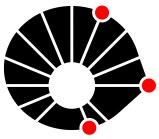

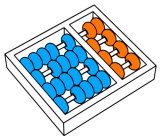

Impactos da LGPD em aplicações da Internet das Coisas

A. L. Barbosa *J. F. Borin*

Relatório Técnico - IC-PFG-21-28
Projeto Final de Graduação
2021 - Dezembro

UNIVERSIDADE ESTADUAL DE CAMPINAS
INSTITUTO DE COMPUTAÇÃO

Impactos da LGPD em aplicações da Internet das Coisas

Alexandre Luciano Barbosa Juliana Freitag Borin*

Resumo

Em 2018 entrou em vigor na União Europeia o Regulamento Geral de Dados (GDPR); em 2021, inspirado no regulamento Europeu, foi a vez do Brasil ter sua lei de dados entrando em vigência em sua plenitude com a Lei Geral de Proteção de Dados Pessoais (LGPD). Levando em consideração que existe uma alta demanda de vários setores econômicos que utilizam dados pessoais para desenvolverem produtos e serviços, este trabalho investiga, através de uma pesquisa documental e uma revisão bibliográfica, o formato das legislações que abordam a temática de tratamento de dados pessoais e como as mesmas impactam diretamente e indiretamente o desenvolvimento de tecnologias e a utilização de dispositivos, principalmente no contexto da Internet das Coisas. Ademais, são pautados os desafios associados a adequação de procedimentos e arquiteturas das soluções baseadas em Internet das Coisas a fim de garantir a segurança e privacidade dos usuários bem como a conformidade com a LGPD.

Palavras-chave: Dados Pessoais. Internet das Coisas. LGPD. GDPR. Tratamento de Dados.

*Instituto de Computação, Universidade Estadual de Campinas, 13081-970 Campinas, SP.

1 Introdução

As legislações que tem como foco a proteção de dados pessoais estão se tornando cada vez mais comuns pelo mundo. A União Europeia foi pioneira nessa questão elaborando o Regulamento Geral de Dados (GDPR) [1], um documento que aborda detalhadamente conceitos sobre o tratamento e proteção de dados pessoais que passou a vigorar no bloco em 2018. Devido sua completude, o GDPR serviu de inspiração para outros países elaborarem legislações parecidas, como foi o caso do Brasil, que no mesmo ano teve sua lei de dados promulgada. A Lei Geral de Dados Pessoais (LGPD) [2] tem como objetivo fornecer diretrizes sobre como dados pessoais devem ser tratados. A lei é composta por 65 artigos que regulam direta e indiretamente a proteção da privacidade e dos dados pessoais de cidadãos que estejam no Brasil. A LGPD discute questões como os tipos de dados que podem ser tratados, quais circunstâncias podem ocorrer no tratamento, as informações que os usuários devem conhecer sobre seus dados coletados além de instituir uma agência fiscalizadora.

Ao observarmos os impactos do GDPR na União Europeia é possível perceber que várias mudanças já ocorreram ao longo dos últimos anos, desde a parte técnica com atualizações nas arquiteturas de sistemas que lidam com dados pessoais, que agora precisam trabalhar com mais segurança, até mesmo na mentalidade da sociedade que agora começa a se preocupar de maneira mais enfática com seus dados. Em função das similaridades da LGPD com o GDPR podemos esperar algo parecido no Brasil; muitas empresas já estão trabalhando de acordo à nova lei, no entanto, o cenário ainda esteja longe do ideal. Mesmo após três anos de sua aprovação, apenas no segundo semestre de 2021 a LGPD começou a ser aplicada em sua plenitude.

Este tipo de regulamentação impacta diretamente muitos setores da economia que antes utilizavam dados pessoais sem nenhum tipo de regra específica. Dentre esses setores, um que se destaca são os que trabalham com tecnologias que envolvem o conceito de Internet das Coisas (do inglês, *Internet of Things* - IoT), já que a LGPD muda totalmente a maneira como os dados são tratados em todas as áreas aplicadas e cria padrões para a proteção dos dados.

A Internet das Coisas possibilita a integração entre inúmeros dispositivos que possuem conexão à Internet, proporcionando controle remoto, automações e compartilhamento de dados. Desse modo, a coleta e o tratamento de dados com o objetivo de oferecer facilidades no cotidiano das pessoas é um dos pilares da IoT. Por muito tempo, sem nada que limitasse suas operações, dispositivos de IoT se concentraram em coletar dados dos usuários e criar soluções a partir dessas informações, algo que a partir de agora, precisa se adequar às diretrizes da LGPD. Deste modo, surge uma série de desafios a serem enfrentados, principalmente em relação a coleta, transmissão e armazenamento de dados pessoais em dispositivos de IoT. Para que soluções baseadas em IoT sejam seguras, elas precisam ser cuidadosamente projetadas, pois lidam com uma grande quantidade de dados trocados entre partes. Além disso, empresas que trabalham com dados precisarão modificar seus processos internos e conscientizar seus colaboradores por meio de treinamentos sobre a obrigação de tratar dados de forma segura, com procedimentos previamente definidos e que cumpram os requisitos da lei.

Há uma demanda latente para a criação de novos métodos para o tratamento de dados

que estejam de acordo com a LGPD. Os novos protocolos exigidos envolvem padrões de segurança para a coleta, transmissão e armazenamento dos dados, levando em consideração a inevitabilidade de deixar claro aos usuários sobre suas ações e possíveis consequências, o que acaba gerando um grande desafio para o setor. Proporcionar ao dono dos dados maior controle sobre o uso de seus dados pessoais, adequar inúmeros dispositivos limitados e sistemas de armazenamento de dados aos padrões de segurança impostos exige um grau maior de investimento e trabalho no desenvolvimento das aplicações.

Este trabalho tem como objetivo investigar os impactos práticos da Lei Geral de Proteção de Dados e como a mesma afeta o desenvolvimento de tecnologias e a utilização de dispositivos que trabalham com dados pessoais levando em consideração que atualmente existe uma alta demanda para o setor, que cresce cada dia mais. Percebe-se a necessidade de se produzir estudos ténico-científicos sobre o tema devido ao ainda pouco material disponível na literatura. O estudo foi realizado por meio de uma pesquisa documental possibilitando assim uma análise a Lei Geral de Proteção de Dados Pessoais (LGPD). Uma revisão bibliográfica também foi realizada para sistematizar um quadro teórico que elucide os principais temas, artigos e trabalhos acadêmicos realizados sobre o assunto, juntamente com a coleta de artigos e notícias pela mídia tradicional que abordaram desde o início a implementação da LGPD.

O restante deste relatório está organizado da seguinte forma: primeiramente, a Seção 2 aborda a Lei Geral de Proteção de Dados, explicando detalhadamente seus principais pontos e conceitos; em seguida, na Seção 3 há uma contextualização sobre o GDPR, os impactos que já ocorrem na União Europeia e uma comparação com a LGPD, mostrando suas principais semelhanças e divergências. As seções seguintes tratam sobre o conceito de Internet das Coisas e como legislações que visam proteger a privacidade impactam no desenvolvimento de tecnologias que trabalham diretamente com dados pessoais, criando inúmeros desafios e limitações.

2 Lei Geral de Proteção de Dados

A Lei Geral de Proteção de Dados Pessoais (LGPD), Lei nº 13.709/2018 [2], é uma lei brasileira com o propósito de fornecer diretrizes sobre como dados pessoais dos cidadãos que estejam no Brasil devem ser gerenciados, composta por mais de 60 artigos que regulamentam, direta e indiretamente a proteção da privacidade e dos dados pessoais.

A nova legislação foi aprovada em 2018, entrou em vigor em agosto de 2020, multas e penalizações começaram a ser aplicadas após três anos, entrando em vigência em 1º de agosto de 2021. Esse intervalo serviu para que muitas empresas começassem a se adequar, mas o cenário ainda está longe do ideal. Uma pesquisa realizada entre janeiro e abril de 2021 pela RD Station mostrou que apenas 15% das empresas estavam prontas ou na reta final de preparação [3].

Com a LGPD, o Brasil ingressou no grupo de países que possuem uma norma específica referente à proteção de dados e privacidade. Uma regulamentação notável serviu como base para o código brasileiro, o Regulamento Geral sobre a Proteção de Dados (GDPR) que começou a ser aplicado na União Europeia em maio de 2018 [1].

Redes sociais, compras on-line, hospitais, escolas, órgãos públicos, publicidade, e até mesmo os eletrodomésticos podem ser afetados pela LGPD. Dados em formato físico, muitas vezes pouco lembrados, também estão sujeitos às mesmas sanções.

> A LGPD corresponde a um regulamento geral para proteção de dados pessoais, independentemente destes passarem por fluxos da Internet ou não. Assim, quaisquer estabelecimentos que coletem dados pessoais — como farmácias, locadoras de carro, postos de gasolina — estão submetidos às disposições legais [4].

A LGPD tem como principal objetivo proteger direitos fundamentais de liberdade e de privacidade de todos os cidadãos que estejam no Brasil. Esta legislação tem grande importância, já que se trata de uma regra única e adequada sobre o uso de dados pessoais, independente do setor econômico, criando assim um cenário com segurança jurídica a todos os negócios que envolvem o tratamento de dados, a padronização de regulamentos e práticas para garantir a proteção aos dados pessoais [5]. Outro benefício gerado é a implementação de um ambiente com desenvolvimento econômico e tecnológico, a partir de regras flexíveis e apropriadas para cuidar de modelos de negócios baseados no uso de dados pessoais. O Brasil também se torna apto a processar dados com origem em países que exigem níveis de proteção de dados.

A redação da LGPD, em seus 65 artigos, abrange inúmeras questões e situações que fundamentam direitos aos titulares de dados e as normas a serem seguidas em operações que envolvem o tratamento de dados pessoais por controladores e operadores. Desse modo, podemos destacar os pontos de maior relevância para esse trabalho como sendo os seguintes:

Definições de conceitos: São estabelecidas definições em relação a muitos termos constantemente presentes quando estamos falando sobre tratamento de dados. Na LGPD, há conceitos jurídicos que identificam todos os envolvidos e afetados pelo tratamento de dados, uma questão importante quando se torna necessário definir responsáveis em caso de descumprimento. Essas definições são fundamentais em uma lei que objetiva regulamentar a proteção de dados pessoais, pois a partir das definições é possível verificar a amplitude do alcance da lei;

> Art. 5º Para os fins desta Lei, considera-se:
> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;
> VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;
> VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
> IX - agentes de tratamento: o controlador e o operador;
> X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, re-

> produção, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;
>
> XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada [2].

Consentimento: O consentimento do titular dos dados é considerado elemento fundamental para o tratamento de dados. A lei estabelece múltiplos direitos aos indivíduos cujos dados são coletados, como revogar o consentimento, solicitar que seus dados sejam excluídos, consultar de forma fácil e gratuita o modo e a duração do tratamento, entre outros. A manifestação do consentimento deve ser realizada de forma voluntária, de maneira desimpedida e não coercitiva;

> Art. 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:
>
> I - mediante o fornecimento de consentimento pelo titular [2].

> Art. 8º, § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento [2].

Finalidade e necessidade: Os objetivos do tratamento e os procedimentos realizados com dados devem ser claramente informados;

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso:
>
> I - finalidade específica do tratamento;
>
> II - forma e duração do tratamento, observados os segredos comercial e industrial [2].

Responsabilização: Define responsabilidades aos agentes de tratamento de dados;

> Art. 42. O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo [2].

Transparência, segurança e gestão de falhas: É estabelecido que devem haver registros de todas as operações realizadas, os agentes precisam tomar medidas de seguranças e quando houver falhas de segurança, como vazamentos, a ANPD e os indivíduos afetados devem ser comunicados;

> Art. 37. O controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse [2].

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito [2].

> Art. 47. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se a garantir a segurança da informação prevista nesta Lei em relação aos dados pessoais, mesmo após o seu término [2].

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares [2].

> Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos padrões de boas práticas e de governança e aos princípios gerais previstos nesta Lei e às demais normas regulamentares [2].

Penalidades: Há previsão de pagamento de multas por descumprimento da lei;

> Art. 52. Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional:
> I - advertência, com indicação de prazo para adoção de medidas corretivas;
> II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração [2].

Fiscalização centralizada: Define um órgão responsável pela fiscalização, a Autoridade Nacional de Proteção de Dados Pessoais (ANPD).

> Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República [2].

É interessante ressaltar que há algumas finalidades em que o uso de dados pessoais não são enquadrados pela lei e estão sujeitos a regulação de legislação específica do tema.

> Art. 4º Esta Lei não se aplica ao tratamento de dados pessoais:

I - realizado por pessoa natural para fins exclusivamente particulares e não econômicos;

II - realizado para fins exclusivamente:

a) jornalístico e artísticos; ou

b) acadêmicos, aplicando-se a esta hipótese os arts. 7º e 11º desta Lei;

III - realizado para fins exclusivos de:

a) segurança pública;

b) defesa nacional;

c) segurança do Estado; ou

d) atividades de investigação e repressão de infrações penais [2].

3 Regulamento Geral sobre a Proteção de Dados

Uma legislação semelhante à LGPD, e que serviu de inspiração para sua redação, é o Regulamento Geral sobre a Proteção de Dados (GDPR). Em vigor desde 2018, o regulamento foi um dos pioneiros ao tratar desse tema, estabelecendo normas de proteção de dados, para o processamento, armazenamento e gerenciamento de dados de pessoas que estão atualmente na União Europeia.

Para entendermos como a LGPD pode impactar de fato o Brasil, podemos olhar para o GDPR dado as suas similaridades, já que as duas possuem um mesmo objetivo: garantir a privacidade de seus cidadãos e enfrentarem os problemas da segurança da informação. No entanto, é bom ressaltar que o GPDR é um regulamento e tem como objetivo, em seus termos estabelecer regras particulares para diferentes situações, já a LGPD é uma lei, ou seja, possui cláusulas mais abertas e subjetivas, portanto, permite interpretações diferentes em alguns pontos.

3.1 Impactos do GDPR

Por estar em vigor desde 2018, já é possível mensurar alguns impactos que o GDPR gerou nos países da União Europeia. No primeiro ano, um estudo feito pela International Association of Privacy Professionals (IAPP), mostrou alguns dados relevantes: 7% dos europeus ouviram em algum momento a respeito do GDPR e 57% têm conhecimento que existe uma autoridade responsável pela proteção de dados pessoais. Nesse período foram realizadas aproximadamente 144.376 reclamações às autoridades e a aplicação do GDPR resultou em um montante de multas no valor de aproximadamente 56 milhões de euros [6].

Mais recentemente, um novo trabalho desenvolvido pela IAPP [7], mostra que após três anos do regulamento 47% das empresas que se autodenominam totalmente em conformidade com o GDPR e mais de 630 ações de fiscalização foram tomadas até o momento, chegando ao valor de 283 milhões de euros em multas. Um dos casos mais notórios de penalização foi a multa de 887 milhões de dólares aplicada à Amazon por não seguir leis de proteção de dados do bloco europeu [8]. Após seus três anos em vigor, é razoável dizer que o GDPR está sendo bem sucedido ao garantir o direito à privacidade e proteção de dados, além de gerar uma conscientização na sociedade sobre a importância do assunto.

Outro ponto que é necessário considerar é o fato do GDPR gerar um grande impacto em tecnologias e arquiteturas que atualmente coletam, armazenam e gerenciam dados pessoais. Um exemplo disso são as redes 5G que se encontram em constante expansão e servirão a um grande grupo de aplicações e setores da economia (como energia, transporte, bancos e saúde, sistemas de controle industrial, eleições), e resultam em um grande volume de dados. A tecnologia sem fio da próxima geração, sob certas circunstâncias, afetaria todas as responsabilidades do GDPR [9].

Portanto, essas tecnologias precisam estar de acordo com o que é exigido pelo regulamento, deste modo, se a indústria de tecnologia emergente da União Europeia (EU) não conseguir resolver efetivamente as condições impostas pelo GDPR através de atualizações tecnológicas significativas, o que parece improvável a curto prazo, ou de outras formas, o desenvolvimento e a aplicação de tecnologias emergentes na UE podem diminuir significativamente [10]. Nesse aspecto é seguro dizer que a realidade brasileira deverá ser bem semelhante à europeia devido aos vários tópicos que a LGPD compartilha com o GDPR.

3.2 Comparações entre o GDPR e a LGPD

Ao analisarmos as duas normas, é possível observar vários pontos de convergência, uma vez que a LGPD foi inspirada no GDPR. Porém, cada uma possui suas próprias características e abordagens. Existem alguns pontos de convergência entre elas, por exemplo, nos dois casos os dados pessoais são definidos como informações referentes a pessoas físicas identificadas ou identificáveis e o consentimento é fortemente resguardado e protegido por ambas.

Para se realizar o tratamento de dados, o GDPR estabelece 6 princípios a serem seguidos: licitude, lealdade e transparência; limitação das finalidades; minimização dos dados; exatidão; limitação da conservação; integridade e confidencialidade; e responsabilidade. Já a LGPD possui 4 princípios a mais, seus 10 pontos são: finalidade; adequação; necessidade; livre acesso; qualidade dos dados; transparência; segurança; prevenção; não discriminação; e responsabilização.

Territorialmente, as duas normas têm competências de serem aplicadas a todos os indivíduos que realizam serviços em seus territórios, independentemente de onde estejam localizadas. Refletindo sobre a parte em que se refere aos direitos do titular dos dados, as duas legislações concedem a prerrogativa de que o titular dos dados possui o direito de excluir, acessar, revogar o consentimento, corrigir os dados e realizar portabilidade de dados ao passo que as organizações devem manter registros de todas as suas atividades de tratamento.

Na relação entre controlador e operador, a LGPD possui regras mais brandas, exigindo somente que o operador realize o tratamento de dados de acordo com as orientações do controlador, garantindo a conformidade do operador, enquanto o GDPR estabelece que exista um contrato contendo as condições que orientam a relação controlador-operador. Outro ponto importante a se destacar é o caso de vazamento de dados, a LGPD solicita que a comunicação seja realizada em um tempo razoável, enquanto o GDPR especifica um prazo de 72 horas.

Para o não cumprimento das leis, há previsão de potenciais multas, sanções ou processos civis. No caso do GDPR, a penalidade pode ser de 2% ou 4% do faturamento anual global

da companhia, chegando a 10 milhões ou 20 milhões de euros, o que for maior. Já a LGPD pode gerar multas com valor de até 2% do faturamento de uma empresa, chegando a um total máximo de 50 milhões de reais por infração.

	LGPD	**GDPR**
Abrangência territorial	Nacional	Continental
Relação controlador-operador	O operador realiza o tratamento de dados de acordo com as orientações do controlado	Necessário um contrato contendo as condições que orientam a relação controlador-operador
Prazo para comunicar violações	Em um prazo razoável	72 horas
Penalidades	2% do faturamento anual da empresa, limitado a 50 milhões de reais	Máximo 4% do faturamento anual global ou 20 milhões de euros
Fiscalização	Autoridade Nacional de Proteção de Dados (ANPD)	Comitê Europeu de Proteção de Dados

Tabela 1: Resumo dos principais pontos de comparação entre LGPD e GDPR.

4 Internet das Coisas

Ao longo de seus primeiros 40 anos, a internet tem sido usada principalmente para conectar pessoas por meio de e-mails, fóruns de discussão e, cada vez mais, por meio de sites de redes sociais que coletam e distribuem dados e informações, através de redes com e sem fio. Atualmente, nota-se que a internet é utilizada para conectar dispositivos, máquinas e outros objetos de posicionamento tecnológico constituindo o que chamamos de Internet das Coisas, do inglês *Internet of Things* (IoT) [11]. O termo Internet of Things foi cunhado em 1999 por Kevin Ashton, um dos pioneiros da tecnologia britânica que ajudou a desenvolver o conceito [12].

A Internet das Coisas é a expressão utilizada para denominar a infraestrutura de hardware e software que viabiliza a conectividade entre inúmeros dispositivos inteligentes que possuem conexão à internet, proporcionando controle remoto, automações e compartilhamento de dados, desde lâmpadas, eletrodomésticos, veículos, entre outros.

A IoT pode ser vista como a combinação de diversas tecnologias, as quais são complementares no sentido de viabilizar a integração dos objetos no ambiente físico ao mundo virtual [13]. A diversidade de aplicações viabilizadas pela IoT pode ser visualmente exemplificada pela Figura 1. As “coisas” que compõem essa rede inteligente são os objetos que possuem capacidade de comunicação e processamento associados a sensores que dão uma utilidade única a esses objetos. Com o surgimento de sensores de baixo custo e com menor

Figura 1: Representação gráfica da diversidade de aplicações IoT [12].

potência, evolução de conceitos e técnicas como computação em nuvem e análise de dados em massa, a Internet das Coisas ganhou notoriedade e hoje está presente em praticamente tudo à nossa volta.

Em 2017, com o objetivo de promover o desenvolvimento sustentável e competitivo da economia brasileira, o BNDES, em parceria com o Ministério da Ciência, Tecnologia, Inovações e Comunicações (MCTIC), apoiou a realização de um estudo [14] para o diagnóstico e a proposição de plano de ação estratégico para o país em Internet das Coisas. O estudo foi conduzido pelo consórcio McKinsey/Fundação CPqD/ Pereira Neto Macedo estimou que, em 2025, IoT pode adicionar entre 4 e 11 trilhões de dólares à economia global e entre 50 e 200 bilhões de dólares para o Brasil. Além de evidenciar todo o potencial econômico que a IoT pode gerar, o estudo elaborou um plano de ação para o Brasil focado em promover o crescimento e desenvolvimento econômico, criar uma sociedade conectada e fortalecer a cadeia produtiva de IoT. E pelo Decreto nº 9.854, de 25 de junho de 2019 foi instituído o Plano Nacional de Internet das Coisas [15] que tem como finalidade implementar e desenvolver a Internet das Coisas no país.

Assim, embora a LGPD não aborde diretamente o conceito de Internet das Coisas em seu texto, não se pode deixar de associar uma legislação sobre dados pessoais com IoT, a LGPD toca em vários pontos sensíveis a IoT. Considerando esse contexto de fomento por parte governamental e o crescimento econômico do setor, uma lei geral de dados ganha ainda mais relevância.

4.1 Tratamento de Dados na IoT

Uma situação cotidiana que demonstra como a IoT está cada vez mais presente na vida das pessoas são as casas inteligentes. Uma *smart home*, termo em inglês, é uma casa com dispositivos inteligentes conectados entre si e projetados para oferecer uma série de serviços dentro e fora de casa através de vários dispositivos. Atualmente, cada vez mais pessoas estão

interessadas em aderir a esse conceito em suas casas, gerando uma alta no mercado [16].

As funcionalidades que uma *smart home* possui incluem a integração de inúmeros aparelhos entre si e o usuário, através de uma conexão com a internet de banda larga. Os dispositivos IoT usam uma variedade de sensores que coletam e processam uma grande quantidade de dados, ou seja, temos dispositivos conectados à rede 24 horas por dias coletando dados. Desta maneira, além de ter consciência sobre o que está acontecendo com essas informações após coletadas é preciso ter a segurança que nenhum dispositivo está suscetível a vulnerabilidades, assim sendo uma porta entrada para pessoas mal intencionadas. Coletar dados como pulsação cardíaca, biometria, informações de localização, informações de rotinas, etc., são casos corriqueiros quando estamos falando de Internet das Coisas e qualquer dispositivo que utilize dados desse tipo estão sujeitos a LGPD. Muitas tecnologias de IoT, no primeiro momento, se concentraram em coletar dados dos usuários e criar soluções a partir dessas informações. No entanto, com o surgimento de legislações que visam regular o uso de dados pessoais, como a LGPD, o debate retoma a dois assuntos que são muito negligenciados: a segurança da informação e a privacidade, tendo em vista que a lei muda totalmente a forma como os dados devem ser tratados em todos os seus momentos de atuação.

Possuir bancos de dados sem saber exatamente sua origem é algo inviável a partir de agora e empresas que se encontram nessa situação serão obrigadas a mudar. Desse modo, em um primeiro momento, será necessário mapear os dados que a empresa detém; esse mapeamento de dados refere-se a um documento essencial quando estamos no processo de adequação às normas de proteção de dados. O mapeamento deve refletir o caminho percorrido pelo dado pessoal dentro da empresa, incluindo os processos e procedimentos pelos quais o dado transita. Ou seja, qual a origem, a base legal que respalda o tratamento deste dado pessoal, o nível de segurança da base de dados a qual o dado pertence, entre outras informações necessárias para a análise de vulnerabilidades técnicas e jurídicas [17]. Esse procedimento se faz necessário para que as empresas se adequem à legislação, pois o artigo 37º da LGPD determina que o controlador e o operador precisam manter os registros das operações de tratamento de dados pessoais que foram realizadas.

Além disso, as companhias necessitarão modificar processos internos e conscientizar seus colaboradores por meio de treinamentos sobre a obrigação de tratar dados de forma segura com procedimentos previamente definidos e que cumpram os requisitos da lei e também realizar atualizações em suas tecnologias e arquitetura de dados.

5 Desafios da IoT no contexto da LGPD

No desenvolvimento de IoT em conformidade com a LGPD, vazamentos de dados e segurança da informação são apenas dois desafios relacionados ao tratamento de dados pessoais. É possível ainda citar a insuficiência de informações por parte dos usuários, a dificuldade em obter consentimento dos usuários, o uso de dados para fins diferentes daqueles para os quais foram inicialmente coletados e o esforço para a anonimização de dados.

Legislações como a LGPD e o GDPR impactam diretamente o conceito de IoT. Muitos autores reconheceram vários pontos em relação à aplicação do GDPR ao processamento

de IoT, como o uso inadequado de dados sem consentimento. Outra questão interessante acerca do debate sobre a temática da GDPR e LGPD são os custos de implementação de medidas adequadas que podem ser proibitivamente alto, considerando a natureza relativamente simples dos sensores e dispositivos de monitoramento que limitam a capacidade de implementar com eficácia medidas técnicas e organizacionais eficientes para ajudar a cumprir os requisitos do GDPR [18].

Os aspectos relatados como desafios gerados pelo GDPR são totalmente aplicáveis a LGPD dado as similaridades das legislações. Demandas de segurança, privacidade e consentimento impostas pela Lei Geral de Proteção de Dados exigirão muitas mudanças complicadas em dispositivos restritos ou sistemas já consolidados a fim de proteger a privacidade dos usuários. E de todos os desafios conhecidos, nenhum deles tem uma influência mais significativa na adaptação à IoT, como segurança e privacidade, o desenvolvimento e utilização da Internet das Coisas dependerá de como ela consegue respeitar as escolhas de privacidade de seus usuários [19].

A utilização de dispositivos que compõem a IoT já proporcionou inúmeros episódios de vulnerabilidades sendo exploradas por criminosos, um ambiente repleto de aparelhos conectados à internet, aumenta ainda mais a possibilidade de ataques maliciosos. Atualmente, para desenvolver qualquer produto que de alguma forma irá lidar com dados pessoais é preciso, desde o começo do seu desenvolvimento, planejar em como estar de acordo com o que é estabelecido pela lei. Essa situação nos traz uma questão bastante pertinente: como continuar a desenvolver tecnologias em que seu principal motor está no tratamento de dados pessoais e ao mesmo tempo respeitar a privacidade dos usuários, garantindo a segurança do mesmo durante a navegação e ainda considerar o custo envolvido nesses novos procedimentos?

Com a quantidade de critérios que precisam ser cumpridos para se estar em conformidade com o GDPR, Christos Karageorgiou Kaneen [20] elaborou uma série de perguntas que ao serem respondidas ajudam a entender o ciclo de vida completo dos dados pessoais em um sistema, e ao serem respondidas elas auxiliam a incorporar os requisitos do GDPR ao design de um sistema.

1. Quais são as entidades de dados fundamentais?
2. Quais são os dados pessoais dentro do sistema?
3. Onde os dados são armazenados?
4. Como e quando os dados foram obtidos?
5. Qual é a necessidade desses dados?
6. Quem tem acesso aos dados?
7. O proprietário dos dados deu consentimento para usar os dados?
8. Os dados estão seguros?
9. Como os dados trafegam pelos sistemas?

Como para o GDPR, essas 9 perguntas também são pertinentes também para a LGPD, respondê-las orientam como verificar de forma clara e objetiva se um sistema se encontra dentro dos padrões estabelecidos pela lei.

A arquitetura da IoT, como pode ser visto na Figura 2, precisa oferecer um alto nível de segurança, precisa suportar uma fonte heterogênea de informações (dispositivos IoT, sensores/atuadores, dispositivos móveis e streams) que são acessadas por uma infinidade de maneiras diferentes e através de vários sistemas de comunicação em cenários onde, em alguns casos, é difícil prever quando e onde os dados são gerados e disponibilizados para o sistema/subsistemas da plataforma [21].

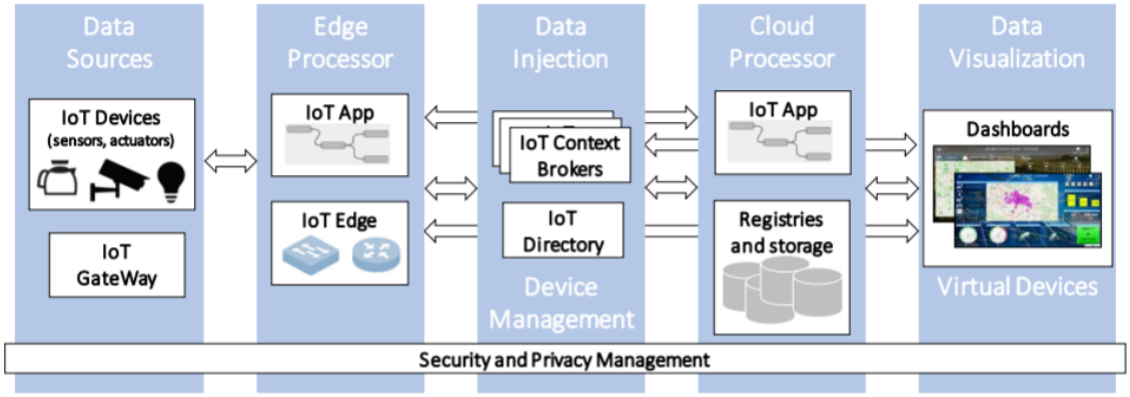

Figura 2: Arquitetura geral da IoT [22].

Os artigos 46º, 47º e 49º da LGPD cobrem exatamente a questão da segurança. Neles é explicitado que os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma em que atendam aos requisitos de segurança e que os agentes de tratamento adotem medidas de segurança, técnicas e administrativas capazes de proteger os dados pessoais de acessos não autorizados. Todas as etapas de um processo seguro devem ser garantidas, tais como soluções para proteger os dados durante todo o seu ciclo de vida, incluindo comunicação, consumo para análise e visualização.

Existem pelo menos três de objetivos desejáveis para segurança em IoT como aponta Zach Shelby [23]:

- **Confidencialidade:** elementos sem autorização podem saber que ocorreu comunicação, mas não sabem seu conteúdo;
- **Integridade:** os dados não podem ser modificados por elementos da rede sem a autorização;
- **Disponibilidade:** garantir que o sistema sempre esteja disponível e seguro contra ataques maliciosos.

A partir de agora para viabilizar o desenvolvimento da IoT que esteja em conformidade com a LGPD, podem ser destacados os seguintes pontos: i) a compreensão das exigências

da Lei, ii) o desenvolvimento de uma estratégia de mitigação de riscos na concepção de novos produtos e serviços, iii) a priorização da transparência no tratamento de dados, iv) a consideração das limitações tecnológicas e de custos da organização e v) a indicação de um encarregado de proteção de dados pessoais pela organização [24].

Nesse sentido, Nairobi Spiecker de Oliveira [25] destaca três pontos em que dispositivos de IoT enfrentarão seus maiores desafios, seja por limitações técnicas ou custos: coleta, transmissão e armazenamento.

5.1 Coleta

Ao citar a coleta de dados estamos falando também de consentimento e, nesse sentido, alguns itens são fundamentais, entre eles a transparência. É necessário informar aos usuários de maneira clara e objetiva todas as informações a respeito dos dados que serão coletados, evidenciar quais dados serão coletados, como eles serão tratados, qual a finalidade e o tempo do tratamento são alguns aspectos que devem ser informados.

Além disso, é vital pedir a autorização do usuário para a realização desses procedimentos de maneira explícita e não abusiva. As permissões de compartilhamento e tratamento carecem refletir os interesses e preferências do usuário. A privacidade desde o design implementado na estratégia visa fornecer aos usuários ferramentas para supervisionar e controlar, gerenciar e compartilhar seus dados com dispositivos e serviços IoT [26].

Um problema que pode surgir na coleta são dispositivos que não possuem uma interface bem definida para exibir todas as informações necessárias ao usuário e solicitar seu consentimento, para muitos aparelhos as telas não são necessárias ou são simples demais. Por exemplo, um *smartwatch* que possui um visor de LED que apenas exibe as horas, mas realiza coleta de batimento cardíacos, nesse caso apenas após o usuário assinar o termo de consentimento os dados de batimento poderiam começar a ser coletados. Uma solução para esse problema seria o usuário ser obrigado a utilizar um aplicativo mobile que se vincularia ao relógio, assim todas as informações seriam exibidas na tela do smartphone e o usuário poderia dar seu consentimento e apenas a partir desse momento o *smartwatch* estaria apto a funcionar em sua plenitude. Dessa forma dispositivos IoT que não possuam uma tela própria provavelmente seriam obrigados a ter algum tipo de integração com dispositivos externos, seja um smartphone ou um website onde é possível realizar todo o gerenciamento dos dados envolvidos já que por si próprio não possuem essa capacidade.

Um outro modo de coleta de dados pessoais que pode passar despercebido é a captação de imagem por câmeras em ambientes públicos ou privados. Pelas definições da LGPD, imagem é um dado pessoal e esse tipo de captação acaba sendo muito comum quando estamos falando do conceito de *Smart Cities*. No entanto, pelo Art. 4º, esse tipo de dado pessoal pode ou não ser enquadrado pela lei, dependendo da sua finalidade. Como IoT, a LGPD não trata especificamente de *Smart Cities*, mas deixa clara a importância da proteção de dados pessoais em diversos contextos, assim todo serviço ou sistema que fuja do que é estabelecido pelo Art. 4º deverá ser tratado como contemplado pela lei e precisará seguir suas normas de consentimento, segurança e privacidade normalmente. Ou seja, caso haja algum fim econômico nesta coleta, quem a realiza precisará desenvolver métodos para buscar o consentimento dos proprietários dos dados. Ainda assim, esse é um tema que pode

gerar discussão, e para questões que se encontram em uma zona cinzenta, a Autoridade Nacional de Proteção de Dados (ANPD) terá papel fundamental para elucidar dúvidas e trazer maior clareza aos pontos ainda incertos.

5.2 Transmissão

A transmissão de dados de acordo com os requisitos exigidos pela LGPD pode requerer a atualização ou a implantação de novos mecanismos de segurança. Devido a forma com que os dados são transmitidos, a IoT torna-se vulnerável à maioria dos ataques comuns de redes sem fio, consequentemente, a IoT requer uma política de segurança, mas o custo para fornecê-la deve ser o mais baixo possível [27]. A camada de rede é provavelmente a camada que mais enfrenta ataques. Isso ocorre devido a sua característica de transmitir dados que passam por inúmeros intermediários até chegar ao seu destino. Dessa forma, a possibilidade de vulnerabilidades aparecerem aumenta muito. Assim sendo, a IoT exige uma política de segurança viável e de baixo custo. Diversos tipos de abordagens de segurança precisam ser analisados a fim de proporcionar a autenticidade, integridade e confidencialidade dos dados dos usuários [28].

Cada dispositivo no universo de IoT pode ser classificado em uma classe, de acordo com sua capacidade de memória e armazenamento de código. As classes são, por sua vez, definidas em 0, 1 e 2 [29]. Dispositivos de classe 0 podem ser definidos como sensores muito restritos sem capacidade de se comunicar diretamente com a Internet de maneira segura. A classe 1, ainda que limitada, já possui capacidade de executar protocolos mais sofisticados. Por fim, a classe 2 é capaz de suportar protocolos mais exigentes capazes de oferecer um nível maior de segurança. Consequentemente, os maiores desafios ocorrem com dispositivos pertencentes à classe 0. Essa classe possui restrições muito altas, apenas coletam uma informação e a enviam utilizando tecnologia sem fio de baixo consumo de energia. Tais equipamentos não possuem recursos para executarem, por exemplo, a pilha TCP/IP e protocolos adaptados para Internet das Coisas na camada de aplicação [25].

5.3 Armazenamento

Quanto ao armazenamento, manter a integridade dos dados após coletados conforme é exigido pela lei também possui seus obstáculos. Podemos verificar que há alguns pontos muito pertinentes, como quais recursos os sistemas de armazenamento precisam ter para serem compatíveis com a LGPD e como a conformidade pode afetar o desempenho de diferentes sistemas. Alguns aspectos que devem ser seguidos são:

- Exclusão: Nenhum dado pessoal pode ser mantido por tempo indeterminado, ou seja, o sistema de armazenamento deve contar com meios de apagar dados pessoais automaticamente quando eles atingem o fim de suas vidas úteis;
- Registros: Todas as operações que os dados sofrerem, seja leitura, gravação e edição, precisam ser registradas;
- Consultas: Os sistemas de armazenamento devem ter interfaces que permitam o acesso rápido e eficiente a conjuntos de dados específicos. Uma consulta pode ser solicitada

a qualquer momento, em vista disso, os dados precisam estar organizados em um formato que facilite o direito ao acesso.

- Criptografia: A criptografia pode ser usada a fim de aumentar a segurança dos dados, no entanto, ao utilizar essa técnica o desempenho dos sistemas pode ser comprometido.

5.3.1 Computação de Borda

Uma forma de mitigar o problema do armazenamento é realizar um processamento dos dados localmente. Assim os dados coletados poderiam ser processados pelo próprio dispositivo, computador ou servidor local, em vez de serem transmitidos para um data center. Dessa forma, apenas o resultado do processamento, se necessário, seria enviado para a nuvem, e os dados coletados poderiam ser excluídos imediatamente após o uso.

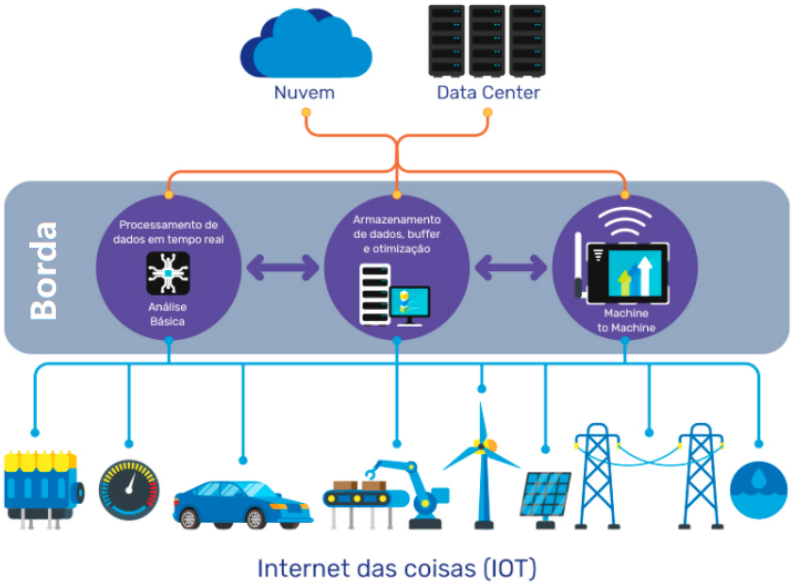

Figura 3: Computação de Borda [30].

Para esse tipo de abordagem, já existem técnicas como a computação de borda, a Figura 3 exemplifica esse conceito. A computação de borda refere-se às tecnologias que permitem que a computação seja realizada na borda da rede para que o processamento aconteça perto das fontes de dados [31]. Além da segurança dos dados, outro benefício apresentado por esse método é que ele diminui o volume de dados e evita o envio de grandes porções de dados brutos para a nuvem computacional. Em vez disso, apenas metadados serão transmitidos. Reduzir o número de transmissões entre os dispositivos IoT também é muito importante para evitar problemas de latência e saturação dos canais sem fio [27].

No entanto, esse tipo de técnica possui algumas limitações, principalmente se tratando de dispositivos móveis que tem poder de processamento e capacidade de energia limitados,

deste modo apenas aplicações que não exigem um alto processamento poderiam adotar essa abordagem.

6 Conclusão

O surgimento de leis como a LGPD deixa claro que tão importante quanto o avanço das tecnologias em si, a proteção à privacidade é uma preocupação e merece atenção, desde o consentimento até a exclusão dos dados ao fim do tratamento. Um aprendizado que podemos tirar do GDPR é a necessidade de se criar uma cultura por parte das empresas para adequar suas operações e garantir a conformidade com a lei brasileira, mitigando riscos, danos financeiros e reputacionais, possibilitando, ainda, um relevante potencial competitivo para seus clientes. Adicionalmente, é necessário criar uma cultura por parte da sociedade que precisa estar atenta aos seus direitos e acionar as autoridades competentes sempre que eles foram violados.

No contexto de utilização de dados pessoais, a Internet das Coisas se destaca possibilitando diversas facilidades em variadas áreas e campos de aplicação, entretanto, a existência de leis que regulam dados pessoais, os quais são fundamentais para a IoT, estabelece uma série de desafios operacionais, técnicos e jurídicos para se estar em conformidade com a lei de proteção de dados, sendo os principais consentimento, segurança e privacidade. No aspecto técnico, a utilização de alguns métodos como criptografia e computação de borda surgem como soluções, mas não sem adicionar novos problemas, tais como aumento no custo e na demanda por processamento. Deste modo, ao desenvolver uma aplicação que utiliza dados pessoais, desde o começo é preciso ponderar quais aspectos devem ser priorizados para se estar em conformidade.

Logo, estar de acordo com tudo o que é exigido é um processo complexo e trabalhoso, podendo afetar diretamente o desenvolvimento de tecnologias. Dispositivos IoT serão muito atingidos, podendo inclusive limitar o escopo das aplicações. No entanto, com o GDPR na Europa e a LGPD no Brasil, não há mais como evitar questões de segurança e privacidade quando estamos falando de dados pessoais.

Referências

[1] UNIÃO EUROPEIA. Regulamento (UE) nº 2016/679 de 27 de abril de 2016. Regulamento Geral sobre a Proteção de Dados (RGPD).

[2] BRASIL. Lei nº 13.709, de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: `http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm`. Acesso em: 10 de agosto de 2021.

[3] Pesquisa Empresas e LGPD: resultados apontam cenários, desafios e caminhos. Disponível em: `https://resultadosdigitais.com.br/blog/pesquisa-empresas-e-lgpd/?\_ga=2.36075368.935640988.1628606832-250818075.1628606832`. Acesso em 10 de agosto de 2021.

[4] CAVALCANTE, Pedro Peres. Privacidade e proteção de dados pessoais:Uma análise comparativa dos quadros regulatórios brasileiro e europeu. Trabalho de Conclusão de Curso (Graduação em Direito) - Universidade Federal de Pernambuco (UFPE), p. 36, 2018.

[5] MAGRI, Marli da Rocha. Lei geral de proteção de dados: principais aspectos e impactos de sua vigência. Anais do I Congresso do Curso Direito, 2019.

[6] GDPR at One Year: What We Heard from Leading European Regulators. Disponível em: `https://iapp.org/resources/article/gdpr-at-one-year-dpas/`. Acesso em 15 de agosto de 2021.

[7] GDPR at Three. Disponível em: `https://iapp.org/resources/article/gdpr-at-three/`. Acesso em 15 de agosto de 2021.

[8] Amazon recebe multa recorde de US$887 milhões na União Europeia por questões de privacidade. Disponível em: `https://g1.globo.com/economia/tecnologia/noticia/2021/07/30/amazon-recebe-multa-recorde-de-746-milhoes-de-euros-na-uniao-europeia-por-questoes-de-privacidade.ghtml`. Acesso em: 26 de agosto de 2021.

[9] RIZOU, S. et al. GDPR Interference With Next Generation 5G and IoT Networks. IEEE Access, v. 8, p. 108052-108061, 2020.

[10] LI, He et al. The impact of GDPR on Global Technology Development. Journal of Global Information Technology Management, v. 22, n. 1, p. 1-6, 2019.

[11] DUTTON, William H. Putting things to work: social and policy challenges for the Internet of things. info, v. 16, n. 3, p. 1-21, 2014.

[12] GUBBI, Jayavardhana et al. Internet of Things (IoT): A vision, architectural elements, and future directions. Future Generation Computer Systems, v. 29, n. 7, p. 1645-1660, 2013.

[13] SANTOS, Bruno Pereira dos et al. Internet das coisas: da teoria à prática. SBRC-Simpósio Brasileiro de Redes de Computadores e Sistemas Distribuídos, 2016.

[14] Internet das Coisas: Um plano de ação para o Brasil. Díponível em: `https://www.bndes.gov.br/wps/portal/site/home/conhecimento/pesquisaedados/estudos/estudo-internet-das-coisas-iot/estudo-internet-das-coisas-um-plano-de-acao-para-o-brasil`. Acesso em 19 de agosto de 2021.

[15] BRASIL. Decreto nº 9.854, de 19 de junho de 2019. Plano Nacional de Internet das Coisas.

[16] IDC projeta alta de 21% para mercado de casa inteligente. Disponível em: `https://newvoice.ai/2021/02/05/idc-projeta-alta-de-21-para-mercado-de-casa-inteligente`. Acesso em: 15 de agosto de 2021.

[17] BRANDAO, Graziela. O que é o mapeamento de dados? Disponível em: `https://blconsultoriadigital.com.br/mapeamento-de-dados/`. Acesso em: 10 de agosto de 2021.

[18] VOJKOVIĆ, Goran et al. IoT and Smart Home Data Breach Risks from the Perspective of Data Protection and Information Security Law. Business Systems Research, v. 11, n. 3, p. 167-185, 2020.

[19] TAWALBEH, Lo'ai et al. IoT Privacy and Security: Challenges and Solutions. Applied Sciences, 2020.

[20] KANEEN, Christos Karageorgiou et al. Towards evaluating GDPR compliance in IoT applications. 24th International Conference on Knowledge-Based and Intelligent Information & Engineering, 2020.

[21] ZHAO, K. et al. A survey on the internet of things security. In 2013 Ninth international conference on computational intelligence and security, p. 663- 667, 2013.

[22] BADII, C. et al. Smart City IoT Platform Respecting GDPR Privacy and Security Aspects. v. 8, p. 23601-23623, 2020.

[23] SHELBY, Zach. et al. 6LoWPAN: The wireless embedded Internet, 2009.

[24] DAVOLI, Gabriela Brum. Série IoT: IoT e os impactos à proteção de dados pessoais. Disponível em: `https://baptistaluz.com.br/espacostartup/iot-protecao-de-dados-pessoais/`. Acesso em: 12 de agosto de 2021.

[25] OLIVEIRA, Nairobi Spiecker de et al. Segurança da Informação para Internet das Coisas (IoT): uma abordagem sobre a Lei Geral de Proteção de Dados (LGPD). Revista Eletrônica de Iniciação Científica em Computação, 2019.

[26] WACHTER, Sandra. Normative challenges of identification in the Internet of Things: Privacy, profiling, discrimination, and the GDPR. Computer Law & Security Review, v. 34, n. 3, p. 436-449, 2018.

[27] STOJKOSKA, Biljana L. Risteska. A review of Internet of Things for smart home: Challenges and solutions. Journal of Cleaner Production, Skopje, Macedonia, v. 140, p.1454-1464, 2017.

[28] GONÇALVES, Rangel Leonardo Moura. Automatização residencial: um estudo de caso da aplicação da internet das coisas. Trabalho de Conclusão de Curso - Universidade do Sul de Santa Catarina (UNISUL), 2019.

[29] BORMANN, Carsten. Terminology for Constrained-Node Networks, 2014.

[30] Edge computing: Saiba o que é a tendência e por que é relevante. Disponível em: `https://blog.cronapp.io/edge-computing/`. Acesso em: 10 de outubro de 2021.

[31] SHI, Weisong et al. The Promise of Edge Computing. Computer, v. 49, n. 5, p. 78-81, 2016.