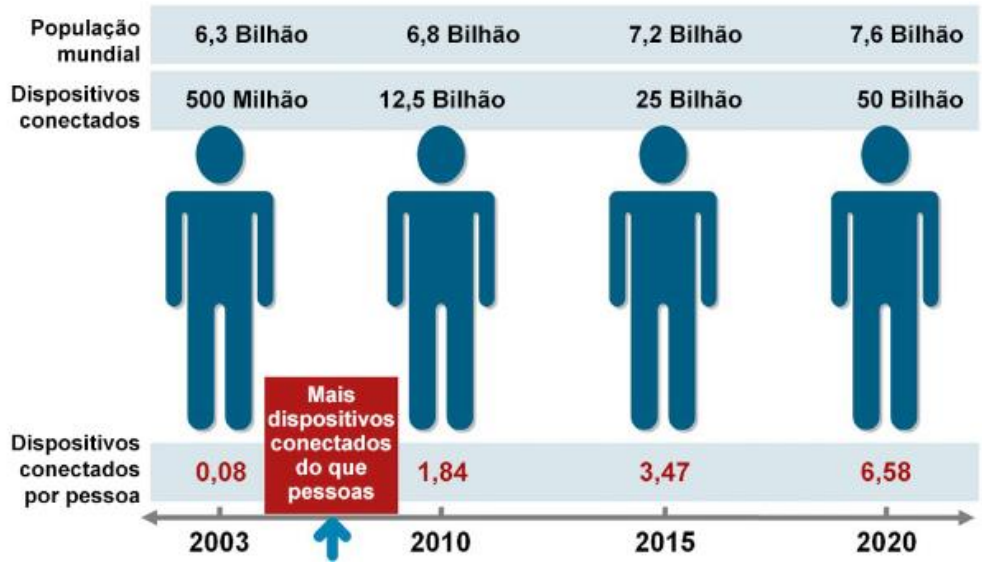
Este trabalho está organizado da seguinte maneira: No capítulo 1 será abordada a nova realidade, já presente nos dias de hoje, mas que ainda tem muito a ser acrescentada com o advento da Internet das Coisas. Posteriormente, no segundo capítulo são abordadas as variantes econômicas consequentes deste novo ecossistema de dados. Exemplos já reais de aplicações práticas de IoT serão vistas no capítulo três. O quarto capítulo condensa tecnologia e privacidade de dados, no capítulo cinco tem-se a delimitação do termo individualidade e a jurisdição dos dados na nuvem. O ordenamento jurídico brasileiro sobre privacidade dos dados será abordado no capítulo seis. O sétimo trará uma breve explanação do protocolo IPv6 e sua adesão no Brasil e no mundo, findando com o oitavo capítulo com uma abordagem que justifica a manutenção do IPv4 em muitas redes domésticas e empresariais. O nono e último capítulo trará uma conclusão.

2 A INTERNET DAS COISAS E SUAS VARIANTES ECONÔMICAS

Neste capítulo, posiciona-se a economia nacional em um cenário de adoção de IoT, por meio de dados que remetam ao promissor crescimento do país neste ecossistema. Mas antes disto: O que é realmente Internet das Coisas? Em uma breve explicação, com o intuito de situar o leitor afirma-se que IoT: é a maneira com que as coisas estão conectadas entre si e se comunicam entre si e com o usuário, através de sensores inteligentes, dispostos em rede, e softwares que transmitem dados dentro desta rede. Compara-se a um grande e complexo sistema nervoso, o que possibilita a troca de informações entre dois ou mais pontos. O resultado disso é um planeta mais inteligente e responsivo. A expressão Internet das Coisas (*Internet of Things*) origina-se do fim da década de 1990 pelo empreendedor britânico high-tech Kevin Ashton, que também possui diversos trabalhos com a tecnologia de etiquetas RFID (Identificação por radiofrequência). O conceito de IoT baseia-se na conexão maquina à máquina (M2M, este tema e outras conexões com IoT são abordados mais adiante), fazendo com que diversos itens diferentes, possam ser conectados entre si, transferindo informações, compartilhando recursos e otimizando seu uso.

Mas de que “coisa” estamos falando? A resposta é: qualquer coisa. Desde um relógio ou uma geladeira, até carros, máquinas, computadores e smartphones. Qualquer utensílio, equipamento ou dispositivo que você consiga imaginar, pode, teoricamente, entrar para o mundo da Internet das Coisas. Atualmente existem mais objetos na internet do que pessoas, o que nos leva a refletir sobre esse processo, o qual representa um enorme mercado consumidor, com perspectiva de crescimento, como mostra a Figura 1.

Figura 1. Estimativa de dispositivos conectados por pessoa para os próximos anos



Fonte: Cisco IBSG, 2011. Disponível em: <https://www.researchgate.net/figure/Cisco-IBSG-estimates-IoT-was-born-sometime-between-2008-and-2009-Source-Cisco-IBSG_fig1_320710095>. Acesso em: 28 ago. 2018.

Trazendo para uma realidade mais próxima, é necessário entender como utilizar a internet das coisas para transformar a sociedade. Melhorar a qualidade de vida das pessoas e, fomentar os negócios, aumentando a produtividade das empresas, deverá ser consequência da adoção deste ecossistema no país. Unido logicamente à uma rede robusta, equipamentos eletrônicos inteligentes com preços acessíveis, bem como profissionais habilitados.

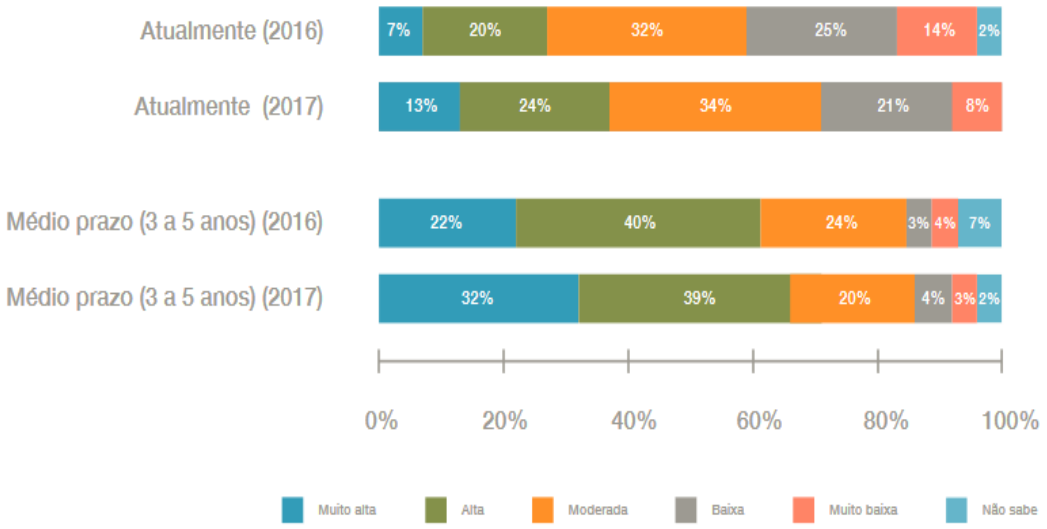
A internet das coisas, ou “de todas as coisas” deve gerar trilhões de dólares na economia mundial nos anos vindouros[8]. O Brasil tem um portfólio de variantes positivas para ser bem-sucedido nesse cotidiano conectado, dentre estes uma enorme faixa de crescimento com o passar dos anos.

2.1 A ADOÇÃO DE IOT NAS EMPRESAS BRASILEIRAS

Mesmo com uma vertente de aplicação bem robusta, e muitos debates sendo gerados sobre a adoção de internet das coisas, a realidade no que se refere a casos práticos no Brasil ainda é pequena mas vem crescendo, de acordo com um estudo realizado (Figura 2) pela Promon Logicalis em 2016 (que, a partir de 1º de março de 2017, passou a se chamar Logicalis). Em 2016, apenas 52% das empresas abordadas na entrevista adotaram IoT em algum percentual entre os níveis moderado e alto, já em 2017 esse percentual é de 58%[6]. Mesmo ainda sendo

baixa, o futuro desta adoção é promissor. Na pesquisa de 2016, cerca de 32% dos participantes do estudo enxergavam a Internet das Coisas como fundamental para seus negócios, este cenário deve ser consideravelmente alterado nos anos seguintes, pois 62% dos participantes acreditam que IoT será extremamente importante, isto, segundo a pesquisa, dentro de três a cinco anos. Em 2017, esse número já é de 71%. Ainda na pesquisa atual, 68% das empresas investirão mais em IoT em 2017, se comparado a 2016. Esta pesquisa denominada “IoT Snapshot” foi realizada com executivos de 160 empresas brasileiras, de diferentes segmentos para entender a e experiência e maturidade de adoção de IoT no Brasil e seu potencial de crescimento nos próximos anos[6].

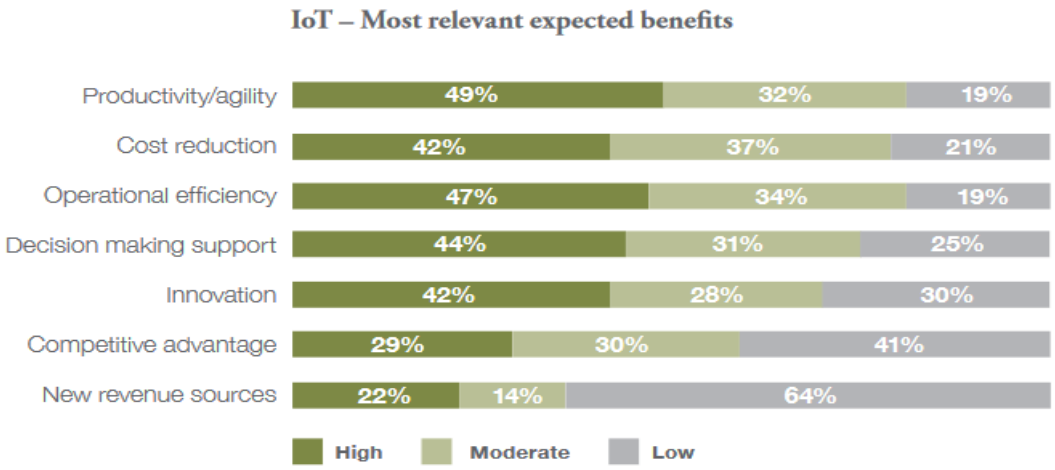
Figura 2. Comparativo entre a importância atual em IoT e a expectativa para de 3 a 5 anos



Fonte: Parreira (2017)[6].

Este estudo, apresentado na Figura 3, ainda avaliou os principais motivos que levam as empresas de diversos segmentos a dotarem o IoT, o setor de utilidades, por exemplo, visa a redução de custo (67%), produtividade (50%) e eficiência operacional (42%), enquanto o setor público mira eficiência operacional (50%) e suporte à tomada de decisão (45%). Por sua vez, o segmento financeiro busca inovação (44%), seguida de diferencial competitivo (33%)[6].

Figura 3. Os benefícios esperados mais relevantes



Fonte: Parreira (2017)[6].

2.2 O IMPACTO DA ECONOMIA BRASILEIRA COM A IMPLANTAÇÃO DE IOT

As principais previsões sugerem que a implementação da Internet das Coisas terá grande impacto positivos na economia brasileira e mundial, dentre eles: cidades mais inteligentes, racionalização e flexibilização da produção, logística e transporte de bens, monitoramento remoto de pacientes, melhor uso de insumos para o agronegócio, melhora da eficiência energética e ampliação do acesso a serviços do setor financeiro.

Segundo a empresa de consultoria Mckinsey Brasil, em 2015 a IoT contribuiu com cerca de 11% do PIB global, algo em torno de US$11,1 trilhões, e algo em torno de mais de 34 bilhões de dispositivos conectados. Inserido neste senário, segundo a CISCO[8], o Brasil ocupará a 9º posição no cenário de crescimento econômico oriundo desta realidade, com um potencial estimado em US$ 70 bilhões até 2022. Medidas de avanço tecnológico como: dispositivos eletrônicos mais rápidos, eficientes, menores e baratos; redes ubíquas de telecomunicações; e sistemas avançados de armazenamento e processamento de dados, etc. Contribuía para esse avanço econômico, segundo dados do BNDES[7]. Outros dados apresentados são as estimativas propostas pela CISCO ao mercado brasileiro, onde mesura que o tráfego Wi-Fi/Fixo que em 2016 foi de 57% cairá para 53% em cinco anos, dando lugar a internet móvel, que mais que dobrará em 2021, saindo dos 7% mensurados no ano passado para 16% em 2021. Sem falar ainda no aumento da

representatividade de TVs 4K e o consequente tráfego de vídeo em IP, o qual chegará na casa dos Exabytes em 2021[8]. Essa realidade econômica se dará com a popularização do ecossistema de IoT em larga escala. Veremos algumas possíveis aplicações práticas oriundas desta nova realidade.

3 FUNCIONALIDADES DA IOT E SEUS TIPOS DE CONEXÕES

Uma das principais aplicações da Internet das Coisas, com certeza será proporcionar conforto e comodidade ao ser humano. Como na criação do controle remoto pela Zenith Radio Corporation (hoje subsidiária da LG Electronics)[9], os dispositivos IoT terão este foco: o conforto. Alguns exemplos desta “comodidade tecnológica”, tem-se:

- Controlar a luminosidade das lâmpadas residenciais com o seu Smartphone

Suponha que uma pessoa tenha acabado de chegar em casa após um longo dia de trabalho, mas percebe que todas as luzes estão apagadas, com isso terá que acende-las, todos uma de cada vez. Caso sua residência possuísse as lâmpadas inteligentes, que se conectam à rede, você poderia programa-las para acenderem no horário predeterminado, facilitando assim o seu trabalho e aumentando a comodidade. Em uma outra realidade, o usuário está prestes a ir dormir, mas se esquece de apagar a lâmpada de um cômodo distante. Com uma lâmpada inteligente (Figura 4) o usuário teria a possibilidade de apaga-la mesmo estando deitado em sua cama, ou quem sabe configurar sua luminosidade por um aplicativo por exemplo[10].

Figura 4. Lâmpada inteligente (*Smart Lamp*)

Fonte: Gazzarrini, 2014[10].

- Enviar e receber mensagens de para filhos de ursinho de pelúcia, dispensando os perigos de um celular:

Para que crianças não precisam, não querem ou não podem terem acesso aos smartphones na mais tenra idade, entretanto, permiti-las uma certa liberdade, já é possível enviar e receber mensagens por meio de um dispositivo eletrônico ligado à rede WiFi, embutido em um brinquedo de pelúcia (Figura 5). É isso que promete o ToyMail, da fabricante de mesmo nome. Assim que a mensagem chegar, enviada pelos pais, um alarme avisa a criança. E pelo próprio dispositivo ela consegue gravar e enviar uma mensagem de voz para quem começou a conversa[11].

Figura 5. Urso inteligente: dispensa o uso de celulares por criança pequenas

Fonte: ToyMail (2018)[11].

- Medir a temperatura de um ambiente, compartimento e enviar à uma central de controle:

Sensores localizados em diversos pontos de plantações (Figura 6) podem enviar informações precisas sobre temperatura local, umidade do solo, probabilidade de chuvas e seu posterior índice pluviométrico, velocidade do vento e outras informações essenciais para o bom rendimento do plantio[12].

Figura 6. Sensor de temperatura agropecuário

Fonte: Tagpoint, 2018[12].

Esses são alguns exemplos de uso inteligentes da Internet das Coisas, entretanto o campo de possibilidades é muito mais vasto, apenas não é o foco do trabalho em questão. Mas como essas funcionalidades se relacionam? A seguir serão apresentados os tipos de relacionamentos, ou conexões no universo IoT.

3.1 AS CONEXÕES NO UNIVERSO DA INTERNET DAS COISAS

Finalizando a ambientação sobre internet das coisas e já introduzindo um preambulo do primeiro objeto de estudo (Privacidade em IoT), vamos abordar os tipos de conexões existentes neste ecossistema, as quais, para implementar soluções de IoT, as empresas devem garantir, examinar e responder por estes três tipos de conexões: M2M, M2P e P2P. Estes são os tipos de relacionamento em que os dispositivos IoT interagem, para possibilitar uma heterogeneidade de comunicação.

- Conexões M2M: Dentre os componentes essenciais dos sistemas M2M (*Machine to Machine*, ou Máquina para Máquina) modernos estão incluídos sensores, atuadores e controladores. Eles devem ter um link de comunicações de rede e de programação que instrui a um dispositivo como interpretar dados e, com base em parâmetros predefinidos, encaminhar esses dados.

  As conexões M2M geralmente estão presentes no controle de ativos físicos, melhorando as operações por meio do sensor de dados e do monitoramento de

sistemas ou de máquinas de forma remota. O tipo mais comum de comunicação M2M é a utilização de sensores de telemetria, utilizados para monitorar comportamentos de forma remota e transmitir medidas de desempenho a um ponto central ou de controle. Produtos com recursos de comunicação M2M integrados são frequentemente comercializados como "produtos inteligentes".

Hoje em dia a heterogeneidade dos dispositivos não favorece a comunicabilidade entre eles. A M2M não possui uma plataforma padronizada de dispositivo conectado. Esses dispositivos se comunicam por meio de protocolos proprietários que são específicos de dispositivos ou tarefas, e são incapazes de se comunicar com outras plataformas. No entanto, à medida que as conexões M2M se tornam mais comuns, a necessidade de padrões acordados se torna mais importante. A comunicação M2M é um aspecto importante em muitos setores, como varejo, fabricação, serviço público e provedores de serviços.

- Conexão M2P: As pessoas desempenham um papel importante em aproveitar a inteligência artificial reunida por conexões M2M. As conexões M2P (*Machine to Person* – Máquina para Pessoa) resultantes são essenciais para a tomada de decisões. Por exemplo, sensores e monitores portáteis podem fornecer informações exatas sobre os sinais vitais de um paciente, mas os serviços de saúde são definitivamente responsáveis por usar essas informações para avaliar pacientes e fornecer tratamento. Conexões M2P significam que as pessoas podem enviar informações para os sistemas técnicos e receber informações desses sistemas. As conexões M2P são transacionais, ou seja, o fluxo de informações se move em ambas as direções, de máquinas para pessoas e de pessoas para as máquinas.

  As tecnologias M2P podem variar de sistemas automatizados de notificação ao cliente com disparadores predefinidos a painéis avançados que ajudam as pessoas a visualizar análises. As pessoas também podem executar operações M2P mais complexas, como testar e analisar os dados recebidos, assim como determinar como apresentar informações aos tomadores de decisões. Além de proporcionar melhorias na eficiência, a IoT oferece benefícios de segurança. Por exemplo, sensores em minas possibilitam a detecção de sinais de risco antes que ocorra um acidente. As vibrações no solo e nas rochas, ou alterações nos sinais vitais de uma pessoa, podem alertar em tempo real as interações M2M ou M2P que salvam propriedades, investimentos e vidas.

As conexões M2M e M2P são um aspecto importante de qualquer solução de IoT. Mas, para disponibilizar uma solução completa da IoT, os indivíduos devem se comunicar e colaborar com outras pessoas que usam conexões P2P.

- Conexões P2P: As conexões P2P (Person *to Person* – Pessoa para Pessoa) são caracterizadas por soluções colaborativas que aproveitam infraestruturas de rede, dispositivos e aplicativos novos e atuais. Essas plataformas otimizadas e seguras permitem que voz, vídeo e dados sejam apresentados em uma única visualização, para e de qualquer dispositivo móvel. Os aplicativos P2P também dão suporte à colaboração online via Web e videoconferências.

  Um dos exemplos da aplicação do P2P é o pagamento realizado pela aproximação do celular, “substituindo” assim as notas de papel, moedas e até o moderno cartão de crédito. A carteira digital, como é conhecida, também pode ser aplicada a postos de gasolina, máquinas de venda automática, compras on-line ou qualquer outro estabelecimento físico ou on-line que possua tecnologia *Near Field Communication* (NFC)[14].

Após esta inicial explanação do que é, e o que se espera da Internet das Coisas, através de aplicações práticas e seus níveis de interação, vamos agora tratar de um assunto de extrema importância quando se aborda este tema, o qual será encarado como primeiro desafio (privacidade dos dados em IoT) para uma realidade ecossistema em Internet das Coisas, onde tudo estará conectado em um fluxo frenético de transferência de dados, e muitos destes privados.

4 CONTEXTUALIZANDO A PRIVACIDADE EM IOT

Dizer que um dispositivo é “inteligente”, não significa dizer que ele é seguro ou que ele não traz vulnerabilidades aos consumidores. Pelo contrário. Conforme notado por estudos técnicos da área e pela própria consulta pública proposta pelo Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC)[13], a qual veremos em detalhes mais adiante, os riscos são elevados, considerando que as vulnerabilidades existem no software utilizado pelo dispositivo, na gestão de identidade e controle de acesso e na comunicação entre dispositivos e sistemas.

Precisa-se entender e discutir de forma ampla como lidar com as questões relacionadas à segurança e privacidade dos dados em um ambiente que, a cada momento, estará mais conectado, utilizando mais dados e informações potencialmente relacionadas aos indivíduos, em nome da melhoria da qualidade de vida, das prestações de serviços, pertinentes as suas liberdades individuais, dentre elas, localização, acesso a produtos, opções de compra, saúde, enfim, um verdadeiro perfil de consumidor.

A partir do momento que um dispositivo qualquer se conecta à rede mundial de computadores com dados do seu usuário, e transmite informações a outros dispositivos, uma infinidade de ameaças podem surgir, dentre elas: A violação de privacidade é a primeira, e mais recorrente. Como o ambiente M2M/IoT, pode-se coletar informações sobre um determinado usuário, e, alguma outra parte pode se aproveitar deste cenário, para de alguma forma, angariar informações outrora desconhecidas por parte do espião. Outro ponto a se destacar é a segurança física do usuário, a qual também pode ser afetada, uma vez que não é mais preciso ter proximidade física para causar lesões a indivíduos.

Como exemplo, uma ameaça possível na área residencial, seria possibilidade de provocar um vazamento de gás e explodir uma casa remotamente, pela simples possibilidade de controlar um fogão à distância. O que representa conforto, praticidade e comodidade, poderia significar uma grande tragédia, se utilizada e controlada por mentes criminosas.

Outro exemplo de ameaça possível é provocar acidentes remotamente em carros conectados. Os carros são o grande chamariz desta realidade de dispositivos inteligentes, desde a descoberta de combustíveis de energia renovável até sua desejável completa automação. Entretanto, esta facilidade eminente poderia causar

grandes tragédias se manipuladas de forma imperita, negligente ou até mesmo terrorista. Ou mesmo transmitir informações de seu trajeto diário, sem que seus condutores tenham ciência desta informação. Produzindo com isso uma gama de informações importantes sobre o usuário.

Como se sabe, a perspectiva é ter bilhões de dispositivos IoT espalhados pelo mundo em alguns anos. Pegando uma grande parcela destes, é possível realizar ataques distribuídos, como por exemplo, um ataque de negação de serviço à uma rede de transmissão e de distribuição de energia, ou mesmo a aeroportos de grandes cidades, onde potencializaria uma tragédia.

Alguns exemplos de falhas típicas em uma realidade de implantação do universo IoT, as quais serão fonte de ameaças ainda maiores no ambiente M2M/IoT, uma vez que esse novo ambiente é caracterizado por:

- Há dispositivos IoT feitos para serem descartáveis, como alguns sensores sem fio de baixa energia armazenada[15], os quais captam informações por um dado período de tempo e remetem a um controlador.
- Grande quantidade de fornecedores de dispositivos, muitos dos quais sem qualquer experiência comprovada em segurança da informação.
- Uma maior quantidade de dispositivos conectados, com isso, será bem maior a superfície de ataque[16].

Desse modo, fica claro que a segurança e a privacidade devem ser assuntos essenciais de qualquer modelo de referência para dispositivos IoT, sendo necessário uma implementação adequada em todos os níveis e camadas, do hardware ao software, das aplicações de negócio e de controle. Logo, 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.

4.1 QUANDO PRIVACIDADE ESTÁ A CARGO DO USUÁRIO

Quando se trata de privacidade no meio digital, deve-se lembrar que isto seja ofertado por direito. Realidade esta que não se observa comumente nos dias de hoje.

Alguns pontos comuns do dia a dia, serão necessários abordar neste momento, quando falamos em privacidade sob a exige do usuário final, dentre estas o acesso à web sites, redes sociais, aplicativos mobile etc.

A Tecnologia da informação e suas variantes, abriram as portas da imaginação e a realidade da auto divulgação. Esta possibilidade se dá devido ao uso indiscriminado das redes sociais[17]. O que, inicialmente, teria o objetivo de aproximar as pessoas, conhecias ou não, tornou-se um ambiente onde tudo é "postado" em busca de "curtidas" "likes", "seguidores" e "comentários", este último, aos milhares. Reclama-se de privacidade, entretanto com apenas uns cliques, é possível descobrir costumes, rotinas, preferências, amizades em comum, instituição e local de trabalho, e chegando a facilitar acesso a telefone e endereço residencial.

Um outro ponto a ser levado em consideração, são os acessos aos diversos web sites. Não especificamente aos de conteúdo impróprio, adulto ou de caráter duvidoso, o que já seria um atentado contra a segurança da informação. Mas aos chamados inofensivos, como sites de notícias, vídeos e principalmente os de compras no varejo. Ao realizar uma busca em um site de compras por exemplo, adquirindo ou não um produto, se é bombardeado posteriormente por anúncios indesejados, os quais se referem aos itens pesquisados[18]. Este é um simples exemplo de políticas de privacidades implícitas em seus códigos, que recolhem informações sem o consentimento consciente do usuário.

No site *http://politicaprivacidade.com/* existe a possibilidade de gerar automaticamente uma política de segurança pré-formatada, atribuir a um determinado site. Em seus primeiros textos de código em html, tem-se as seguintes informações:

```
<h2>Política de privacidade para <a href='http://www.siteteste.com.br'>Site de Teste TCC</a></h2><p>Todas as suas informações pessoais recolhidas, serão usadas para o ajudar a tornar a sua visita no nosso site o mais produtiva e agradável possível.</p>
```

Ao acessar um site com esta política, estamos concordando com essa prática implícita. Ou seja, o simples acesso a um site subentende que o usuário concorda com a política de privacidade do mesmo.

Como exemplo prático da política de privacidade de um site, cita-se o da empresa Americanas® em *https://www.americanas.com.br/***.** Inicialmente, o acesso a esta informação já é no mínimo não usual. Ela não vem de forma tão clara como se observa nas informações relativas aos produtos à venda, entretanto em uma busca não muito demorada encontra-se esta política. Esta informação, de suma importância por parte dos clientes, tão quanto o produto a ser comercializado, deveria estar mais aparente e conforme prevê literaturas do gênero, não demandar muito esforço dos usuários, disponibilizando um acesso mais intuitivo, como no trecho:

> "...Penso nisso da seguinte forma: Quando estou olhando uma página que não me faz pensar, tudo o que vem em minha cabeça são coisas como… OK, aí está o___, isto é um ___, aqui está o que eu quero..." (Não me faça Pensar, Krug, Steve. Cap 1, Pg 12).

Igualmente, ainda na busca de políticas de privacidade em outros sites, cita-se outro de grande apelação de consumo, o da Netshoes®, em *http://www.netshoes.com.br/*. Neste a informação vem de forma bem mais intuitiva e, para um usuário interessado neste tipo de informação, não será difícil o seu acesso.

Neste site, as informações são bem mais claras que as do site anterior, e ocupam um maior espaço da página, esclarecendo ao usuário toda e quaisquer dúvidas sobre o assunto. Deste vale ressaltar uma informação importante. Esta se refere à retirada dos "Cookies".

Contudo, os serviços podem não funcionar de maneira adequada com os cookies desabilitados.

> *Cookies*:
>
> Os principais navegadores de internet possibilitam ao cliente gerenciar a utilização dos cookies em sua máquina. A nossa recomendação é que mantenha o salvamento de cookies ligados. Desta forma, é possível utilizar todos os recursos de navegação personalizada oferecidos pela Netshoes, mas, caso o cliente não concorde, é possível desabilitar esta função.
>
> Para remoção dos *Cookies* ou *Cache* siga os procedimentos indicados pelos fabricantes* para cada navegador…(*http://www.netshoes.com.br/*).

Basicamente, um *Cookie* é um arquivo de texto muito simples, cuja composição depende diretamente do conteúdo do endereço Web visitado. Por exemplo, a maioria dos sites armazenam informações básicas, como endereços IP e preferências sobre idiomas, cores, etc. Contudo, em portais como o Gmail e o Hotmail, nomes de usuários e senhas de e-mail também fazem parte dos *Cookies*.

Quando você visita um site pela primeira vez, este envia um *Cookie* como resposta para o seu navegador, contendo as suas preferências, em formato de texto. Este pequeno arquivo ficará armazenado em seu computador até que perca sua validade.

Enquanto o *cookie* estiver salvo em seu PC, toda vez que você digitar o endereço do site, o seu navegador enviará este arquivo para o site que você está conectado. Desta maneira, as suas configurações serão aplicadas de maneira automática. Esta utilização de *Cookies*, segundo o site, serve para montar um perfil de consumo do cliente.

Esses são pequenos exemplos em que o indivíduo é responsáveis ou corresponsáveis pela perda ou violação de sua própria individualidade. Pois ao acessar um determinado site, já estamos concordando com sua política. Entretanto nesta relação não há paridade de armas, uma vez que o consumidor, em caso de desacordo com a política empregada, não pode negociar tal prática com o site[18].

5 A INDIVIDUALIDADE E A DELIMITAÇÃO DE SEU ESCOPO

A realidade virtual se confunde com a real quando se está falando de tecnologia da informação. Entretanto, muitas vezes encontra-se no meio virtual uma forma de fuga, seja dos problemas, das pessoas, da falta ou excesso de algo. Também há quem acredite que nos meios de TI, é possível se esconder, ou camuflar atitudes levianas, discursos de ódio e posturas criminosas. Segundo definição dada pela assessora Jurídica do Nic.br, a Dra Kelli Angelini, no V seminário de Proteção à Privacidade e aos Dados Pessoais, “o ordenamento jurídico brasileiro relacionado à privacidade dos dados na internet, se assemelha à uma colcha de retalhos”, tendo em vista a sua fragmentação em diversas leis e dispositivos legais, tais como: Constituição Federal, Novo Código Civil, Código de Defesa do Consumidor, Lei das Comunicações, Marco Civil da Internet, entre outros.

Contudo observa-se que o direito do cidadão à privacidade, refere-se não só ao mundo real, mas também ao mundo virtual, o qual também está contemplado na ordem jurídica brasileira, bem como deve ser uma garantia, em face de se configurar como critério para a identificação e tomada de medidas em razão de violações virtuais, estas que se multiplicam cotidianamente, gerando danos à pessoa.

Sugere-se que seria comum raciocinar que existe alguma diferença entre a segurança da integridade física propriamente dita, e segurança de dados pessoais. Mesmo sendo estes assuntos diretamente ligados a vida privada da pessoa. Ou seja, há uma tênue diferença entre o direito à privacidade virtual e o direito à privacidade material. Pode-se inferir que, entre os direitos da personalidade humana, existem aqueles que, potencialmente, são mais suscetíveis de violação que outros, o que é o caso dos direitos à privacidade no mundo virtual. Para ter privacidade em IoT, os indivíduos deveriam ser capazes de determinar quando outros podem coletar e como eles podem usar suas informações pessoais. Isso requer uma habilidade suficiente para o controle de coleta e uso, e a capacidade de dar ou reter consentimento livre e esclarecido[19]. Parafraseando Pedro Vasconcelos, personalidade é a “qualidade de ser pessoa” (VASCONCELOS, Pedro Pais de, Direito de Personalidade. Coimbra: Almedina, 2006). Nesse caminho, os direitos de personalidade têm a ver com a posição das pessoas humanas no direito, com a exigência de sua dignidade.

A Será apresentado mais a frente, trechos de algumas legislações pertinentes ao assunto, para que se possa ter uma ideia de como está sendo tratado questões de privacidade em IoT, dentre elas, o polêmico Marco Civil da Internet.

Recentemente, o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC) lançou, uma consulta para subsidiar o Plano Nacional de Internet das Coisas no site *http://www.participa.br/cpiot/itens-da-consulta*. O objetivo é construir um mapa de empresas e instituições científicas e tecnológicas (ICTs) que ofertam tecnologias, produtos, serviços e soluções de IoT no Brasil. Esse mapeamento vai facilitar muito a troca de informações e a formação de parcerias entre as empresas e as ICTs, o que será essencial para o desenvolvimento do setor. Os dados serão recebidos pelo consórcio que está conduzindo o estudo que irá apoiar o Plano Nacional de IoT. Este estudo foi estruturado e coordenado em parceria pelo Banco Nacional de Desenvolvimento Econômico e Social (BNDES) e pelo MCTIC, o qual inclui três fases: diagnóstico e aspiração do Brasil em IoT; definição dos setores prioritários da economia brasileira para receber investimentos necessários para o desenvolvimento de IoT; e formulação de ações voltadas para acelerar a implantação do mercado de IoT no país. Inserido nesta consulta pública, como já era de se imaginar, existe um tópico inteiramente destinado à segurança e privacidade em IoT permeado com um rico debate sobre o tema.

5.1 O PARADIGMA DO DIREITO À PRIVACIDADE

Antes de abordar de forma mais ampla as legislações em vigor que tratam deste assunto, e diante do acima exposto, o país se viu frente a grande necessidade de legislar sobre privacidade e uso dos dados digitais. Inicialmente, por volta de 2009, quando dos primeiros debates a cargo do Poder Executivo sobre dados pessoais e privacidade no Brasil, os responsáveis se viram na necessidade de atribuir uma conduta nacional, entretanto encontravam-se sobre dois paradigmas de regulamentação, o Europeu e o Americano, ambos de grande relevância, entretanto contrapostos em muitos pontos[18].

Sobre a diretiva europeia, tem-se que é mais conservadora se comparada a americana, e tem o objetivo de restituir aos cidadãos o controle sobre os dados pessoais e simplificar o quadro regulamentar para as empresas. Possuindo as

seguintes características: acesso facilitado aos dados, liberdade de transferência entre os servidores, consentimento explicito, jurisdição e territorialidade[20].

Nos EUA não há um marco geral normativo de controle de acesso aos dados, mas sim leis fragmentadas e setorizadas que regem este assunto. Valendo-se, em algumas situações do ditado “cada caso é um caso”, interpreta de forma individualizada os casos de privacidade de dados, guardadas as devidas proporções.

Esta disparidade entre os dois modelos de controle de informações observados na UE e nos EUA, causavam uma grande dificuldade sobre a transferência de dados/informações entre as duas regiões geográficas, pois apesar de uma potência econômica, os EUA sempre presaram pela liberdade, e isto causa reflexo também quando o assunto é privacidade de dados na tecnologia da informação. Contudo, nos anos 2000 foi criado um instrumento de auto certificação, onde as próprias empresas responsáveis por armazenar os dados dos clientes, garantiam a privacidade na manipulação destes dados, e isso, amenizou a principal pendência para transferência de dados entre essas duas regiões. Contudo deixar às empresas a responsabilidade de policiar-se acerca do acesso/divulgação de dados tornou-se potencialmente perigoso.

O caso conhecido como o “Caso de Edward Snowden”[21], motivou a revogação desta lei, uma vez que revelou em detalhes alguns dos programas de vigilância que o país usa para espionar a população americana, utilizando servidores de empresas como Google, Apple e Facebook – e vários países da Europa e da América Latina, entre eles o Brasil, inclusive fazendo o monitoramento de conversas da presidente Dilma Rousseff com seus principais assessores.

A escolha pelo modelo europeu, baseado na proximidade de entendimento e perfil brasileiro, e em função do quadro constitucional, que coloca a privacidade, a preservação da vida privada como direitos fundamentais do cidadão. Com isso o Marco Civil da Internet trouxe mais profundidade sobre o assunto, legislação essa que será abordada com mais detalhes a frente.

Mesmo com a doção de um modelo de excelência, segundo os debatedores do VIII Seminário de Privacidade deste ano contou com importantes nomes da proteção de dados em outros países, como México, Chile e França. Não que precisasse ser lembrado, especialmente considerando o público-alvo dos discursos,

mas todos foram enfáticos em alertar para o atraso brasileiro na regulamentação da proteção de dados.

No âmbito internacional, somos um país com nível de proteção de dados considerado insuficiente e inadequado, o que, além de gerar tremenda insegurança para titulares de dados e empresas da economia digital, afasta, diariamente, incontáveis oportunidades de investimento no Brasil.

Para corrigir essa lacuna legislativa, o Deputado Federal Orlando Silva do PCdoB de São Paulo**,** presente no evento na qualidade de um dos parlamentares à frente da condução do principal Projeto de Lei sobre o tema (PL 5276/2016, que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.), garantiu que não está medindo esforços para que o texto legislativo seja votado no plenário o quanto antes. Por outro lado, o cenário político conturbado enfrentado pelo país, dificulta que a tramitação ocorra com a celeridade necessária.

Para que termine estas breves considerações com certo otimismo, é importante destacar que o Governo Federal, por meio de representante do Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), confirmou que pretende consolidar o plano de transformação digital (atualmente em consulta pública) até o final deste ano. A boa notícia é que a proteção aos dados pessoais é um dos eixos fundamentais de tal plano, espera-se que fatores políticos sejam catalisadores (e não obstáculos) da aprovação da necessária Lei Geral de Proteção de Dados Pessoais.

5.2 O FRACIONAMENTO DOS DADOS INDIVIDUAIS NA NUVEM E SUA JURISDIÇÃO

Qual a importância de falar de privacidade no ecossistema de internet das coisas? Antigamente, o termo tecnologia remetia a apenas um nicho da sociedade, referia-se apenas às pessoas com maior proximidade com os meios de tecnologia da informação. Entretanto, hoje em dia, todas as áreas da esfera profissional, pessoal e privada do indivíduo são afetadas, e isto gera consequências incalcináveis, trazendo a necessidade de alguma regulamentação, a cerca desta imensa quantidade de dados hoje em circulação. Tudo em volta sofre tendências da tecnologia, relações pessoas e familiares, economia, cadeias de produção,

comunicações, moda, esportes, etc. Isto se deve a grande quantidade de dispositivos conectados à internet, os “Smart tudo”, celulares, relógios, eletros domésticos[1], bem como a grande quantidade de dados gerados a partir destes dispositivos.

Quando se fala em dados, principalmente aos relacionados à IoT, logo sobrevém o termo empregado para esse fim: “BIG DATE”. Talvez um pouco impreciso, mas refere-se a grande quantidade de informações geradas como já abordamos no início deste trabalho. No ambiente de Internet das Coisas, quando se fala em dados, inevitavelmente, remete-se à armazenamento na nuvem.

O *cloud computing* é carro-chefe da internet das coisas. Computação em nuvem é uma das tecnologias mais importantes do mundo dos negócios atualmente. Com um mercado global que deve alcançar 120 bilhões de dólares em 2018, Computação em Nuvem e Internet das Coisas caminham juntas para estabelecer um novo cenário de tecnologia mundial. A Internet das Coisas demanda Computação em Nuvem em diversos níveis de serviço, incluindo infraestrutura, plataforma, software e análise de dados. Em um mundo com bilhões de dispositivos gerando dados, serão necessários serviços escaláveis, robustos e de alta disponibilidade para armazenar, processar, personalizar e entregar informações de alto valor agregado para os clientes, a qualquer momento, em qualquer lugar.

Não é tema deste trabalho explicar os conceitos e aplicações da nuvem em internet das coisas, mas sim, relaciona-la com a privacidade dos dados e com o ordenamento jurídico de IoT. Pois bem, em que as duas se relacionam? Em tudo. Principalmente quando falamos em jurisdição, tendo em vista os dados estarem trafegando em países diferentes, com regras de privacidade diferentes, o que dificulta o tratamento de assuntos específicos sobre privacidades com dados pulverizados em diversos servidores, localizados em diversos países.

As indústrias produtoras destes dispositivos têm função importantíssima na efetividade destas leis, uma vez que produzem equipamentos, onde o próprio usuário delimite seu nível de privacidade, ou mesmo níveis diferentes, para grupos diferentes. Todas as exposições da lei as quais estão em um nível de abstração muito grande não se efetivarão se não tiverem o comprometimento da indústria para torná-las reais e manejável por parte do titular dos dados.

6 O ORDENAMENTO JURÍDICO BRASILEIRO EM IOT SEUS PARÂMETROS

No mês de setembro deste ano, ocorreu em São Paulo um dos mais importantes eventos sobre Privacidade e Proteção de Dados: o VIII Seminário de Proteção à Privacidade e aos Dados Pessoais, como já referenciado neste trabalho anteriormente, idealizado pelo Comitê Gestor da Internet (CGI.br) em parceria com o Núcleo de Informação e Coordenação do Ponto BR (NIC.br). Foram abordados diversos temas, como criptografia irreversível, autoridade garantidora da proteção de dados, o atraso brasileiro em produzir uma regulamentação consistente sobre a privacidade dos dados, entre outros.

Observar-se-á agora observar o que de mais relevante existe em relação a segurança e manipulação dos dados pessoais no ordenamento jurídico brasileiro. Inicialmente na a Constituição Federal, de 1988, em seu Art. 5º que trada da Direitos e Deveres Individuais e Coletivos, tem-se:

> Inciso 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;
>
> Inciso 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;
>
> Inciso 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;
>
> Inciso LXXII - conceder-se-á *habeas data*:
>
> a) para assegurar o conhecimento de informações relativas à pessoa do impetrante, constantes de registros ou bancos de dados de entidades governamentais ou de caráter público;

No Novo Código Civil, Lei Nº 10.406, de 10 Jan 2002, versa sobre os direitos da personalidade, do não constrangimento e da inviolabilidade da vida privada:

> Art. 11. Com exceção dos casos previstos em lei, os direitos da personalidade são intransmissíveis e irrenunciáveis, não podendo o seu exercício sofrer limitação voluntária.
>
> Art.12 Pode-se exigir que cesse a ameaça, ou a lesão, a direito da personalidade, e reclamar perdas e danos, sem prejuízo de outras sanções previstas em lei.

> Parágrafo único. Em se tratando de morto, terá legitimação para requerer a medida prevista neste artigo o cônjuge sobrevivente, ou qualquer parente em linha reta, ou colateral até o quarto grau.
>
> Art. 13. Salvo por exigência médica, é defeso o ato de disposição do próprio corpo, quando importar diminuição permanente da integridade física, ou contrariar os bons costumes.
>
> Parágrafo único. O ato previsto neste artigo será admitido para fins de transplante, na forma estabelecida em lei especial.
>
> Art. 14. É válida, com objetivo científico, ou altruístico, a disposição gratuita do próprio corpo, no todo ou em parte, para depois da morte.
>
> Parágrafo único. O ato de disposição pode ser livremente revogado a qualquer tempo.
>
> Art. 15. Ninguém pode ser constrangido a submeter-se, com risco de vida, a tratamento médico ou a intervenção cirúrgica.
>
> Art. 16. Toda pessoa tem direito ao nome, nele compreendi dos o prenome e o sobrenome.
>
> Art. 17. O nome da pessoa não pode ser empregado por outrem em publicações ou representações que a exponham ao desprezo público, ainda quando não haja intenção difamatória.
>
> Art. 18. Sem autorização, não se pode usar o nome alheio em propaganda comercial.
>
> Art. 19. O pseudônimo adotado para atividades lícitas goza da proteção que se dá ao nome.
>
> Art. 20. Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se se destinarem a fins comerciais.
>
> Parágrafo único. Em se tratando de morto ou de ausente, são partes legítimas para requerer essa proteção o cônjuge, os ascendentes ou os descendentes.
>
> Art. 21. A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma.

Até mesmo no Código de Defesa do Consumidor, Lei nº 8.078, de 11 Set de 1990(Publicada no suplemento ao DOU de 12/9/1990), aborda assuntos relativos a privacidade das informações em seu Art nº 43, quando fala em veracidade dos dados armazenados ou sua devida correção, o direito ao acesso às informações bem como o caráter dos bancos de dados relativos ao consumidor.

> art. 43. O consumidor, sem prejuízo do disposto no art. 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e

> de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes.
>
> § 1º Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a período superior a cinco anos.
>
> § 2º A abertura de cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele.
>
> § 3º O consumidor, sempre que encontrar inexatidão nos seus dados e cadastros, poderá exigir sua imediata correção, devendo o arquivista, no prazo de cinco dias úteis, comunicar a alteração aos eventuais destinatários das informações incorretas.
>
> § 4º Os bancos de dados e cadastros relativos a consumidores, os serviços de proteção ao crédito e congêneres são considerados entidades de caráter público.

A privacidade dos dados pessoais também é abordada na Lei das Telecomunicações (Lei nº 9.472, de 16 Jul 97).

> Art. 3º O usuário de serviços de telecomunicações tem direito:
>
> .....
>
> inciso IX - ao respeito de sua privacidade nos documentos de cobrança e na utilização de seus dados pessoais pela prestadora do serviço;

O Marco Civil, é uma lei que visa orientar os direitos e deveres dos usuários, provedores de serviços e conteúdos e demais envolvidos com o uso da internet no Brasil. Marco Civil da Internet é o nome popular da Lei nº 12.965, de 23 de abril de 2014 – conhecida por “Constituição da Internet” – e é responsável por estabelecer os princípios e garantias normativas do convívio civil na rede mundial online de computadores.

O principal objetivo do Marco Civil da Internet é prevê práticas criminosas no contexto online (cibercrimes), além de prezar pelos ideais da neutralidade de rede, liberdade de expressão, da privacidade dos usuários e dos direitos humanos. A neutralidade de rede consiste na “democratização” da qualidade e velocidade do acesso à internet, sem discriminações de conteúdos que estão disponíveis no ambiente online. O princípio da liberdade de expressão garante a impossibilidade da censura por parte dos sites e redes sociais, por exemplo, que ficam proibidos de excluir conteúdos dos usuários sem determinação exclusiva de uma ordem judicial (com exceção de conteúdos com nudez ou atos sexuais explícitos e privados, por

exemplo). Como observado na emenda proposta pelo deputado Áureo (SD-RJ), a qual previa os provedores de aplicativos e redes sociais fossem obrigados a suspender a publicação quando for denunciada por ter informação falsa ou discurso de ódio até que o autor seja identificado. Esta emenda foi vetada pelo presidente da república[22].

Dentre outros fatores acerca dos direitos e garantias do usuário, o Marco Civil da Internet prevê:

> Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
>
> 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, salvo por ordem judicial, na forma da lei;
>
> III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
>
> ……
>
> VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
>
> VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:
>
> a) justifiquem sua coleta;
>
> b) não sejam vedadas pela legislação; e
>
> c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;
>
> IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
>
> X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta lei;
>
> Subseção II – Da Guarda de Registros de Acesso a Aplicações de internet na Provisão de Conexão.

Ainda na análise do Marco Civil da Internet, temos no Art. 10º a abordagem Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

> Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais

e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no caput, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no caput não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no caput aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no caput aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10º e 11º ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

> II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
>
> III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
>
> IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11º.
>
> Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o caput sua filial, sucursal, escritório ou estabelecimento situado no País.

Outras disposições ainda nesta lei temos

> Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento.
>
> Art. 14º. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.
>
> Subseção III – Da Guarda de Registros de Acesso a Aplicações de internet na Provisão de Aplicações
>
> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de seis meses, nos termos do regulamento.
>
> Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

E mais:

- Projetos: APL, PL nº 181/2014;
- Projeto de Lei nº 131/2014;
- Projeto de Lei nº 330/2013 – Senado;
- Projeto de Lei no 4060/2012 Câmara.
- Projeto de Lei N.º 5.276, de 2016.

Com relação à privacidade e proteção de dados pessoais, entende-se que o fomento da indústria de Internet das Coisas, sem a aprovação da lei geral de proteção de dados pessoais é extremamente danosa, considerando que o projeto de lei n. 5276/16 estabelece uma sistemática principiológica sobre a coleta e tratamento de dados pessoais, definindo regras fundamentais como o “legítimo interesse” (coleta de dados a partir do que foi informado ao consumidor e para os fins legítimos daquela atividade comercial) e o “princípio da necessidade”, que afirma: ser dever daquele que realiza a coleta e processamento de dados a utilização mínima, limitada ao necessário, para as funcionalidades esperadas pelo consumidor. As considerações sobre privacidade e proteção de dados pessoais não devem se ater apenas os dispositivos relacionados ao consentimento expresso do Marco Civil da Internet (art. 7., inciso IX), mas devem considerar a arquitetura jurídica presente nos diversos dispositivos legais, fruto de amplos debates com a sociedade civil e diferentes partes interessadas[18].

Este trabalho traz a seguinte reflexão sobre privacidade e justiça:

- Regulamentação da lei, bem elaborada;
- Corregulamentação por parte das empresas;
- Proteção via Tecnologia dos próprios dispositivos;
- Mobilização da própria população para a proteção de dados. (Conscientizar a população acerca de privacidade de dados e segurança da informação, a partir das mais tenras idades, principalmente nas escolas, bem como nas universidades).

7 PROTOCOLO IP VERSÃO 6 (IPV6)

A internet deixou de ser uma rede majoritariamente acadêmica e militar e passou a ser explorada economicamente no fim da década de 1980. Com o objetivo inicial de comunicação entre máquinas, hoje a internet une pessoas, empresas e instituições. Assim, vive -se uma grande transformação, que foi o berço das redes sociais, que se tornam, cada vez mais, meios de comunicação mais usados em detrimento de outros meios ditos mais tradicionais ou usuais.

Uma etapa nova está se iniciando. Com ela, vem a capacidade de interconexão de vários tipos de dispositivos, exigindo cada vez mais disponibilidade de números de IP, utilizados para o encaminhamento de dados dentro desta nova grande rede. Não necessariamente computadores tradicionais. No passado, estimava-se que quatro bilhões de IPs seriam suficientes para atender a demanda por décadas, porém, o protocolo utilizado atualmente, IPv4, já está esgotado, tornando-se assim um obstáculo a ser superado.

Esse problema é antigo. Já em 1992, surgiram as primeiras iniciativas para repensar a organização de endereçamento IPv4. Ações como o CIDR (*Classless Inter-Domain Routing*), o DHCP e o NAT – com o princípio básico de extinguir o uso de classes de endereços, permitindo a alocação de blocos de tamanho apropriado à real necessidade de cada rede, acabaram ampliando a vida desta versão de IP. Com a avaliação dessas e outras propostas, foi definida, em 1996, a primeira versão do IPv6, que foi oficializada em 1998.

O IPv6, conhecido também como “IPng” – *Internet Protocol Nex Generation* Protocolo de Internet da Próxima Geração, que tem como objetivo em longo prazo substituir o IPv4, uma vez que o número de suas possibilidades é praticamente infinitas: estima-se que seja um número superior a 341 decilhões de ips, ou seja, 2^{128} ou $3{,}4\times10^{38}$, ou ainda 340.282.366.920.938.463.463.374.607.431.768.211.456 endereços IP disponíveis.

É fato que esse novo protocolo resolverá o problema de limitação do endereçamento IPv4, mas, embora isso seja altamente relevante, vale destacar que o IPv6 gerará um novo paradigma de rede e mobilidade. Com ele, o novo mundo será conhecido como a era da "Internet das Coisas", pois possibilitará que tenhamos conexão em todos os dispositivos eletrônicos e, inclusive, em eletrodomésticos. A

grande vantagem é que tudo isso será possível sem preocupações com a economia de IP, pois haverá disponibilidade para qualquer pessoa, empresa e quaisquer dispositivos que precisem ser conectados à internet.

O IPv4 se esgotou e o IPv6 resolve o problema ampliando exponencialmente as possibilidades de conexão. Com isso, também expande a mobilidade e abre uma ampla gama de oportunidades para novos serviços, aumentando a demanda por profissionais especializados. Por isso, podemos afirmar com segurança: uma nova era de possibilidades já começou e o momento do IPv6 é agora.

7.1 COMO ESTÁ O PROCESSO DE MIGRAÇÃO NO BRASIL E NO MUNDO

Quando os endereços IPs na versão 4 foram criados nos anos 80 pensou-se que 4,2 bilhões de endereços seriam suficientes para todas as necessidades computacionais, e como vimos não foi. A entrada de cada vez mais dispositivos e aplicações na rede mundial, fizeram com que esse valor se esgotasse rapidamente. É importante destacar que esse momento já vinha sendo anunciado e esperado há bastante tempo, mas não deixa de ser um marco importante. O estoque de endereços IP é um recurso finito e limitado, e o crescimento de usuários e serviços na internet implicou naturalmente em um consumo mais rápido desses recursos, mesmo com todas as medidas técnicas paliativas adotadas desde 1996. A solução para o contínuo crescimento da rede é o uso do endereçamento IP na versão 6 (IPv6), que tem um enorme espaço de endereçamento, de tamanho adequado para atender por muito tempo as necessidades futuras da internet.

Anunciado desde junho de 2014, o esgotamento do protocolo de endereçamento IPv4, foi separado em quatro fases pela LACNIC (registro de endereços da internet para a América Latina e o Caribe), entidade que cuida dos endereçamentos na América Latina. A qual define de forma gradual o esgotamento desta versão de endereços. A partir de agora, apenas novas empresas, que não haviam ainda solicitado espaço IPv4, poderão solicitar um número limitado de endereços (1.024), sem possibilidade de renovação do pedido. De acordo com o LACNIC, ainda existe uma reserva de 4,242432 milhões de endereços IP, com a possibilidade de o número até aumentar com a recuperação de endereços revogados e recebidos pela *Internet Assigned Numbers Authority* (IANA), que

controla os números e alocações de endereços. Ainda assim, a diretriz agora é encorajar a adoção em massa da geração mais nova de protocolo, o IPv6[4].

Segundo dados da LACNIC, a situação é a de última fase do esgotamento gradual de endereços do protocolo IPv4 na América Latina, área sob responsabilidade do órgão. Nesta fase, contém a reserva do último espaço de endereços disponíveis, composto por blocos de IPv4 alocados pela *Internet Assigned Numbers Authority* (IANA), que traduzido seria Autoridade para Atribuição de Números da Internet, junto com blocos recuperados e devolvidos. Desse espaço somente poderão ser feitas designações entre um /22 e um /24. Cada novo membro poderá receber apenas uma designação inicial desse espaço. A Tabela 1 apresenta como se encontra o Relatório de Alocações de Endereços IPv4 – Fase 3.

Tabela 1. Relatório de alocações de endereços

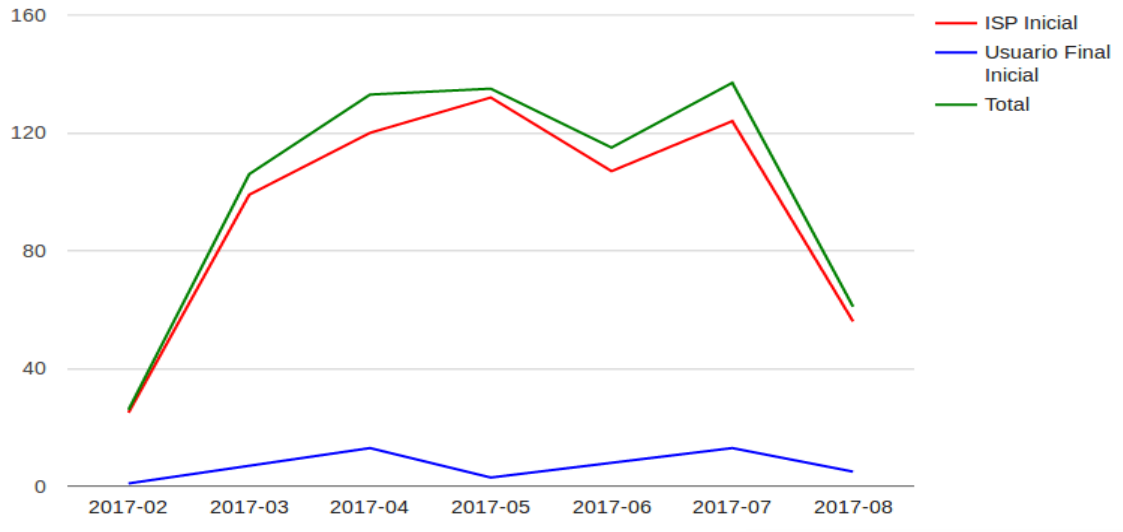
Relatório de Alocações de Endereços IPv4 - Fase 3			
Reservados para a Fase 3	**Alocados nesta fase**	**Devolvidos/ revogados nesta fase**	**Disponíveis nesta fase:**
4963584	721152	850432	4242432

Fonte: Lacnic, 2018[4].

Como a finalização de estoque de IPv4, as empresas da América Latina e do Caribe precisarão implantar o IPv6 em suas redes. No Brasil, muitas organizações já alocaram seus blocos IPv6, mas ainda será necessário substituir os equipamentos dos clientes, como modems e roteadores, por exemplo. Isso não será feito de uma vez só: a transição será gradual e acontecerá nos próximos anos.

A maioria dos sistemas operacionais e dispositivos novos já suportam ambos os protocolos. Ultimamente, percebe-se um aumento significativo na quantidade de IPv6 entre equipamentos, que têm sido atualizados e permitem que usuários façam comunicação exclusiva em IPv6. Nos Estados Unidos e na Europa o endereçamento de versão 4 já finalizou, o último continente a ter endereços IPv4 esgotados será a África: a previsão é que isso aconteça por volta de 2020. O gráfico apresentado na Figura 7, mostra a quantidade de endereços IPv4 alocados dentro da FASE 3 (Última fase -Iniciada em 15 Fev 2017).

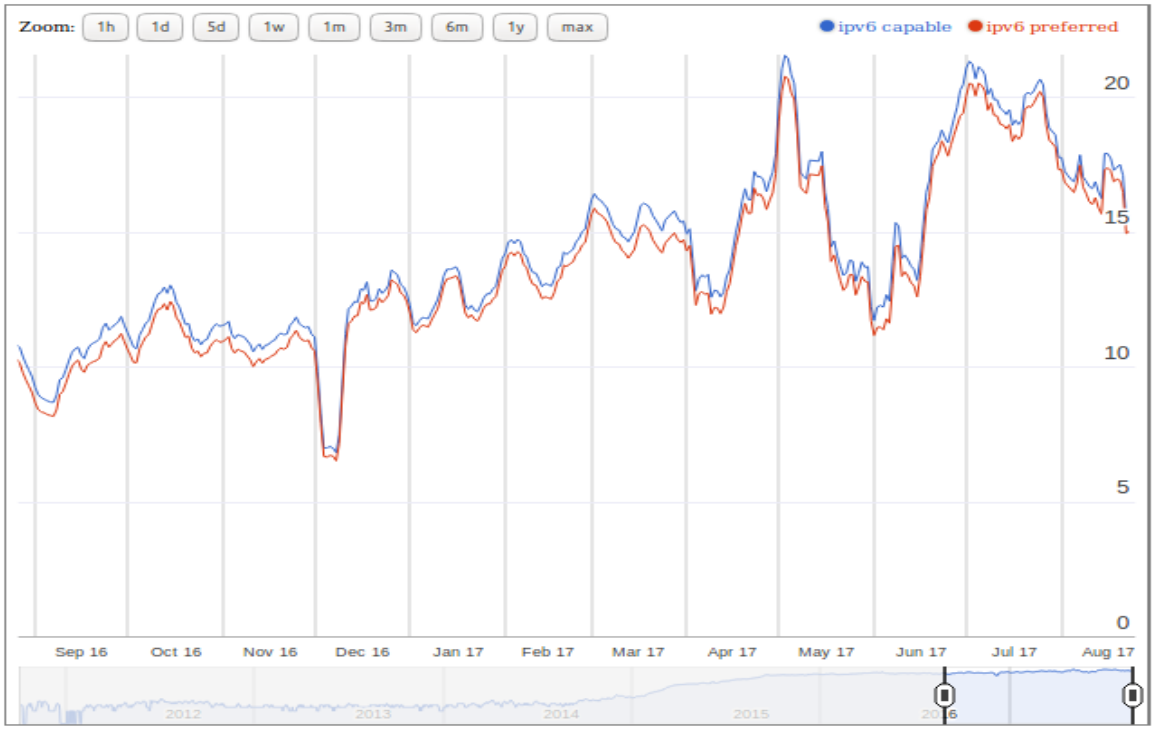
Figura 7. Quantidade de endereços IPv4 alocados dentro da FASE 3



Fonte: Lacnic, 2018[4].

Observa-se no gráfico da Figura 8, como está o percentual de adesão ao protocolo IPv6 no país. Esta informação pode ser acessada em tempo real no site da LACNIC.

Figura 8. O percentual de adesão ao protocolo IPv6 no Brasil



Fonte: Lacnic, 2018[4].

Na Tabela 2 tem-se a adesão do IPv6 no mundo, observada por continentes.

Tabela 2. Adesão por continente do protocolo IPv6

Code	Region	IPv6 Capable	IPv6 Preferred	Samples
XA	World	15.46%	14.87%	425,077,943
XG	Unclassified	86.70%	86.40%	4,778,507
XC	Americas	24.70%	23.58%	84,427,230
XE	Europe	15.37%	14.90%	70,807,587
XD	Asia	14.46%	13.95%	230,243,264
XF	Oceania	12.86%	11.83%	3,407,119
XB	Africa	0.64%	0.63%	36,192,570

Fonte: Lacnic, 2018[4].

8 ENTENDENDO O PORQUÊ DA MANUTENÇÃO DO PROTOCOLO IPV4 EM DETRIMENTO DO IPV6

Neste capítulo, serão abordadas algumas informações técnicas, as quais dão semântica ao novo protocolo de endereçamento, uma vez que o IPv6 foi bastante impulsionado pelo surgimento dos smartphones, a expansão das redes 3G, 4G e 5G, a computação ubíqua, ou computação pervasiva (é um termo usado para descrever a onipresença da informática no cotidiano das pessoas). Com isso tem-se a necessidade de atribuir uma identificação individualizada, ou seja, endereços válidos a cada um destes dispositivos, chamada também de comunicação fim a fim. Tudo isto graças ao seu tamanho de 128 bits, o que faz o IPv6 ser cerca de 79 trilhões de vezes maior que IPv4.

Os pacotes IPv6 não são fragmentados nos roteadores intermediários, como ocorre no IPv4, pois isso é considerado um desperdício de recursos. No IPv4, como a origem não sabe o MTU das redes vizinhas, normalmente ocorre de encaminhar pacotes maiores que a capacidade destas redes, gerando latência e desperdício de recursos na comunicação. No IPv6, a fragmentação só ocorre na origem, essa estratégia diminuiu a carga sobre os roteadores no meio do caminho.

Contrariando o que alguns dizem sem conhecimento de causa, o IPv6 não é uma atualização do IPv4, é um protocolo completamente novo que exige um grande esforço de implementação nos equipamentos de rede (roteadores e switches), nos sistemas operacionais e nas aplicações que foram criadas para suportar apenas o protocolo IPv4.

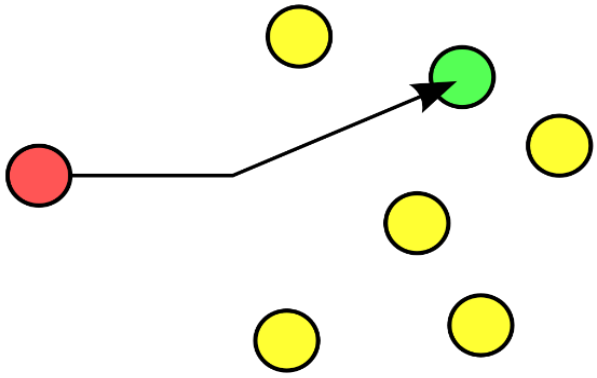
O formato de seu endereço difere e muito do seu antecessor: 2221:0CC8:DD1F:12D0:BABA:AAFD:B1FF:84C1. As Sequências de 0000 podem ser omitidas e trocadas por “::” ou “:0:”, como exemplo, temo o endereço 1080:0:0:0:8:0400:200C:0417 torna-se 1080::8:400:200C:417. Apenas uma sequência de zeros pode ser simplificada para não gerar um endereço errado, como em 1080:0000:0000:A3CC:0000:0000:200C:0417 podendo-se simplificar para 1080:0:0:A3CC::200C:417 ou 1080::A3CC:0:0:200C:417. Caso seja simplificada as 2 sequências de “zeros”, não seria possível deduzir a sequência original.

8.1 PROPAGAÇÕES DO PROTOCOLO IPV6

O IPv6 não propaga em broadcast. Este tipo de comunicação é aquela onde um quadro é enviado de um endereço para todos os outros endereços. Nesse caso, há apenas um remetente, mas as informações são enviadas para todos os receptores conectados. O IPv6 possui três tipos de encaminhamento:

a. *Unicast*: Comunicação na qual um quadro é enviado de um único *host* na rede, e endereçado a um destino específico, camada também de comunicação fim à fim. Na transmissão *unicast*, apresentada na Figura 9, há apenas um remetente e um receptor. A transmissão *unicast* é a forma predominante de transmissão em redes locais e na internet com p IPv6.

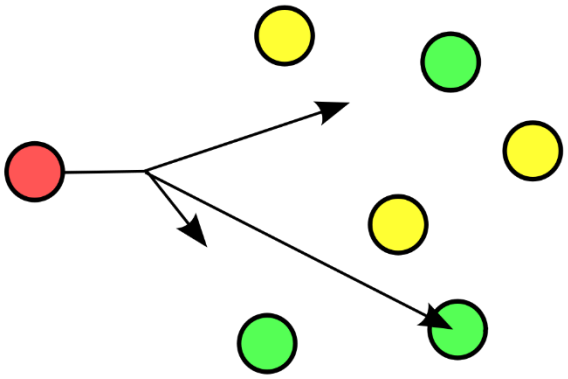
Figura 9. Propagação *unicast* do IPv6



Fonte: Cunha (2012)[23].

b. *Anycast*: Identifica um conjunto de *hosts* e encaminha os pacotes para os destinos próximos da origem desses pacotes (Figura 10). Possibilitando com isso o balanceamento de carga e redundância em *clusters* e nuvem. Transfere para no nível do protocolo de rede a capacidade redundância e balanceamento de carga. Como exemplificação, cito a realidade de quando uma pessoa liga para o 190 (Policia Militar), mesmo que seu celular seja de um outro estado, a chamada é direcionada para as forças de segurança local, isso de forma transparente ao usuário.

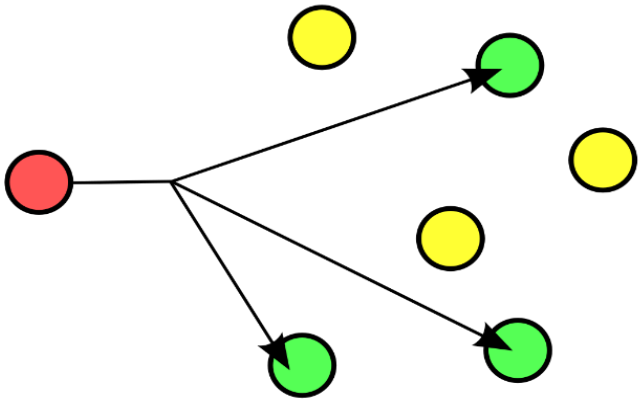
Figura 10. Propagação *anycast* IPv6



Fonte: Cunha (2012)[23].

c. *Multicast*: Comunicação na qual um quadro é enviado para um grupo específico de dispositivos ou clientes (Figura 11). Os clientes da transmissão *multicast* devem ser membros de um grupo multicast lógico para receber as informações. Um exemplo de transmissão *multicast* é a transmissão de vídeo e de voz associada a uma reunião de negócios colaborativa, com base em rede.

Figura 11. Propagação *multcast* IPv6



Fonte: Cunha (2012)[23].

Exemplos de representação de endereços IPv6:

- *Unicast*: 1080:0:0:0:8:800:200C:417A ou 1080::8:800:200C:417A
- *Multicast*: FF01:0:0:0:0:0:0:43 ou FF01::43
- *Loopback*: 0:0:0:0:0:0:0:1 ou ::1

8.2 TÉCNICAS DE TRADUÇÃO DE IPV4 PARA IPV6

A possibilidade de possuir as duas versões de endereçamento trabalhando lado a lado, com certeza tende a ser um dos principais motivos da permanência do IPv4, permitindo uma transição lenta, gradual e segura. O IPv6 não foi projetado para ser uma extensão/ atualização, ou complemento, do IPv4, mas sim, um substituto completo, destinado a resolver os gaps de esgotamento de endereços. Embora não interoperem, os protocolos podem funcionar em paralelo nos mesmos equipamentos, possibilitando realizar a transição de forma gradual.

Assim a estratégia projetada seria: Logo que o IPv6 estivesse pronto, sua implantação teria início aos poucos e em conjunto com o IPv4. Esse cenário é chamado de pilha dupla, ou *dual stack*. Quando o IPv6 estivesse implantado em todos os dispositivos, o IPv4 poderia ser abandonado paulatinamente.

No período de implantação do IPv6 haveria necessidade de técnicas auxiliares de transição, inicialmente para interconectar ilhas IPv6 em uma internet majoritariamente IPv4 e, depois de algum tempo, para fazer o contrário. A transição feita desta forma seria muito simples de ser executada tecnicamente. Contudo, por diversas razões, não foi o que aconteceu. Atualmente o IPv6 ainda não está sendo amplamente utilizado na internet e o esgotamento do IPv4 já é uma realidade. Hoje existe a necessidade de se implantar o IPv6 em uma internet sempre crescente, onde os novos usuários ainda precisam de conectividade, mas sem endereços IPv4 livres para atendê-los. Assim, novas técnicas auxiliares foram e continuam sendo desenvolvidas.

O período de transição e de coexistência entre os protocolos IPv6 e IPv4 exigiu o desenvolvimento de técnicas auxiliares, inicialmente para resolver problemas de como conectar as novas redes IPv6 com o conteúdo das demais redes majoritariamente IPv4. Com o aumento da adoção do IPv6, esse cenário se inverterá e técnicas para garantir o acesso IPv6 a redes IPv4 legadas surgirão. Além disso, existe um terceiro tipo de técnica que busca aumentar a sobrevida do IPv4 enquanto a transição completa não ocorre.

As técnicas de transição podem ser classificadas segundo sua funcionalidade:

- Pilha dupla: Refere-se à manutenção do IPv4 conjuntamente ao IPv6 nos mesmos equipamentos, de forma nativa, simultaneamente. Essa técnica é a

técnica padrão escolhida para a transição para IPv6 na internet e deve ser usada sempre que possível.

- Túneis: Possibilita que redes que trabalham com o IPv4, consigam se comunicar com redes IPv6, ou vice-versa.
- Tradução: Permitem que equipamentos usando IPv6 comuniquem-se com outros que usam IPv4, por meio da conversão dos pacotes.

Essas técnicas podem ser classificadas, ainda, entre *statefull* e *stateless*. Técnicas *stateful* são aquelas em que é necessário manter tabelas de estado com informações sobre os endereços ou pacotes para processá-los. Já técnicas *stateless* não tem essa necessidade, cada pacote é tratado de forma independente. De forma geral técnicas *stateful* são mais caras: gastam mais CPU e memória, por isso não escalam bem. Sempre que possível deve-se dar preferência a técnicas *stateless*.

De forma geral, os critérios que devem ser utilizados na escolha da técnica a ser utilizada, são eles:

- Preferir técnicas que impliquem na utilização de IPv6 nativo pelos usuários finais, de forma que túneis IPv4 dentro de IPv6 devem ser preferidos em detrimento de túneis IPv6 sobre IPv4;
- Preferir técnicas *stateless* em detrimento de técnicas *statefull*;
- Evitar técnicas para prolongar o uso do protocolo IPv4, sem a adoção concomitante do IPv6;
- Analisar a adequação da técnica à topologia da rede onde será aplicada e;
- Analisar a maturidade da técnica e as opções de implantação, como por exemplo suporte à mesma nos equipamentos de rede e em softwares.

8.3 A TRINCA DE OURO RESPONSÁVEL PELA SOBREVIDA DO IPV4

O *Network Address Translation*, é um recurso que permite converter/mascarar endereços da rede interna em endereços da internet. Observa-se este recurso mais comumente quando se quer compartilhar a conexão com a internet oriunda de um único ponto. O compartilhamento pode ser feito usando em um servidor com duas placas de rede, um modem ADSL, um roteador, etc. Em suma, em outras palavras, podemos dizer que NAT é um tradutor de endereços de rede que visa minimizar a escassez dos endereços IP. O NAT não é um protocolo nem um padrão, é apenas

uma série de tarefas que um roteador (ou equipamento equivalente) deve realizar para converter endereços IPs entre redes distintas. Um equipamento que tenha o recurso de NAT deve ser capaz de analisar todos os pacotes de dados que passam por ele e trocar os endereços desses pacotes de maneira adequada.

Uma rede com NAT pode ser configurada com regras de iptables onde o sistema pode ativar o *gateway* e fornecer acesso à internet para vários usuários em uma rede local utilizando apenas um endereço de IP público. Isso é feito reescrevendo a fonte e/ou endereço de destino dos pacotes que passam pelo NAT. Como não é o foco deste, não entraremos em especificações técnicas destas regras de iptables.

O servidor permanece conectado simultaneamente às duas redes, por meio das duas placas de rede, uma à internet e outra à rede local. Nesta rele local encontram-se as estações as quais se deseja compartilhar a internet. Ele pode ter o endereço IP 192.168.10.1 na interface conectada à na internet e o IP 10.42.8.25 na rede interface conectada à rede local por exemplo. Se um dos PC da rede local abre uma página no *www.utfpr.edu.br/,* por exemplo, o pedido será enviado ao servidor, que por sua vez o encaminhará para o endereço correspondente na internet. O site responderá ao servidor que fez a solicitação, uma vez que o mesmo não enxerga as estações da rede local.

Ou seja, o PC local enxerga apenas o servidor de conexão e fica invisível para todos os mais dispositivos da internet, a qual verá apenas o servidor e não os PCs da rede local.

Esta ferramenta tem contribuído sobremaneira para a permanência ativa do IPv4 em detrimento do novo protocolo de rede. Pois a operadora necessita fornecer apenas um IP válido, e este pode gerar uma rede com dezenas, centenas de outros dispositivos.

O NAT trabalha de mão dadas com um dos serviços mais importantes de uma rede de computadores, o *Dynamic Host Configuration Protocol* (DHCP). É um protocolo utilizado em redes de computadores que permite às máquinas obterem um endereço IP automaticamente.

O protocolo DHCP permite que um administrador de rede não necessite atribuir localmente endereços Ips aos dispositivos conectados. Por meio deste serviço um servidor é capaz de distribuir automaticamente endereços de IP diferentes a todos os computadores à medida que eles realizem a solicitação de

conexão com a rede. Essa distribuição dos IPs é feita em um intervalo (*range*) pré-definido e configurado no servidor. Sempre que uma das máquinas for desconectada o IP ficará livre para o uso em outra. Entretanto existem configurações de DHCP, onde a distribuição não é tão livre assim, pois tal endereçamento é realizado via endereço MAC da interface de rede, proporcionando mais controle e segurança à rede local.

Resumidamente, utilizando um modelo cliente-servidor, o DHCP faz o seguinte:

- Quando um cliente se conecta a uma rede ele envia um pacote com um pedido de configurações DHCP.
- O servidor DHCP gerencia uma faixa fixa de IPs disponíveis juntamente com as informações e parâmetros necessários (*gateway* padrão, nome de domínio, DNS, etc).
- Quando este servidor recebe um pedido, ele entrega um destes endereços e configurações para o cliente.

Ele pode operar de três formas: automática, dinâmica e manual; são elas:

- Automática, no qual uma quantidade de endereços de IP (dentro de uma faixa) é definida para ser utilizada na rede. Neste caso, sempre que um dos computadores de uma rede solicitar a conexão com ela, um destes IPs será designado para a máquina em questão.
- Na dinâmica o procedimento é bem parecido com o efetuado pela maneira automática, porém a conexão do computador com determinado IP é limitada por um período de tempo pré-configurado que pode variar conforme desejado pelo administrador da rede.
- No modo manual o DHCP aloca um endereço de IP conforme o valor de MAC (Medium Access Control) de cada placa de rede, de forma que cada computador utilizará apenas este endereço de IP. Utiliza-se este recurso quando é necessário que uma máquina possua um endereço de IP fixo.

Como o DHCP possui suporte para diversas plataformas, ele traz uma solução eficiente e fornece uma grande ajuda para os administradores de rede. O NAT e o DHCP tiveram o auxílio de uma técnica binária que permitiria um melhor aproveitamento do dos endereçamentos IPv4, o *Classless Inter-Domain Routing*(CIDR)/VLSM

Os endereços IP identificam cada *host* (ou seja, cada estação) na rede, como já abordado anteriormente. A regra básica é que cada *host* deve ter um endereço IP diferente e devem ser utilizados endereços dentro da mesma faixa. Um endereço IP é composto de uma sequência de 32 bits, divididos em 4 grupos de 8 bits cada, chamados de octetos e cada octeto permite o uso de 256 combinações diferentes (dois elevados à oitava potência).

Para facilitar a configuração dos endereços, usamos números de 0 a 255 para representar cada octeto, formando endereços como 192.168.0.1 ou 175.56.4.9. Isso torna a tarefa de configurar e memorizar os endereços bem mais fácil do que seria caso precise decorar sequências de números binários.

O endereço IP é dividido em duas partes. A primeira identifica a rede à qual o *host* está conectado (necessário, pois, em uma rede TCP/IP, podemos ter várias redes conectadas entre si, como no caso da internet) e a segunda identifica o *host*, o qual pertence aquela rede. Por padrão, os primeiros bits do endereço servirão para identificar a rede e os últimos servirão para identificar o computador propriamente dito. Como são apenas 4 octetos, qualquer divisão fixa limitaria sobremaneira o número de endereços possíveis, o que seria uma grande problemática no caso da internet, onde existe um número muito grande de redes diferentes, muitas delas com um número muito grande de dispositivos conectados.

Se fosse reservado apenas o primeiro octeto do endereço, ter-se-ia um grande número de *hosts* (micros conectados a cada rede), mas em compensação apenas 256 redes diferentes, o que seria muito complicado, se considerado em escala mundial. Mesmo se fossem reservados dois octetos para a identificação da rede e dois para a identificação do *host*, os endereços possíveis seriam insuficientes, pois existem mais de 65 mil redes diferentes, conectadas entre si através da internet, e em muitas com mais de 65 mil *hosts*.

A primeira solução para o impasse foi a divisão dos endereços em três classes, onde cada classe reserva um número diferente de octetos para o endereçamento da rede. Atualmente, esta designação não é inteiramente válida, pois é cada vez mais usado o sistema CIDR, onde são usadas máscaras variáveis para criar faixas de endereços de diversos tamanhos, a ser abordados mais adiante. Quanto a divisão tradicional:

Na classe A, apenas o primeiro octeto identifica a rede, na classe B são usados os dois primeiros octetos e na classe C (a mais comum) tem-se os três

primeiros octetos reservados para a rede e apenas o último reservado para a identificação dos *hosts*. O que diferencia uma classe de endereços da outra é o valor do primeiro octeto. Se for um número entre 1 e 126 (como em 113.221.34.57), tem-se um endereço de classe A. Se o valor do primeiro octeto for um número entre 128 e 191, um endereço de classe B (como em 167.27.135.203) e, finalmente, caso o primeiro octeto seja um número entre 192 e 223, um endereço de classe C, como em 212.23.187.98.

Esta é a designação tradicional, abordada nos livros e manuais. O grande problema é que esta divisão tradicional fazia com que um grande número de endereços fosse desperdiçado. Um provedor de acesso que precisasse de 10.000 endereços IP, por exemplo, precisaria ou utilizar uma faixa de endereços classe B inteira (65 mil endereços), o que geraria um grande desperdício, ou utilizar 40 faixas de endereços classe C separadas, o que complicaria a configuração. Existia ainda o problema com as faixas de endereços classe ”A”, que geravam um brutal desperdício de endereços, já que nenhuma empresa ou organização sozinha chega a utilizar milhões de endereços IP. A solução para o problema foi a implantação do sistema CIDR.

Abreviação CIDR significa "*Classless Inter-Domain Routing*". Entender as classes de endereços A, B e C é importante para compreender o uso das máscaras de sub-rede e por isso elas ainda são muito estudadas, mas é importante ter em mente que, na prática, elas são uma designação obsoleta. Naturalmente, ainda existem muitas redes que utilizam faixas de endereços de classe A, B e C (já que as faixas alocadas no passado não podem ser simplesmente revogadas de uma hora para a outra), mas as faixas alocadas atualmente utilizam quase sempre o novo sistema.

No CIDR são utilizadas máscaras de tamanho variável (o termo em inglês é VLSM, ou *Variable-Length Subnet Mask*), que permitem uma flexibilidade muito maior na criação das faixas de endereços. Se são necessários apenas 1000 endereços, por exemplo, poderia ser usada uma máscara /22 (que permite o uso de 1022 endereços), em vez de uma faixa de classe B inteira, como seria necessário antigamente. Outra mudança é que as faixas de endereços não precisam mais iniciar com determinados números. Uma faixa com máscara /24 (equivalente a uma faixa de endereços de classe C) pode começar com qualquer dígito e não apenas com de 192 a 223. O CIDR permite também que várias faixas de endereços

contínuas sejam agrupadas em faixas maiores, de forma a simplificar a configuração. É possível agrupar 8 faixas de endereços com máscara 255.255.255.0 (classe C) contínuas em uma única faixa com máscara /21, por exemplo, que oferece um total de 2045 endereços utilizáveis (descontando o endereço da rede, endereço de broadcast e o endereço do *gateway*). As faixas de endereços são originalmente atribuídas pela IANA às entidades regionais. Elas dividem os endereços em faixas menores e as atribuem às empresas de hospedagem, provedores de acesso e outras instituições. Estas, por sua vez, quebram os endereços em faixas ainda menores, que são atribuídas aos consumidores finais.

Com isso observa-se que a máscara de sub-rede determina qual parte do endereço IP é usada para endereçar a rede e qual é usada para endereçar os *hosts* dentro dela. No endereço 200.232.211.54, com máscara 255.255.255.0 (/24), por exemplo, os primeiros 24 bits (200.232.211) endereçam a rede e os 8 últimos endereçam o *host*. Quando usamos máscaras simples, podemos trabalhar com os endereços em decimais, pois são sempre reservados 1, 2 ou 3 octetos inteiros para a rede e o que sobra fica reservado ao *host*. Esta é a ideia usada nas faixas de endereços classe A, B e C.

Quando falamos em máscaras de tamanho variável, entretanto, precisamos começar a trabalhar com endereços binários, pois a divisão pode ser feita em qualquer ponto. Imagine, por exemplo, o endereço "72.232.35.108". Originalmente, ele seria um endereço de classe A e utilizaria máscara "255.0.0.0". Mas, utilizando máscaras de tamanho variável, ele poderia utilizar a máscara "255.255.255.248", por exemplo. Nesse caso, teríamos 29 bits do endereço dedicados a endereçar a rede e apenas os 3 últimos bits destinados ao *host*. Convertendo o endereço para binário teríamos o endereço "01001000.11101000.01100000.01101100", onde o "01001000.11101000.01100000.01101" é o endereço da rede e o "100" é o endereço do *host* dentro dela. Como temos 29 bits dedicados à rede, é comum o uso de um "/29" como máscara, no lugar de "255.255.255.248". Na Tabela 3 apresenta-se um resumo de como ficariam as quantidades de *hosts* e redes considerando as máscaras de tamanho variável.

Tabela 3. Tabela CIDR (*Classless Inter-Domain Routing*)

Tabela CIDR						www.netadm.com.br
Prefixo CIDR	Máscara em Decimal	Máscara em Hexadecimal	Máscara Reversa	Máscara de Rede em Binário	Nº de Redes Classful	Nº de hosts
/1	128.0.0.0	80 00 00 00	127.255.255.255	1000 0000 0000 0000 0000 0000 0000 0000	128 As	2,147,483,646
/2	192.0.0.0	C0 00 00 00	63.255.255.255	1100 0000 0000 0000 0000 0000 0000 0000	64 As	1,073,741,822
/3	224.0.0.0	E0 00 00 00	31.255.255.255	1110 0000 0000 0000 0000 0000 0000 0000	32 As	536,870,910
/4	240.0.0.0	F0 00 00 00	15.255.255.255	1111 0000 0000 0000 0000 0000 0000 0000	16 As	268,435,454
/5	248.0.0.0	F8 00 00 00	7.255.255.255	1111 1000 0000 0000 0000 0000 0000 0000	8 As	134,217,726
/6	252.0.0.0	FC 00 00 00	3.255.255.255	1111 1100 0000 0000 0000 0000 0000 0000	4 As	67,108,862
/7	254.0.0.0	FE 00 00 00	1.255.255.255	1111 1110 0000 0000 0000 0000 0000 0000	2 As	33,554,430
/8	255.0.0.0	FF 00 00 00	0.255.255.255	1111 1111 0000 0000 0000 0000 0000 0000	1 A or 256 Bs	16,777,214
/9	255.128.0.0	FF 80 00 00	0.127.255.255	1111 1111 1000 0000 0000 0000 0000 0000	128 Bs	8,388,606
/10	255.192.0.0	FF C0 00 00	0.63.255.255	1111 1111 1100 0000 0000 0000 0000 0000	64 Bs	4,194,302
/11	255.224.0.0	FF E0 00 00	0.31.255.255	1111 1111 1110 0000 0000 0000 0000 0000	32 Bs	2,097,150
/12	255.240.0.0	FF F0 00 00	0.15.255.255	1111 1111 1111 0000 0000 0000 0000 0000	16 Bs	1,048,574
/13	255.248.0.0	FF F8 00 00	0.7.255.255	1111 1111 1111 1000 0000 0000 0000 0000	8 Bs	524,286
/14	255.252.0.0	FF FC 00 00	0.3.255.255	1111 1111 1111 1100 0000 0000 0000 0000	4 Bs	262,142
/15	255.254.0.0	FF FE 00 00	0.1.255.255	1111 1111 1111 1110 0000 0000 0000 0000	2 Bs	131,07
/16	255.255.0.0	FF FF 00 00	0.0.255.255	1111 1111 1111 1111 0000 0000 0000 0000	1 B or 256 Cs	65,534
/17	255.255.128.0	FF FF 80 00	0.0.127.255	1111 1111 1111 1111 1000 0000 0000 0000	128 Cs	32,766
/18	255.255.192.0	FF FF C0 00	0.0.63.255	1111 1111 1111 1111 1100 0000 0000 0000	64 Cs	16,382
/19	255.255.224.0	FF FF E0 00	0.0.31.255	1111 1111 1111 1111 1110 0000 0000 0000	32 Cs	8,19
/20	255.255.240.0	FF FF F0 00	0.0.15.255	1111 1111 1111 1111 1111 0000 0000 0000	16 Cs	4,094
/21	255.255.248.0	FF FF F8 00	0.0.7.255	1111 1111 1111 1111 1111 1000 0000 0000	8 Cs	2,046
/22	255.255.252.0	FF FF FC 00	0.0.3.255	1111 1111 1111 1111 1111 1100 0000 0000	4 Cs	1,022
/23	255.255.254.0	FF FF FE 00	0.0.1.255	1111 1111 1111 1111 1111 1110 0000 0000	2 Cs	510
/24	255.255.255.0	FF FF FF 00	0.0.0.255	1111 1111 1111 1111 1111 1111 0000 0000	1 C	254
/25	255.255.255.128	FF FF FF 80	0.0.0.127	1111 1111 1111 1111 1111 1111 1000 0000	1/2 C	126
/26	255.255.255.192	FF FF FF C0	0.0.0.63	1111 1111 1111 1111 1111 1111 1100 0000	1/4 C	62
/27	255.255.255.224	FF FF FF E0	0.0.0.31	1111 1111 1111 1111 1111 1111 1110 0000	1/8 C	30
/28	255.255.255.240	FF FF FF F0	0.0.0.15	1111 1111 1111 1111 1111 1111 1111 0000	1/16 C	14
/29	255.255.255.248	FF FF FF F8	0.0.0.7	1111 1111 1111 1111 1111 1111 1111 1000	1/32 C	6
/30	255.255.255.252	FF FF FF FC	0.0.0.3	1111 1111 1111 1111 1111 1111 1111 1100	1/64 C	2
/31	255.255.255.254	FF FF FF FE	0.0.0.1	1111 1111 1111 1111 1111 1111 1111 1110	1/128 C	0
/32	255.255.255.255	FF FF FF FF	0.0.0.0	1111 1111 1111 1111 1111 1111 1111 1111	1/256 C	1

Fonte: Redes Linux: Tabela CIDR. Disponível em: <https://linuxrede.wordpress.com/2012/12/11/tabela-de-subnets-ipv4/tabela_cidr1/>. Acesso em: 30 ago. 2018.

8.4 BAIXA ENERGIA E ADPTAÇÃO DO IPV6 NO EMCOSSISTEMA DE IOT

O *low-power Wi-Fi* é uma tecnologia baseada em Wi-Fi que tem como principal objetivo minimizar o consumo de energia de um determinado aparelho. Tal minimização é feita tanto em relação ao hardware, por meio do desenvolvimento de arquiteturas de placas de rede e outros componentes de um computador com tecnologia de baixo consumo, quanto em relação ao software, por meio do desenvolvimento de sistemas operacionais e/ou aplicativos que sejam capazes de comunicar entre si de maneira econômica. Também existem protocolos, baseados no padrão IEEE, que favorecem aparelhos que possuem bateria, permitindo que esses operem em baixos ciclos de trabalho.

Cada vez mais o computador tem se tornado um bem imprescindível para as pessoas e o tempo mais escasso. Nesse contexto, a portabilidade ganhou força, porém, o seu maior inimigo é duração da bateria, pois com o grande volume de informações, cresce a necessidade de maior processamento, maior

armazenamento, entre outros, acarretando em um maior consumo de energia. Além disso, com o advento da “Internet das Coisas”, os dispositivos precisam se comunicar, o que demanda mais energia. Para minimizar o gasto energético, o Low-Power Wi-Fi se apresenta como uma tecnologia promissora, capaz de prolongar a duração da bateria sem comprometer a experiência do usuário.

O “6LoWPAN”, pronunciado “six-lowpan”, acrônimo de *IPv6 over Low Power Wireless Personal Area Networks*, é um grupo de desenvolvedores responsável por produzir meios que permitem os pacotes do protocolo IPv6 sejam transmitidos e recebidos dentro de uma rede baseada no protocolo 802.15.4, por meio de encapsulamento e fragmentação do cabeçalho dos pacotes. Com a adoção deste protocolo, possibilita-se a existência de muito mais endereços IP.

O protocolo 802.15.4 é um padrão IEEE que especifica a camada física e efetua o controle de acesso para redes sem fio pessoais de baixas taxas de transmissão. Foi desenvolvido para prolongar a duração da bateria do dispositivo, que necessita de baixo ciclo de trabalho para reduzir o consumo de energia. Esses dispositivos passam pouca parte do tempo em estado ativo, tendo que periodicamente ouvir o canal para saber se existe uma mensagem para ele. Esse mecanismo permite que a aplicação seja balanceada entre o consumo de bateria e a latência das mensagens. Por trabalhar com baixa taxa de transferência, as redes 802.15.4 são conhecidas como *Low Rate – Wireless Personal Area Network* (LR-WPAN), trabalhando com taxas de transmissão de até 250kbps.

O grupo de trabalho 6LoWPAN da IETF também une esforços no sentido de que seja possível a comunicação pelo protocolo IPv6 nas redes IEEE 802.15.4. As questões mais pertinentes passam pela fragmentação/desfragmentação e a compressão dos cabeçalhos IPv6. A MTU máximo do IPv6 é de 1280 bytes, enquanto no IEE 802.15.4 é de 127 bytes, tornando-se importante o uso de fragmentação e desfragmentação. Normalmente nas redes LoWPAN o cabeçalho IP e UDP contêm muitos campos desnecessários e outros que também podem ser comprimidos. Portanto é importante e indispensável a compressão dos cabeçalhos IPv6 para o sucesso e futuro do uso de IPv6. O 6LOWPAN cria uma camada de adaptação entre o IEEE 802.15.4 e o IPv6, com cabeçalhos específicos que podem ser adicionados ou removidos mediante a sua necessidade, permitindo que seja apenas enviado o que realmente é útil.

8.5 O IPV6 É ESSENCIAL PARA A CONECTIVIDADE EM IOT

A Internet das Coisas (IoT) é um novo paradigma que está rapidamente tomando valor nas comunicações digitais, principalmente de tecnologia sem fio. O ponto central é que, atualmente, há variedade de coisas ou objetos como: identificação por radiofrequência (RFID), etiquetas, sensores, atuadores, telefones celulares, etc. – que são capazes de interagir e cooperar com os seus vizinhos para atingir objetivos comuns. Como usuários, a IoT vai estar cada vez mais presente nas vidas das pessoas. A sociedade moderna, principalmente nas cidades, tem um forte atrativo para que os governos e as companhias invistam em oferecer mais serviços aos usuários. Os governos que pretendam prestar melhores serviços aos cidadãos poderão incluir aplicativos de IoT para otimizar os serviços de e-governo. As empresas, por sua vez, terão uma boa oportunidade de negócios ao adotarem estas tecnologias. Por outro lado, as escolas técnicas e universidades, irão formar profissionais qualificados para realizar projetos de IoT.

A única tecnologia possível para construir a Internet das Coisas é o IPv6. Diante da perspectiva de que bilhões de dispositivos serão conectados à internet em um futuro próximo e, além disso, a realidade dos endereços do IPv4 que estão se esgotando, é natural que IoT deva ser implementada sobre o IPv6.

De acordo aos prognósticos econômicos atuais, a IoT vai ser uma tecnologia de grande futuro, a partir da ideia de que a procura popular em combinação com os avanços tecnológicos, irão impulsionar o uso generalizado de IoT. Isso poderia contribuir inestimavelmente no desenvolvimento econômico, da forma que acontece com a internet atual. Além disso, como tem-se observado, um ponto importante para alcançar total interconectividade é a padronização dos protocolos de interconexão. Como vem acontecendo desde os anos 80, para que os dispositivos se conectem todos entre si, a melhor forma é usar padrões abertos. Por isso, vislumbra-se que o IETF tem e vai ter um papel muito importante no crescimento da IoT. De fato, hoje já se está usando protocolos como 6lowPAN, RPL, CoAP, etc. Todos eles padronizados pelo IETF[4].

9 CONCLUSÃO

A internet das coisas possui uma demanda muito ampla. A pesar de sua vasta presença no dia a dia das pessoas, ainda não se atingiu, nem de longe, suas reais possibilidades.

Contudo, esse nicho deverá vir acompanhado de preceitos técnicos e sociais, de maneira que, ao passo que desenvolva e melhore a vida das pessoas, não fira os preceitos éticos das mesmas.

Para isto, muitos desafios necessitam serem transpostos. Privacidade dos dados e o protocolo IPv6 são apenas dois de muitos outros. A sociedade civil organizada, o poder público e os profissionais inseridos neste contexto devem conscientizar-se da necessidade de vencer estes desafios, contribuindo com isso para um país mais conectado.

REFERÊNCIAS

1. SONG, T. et al. **Privacy preserving communication protocol for IoT applications in smart homes.** IEEE Internet of Things Journal, v. 4, n. 6, dez. 2017. Disponível em: <https://ieeexplore.ieee.org/document/7932843/>. Acesso em: 26 ago. 2018.

2. SENGUL, C. **Privacy, consent and authorization in IoT**. 20th Conference on Innovations in Clouds, Internet and Networks (ICIN), mar. 2017. Disponível em: <https://ieeexplore.ieee.org/document/7899432/>. Acesso em: 26 ago. 2018.

3. ROHLING, L. J. **Curso de extensão: A internet de todas as coisas**. Instituto de Engenharia do Paraná, 2017. Disponívem em: <http://iep.org.br/iep/curso/curso-de-extensao-a-internet-de-todas-as-coisas/>. Acesso em: 27 ago. 2018.

4. LACNIC. **Fases de Esgotamento IPv4**. Lacnic, ago. 2018. Disponível em: <http://www.lacnic.net/1077/3/lacnic/fases-de-esgotamento-do-ipv4>. Acesso em: 28 ago. 2018.

5. IBGE. **População do Brasil**. IBGE, ago. 2018. Disponível em: <http://www.ibge.gov.br/apps/populacao/projecao/index.html>. Acesso em: 28 ago. 2018.

6. PARREIRA, R. **Um retrato da adoção e do potencial da internet das coisas no mercado brasileiro**. Logicalis, 2017. Disponível em: <https://www.la.logicalis.com/globalassets/latin-america/advisors/pt/_iot_snapshot_2017_vfinal_web.pdf>. Acesso em: 28 ago. 2018.

7. BNDS. **Internte das coisas: estimando impactos na economia**: BNDS, fev. 2017. Disponível em: <https://www.bndes.gov.br/wps/portal/site/home/conhecimento/noticias/noticia/internet-coisas-iot>. Acesso em: 28 ago. 2018.

8. CISCO. **The Internet of Everything: global public sector economic analysis**. CISCO, 2013. Disponível em: <https://www.cisco.com/c/dam/en_us/about/ac79/docs/innov/IoE_Economy_FAQ.pdf>. Acesso em: 28 ago. 2018.

9. GALILEU. **Inventor do Controle Remoto**. Redação da Revista Galileu. Disponível em: <http://revistagalileu.globo.com>. Acesso em: 28 ago. 2018.

10. GAZZARRINI, R. **LG Smart Lamp: conheça a primeira lâmpada inteligente da LG**. Tecmundo, mar. 2014. Disponível em: <https://www.tecmundo.com.br/lampada/52720-lg-smart-lamp-conheca-a-primeira-lampada-inteligente-da-lg.htm>. Acesso em: 28 ago. 2018.

11. TOYMAIL. **ToyMail: brinquedo de pelúcia para gravar, enviar e receber mensagens de voz**. ToyMail, 2018. Disponível em: <https://toymail.co/>. Acesso em: 28 ago. 2018.

12. TAGPOINT. **Sensor de temperatura agropecuário**. Tagpoint, 2018. Disponível em: <http://tagpoint.com.br>. Acesso em: 28 ago. 2018.

13. ANDRADE, R. **Pesquisa pública sobre IoT**. Participa.br, dez. 2016. Disponível em: <http://www.participa.br/portal/blog/consulta-publica-iot>. Acesso em: 28 ago. 2018.

14. SANTOS, M. **Digital Banking: carteira eletrônica e transferência de valores P2P**. ComputerWorld, abr. 2015. Disponível em: <http://computerworld.com.br/digital-banking-carteira-eletronica-e-transferencia-de-valores-p2p>. Acesso em: 28 ago. 2018.

15. NADAS, J. P. B. et al. **Energy efficient beacon based synchronization for alarm driven wireless sensor networks.** IEEE Signal Processing Letters, v. 23, n. 3, mar. 2016. Disponível em: <https://ieeexplore.ieee.org/document/7374658/>. Acesso em: 28 ago. 2018.

16. CAI, H. et al. **IoT-based big data storage systems in cloud computing: perspectives and challenges**. IEEE Internet Of Journal Of Things, v. 4, n. 1, fev. 2017. Disponível em: <https://ieeexplore.ieee.org/document/7600359/>. Acesso em: 28 ago. 2018.

17. CRUZ, C. H. **O Mau uso das Redes sociais pode parar na Justiça**. CHC Advocacia, 2014. Disponível em: <https://chcadvocacia.jusbrasil.com.br/noticias/233444285/o-mau-uso-das-redes-sociais-pode-ir-parar-na-justica>. Acesso em: 28 ago. 2018.

18. SEMINÁRIO. **VIII Seminário de proteção à privacidade e aos dados pessoais**. nic.br e cgi.br, set. 2017. Disponível em: <https://seminarioprivacidade.cgi.br/2017/>. Acesso em: 28 ago. 2018.

19. SLOAN, Robert H.; WANER, R. **Beyond notice and choice: privacy, norms, and consent**. Suffolk University Journal of High Technology, v. 14, n. 2, p. 370-412, mar. 2013. Disponível em:

<https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2239099>. Acesso em: 28 ago. 2018.

20. EUROPEAN UNION. **EU institutions and bodies in brief**. EU, mai. 2018. Disponível em: <https://europa.eu/european-union/about-eu/institutions-bodies_en>. Acesso em: 28 ago. 2018.

21. G1. **Entenda o caso de Edward Snowden, que revelou espionagem dos EUA**. g1.globo.com, São Paulo, jul. 2013. Disponível em: <http://g1.globo.com/mundo/noticia/2013/07/entenda-o-caso-de-edward-snowden-que-revelou-espionagem-dos-eua.html>. Acesso em: 28 ago. 2018.

22. MODZELESKI, A. **Autor da emenda apontada como 'censura' diz que vai pedir para Temer vetar o texto**. g1.globo.com, Brasília, out. 2017. Disponível em: <https://g1.globo.com/politica/noticia/autor-da-emenda-apontada-como-censura-diz-que-vai-pedir-para-temer-vetar-o-texto.ghtml>. Acesso em: 28 ago. 2018.

23. CUNHA, Erivan Amorim da. **IPTV: um entretenimento promissor**. Trabalho de Conclusão de Curso de Pós Graduação, Faculdade Pitágoras, Uberlândia/MG, jul. 2012. Disponível em: <http://www.teleco.com.br/tutoriais/tutorialiptvev/default.asp>. Acesso em: 25 ago. 17.