UNIVERSIDADE TECNOLÓGICA FEDERAL DO PARANÁ
PROGRAMA DE PÓS-GRADUAÇÃO EM PLANEJAMENTO E GOVERNANÇA PÚBLICA

MATHEUS FOGAÇA MACHADO

MEDIDAS DE PROTEÇÃO DE DADOS PESSOAIS NO PLANEJAMENTO E OPERAÇÃO DE *SMART GRID* UTILIZANDO COMPUTAÇÃO EM NUVEM: Estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil.

CURITIBA

2019

MATHEUS FOGAÇA MACHADO

MEDIDAS DE PROTEÇÃO DE DADOS PESSOAIS NO PLANEJAMENTO E OPERAÇÃO DE *SMART GRID* UTILIZANDO COMPUTAÇÃO EM NUVEM: Estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil.

Dissertação apresentada ao Programa de Pós-Graduação em Planejamento e Governança Pública, da Universidade Tecnológica Federal do Paraná, como requisito parcial à obtenção do título de Mestre em Planejamento e Governança Pública. Área de Concentração: Planejamento Público e Desenvolvimento.

Orientador: Prof. Dr. Décio Estevão do Nascimento

Coorientadora: Profa. Dra. Keiko Veronica Ono Fonseca

CURITIBA

2019

Dados Internacionais de Catalogação na Publicação

Machado, Matheus Fogaça
Medidas de proteção de dados pessoais no planejamento e operação de smart grid utilizando computação em nuvem [recurso eletrônico] : estudo no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD) do Brasil / Matheus Fogaça Machado.-- 2019.
1 arquivo texto (117 f.) : PDF; 1,20 MB.

Modo de acesso: World Wide Web.
Título extraído da tela de título (visualizado em 18 nov. 2019).
Texto em português com resumo em inglês
Dissertação (Mestrado) - Universidade Tecnológica Federal do Paraná. Programa de Pós-graduação em Planejamento e Governança Pública, Curitiba, 2019
Bibliografia: f. 97-107

1. Administração pública - Dissertações. 2. Computação em nuvem - Medidas de segurança. 3. Ciberespaço - Medidas de segurança. 4. Redes de computadores - Medidas de segurança. 5. Computadores - Medidas de segurança. 6. Proteção de dados - Brasil - Legislação. 7. Direito à privacidade - Brasil - Legislação. 8. Personalidade (Direito) - Legislação - Brasil. 9. Redes elétricas inteligentes. 10. Brasil. Lei Geral de Proteção de Dados Pessoais no Brasil (2018). I. Nascimento, Décio Estevão do. II. Fonseca, Keiko Verônica Ono. III. Universidade Tecnológica Federal do Paraná. 6. Programa de Pós-graduação em Tecnologia e Sociedade. IV. Título.

CDD: Ed. 22 -- 351

Biblioteca Central da UTFPR, Câmpus Curitiba
Bibliotecário: Adriano Lopes CRB-9/1429

TERMO DE APROVAÇÃO DE DISSERTAÇÃO N° 99

A Dissertação de Mestrado intitulada **Medidas de proteção de dados pessoais no planejamento e operação de Smart Grid utilizando computação em nuvem: estudo no contexto da Lei Geral De Proteção De Dados Pessoais (LGPD) do Brasil**, defendida em sessão pública pelo(a) mestrando(a) **Matheus Fogaça Machado**, no dia 9 de setembro de 2019, foi julgada para a obtenção do título de Mestre em Planejamento e Governança Pública, área de concentração Planejamento Público e Desenvolvimento, e aprovada em sua forma final, pelo **Programa de Pós-Graduação em Planejamento e Governança Pública**.

BANCA EXAMINADORA:

Prof. Dr. Décio Estevão do Nascimento – UTFPR (Presidente)
Prof.a Dr.a Maria Lucia Figueiredo Gomes de Meza – UTFPR
Prof. Dr. Rodrigo José Firmino – PUCPR

A via original deste documento encontra-se arquivada na Secretaria do Programa, contendo a assinatura da Coordenação após a entrega da versão corrigida do trabalho.

Curitiba, 9 de setembro de 2019

Carimbo e Assinatura do(a) Coordenador(a) do Programa

À minha parceira, por tudo, para sempre.

AGRADECIMENTOS

Agradeço ao meu orientador por todo o auxílio e apoio desde o ingresso no programa de Mestrado. Pela sua disposição em acomodar meus interesses de pesquisa, incentivá-los e refiná-los para a condução desta, por sua dedicação e paciência em revisar diversas versões de um mesmo texto, sempre indicando claramente oportunidades de avanço, tanto no conteúdo quanto na forma. Por toda a sua compreensão com os problemas enfrentados ao longo do caminho e por ter me apresentado à minha coorientadora.

Agradeço à minha coorientadora pelo interesse em auxiliar nesta pesquisa, oferecer novas perspectivas e acomodar o desenvolvimento de meus interesses de pesquisa em um projeto em andamento, oportunidade frutífera para a multidisciplinaridade deste estudo. Pela sua disposição e paciência em revisar os textos produzidos, apontando sentidos para seu desenvolvimento e oferecendo clareza. Por toda a sua compreensão com os problemas enfrentados e pelas oportunidades oferecidas.

Agradeço à banca pelas valiosas sugestões nos momentos da qualificação e defesa, oferecendo novos olhares ao texto e aumentando sua capacidade de resposta às perguntas de pesquisa.

Agradeço à Rede Nacional de Ensino e Pesquisa e Horizon 2020 da União Europeia pela concessão da bolsa durante o mestrado e liberdade para o desenvolvimento da pesquisa nos termos propostos.

Agradeço à minha família por todo o apoio.

> Já muitas vezes tinha meditado se não seria conveniente redigir um escrito de defesa para ser apresentado à justiça. Faria nele uma breve descrição de sua vida até esse momento, e em cada fato que pudesse assumir alguma importância explicaria as razões pelas quais tinha agido de uma determinada maneira. (KAFKA, 1925, p. 125)

RESUMO

MACHADO, Matheus F. **Medidas de proteção de dados pessoais no planejamento e operação de Smart Grid utilizando computação em nuvem:** estudo no contexto da Lei Geral De Proteção De Dados Pessoais (LGPD) do Brasil. 117 f. 2019. Dissertação (Mestrado em Planejamento e Governança Pública), Programa de Pós-Graduação em Planejamento e Governança Pública, da Universidade Tecnológica Federal do Paraná, Curitiba. 2019

A transição do setor de geração e consumo de energia para o modelo de *Smart Grid* (rede elétrica inteligente) tem o potencial de modernizar o setor elétrico, aumentar a disponibilidade de carga, diversificar as fontes geradoras, ampliar o uso de veículos elétricos, entre outras vantagens. Ao mesmo tempo, os *Smart Meters* (medidores inteligentes), peças indispensáveis à modernização da rede, introduzem uma nova fonte de dados pessoais que causam preocupação quanto à possibilidade de invasão de privacidade. Este estudo pretende propor um conjunto de medidas voltadas à proteção de dados pessoais para planejamento e operação de *Smart Grid* utilizando computação em nuvem. Realizou-se levantamento bibliográfico baseado em levantamento bibliométrico e Análise de Conteúdo com a finalidade de identificar ameaças à privacidade e propostas técnicas e organizacionais de proteção de dados pessoais em *Smart Grids* para que subsidiassem a condução de um processo de Avaliação de Impacto à Proteção de Dados. Como principais resultados, a pesquisa mostrou que as medidas são mais eficazes quando tomadas no planejamento do projeto e possam orientar seu desenvolvimento para modelos que busquem a minimização dos dados, principalmente pela limitação de uso e coleta ao mínimo necessário para cada função, mas também por técnicas de criptografia e anonimização. O uso exclusivo de procedimentos técnicos sobre sistemas executando sob o modelo de "coletar primeiro, processar depois" podem não ser eficazes, reforçando a importância de integração de medidas de proteção de dados pessoais de maneira preventiva e abrangente aos componentes do sistema.

Palavras-chave: Privacidade. Proteção de dados. *Smart Grid*. Avaliação de Impacto à Proteção de Dados. Nuvem segura.

ABSTRACT

MACHADO, Matheus F. **Data protection measures in planning and operation of Smart Grid using cloud computing:** study in the context of the General Data Protection Law of Brazil. 117 f. 2019. Dissertação (Mestrado em Planejamento e Governança Pública), Programa de Pós-Graduação em Planejamento e Governança Pública, da Universidade Tecnológica Federal do Paraná, Curitiba. 2019

The energy generation and consumption sector's transition to the Smart Grid model has the potential to modernize the electric sector, increase the load availability, diversify the energy sources, and increase the use of electric vehicles, among other advantages. At the same time, the smart meters, imperative to the grid's modernization, insert a new source of personal data that cause concern regarding the possibility of privacy invasion. This study aims to propose a set of measures for data protection in the Smart Grid planning and operation using cloud computing. A bibliographic survey was fulfilled through bibliometric survey and content analysis seeking to identify privacy threats and technical and organizational propositions of data protection in Smart Grids to subsidize the undertaking of a Data Protection Impact Assessment. The main results show that the measures are more effective when taken on the system planning and can orient its development to models that seek data minimization, mainly through use and collection limitation to the least amount necessary to perform each function, but also through cryptography and anonymization technics. The solely use of technical procedures on systems executing under the "collect first, process later" model may not be effective, reinforcing the importance of integrating data protection measures preemptively and thoroughly to the system's components.

Keywords: Privacy. Data Protection. Smart Grid. Data Protection Impact Assessment. Secure Cloud.

LISTA DE FIGURAS

Figura 1 - Etapas da pesquisa bibliométrica 57
Figura 2 - Teste de Aderência das Palavras-chave dos grupos 1 e 2. 62
Figura 3 - Formação do banco de artigos bruto 66
Figura 4 - Fases da Análise de Conteúdo 69
Figura 5 - Etapas do processo de Avaliação de Impacto à Proteção de Dados Pessoais 79
Figura 6 - Modelo de fluxo de dados SecureCloud 84

LISTA DE QUADROS

Quadro 1 - A *Smart Grid* comparada à Rede Elétrica existente 38
Quadro 2 - Síntese de preocupações de privacidade relacionadas à S*mart Meters*. 40
Quadro 3 - Definição das Categorias de Análise, Unidades de Registro e Contexto finais 74
Quadro 4 - Requisitos de privacidade, Ameaças e Contramedidas 91

LISTA DE TABELAS

Tabela 1 - Levantamento bibliográfico preliminar.....57
Tabela 2 - Levantamento bibliográfico preliminar (continuação) 59
Tabela 3 - Teste de Aderência das Palavras-chave do grupo 1.....63
Tabela 4 - Teste de Aderência das Palavras-chave do grupo 2.....64
Tabela 5 - Teste de Aderência das Palavras-chave do grupo 3.....65

LISTA DE ABREVIATURAS OU SIGLAS

AIP	- Avaliação de Impacto à Privacidade
AIPD	- Avaliação de Impacto à Proteção de Dados Pessoais
ANEEL	- Agência Nacional de Energia Elétrica
ANPD	- Agência Nacional de Proteção de Dados Pessoais
CEE	- Companhia de Energia Elétrica
CPTM	- Cloud Privacy Threat Modeling
ICO	- Information Comissioner's Office
IPC	- Information and Privacy Commissioner of Ontario
LGPD	- Lei Geral de Proteção de Dados Pessoais
OVIC	- Office of the Victorian Information Commissioner
PbD	- Privacy by Design
PETs	- Privacy Enhancing Technologies
RIPD	- Relatório de Impacto à Proteção de Dados Pessoais
RGK	- Registratiekamer
SG	- Smart Grid
SM	- Smart Meter
SGX	- Secure Guard eXtension
TIC	- Tecnologias da Informação e Comunicação
UC	- Unidades consumidoras

SUMÁRIO

1 INTRODUÇÃO 16
1.1 TEMA 16
1.2 DELIMITAÇÃO DA PESQUISA 21
1.3 PROBLEMA, PERGUNTA E PREMISSA DA PESQUISA 23
1.4 OBJETIVOS 25
1.4.1 Objetivo geral 25
1.4.2 Objetivos específicos 25
1.5 JUSTIFICATIVA 26
1.6 PROCEDIMENTOS METODOLÓGICOS 28
1.7 EMBASAMENTO TEÓRICO 29
1.8 ESTRUTURA DA DISSERTAÇÃO 30
2 FUNDAMENTAÇÃO TEÓRICA 31
2.1 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS 31
2.2 *PRIVACY BY DESIGN - PBD* 34
2.3 SMART GRID 36
2.3.1 Privacidade e Segurança em *Smart Grid* (*SG*) 39
2.3.2 Aspectos regulatórios de *Smart Grid* (*SG*) 41
2.4 AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (AIPD) 42
2.4.1 AIPD na legislação 44
2.5 COMPUTAÇÃO EM NUVEM (*CLOUD COMPUTING*) 47
2.5.1 Características essenciais 48
2.5.2 Modelos de serviço 48
2.5.3 Modelos de implantação (*Deployment models*) 49
2.5.4 Desafios da computação em nuvem 50
3 METODOLOGIA DA PESQUISA 52
3.1 O PROCESSO DE AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (AIPD) 52
3.2 *ADVANCED CLOUD PRIVACY THREAT MODELING* (*CPTM*) 53
3.2.1 *Compliance* regulatório de privacidade 54
3.2.2 Especificação de ambiente de nuvem 54
3.2.3 Identificação de ameaças à privacidade 55
3.2.4 Avaliação de risco 55

3.2.5 Mitigação de ameaças.....55
3.3 LEVANTAMENTO BIBLIOMÉTRICO 56
3.3.1 Levantamento bibliográfico preliminar 57
3.3.2 Seleção do portfólio bibliográfico.....59
3.3.2.1 Seleção do Banco de Artigos Bruto 60
3.3.2.2 Filtragem dos artigos 66
3.3.2.3 Análise Sistêmica 67
3.4 ANÁLISE DE CONTEÚDO.....68
3.4.1 Pré-análise 69
3.4.2 Exploração do material.....70
3.4.3 Definição das Categorias de Análise finais 71
4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS 77
4.1 CONDUÇÃO DA AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS 78
4.1.1 Identificar a necessidade de uma AIPD.....80
4.1.2 Requisitos de privacidade (RP) 81
4.1.3 Descrever os fluxos informacionais.....82
4.1.4 Avaliar a necessidade e proporcionalidade 84
4.1.5 Identificar ameaças à privacidade 85
4.1.6 Identificar as soluções de privacidade.....88
5 CONSIDERAÇÕES FINAIS 94
REFERÊNCIAS.....97
APÊNDICE 1 – PORTFÓLIO DE ANÁLISE 108
APÊNDICE 2 – PORTFÓLIO DE INTERESSE.....115
ANEXO 1 – FREQUÊNCIA DE PALAVRAS PARA O GRUPO DE TEXTOS DE PBD 117

1 INTRODUÇÃO

Neste capítulo serão apresentados o tema, a delimitação da pesquisa, o problema, a pergunta e a premissa da pesquisa, os objetivos gerais e específicos, as justificativas teóricas e práticas, uma visão geral sobre os procedimentos metodológicos, o marco teórico e, finalmente, a estrutura do trabalho.

1.1 TEMA

Com a mudança na dinâmica econômica global os dados pessoais tomaram posição central na vida em sociedade (DONEDA, 2011). Por vezes, os próprios dados, seu tratamento, análise e agregação, tornam-se um serviço mercantilizado. O aumento da quantidade e qualidade das bases de dados, em paralelo ao aumento da capacidade de processamento e análise destas informações representam uma ameaça crescente à privacidade dos cidadãos (QUINN, 2009).

A preocupação em torno da proteção aos dados se intensifica na atualidade em decorrência do fato de que, na utilização de praticamente todos os produtos ou serviços os usuários são compelidos a se identificarem, a se autenticarem por meio da comunicação de seus dados pessoais. Tanto nas interações *online* como em estabelecimentos físicos é notório como os dados passam a construir um perfil cada vez mais detalhado sobre as vidas das pessoas. Os sistemas que se alimentam de dados pessoais abstraem o humano de sua territorialidade física em diversos fluxos de dados e os remonta virtualmente como seus “dublês de dados” (*data double*) (HAGGERTY; ERICSON, 2000). Levando-se em conta que em diversas interações os dados pessoais substituem a pessoa, dispensam-lhe a presença, conclui-se que cada vez mais os dados pessoais são, na prática, a pessoa (DONEDA, 2011).

Recentes escândalos de vazamentos de dados, como o do *bureau* de crédito americano Equifax, que resultou na publicação de informações pessoais de 145,5 milhões de pessoas (SWEET, 2017), e da empresa brasileira Netshoes, expondo dados pessoais de mais de 2 milhões de clientes (PAYÃO, 2018), causados por ataques maliciosos, não são novidades nem casos isolados. Em paralelo aos recorrentes vazamentos de dados, casos como o da empresa Cambridge Analytica, central no escândalo de microdirecionamento de publicidade de campanha política nos Estados Unidos (GUIMÓN, 2018), demonstram como informações granulares

sobre preferências e comportamentos podem subsidiar técnicas de *profiling* (perfilamento) e prejudicar o sujeito dos dados.

Este estudo focará as análises para o contexto de medição inteligente e *Smart Grid* (Rede Elétrica Inteligente), na medida em que, para além das informações já divulgadas pelo uso de redes sociais e serviços conectados, os dados oriundos dos *Smart Meters* (medidores inteligentes) se configuram como nova fonte de informações que colocam em risco a divulgação de comportamentos dotados de alta expectativa de privacidade, configurando possibilidade de invasão da “santidade do lar” (LERNER; MULLIGAN, 2008; QUINN, 2009).

O desenvolvimento da *Smart Grid* (*SG*) especificamente, promete transformar o setor de geração e consumo de energia permitindo a conexão de múltiplas fontes renováveis e o fluxo bidirecional de informação e energia (EUROPEAN COMMISSION *et al*., 2013). Uma *SG* compreende a integração de tecnologias de energia, comunicações e informação para uma infraestrutura de energia elétrica que melhor entregue carga ao mesmo tempo em que permita uma constante evolução das aplicações de uso final (IEEE STANDARDS COMMITTEE *et al*., 2011). Por meio do desenvolvimento da *SG*, espera-se obter uma série de inovações, entre elas possibilitar que o fornecedor de energia receba informações precisas sobre o estado de suas redes e que o consumidor final possa adaptar seus hábitos de consumo de acordo com a situação de fornecimento (MÁRMOL *et al*., 2012).

As redes elétricas tradicionais transmitem energia de um gerador central a muitos usuários, enquanto a *SG* utiliza fluxos bidirecionais de energia e informação para criar uma rede avançada automatizada e distribuída de entrega de energia (FANG *et al*., 2012). Os fluxos bidirecionais de informação se dão utilizando medidores eletrônicos, *Smart Meters* (*SM*), instalados nas Unidades Consumidoras (UC). A geração de valor esperada com a rede inteligente, *Smart Grid* (*SG*), advém da disponibilidade de uma nova gama de informações geradas pelo uso dos *SM*. Enquanto um medidor eletromecânico tradicional fornece o valor de consumo acumulado, geralmente coletado mensalmente, os *SM* podem fornecer informações sobre a carga ao longo do tempo, processar os dados e enviá-los em tempo real e receber comandos e atualizações (MINAMIZAKI *et al*., 2013).

Quinn (2009) lista quatro motivações macro para o aumento em quantidade e detalhamento das informações de consumo de energia: Capacidade de resposta de demanda e balanceamento de carga; acomodação de entradas variáveis de fontes

renováveis; gerenciamento de demanda pela conscientização e pressão social do usuário e mudança nas estruturas de tarifação.

Segurança e privacidade serão fatores essenciais ao desenvolvimento e aceitação pública dos medidores eletrônicos *(SM)* (EFTHYMIOU; KALOGRIDIS, 2010; MINAMIZAKI *et al*., 2013). A principal preocupação quanto aos riscos de privacidade, relacionada ao uso dos *SM*, decorre do fato de que, na medição detalhada de uso realizada em curtos intervalos de tempo, é possível a inferência sobre diversos aspectos da Unidade Consumidora (UC). Esta medição detalhada possibilita inferências sobre a ocupação da UC, quais eletrodomésticos são utilizados, quais hábitos os moradores possuem e até qual peça de audiovisual está sendo assistida, nesse caso, quando a medição do conteúdo para comparação tenha sido realizada previamente (CARLUCCIO; BRINKHAUS, 2011; LAM; FUNG, 2007; McKENNA; RICHARDSON; THOMSON, 2012; PARSON *et al*., 2012; WYNN, 2010). Quanto maior a disponibilidade de informações granulares, maior a capacidade de geração de conhecimento e aplicações inovadoras, contudo, aumenta também o risco de invasão à privacidade (McKENNA; RICHARDSON; THOMSON, 2012).

Um dos desafios para a obtenção das vantagens esperadas com a *SG* é como gerenciar eficientemente tantos dispositivos integrados e processar uma grande quantidade de dados que passarão a ser disponibilizados pelas tecnologias do sistema. O uso de computação em nuvem (*cloud computing*) é uma alternativa apontada para solucionar tal desafio (BIRMAN; GANESH; RENESSE, 2011; RUSITSCHKA; EGER; GERDES, 2010). Vantagens típicas da computação em nuvem são a flexibilidade, escalabilidade, agilidade, eficiência energética e diminuição de custos (HAYES, 2008). O uso de computação em nuvem permite o gerenciamento de grandes quantidades de informação e economiza-se energia por permitir *frameworks* (estruturas de trabalho) escaláveis rapidamente e propiciar intensa utilização de recursos computacionais (BAEK *et al*., 2015).

Os usuários de computação em nuvem possuem a expectativa de confidencialidade dos dados utilizados, contudo, a configuração de nuvem que se apresenta visa apenas proteger o acesso de execução não-privilegiada (usuário) à área privilegiada (provedor), sem medidas que evitem o acesso de informações do usuário pelo provedor (BAUMANN; PEINADO; HUNT, 2015).

Birman, Ganesh e Renesse (2011) e Rusitschka, Eger e Gerdes (2010) demonstram a aplicabilidade e interconexão entre necessidades de *SG* e uso de

computação em nuvem. Aplicações de *Smart Grid* podem se beneficiar destas soluções desde que a segurança e privacidade obtidas atendam aos requerimentos da aplicação (RIELLA *et al*., 2018). Por exemplo, é preciso considerar que o provedor do serviço tem acesso aos dados armazenados em nuvem, sendo a privacidade garantida por confiança implícita ou contratual, não assegurada por meios técnicos controlados pelo contratante.

A coexistência das informações dos *SM* com bancos de dados de redes sociais ou serviços *online* de maneira pública (intencional ou por vazamentos) permitiria cruzamentos entre aspectos da vida *online* e *off-line* de maneiras não consentidas e prejudiciais (MANTELERO, 2016). Além dos aspectos prejudiciais aos cidadãos, casos de falha na proteção à privacidade afetam a confiança pública sobre a empresa e podem se configurar em perdas financeiras pela perda de consumidores (INSTITUTO PONEMON, 2017). Preocupações sobre a possibilidade de invasão à privacidade decorrente das informações disponibilizadas pelos *Smart Meters* impediram sua distribuição como inicialmente planejado na Holanda e forçaram as autoridades a revisitarem seu planejamento levando em conta as demandas dos consumidores (HOENKAMP; HUITEMA; DE MOOR-VAN VUGT, 2011).

Recentemente foi aprovada a Lei nº 13.709 de 14 de agosto 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) que cria determinações e salvaguardas ao uso de dados pessoais no país, com aplicabilidade deferida para 24 meses após sua aprovação. A lei é um avanço e uma conquista após anos de organização e esforços conjuntos entre sociedade civil, ONGs, empresas e entidades especializadas (IDEC, 2018). No momento da sanção foram vetados os artigos que tratavam da criação da Autoridade Nacional de Proteção de Dados (ANPD), sob a justificativa de vício de iniciativa. No final de 2018 foi apresentada Medida Provisória nº 869 pelo governo para a criação da ANPD, o que finalmente ocorreu com a aprovação da Lei nº 13.853/2019 que, além de criar a ANPD altera dispositivos na LGPD (BRASIL, 2019).

A General Data Protection Regulation (GDPR), Lei de proteção de dados da Europa, e a LGPD adotam concepção expansionista sobre dados pessoais, conceituando-os como aqueles relativos à pessoa “identificada ou identificável” (BRASIL, 2018; EUR-LEX, 2018). A definição considera o panorama no qual os dados não precisam estar vinculados diretamente a uma pessoa específica para que o sujeito de dados receba os efeitos do tratamento, como ocorreria com uma definição reducionista de dados pessoais (BIONI, 2015). Mesmo com o avanço em pesquisas

sobre anonimização de bases de dados, discute-se a ineficácia da proteção oferecida pela de-identificação dos dados (remoção de propriedades que identificariam o dado ou o relacionariam a um sujeito) como solução completa (NARAYANAN; SHMATIKOV, 2010).

Para que as vantagens esperadas com a implantação da *Smart Grid* sejam concretizadas, é preciso que dados granulares de consumo possam ser utilizados pelo fornecedor de energia sem a invasão da privacidade da UC. É possível implementar a privacidade diretamente à *Smart Grid* fazendo com que ela seja o padrão no aspecto físico, administrativo e tecnológico do sistema (CAVOUKIAN; POLONETSKY; WOLF, 2010). Privacidade é bom para os negócios (MCQUAY; CAVOUKIAN, 2010) e a preocupação com a proteção da privacidade desde a concepção do projeto permite que potenciais riscos sejam identificados preventivamente, evitando o surgimento do dano e aumentando a eficiência nas soluções (WRIGHT, 2012). Uma AIPD é um processo reprodutível com o objetivo de identificar riscos à privacidade e maneiras de superá-los e pode ajudar a organização a ganhar a confiança do público de que a privacidade foi considerada na concepção do projeto ou serviço (WRIGHT, 2013).

Contudo, o processo de AIPD não pode ser executado como um mero *checklist* (LINE, 2014). O Office of the Victorian Information Commissioner (OVIC), regulador independente de acesso à informação, privacidade e proteção de dados de Vitória, Australia, publicou relatório analisando caso recente em que uma Avaliação de Impacto à Privacidade (AIP) malconduzida autorizou a liberação de um conjunto de dados para análise que foi facilmente reidentificado. O incidente ocorreu no contexto de uma maratona de investigação de usos inovadores de dados, promovida pela Data Science Melbourne, utilizando um conjunto de dados fornecido pela agência de transporte público Public Transport Victoria (PTV) (OVIC, 2019).

A PTV forneceu o conjunto de dados real, de mais de 15 milhões de usuários ao longo de três anos, de alta granularidade (especificidade de 1 segundo), contendo informações de entrada e saída, localização, informação do veículo (rota, número de paradas) e um identificador único, substituindo o número de identificação do usuário no cartão (OLEJNIK, 2019). A AIP conduzida aprovou a substituição dos identificadores do cartão dos usuários por outros identificadores únicos como forma de de-identificar os dados, contudo, pesquisadores demonstraram ser possível re-identificar indivíduos nos dados considerados anonimizados (ANNAN BOAG, 2019).

Em trabalho que levanta preocupações sobre a natureza e granularidade do conjunto de dados liberado, Culnane, Rubinstein e Teague (2019) demonstram a facilidade com que identificaram a si, companheiros de viagem e completos estranhos no conjunto de dados. O relatório da investigação conduzida pela OVIC indica que de-identificar conjuntos de dados grandes e complexos é difícil, podendo ser impossível em alguns casos; que as organizações não deveriam depender apenas de de-identificação para proteger os dados; que para definir se informação de-identificada é pessoal, contexto é essencial; que definição de responsabilidades entre os atores é necessária para governança de dados efetiva e que AIPs, se feitas de maneira incorreta, podem passar uma falsa noção de segurança (ANNAN BOAG, 2019).

1.2 DELIMITAÇÃO DA PESQUISA

O termo *Smart Grid (SG)* comporta diversas definições, contudo, todas incluem a adição e integração de variadas tecnologias e serviços à infraestrutura de energia (NIST, 2014b, p. 25). Há S*mart Meters* (*SM*) com funções de medição de consumo detalhado de água e gás, contudo, a menos que explicitado de outra forma, os *SM* e a *SG* aqui referidos serão considerados apenas no âmbito de energia elétrica.

Este estudo aborda a *SG* utilizando nuvem pública para operar e conduz avaliação sistemática para identificar ameaças à proteção de dados e suas correspondentes soluções. Nuvens privadas, restritas a uma rede privada, podem ter mais garantias de segurança, mas os custos associados ao modelo são altos (PEARSON; BENAMEUR, 2011), o que direciona a análise para o contexto de nuvem pública.

Uma forma de minimizar os riscos à privacidade decorrentes da intensificação do uso de dados de energia é por meio da implementação do conceito de *Privacy by Design* (*PbD*), que pode ser considerada a abordagem de integrar a privacidade nas especificações de concepção de variadas tecnologias, fazendo com que ela seja o padrão do começo ao fim do sistema (CAVOUKIAN, 2010a). As principais críticas que se apresentam ao conceito de *Privacy by Design* relacionam-se às dificuldades de transformação de preocupações éticas, sociais e legais em especificações técnicas e requisitos de sistema (GURSES; TRONCOSO; DIAZ, 2015; RUBINSTEIN; GOOD,

2012) e falta de incentivos econômicos e dificuldade de implantação em sistemas legados (VAN LIESHOUT *et al*., 2011).

Justifica-se a adoção do conceito de *PbD* como norteador das recomendações deste estudo pela sua capacidade de acomodar as demandas por inovação e geração de valor mantendo o respeito à privacidade, além de sua requisição explícita na GDPR e implícita na LGPD. Por meio de sua operacionalização é possível que a privacidade se dê ao lado de outros requisitos críticos como (CAVOUKIAN, 2010b): funcionalidade, controle organizacional e processos de negócios em uma lógica de soma positiva (*win-win*).

Uma outra maneira de se implementar privacidade em sistemas é por meio das *Privacy Enhancing Technologies* (*PETs*), tecnologias que protegem a privacidade por minimizar ou eliminar a coleta de informação identificável (HES; BORKING, 1998). A preferência neste estudo pelo foco em *PbD* e não em *PETs* se justifica pelo fato de que o primeiro prevê a implantação da privacidade "diretamente no *design* e operação, não apenas da tecnologia, mas também de sistemas de operação, processos de trabalho, estruturas de gerenciamento, espaços físicos e infraestrutura conectada" (CAVOUKIAN, 2010b, p. 248, tradução nossa).

Proteção de dados passa a ser um requisito legal e um processo sistemático para avaliação de riscos poderá ser requisitado por Autoridade competente ou na própria legislação. O processo de AIPD é requisito na GDPR (EUR-LEX, 2018) e pode ser requisitado pela ANPD no Brasil (BRASIL, 2018). Para se obter as recomendações com foco em *PbD* optou-se por conduzir processo de AIPD apoiado por metodologia de modelagem de ameaças para aumentar sua especificidade e relação com o contexto analisado.

O processo de modelagem de ameaças é tipicamente empregado para o desenvolvimento seguro de *software* (SCANDARIATO; WUYTS; JOOSEN, 2015) e a metodologia apresentada para modelagem de ameaças de privacidade em ambiente de nuvem foi eleita para contribuir com as especificações de privacidade no contexto estudado (GHOLAMI *et al*., 2016). O processo está detalhado no item 3.2 ADVANCED CLOUD PRIVACY THREAT MODELING e, nesta dissertação, considera os princípios contidos na LGPD para levantar requisitos de privacidade no estágio inicial do projeto. Os requisitos definidos norteiam a fase de desenvolvimento do projeto para modelar ameaças aos requisitos e contramedidas para eliminar ou minimizar tais ameaças.

A opção pela concentração na legislação brasileira deve-se ao momento oportuno em que a Lei está sob *vacatio legis* e carece de interpretação e operacionalização para sua aplicação prática.

Este estudo se dá no âmbito de uma investigação maior conduzida por um consórcio internacional para a execução do projeto SecureCloud (SECURECLOUD, 2017). O projeto busca o desenvolvimento de tecnologias de processamento seguro de grandes volumes de dados em nuvens não confiáveis no qual a segurança é delegada a mecanismos de hardware, em específico à Secure Guard eXtensions (SGX) da Intel, o que permite a execução protegida de dados criptografados em que o dado descriptografado reside apenas na área de memória protegida do processador (*Trusted Execution Environment*) (KELBERT *et al*., 2017; SECURECLOUD, 2017). Os outros produtos de pesquisa do projeto SecureCloud são principalmente voltados ao desenvolvimento das aplicações e sua melhoria tecnológica. A privacidade é obtida pela conjugação de técnicas e processos (NIST, 2014a) motivo pelo qual esta investigação contribui para o caráter multidisciplinar do projeto SecureCloud. Os casos de uso propostos para a demonstração da arquitetura SecureCloud são de *Smart Grids*.

1.3 PROBLEMA, PERGUNTA E PREMISSA DA PESQUISA

A *SG* carrega a promessa de diversas vantagens que motivam sua implantação e a busca por estas vantagens pode relativizar a proteção de dados como uma preocupação acessória. Dados de *SM* carregam potencial econômico e mecanismos de controle e consentimento não impedem seu mau uso (JAWUREK, 2013). Requisitos de privacidade não são facilmente incorporados a requisitos de engenharia do sistema (GURSES; TRONCOSO; DIAZ, 2015; WALDMAN, 2018). Mesmo quando haja intenção de proteção de dados, o tópico é complexo propenso a técnicas que tragam a falsa sensação de proteção. Uma vez implementado ignorando estes aspectos, o sistema dificilmente pode ser protegido de maneira eficaz. Ignorar preocupações de privacidade pode levar a medidas de adaptação de privacidade custosas e potencialmente ineficazes (TANCOCK; PEARSON; CHARLESWORTH, 2013), multas por descumprimento de legislação e atrasar a implantação do sistema (CUIJPERS; KOOPS, 2013; HOENKAMP; HUITEMA; DE MOOR-VAN VUGT, 2011).

A implementação direta da *SG*, sem a consideração de preocupações de privacidade pode levar invasões sem precedentes à privacidade do consumidor (CAVOUKIAN; POLONETSKY; WOLF, 2010) configurando-se como um aparato de vigilância. A vigilância passa a ser corriqueira e contra todos, ainda que com caráter dual, em algumas circunstâncias aumentando a eficiência, produtividade, conveniência e conforto. A associação da vigilância com a diminuição dos riscos (ex: câmeras de vigilância aumentariam a segurança) tende a esconder as maneiras como o aumento da vigilância pode contribuir para o aumento dos riscos, renovados sobre os mais vulneráveis e já vítimas de vigilância (LYON, 2005).

A ANPD tem a capacidade de uniformizar e recomendar práticas, fiscalizar abusos e diminuir a assimetria informacional entre os sujeitos de dados e as entidades que os utilizam, diminuindo as chances de resolução de conflitos pela longa e custosa via judicial (DONEDA, 2018). Ao longo da LGPD (Art. 3º, IV, § 3º; Art. 10, II, § 3º; Art. 32; Art. 38) é delegada à ANPD a responsabilidade por requerer, recomendar e avaliar relatórios de impacto à proteção de dados pessoais (RIPD), resultados do processo de Avaliação do Impacto à Proteção de Dados Pessoais (AIPD), um dos temas deste estudo. Até que a ANPD comece a produzir material de apoio sobre a aplicação da LGPD, o país segue sem recomendações governamentais sobre este processo.

Não há no ordenamento jurídico nacional instrumentos que estabeleçam políticas públicas para o desenvolvimento de *SG*, não há também *framework* sobre a temática, dificultando a definição de conceitos, e inexistem medidas educativas que expliquem as possíveis vantagens do sistema. Este cenário de desregulação e ausência de incentivos dificulta o avanço do desenvolvimento do sistema e limita a capacidade de planejamento dos fornecedores em dimensionar os investimentos necessários para a implantação da *SG* (CARVALHO, 2015; GUIMARÃES, 2017; MOREIRA, 2015). Por outro lado, permite experiências auto regulatórias e adoção voluntária de boas-práticas. O processo de AIPD pode auxiliar, tanto na obtenção de *compliance* com regulação existente e observância de princípios gerais de privacidade, como os contidos na GDPR e LGPD, quanto na demonstração de auto regulação por expor as medidas adotadas para prevenção de danos (WRIGHT, 2012).

A Resolução Normativa nº 502, de 7 de agosto de 2012 da Aneel, que regulamenta sistemas de medição de energia elétrica de Unidades Consumidoras do Grupo B, estabelece que “a distribuidora deve adotar procedimentos e tecnologias que assegurem a segurança dos dados trafegados e, especialmente, das informações de

caráter pessoal coletadas das unidades consumidoras” (ANEEL, 2012) sem, contudo, especificar quais procedimentos ou tecnologias seriam estes.

Neste contexto, os resultados desta pesquisa podem contribuir para tomada de decisão de atores envolvidos em projetos de implementação de *Smart Grid* no cenário brasileiro.

Portanto, este estudo busca responder à seguinte pergunta de pesquisa:

Quais medidas de proteção de dados pessoais precisariam ser consideradas no planejamento e operação de *Smart Grid* utilizando computação em nuvem?

A premissa da pesquisa é que o processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD), ou *Data Protection Impact Assessment* (*DPIA*), é capaz de operacionalizar o conceito de *PbD* para *Smart Grids* e congregar técnicas e processos para a preservação da privacidade em consonância com a Lei Geral de Proteção de Dados Pessoais (LGPD).

1.4 OBJETIVOS

Nesta seção serão apresentados os objetivos geral e específicos da pesquisa, que representam as soluções às perguntas principal e secundárias desta pesquisa

1.4.1 Objetivo geral

Propor um conjunto de medidas de proteção de dados pessoais que precisariam ser consideradas no planejamento e operação de *Smart Grid* utilizando computação em nuvem.

1.4.2 Objetivos específicos

a) Caracterizar o processo de Avaliação de Impacto à Proteção de Dados Pessoais;
b) Mapear aspectos relevantes do conjunto de princípios de *Privacy by Design;*
c) Caracterizar o uso de *cloud* segura com privacidade em *Smart Grid.*

1.5 JUSTIFICATIVA

Nesta seção é apresentada a justificativa da pesquisa.

A implantação dos SM em diversos países se mostrou complicada e consumidores e jornalistas levantaram questionamentos sobre as possíveis invasões à privacidade e falta de transparência sobre os serviços oferecidos (JAMIESON, 2009; MINAMIZAKI *et al*., 2013; WYNN, 2010).

Tanto no âmbito nacional quanto internacional, é notável a crescente preocupação com a proteção da privacidade. Em maio de 2018 entrou em vigor na União Europeia a Lei Geral de Proteção de Dados, (GDPR - *General Data Protection Regulation*) (EUR-LEX, 2018). Recentemente foi aprovada a Lei nº 13.709 de 2018, Lei Geral de Proteção de Dados Pessoais (LGPD) que cria determinações e salvaguardas ao uso de dados pessoais no país. Ambas trazem disposições sobre a proteção de privacidade e preveem a realização de processo sistemático para a avaliação de riscos à privacidade. A LGPD define o relatório de impacto à proteção de dados pessoais (RIPD) como: “documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco” (BRASIL, 2018).

Não consta na Lei previsão de obrigatoriedade de apresentação do referido relatório, ficando a cargo da autoridade competente, a Autoridade Nacional de Proteção de Dados (ANPD), sua requisição para cada caso específico. A Lei também não dispõe de detalhes ou procedimentos para a preparação de tal relatório, incluindo entre as atribuições da ANPD a edição de regulamentos e procedimentos sobre este. Parte dos resultados desta pesquisa, bem como as considerações do Article29 Working Party (WP29, 2017), órgão implementado para fornecer guias à regulação europeia antes de sua entrada em vigor, apontam para a necessidade de condução de processo sistemático para endereçar os riscos à privacidade decorrentes da implantação da Rede Elétrica Inteligente.

Ainda que o processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD), ao final do qual se obtém um relatório de impacto à proteção de dados pessoais, seja estudado e documentado internacionalmente, a literatura nacional ainda não se debruçou sobre o tema, conforme se demonstra na seção 3.3.1 –

LEVANTAMENTO BIBLIOGRÁFICO PRELIMINAR. O levantamento preliminar também aponta a ausência de estudos que conjuguem o processo com recomendações para *SG* utilizando computação em nuvem.

A delimitação ao escopo de medição inteligente se justifica pelos casos de uso escolhidos no âmbito do projeto SecureCloud. Contudo, espera-se que a metodologia estabelecida para este caso possa ser generalizada para o desenvolvimento de demais aplicações, como para o planejamento de privacidade em *Smart Cities* (SETO, 2015). A documentação da metodologia aplicada na pesquisa objetiva permitir a reprodutibilidade do estudo e trabalhos futuros poderão investigar a aplicabilidade dos processos a outros objetos de estudo.

A pesquisa está alinhada aos objetivos do Programa de Pós-Graduação em Planejamento e Governança Pública (PGP), especificamente à linha de Planejamento e Políticas Públicas e ao projeto de pesquisa estruturante “Políticas Públicas em Perspectiva: análises e processos” no sentido de que busca definições para a implementação de um processo a ser realizado na modernização da eletrificação do território urbano. Será discutida a ausência de políticas públicas que permitam o planejamento destas iniciativas e a restrição do tratamento legal à eletrificação, podendo representar dificuldade para a interoperabilidade com outras iniciativas de potencial transformador, como as de *Smart Cities*. Tais características serão analisadas de forma multidimensional e levarão em conta os atores e instituições envolvidas.

A modernização esperada pelas *Smart Cities*, assim como a esperada pela *Smart Grid* depende da intensificação na coleta de dados e capacidade de processamento para extração de valor. Os dados obtidos quando o cidadão interage com o território podem ter caráter pessoal e devem ser alvos de proteção. As Tecnologias da Informação e Comunicação vêm servindo para a intensificação da vigilância e controle dos espaços urbanos, tanto por agentes públicos quanto privados (FIRMINO, 2017). O desenvolvimento de Políticas Públicas no contexto da sociedade da informação e da crescente informatização dos serviços governamentais necessita de estratégias para a proteção de dados. A discussão sobre o conceito de *Privacy by Design* informará a condução deste trabalho e pode subsidiar outras iniciativas que pretendam considerar a privacidade no planejamento urbano.

A localização da pesquisa na Universidade Tecnológica Federal do Paraná (UTFPR), sediada em Curitiba é oportuna em vista dos projetos iniciais de implantação

de *Smart Grid* realizados na cidade em parceria com a COPEL (LACTEC, 2015) e o Projeto Smart Energy Paraná, criado pelo decreto nº 8842, de 04 de setembro de 2013 (PARANÁ, 2013). Para que os avanços esperados com as novas tecnologias possam se dar plenamente, as capacidades de planejamento de privacidade e segurança da informação serão essenciais aos tomadores de decisão. No campo prático ainda, a pesquisa contribui para a área de formação e áreas de interesse do pesquisador, conjugando Direito e tecnologia.

O processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD), que norteia o desenvolvimento da pesquisa, é de caráter eminentemente prático e a produção de conhecimento sobre este contribui com a produção de material sobre a LGPD ainda em seu período de *vacatio legis*, além de divulgar seu uso como instrumento possível no gerenciamento de privacidade e promoção dos conceitos de *Privacy by Design.*

1.6 PROCEDIMENTOS METODOLÓGICOS

Levando-se em conta os critérios de classificação de pesquisas apresentados por Gil (2010), considera-se que quanto aos seus objetivos este trabalho é descritivo por buscar a definição do processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD), por meio do levantamento bibliográfico sobre o tema. A pesquisa busca relacionar o processo de AIPD ao gerenciamento de privacidade em *Smart Grids* (*SG*) e avançar na concepção de planejamento de privacidade, assim, podemos classificá-la também como uma pesquisa de caráter exploratório.

Trata-se de pesquisa aplicada por buscar novos conhecimentos sobre o tema estudado e dirigir-se a um objetivo prático (OECD, 2007). O delineamento metodológico foi realizado por pesquisa bibliográfica e documental utilizando-se do que foi produzido pela academia e do levantamento da legislação aplicável e de guias e *frameworks* para a proteção da privacidade.

Foram adotadas contribuições de Ensslin, Ensslin e Pinto (2013) em sua proposta de pesquisa bibliométrica e de Conforto (*et al.* 2011), por meio de Revisão Bibliográfica Sistemática (RBS) para o levantamento de conceitos, ameaças e métodos de gerenciamento de privacidade no contexto de *Smart Grid*.

Quanto à abordagem do problema, a pesquisa é qualitativa na análise do corpus bibliográfico obtido com a RBS e pode se dar pela sequência de atividades

iniciadas pela redução e categorização dos dados, interpretação e redação de relatório (GIL, 2010). O *corpus* bibliográfico obtido foi analisado por meio de Análise de Conteúdo segundo método proposto por Bardin (2011).

Ao final, foi realizada uma Avaliação de Impacto à Proteção de Dados Pessoais para *Smart Grid* utilizando computação em nuvem, subsidiada por modelagem de ameaças de privacidade, valendo-se do conhecimento levantado pela Análise de Conteúdo para recomendar boas práticas, que foram verificadas contra os princípios de *Privacy by Design*.

1.7 EMBASAMENTO TEÓRICO

Esta pesquisa utilizará *corpus* documental, materiais considerados de base para o estudo e *corpus* dinâmico obtido pelo levantamento bibliográfico realizado utilizando bibliometria conforme apresentado no Capítulo 3 – Metodologia da Pesquisa.

Nas discussões sobre privacidade, proteção de dados pessoais e privacidade por desenho serão consideradas as contribuições de Bioni (2018); Boillat e Morten (2014), Cavoukian (2010) e Doneda (2011). São considerados essenciais ao estudo do processo de Avaliação do Impacto à Privacidade os trabalhos de Clarke (2009), Flaherty (2015), Stewart (1996; 2002) e Wright (2012).

As discussões sobre *Smart Grid* utilizam contribuições de Amin e Wollenberg (2005), Fang (*et al*,. 2012), Farhangi (2010), Carvalho (2015), Mármol *et al*.(2012), McDaniel e McLaughlin (2009), McKenna, Richardson e Thomson (2012), Minamizaki *et al*. (2013) e Quinn (2009).

Os documentos utilizados foram legislações sobre privacidade e guias e *frameworks* publicados por entidades internacionais como procedimento para a realização de Avaliação de Impacto à Proteção de Dados Pessoais, implementação de Privacidade por Desenho e Interoperabilidade de *Smart Grids*, como: ANEEL (2012), Brasil (2018), CNIL (2015), EUR-LEX (2018), ICO (2009; 2014; 2018), IEEE STANDARDS COMMITTEE *et al*. (2011), NIST (2014a; 2014b) e WP29 (2017). Os materiais compreendem o *corpus* estático da pesquisa e serão utilizados em conjunto com o *corpus* dinâmico obtido pela pesquisa bibliométrica.

1.8 ESTRUTURA DA DISSERTAÇÃO

Além deste capítulo introdutório (1), o Capítulo 2 apresenta a fundamentação teórica sobre Privacidade e proteção de dados pessoais, *Privacy by Design*, *Smart Grid*, Avaliação de Impacto à Proteção de Dados Pessoais (AIPD) e *cloud computing*. No terceiro capítulo é apresentada a metodologia empregada para a condução do estudo, primeiramente descrevendo os processos de AIPD e de *Advanced Cloud Privacy Threat Modeling*, posteriormente descrevendo o levantamento bibliográfico com base em levantamento bibliométrico para culminar na Análise de Conteúdo sobre a bibliografia levantada. O quarto capítulo traz os resultados da dissertação e contém os passos empreendidos no processo de AIPD em conjunto com a metodologia de modelagem de ameaças. No quinto capítulo são apresentadas as considerações finais bem como as sugestões para trabalhos futuros.

2 FUNDAMENTAÇÃO TEÓRICA

Nesta seção serão apresentadas as fundamentações teóricas sobre os temas relativos à privacidade e proteção de dados pessoais, *Privacy by Design, Smart Grid*, ao processo de Avaliação de Impacto à Privacidade e à computação em nuvem.

2.1 PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Preocupações de privacidade relacionadas a novas tecnologias têm motivado avanços legislativos e reações que buscam restringir o acesso ao conhecimento da vida privada pelo público. O trabalho considerado seminal no estabelecimento do direito à privacidade surge nos Estados Unidos como reação à invasão trazida pelo advento da fotografia instantânea, que anteriormente requeria o consentimento do sujeito fotografado pelo tempo que deveria permanecer posando (BRANDEIS; WARREN, 1890). A publicação do artigo *"The Right to Privacy"* no periódico *"Harvard Law Review"*, no ano de 1890, pelos autores Louis D. Brandeis e Samuel D. Warren atenta para o fato de que a aplicação apenas das leis existentes não garantiria ao sujeito o "direito de ser deixado em paz" e que a privacidade não teria natureza contratual, mas sim de direito da personalidade, oponível contra todos (BRANDEIS; WARREN, 1890).

A Constituição Federal em seu Art. 5º, inciso X indica que "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" (BRASIL, 1988), bem como o Código Civil em seu art. 21 assinala "A vida privada da pessoa natural é inviolável, e o juiz, a requerimento do interessado, adotará as providências necessárias para impedir ou fazer cessar ato contrário a esta norma" (BRASIL, 2002). Bastos (2000, p.45) argumenta que o direito à privacidade é:

> [...] a faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano.

Ainda, pode-se definir o direito à privacidade como “direito do indivíduo de estar só e a possibilidade que deve ter toda pessoa de excluir do conhecimento de terceiros aquilo a que a ela só se refere, e que diz respeito ao seu modo de ser no âmbito da vida privada” (LAFER, 1991, p. 20). As concepções de privacidade, portanto, concentram-se na distinção entre o que é público e o que é privado, aquilo que se deseja restringir, controlar, selecionar o acesso. Ao mesmo tempo, conceituar privacidade é uma tarefa árdua uma vez que as definições podem ser consideradas amplas demais ou limitadoras demais (SOLOVE, 2002).

Bioni (2018), em extensa obra sobre a proteção de dados pessoais e os limites do consentimento, apresenta discussão teórica que relaciona o direito à privacidade, essencial à democracia por permitir o livre desenvolvimento da personalidade, com o direito à proteção de dados, uma proteção dinâmica (mais abrangente que a marcada diferenciação entre privado e público no direito à privacidade) e ativa. O direito à proteção de dados se opera sobre os dados pessoais, que podem ser informação pública ou privada, e nos efeitos que pode sofrer o sujeito de dados em decorrência de seu tratamento (BIONI, 2018).

Este sentido pode ser depreendido também no objetivo apresentado no primeiro artigo da Lei Geral de Proteção de Dados Pessoais que indica (BRASIL, 2018):

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Ou seja, a proteção de dados figura como acessório ao direito à privacidade. O objetivo das atitudes tomadas para proteção de dados não se resume aos dados, mas à finalidade maior de permitir o livre desenvolvimento da personalidade. Bioni (2018) considera o direito à proteção de dados como uma categoria autônoma dos direitos da personalidade, visando ao controle das informações pessoais sem a necessidade de distinção entre público e privado.

Cumpre ressaltar que “Privacidade” é considerada por alguns autores como um conceito fundado em suposições liberais sobre a subjetividade e direitos humanos, insuficiente para lidar com os aspectos discriminatórios de uma sociedade de vigilância e focada em danos individuais (BENNET, 2011). Bennett e Parsons (2013)

argumentam que o conceito de privacidade não é capaz de transmitir os danos sociais e institucionais amplos decorrentes da constante observação e categorização de nossas atitudes e preferências. O conceito de vigilância adotado nesta dissertação não implica a noção de um “inimigo” acompanhando as ações de uma “vítima”, mas, de acordo com Lyon (2001), trata-se do monitoramento da vida diária, em que não há a necessidade de ser um “suspeito” para ser sujeito à vigilância. Não está claro que mais privacidade é solução para os efeitos da vigilância ainda que princípios de privacidade possam diminuir as desigualdades geradas pela vigilância e classificação social (LYON, 2005).

Medidas de segurança para a proteção de dados buscam evitar danos decorrentes do acesso não autorizado ao sistema, contudo, danos podem emergir do tratamento autorizado da informação pessoal (BROOKS *et al*., 2017). Não foi a impressão que as entidades envolvidas não conseguiriam garantir a segurança dos dados que impediu a implantação inicial da *SG* na Holanda, mas sim o temor de que a rede acabaria se configurando como mais um aparato de vigilância (CUIJPERS; KOOPS, 2013; HOENKAMP; HUITEMA; DE MOOR-VAN VUGT, 2011)

O objeto da proteção de dados, o dado pessoal, é conceituado na LGPD como “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018) tendo como antítese o dado anonimizado, conceituado como “dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (BRASIL, 2018). Essa definição leva em conta o fato de que o tratamento sobre os dados gera efeitos mesmo quando o sujeito não esteja diretamente identificado.

As recomendações apresentadas como resultado deste trabalho levarão em conta os princípios de proteção de dados contidos na LGPD, o fato de que a anonimização é uma medida frágil e pouco efetiva para a proteção de dados e que o sistema tem o potencial de se tornar uma ferramenta de vigilância. De maneira geral, portanto, as medidas de proteção de dados propostas buscarão privilegiar alternativas que evitem a coleta e o acúmulo de dados e que limitem e restrinjam seu uso e acesso ao mínimo necessário.

2.2 *PRIVACY BY DESIGN - PBD*

O modelo conceitual de *Privacy by Design* (*PbD*) é desenvolvido por Cavoukian (2010a) em 7 princípios fundacionais que indicam, sinteticamente, que a privacidade deve ser considerada na concepção do projeto, sem diminuir-lhe a funcionalidade, proativamente e não reativamente, fornecendo transparência e por padrão. O conceito foi apresentado nos anos 90 pela então Comissária de Privacidade de Ontario, no Canadá após trabalho conjunto realizado pelo Information and Privacy Commissioner of Ontario (IPC) e pela autoridade de proteção de dados holandesa Registratiekamer (RGK) sobre tecnologias de privacidade (HES; BORKING, 1998). A seguir serão elencados os 7 princípios de *PbD* (CAVOUKIAN, 2010a):

1) Proativa, não reativa; Preventiva, não remedial

A ideia de *Privacy by Design* é a tomada ações para evitar a ocorrência do dano, e não em resposta a este. A abordagem antecipa e previne eventos invasivos à privacidade, sem esperar que seus riscos se materializem. Segundo a autora, isso requer um comprometimento dos altos níveis da organização com a definição e execução de altos padrões de privacidade, que possam ser demonstrados aos *stakeholders* para contínua melhora, além do estabelecimento de métodos para o reconhecimento de concepções fracas de privacidade, antecipação de resultados e correção de impactos negativos de maneira proativa, sistemática e inovadora;

2) Privacidade por padrão

A abordagem de *PbD* busca entregar o máximo de privacidade garantindo que informação pessoal seja protegida automaticamente, por padrão, sem a necessidade de interação ou ação por parte do sujeito de dados. Caso o indivíduo não aja, sua privacidade permanece intacta.

3) Privacidade embutida no *design*

A privacidade é embutida na concepção do sistema ou da tecnologia, como parte integral e não como acessório adicionado posteriormente. Deve ser integrada

de maneira holística, considerando contextos amplos de usos e consequências, integrativa, consultando os interessados e criativa, quando as escolhas disponíveis sejam consideradas inaceitáveis.

4) Funcionalidade completa – Soma positiva (*win-win*)

O conceito de *PbD* pretende acomodar todos os interesses legítimos da organização, evitando falsas dicotomias, como privacidade *vs*. segurança. A privacidade, portanto, não competiria com outros interesses do negócio, mas se realizaria integralmente com estes.

5) Proteção de ponta a ponta (*end-to-end*)

Com a *PbD* sendo implantada antes do início do uso do sistema, a informação pessoal estará protegida desde sua inserção, em sua retenção e uso até sua eventual destruição por rigorosos padrões de segurança. Os padrões devem garantir a confidencialidade, integridade e disponibilidade dos dados pessoais por todo o seu ciclo, incluindo garantia de destruição segura, criptografia apropriada e rigorosos métodos de registro (*logging*) e controle de acesso.

6) Visibilidade e Transparência

Estes princípios buscam garantir que o sistema ou tecnologia envolvida de fato está operando de acordo com os propósitos declarados, sujeito à verificação independente. Os princípios são integrais ao estabelecimento de responsabilização e confiança, além da utilidade na demonstração de *compliance*.

7) Respeito à privacidade do usuário

Os melhores resultados são obtidos quando o sistema é conscientemente concebido com foco nas necessidades dos usuários, com fortes padrões de privacidade, comunicação apropriada e permitindo aos sujeitos de dados exercerem um papel ativo na administração de suas informações.

A legislação de proteção de dados tem reconhecido e requerido *PbD*. O artigo 25 da GDPR pede por proteção de dados por padrão e *by design* (EUR-LEX, 2018) e a LGPD indica que as atividades de tratamento de dados pessoais deverão observar, entre outros, o princípio da prevenção, com adoção de medidas para evitar a ocorrência de danos (BRASIL, 2018). A despeito de sua crescente adoção como conceito legal, seus princípios permanecem vagos (GURSES; TRONCOSO; DIAZ, 2015), e sua aplicação prática não é clara (WALDMAN, 2018).

Projetar sistemas focados em privacidade requer integrar requisitos de privacidade às atividades típicas de engenharia de sistemas, essencialmente identificando e analisando requisitos funcionais e de privacidade; desenvolvendo e implementando *designs* que cumpram tais requisitos e testando que na implementação estes foram atendidos (GURSES; TRONCOSO; DIAZ, 2015). Como os requisitos de privacidade dependem de mecanismos de segurança para garantir a confidencialidade, integridade e disponibilidade, atividades de engenharia de segurança, como análise de ameaças e riscos, devem acompanhar o processo (GURSES; TRONCOSO; DIAZ, 2015).

Considerando essas ponderações, as sugestões apresentadas nesta dissertação se deram após condução de processo sistemático para avaliação de impacto à proteção de dados em conjunto com modelagem de ameaças. O processo de modelagem de ameaças é tipicamente utilizado em engenharia de segurança, contudo, no presente estudo utilizou-se metodologia adaptada pelos autores especificamente para endereçar preocupações de privacidade em sistemas que operassem com computação em nuvem (GHOLAMI *et al*., 2016) que está detalhada na seção 3.2 Advanced Cloud Privacy Threat Modelling.

2.3 SMART GRID

A rede elétrica tradicional é unidirecional, com a eletricidade fluindo das estações de geração de energia para os usuários finais por meio de uma grande rede de cabos e transformadores (EFTHYMIOU; KALOGRIDIS, 2010). Ainda que tenha sido adequada ao longo dos últimos anos, a sociedade moderna demanda um sistema mais confiável, escalável, gerenciável, seguro e inter operável, sem a diminuição de seu custo-benefício (BARI *et. al*, 2014).

A necessidade de modernização da rede elétrica decorre tanto do envelhecimento da infraestrutura quanto de novas pressões ambientais e sociais (CARVALHO, 2015; EFTHYMIOU; KALOGRIDIS, 2010). Tem-se discutido questões de confiabilidade na rede elétrica desde o seu nascimento. Além das vantagens ambientais, espera-se que com a *Smart Grid* a confiabilidade na rede elétrica aumente significativamente (AMIN; WOLLENBERG, 2005; WEN *et al*., 2015). Conforme aumenta a dependência de sistemas eletrônicos e interconectados na sociedade da informação, aumentam os impactos negativos de uma falha ou ataque à rede que levem a um apagão.

A Plataforma de Tecnologia Europeia para *Smart Grids* define *Smart Grid* (*SG*) como uma rede de eletricidade que possa inteligentemente integrar as ações de todos os usuários a ela conectados, consumidores e geradores, para de maneira eficiente entregar suprimentos de energia sustentáveis, econômicos e seguros (ETP SMART GRIDS, 2006).

Nos Estados Unidos, por exemplo, defende-se que a *SG* (NIST, 2014b, p. 27, tradução nossa):

- Melhora a confiabilidade e qualidade da energia
- Otimiza a utilização de instalações e evitar a construção de usinas elétricas de reserva
- Aumenta a capacidade e eficiência das redes elétricas existentes
- Melhora a resiliência à interrupção por desastres naturais e ataques
- Permite manutenção preditiva e respostas de “auto-reparação” para perturbações do sistema
- Facilita a implantação expandida de fontes renováveis de energia
- Acomoda fontes de energia distribuídas
- Automatiza a manutenção e operação
- Reduz a emissão de gases poluentes por possibilitar veículos elétricos e novas fontes de energia
- Reduz o consumo de combustíveis fosseis por reduzir a necessidade de geração por turbinas a gás durante períodos de pico de uso
- Apresenta oportunidades para melhorar a segurança da rede
- Permite a transição para veículos elétricos *plug-in* e novas opções de armazenamento de energia
- Fornece aos consumidores informações úteis e oportunas sobre seu uso de energia
- Aumenta a escolha do consumidor e permite novos produtos, serviços e mercados

Os *Smart Meters* (*SM*), medidores eletrônicos inteligentes, realizam o papel de medição e comunicação dos dados e estabelecem o fluxo bidirecional de informação. A gama de informações fornecidas pelos *SM* em tempo real pode ser utilizada para aplicações de detecção de falhas, autocorreção de falhas e

gerenciamento de demanda. A possibilidade de variação tarifária e a comunicação bidirecional transformam o usuário final, tradicionalmente passivo, em agente ativo no sistema, além de reduzir o perfil geral de demanda das estações de geração (FANG *et al*., 2012).

O envolvimento do usuário final é foco de um número crescente de projetos na Europa, com a promessa de benefícios como economia de energia, gerenciamento da demanda, serviços inovadores como automação do lar e competição no mercado de distribuição (EUROPEAN COMMISSION *et al*., 2013). Quando desenhados com a função de fornecer informações significativas sobre o consumo de energia às Unidades Consumidoras (UC), os *SM* podem aumentar a consciência dos usuários sobre padrões de uso e postos tarifários, influenciando os objetivos de sustentabilidade (MINAMIZAKI *et al*., 2013).

Fatores de motivação comumente encontrados em projetos de *SG* na Europa são, em ordem de importância (EUROPEAN COMMISSION *et al*., 2013): (i) preocupações ambientais, (ii) redução de/controle sobre as contas de eletricidade e (iii) maior conforto.

Farhangi (2010) apresenta uma breve comparação entre a rede elétrica tradicional e a *Smart Grid* (Quadro 1).

Quadro 1 - A *Smart Grid* comparada à Rede Elétrica existente

Característica	Rede Elétrica Existente	*Smart Grid*
Medidores	Eletromecânicos	Digitais
Fluxo de comunicação	Unidirecional	Bidirecional
Geração	Centralizada	Distribuída
Estruturação	Hierárquica	Em Rede
Sensoriamento	Poucos sensores	Sensores espalhados
Monitoramento	“Cega”	Automonitoramento
Manutenção	Restauração manual	Autorreparação
Modo de falha	Falhas e apagões	Adaptativa e segregativa
Mercado final	Poucas opções aos consumidores	Várias opções aos consumidores

Fonte: Adaptado de Farhangi (2010)

Em suma, uma *Smart Grid* é “a combinação de uma rede tradicional de distribuição e uma rede bidirecional de comunicação para detecção, monitoramento e dispersão de informação sobre consumo de energia” (BARI *et al*., 2014, p. 2).

Na seção seguinte será apresentada uma breve síntese sobre as preocupações de privacidade apresentadas pela literatura como consequências potenciais do desenvolvimento da *SG.*

2.3.1 Privacidade e Segurança em *Smart Grid* (*SG*)

Sabe-se que quanto mais complexo, mais vulnerável é um sistema (WEN *et al*., 2015). A dependência de Tecnologias de Informação e Comunicação (TIC) e a interconexão com a internet trazem novas preocupações de segurança e privacidade ao desenvolvimento de *Smart Grids* (*SG*) (LESZCZYNA, 2018). A arquitetura heterogênea e complicada da *SG*, faz com que a atividade de a proteger seja desafiadora (FAN; GONG, 2013). Segurança e privacidade serão assuntos de suma importância no desenvolvimento de *Smart Grids* (EFTHYMIOU; KALOGRIDIS, 2010; MINAMIZAKI *et al*., 2013). Em última instância, o desenvolvimento da rede elétrica inteligente depende da aceitação dos consumidores finais sobre os produtos e serviços da *Smart Grid* (*SG*), como os *smart meters* (*SM*) e os serviços de medição avançada (PARK; KIM; KIM, 2014).

O cenário de privacidade é dinâmico, de modo que apenas analisar um contexto de potencial invasão não é o suficiente (QUINN, 2009). Ainda que tenha sido realizado levantamento bibliográfico extenso, os riscos à privacidade identificados não configuram lista exaustiva, mas sim exemplificativa. O Quadro 2 apresenta uma síntese das principais preocupações de privacidade relacionadas aos SM e agrupadas por tipo de uso dos dados, a partir das contribuições de McKenna, Richardson, Thomson (2012) e Quinn (2009).

Quadro 2 - Síntese de preocupações de privacidade relacionadas a S*mart Meters*

Tipo de uso	Exemplos de preocupação
Usos ilegais	Ladrões descobrindo quando a casa está desocupada; Presença e frequência de uso de sistema de alarme; *Stalkers* rastreando os movimentos de suas vítimas;
Usos comerciais	Publicidade direcionada (Em quais dias/horários se assiste TV? Quanto tempo em casa se passa em frente ao computador? Com qual frequência se come em casa? Qual a frequência de refeições preparadas no micro-ondas? Há eletrodomésticos operando abaixo da eficiência ótima? Com qual frequência se acorda durante a noite?); Ajuste de valores de seguros (Com qual frequência se dorme uma noite completa vs. dirige-se sem ter dormido? Com qual frequência se sai atrasado para o trabalho? O tempo que se levaria para chegar ao trabalho requereria ultrapassar os limites de velocidade? Com qual frequência se esquece aparelhos ligados ao sair de casa?)
Usos pela polícia	Detecção de atividades ilegais (Fábricas de trabalho escravo; atividades comerciais não licenciadas; produção de drogas) Verificando alegações do réu (Que afirma por exemplo ter estado em casa a noite toda)
Usos por outras partes em litígios	Em um processo de guarda: A criança é deixada sozinha em casa? Em um processo trabalhista: Como foi possível ligar as luzes no andar de cima tão pouco tempo depois de desligar as luzes do andar de baixo com a alegada lesão trabalhista severa?
Usos por coabitantes	Parceiros ou pais abusivos espionando o comportamento dos coabitantes
Usos médicos	Pacientes clinicamente depressivos ou bipolares apresentam perfis de consumo característico? E pacientes com transtornos comportamentais?

Fonte: Adaptado de McKenna, Richardson e Thomson (2012, p. 7) e Quinn (2009, p. 31)

As preocupações exemplificadas no Quadro 2 derivam de uma mesma ameaça: que os *smart meters* (*SM*) possam ser utilizados para revelar certas atividades usualmente consideradas privadas por ocorrerem no interior do lar (McDANIEL; McLAUGHLIN, 2009; McKENNA; RICHARDSON; THOMSON, 2012). O que determinará quais informações podem ser obtidas do conjunto de dados disponíveis é sua resolução, ou seja, a frequência com que os dados são coletados e o tipo de processamento realizado. Uma informação coletada diariamente pode revelar padrões de ocupação ou permitir outras inferências quando acumulada, mas não permitirá, por exemplo, a identificação individualizada de eletrodomésticos (McKENNA; RICHARDSON; THOMSON, 2012).

Outros usos prejudiciais podem ainda não terem sido vislumbrados, em especial aqueles decorrentes do cruzamento de informações de consumo energético

com outros conjuntos de dados sobre os indivíduos. Uma lista como esta nunca poderá ser exaustiva, dado o caráter dinâmico do tema (QUINN, 2009), motivo pelo qual uma das premissas deste trabalho é que deve ser adotada *Privacy by Design* (CAVOUKIAN, 2010) na concepção de projetos de *Smart Grid* (*SG*), pelo princípio de que a privacidade deve ser considerada proativamente, conforme Art. 6º, VIII da LGPD (princípio da prevenção), e não em resposta a incidentes específicos (BRASIL,2018).

2.3.2 Aspectos regulatórios de *Smart Grid* (*SG*)

A regulação específica de *Smart Grid* no território brasileiro fica a cargo da Aneel. Todos os assuntos de energia são de competência legislativa do Governo Federal e a definição dos parâmetros técnicos mínimos para a aprovação de medidores eletromecânicos, bem como sua efetiva aprovação, fica a cargo do Inmetro (Instituto Nacional de Metrologia Qualidade e Tecnologia) (CARVALHO, 2015).

A Resolução Normativa nº 502, de 7 de agosto de 2012, da Aneel, que regulamenta sistemas de medição de energia elétrica de Unidades Consumidoras do Grupo B, ao tratar sobre medidores eletrônicos que possuam comunicação remota, prevê (ANEEL, 2012):

> Art. 7º Na hipótese de o sistema de medição ser provido de sistema de comunicação remota, a distribuidora deve adotar procedimentos e tecnologias que assegurem a segurança dos dados trafegados e, especialmente, das informações de caráter pessoal coletadas das unidades consumidoras.
> Parágrafo único. É vedado à distribuidora disponibilizar dados coletados das unidades consumidoras a terceiros sem a autorização do titular.

Ainda sobre a implantação dos medidores e a referida importância do engajamento do consumidor final, a Resolução prevê (ANEEL, 2012):

> Art. 9º Para as unidades consumidoras em que os sistemas de medição de que trata esta Resolução vierem a ser instalados, os consumidores devem ser informados, previamente à instalação, acerca das funcionalidades do referido sistema e das informações que lhes passarão a ser disponibilizadas.

As informações transmitidas ao consumidor podem auxiliar na modificação de padrões de consumo para obtenção de vantagem econômica e consequente diminuição de picos de demanda. Ao mesmo tempo, informar o consumidor sobre

como os dados coletados em sua Unidade Consumidora são utilizados, um passo essencial para a obtenção de consentimento informado para o tratamento de dados.

2.4 AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (AIPD)

Uma Avaliação de Impacto à Proteção de Dados Pessoais (AIPD) é “um processo para auxiliar na identificação e minimização de riscos à proteção de dados de um projeto” (ICO, 2018). O processo orienta os tomadores de decisão no sentido de quais soluções, organizacionais e técnicas, são mais eficazes para cada fonte de risco identificada, buscando-se obter ao final uma solução que assegure a privacidade e a intimidade sem diminuir a utilidade dos dados. Um processo onde um esforço consciente e sistemático é realizado para avaliar os impactos à proteção de dados das opções disponíveis relativas à uma proposta (STEWART, 1996). O processo de AIPD é caracterizado também como forma de autorregulação e demonstração voluntaria de *compliance* com princípios gerais de privacidade (WRIGHT, 2012), o que possibilita aos agentes envolvidos capitanear o desenvolvimento de procedimentos nacionais baseados em boas práticas discutidas na literatura.

O termo Avaliação de Impacto à Privacidade – AIP (*Privacy Impact Assessment – PIA*) é rotineiramente utilizado para se referir ao mesmo conceito (ART.29WP, 2017; DE HERT, 2012). Nesta dissertação privilegiou-se a nomenclatura AIPD por ser, implicitamente, a adotada pela Lei Geral de Proteção de Dados (LGPD) na nomenclatura do relatório produto do processo sistemático de avaliação, contudo, utilizou-se material publicado sobre ambos e foram tratados indistintamente na revisão.

A LGPD apresenta o conceito de Relatório de Impacto à Proteção de Dados Pessoais (RIPD) como a descrição e documentação dos riscos às liberdades civis e aos direitos fundamentais decorrentes do tratamento de dados pessoais, e demonstração dos mecanismos de mitigação correspondentes, de responsabilidade do controlador (BRASIL, 2018). A LGPD não descreve o processo ou determina sua obrigatoriedade, encarregando a Autoridade Nacional de Proteção de Dados (ANPD) da publicação de material auxiliar e requisição ao controlador quando necessário. Uma das expectativas deste estudo é contribuir para a discussão deste processo na literatura nacional, em especial sob o ponto de vista da LGPD.

Uma AIPD é um tipo de análise, estruturada e possível de ser reproduzida, sobre como são processadas informações relacionadas a indivíduos. Um processo completo para determinar a privacidade, confiabilidade e riscos de segurança associados à coleta, uso e revelação de informação pessoal. Ao final é produzido um relatório para descrever os tipos de riscos à proteção de dados descobertos e prover recomendações para mitigá-los (NIST, 2014ª; STEWART, 2002; WRIGHT, 2012).

As primeiras referências ao processo de AIP datam do começo dos anos 1990 (STEWART, 2002) tendo sido utilizado inicialmente na Austrália, Canadá, Nova Zelândia e Estados Unidos (WRIGHT, 2012). Em 2007, o Information Commissioner's Office do Reino Unido publica o primeiro guia de Avaliação do Impacto à Privacidade da Europa, revisado em 2009. Desde então AIPs se tornaram uma parte importante do cenário de proteção de dados pessoais (ICO, 2014). O guia é consolidado como um código de prática para AIP em 2014 (ICO, 2014) e posteriormente adequado à nova terminologia contida na GDPR (AIPD) em 2018 (ICO, 2018).

O processo de AIPD se funda em dois pilares: o da garantia de direitos fundamentais, que não são negociáveis ou renunciáveis; e o do gerenciamento dos riscos sobre a proteção de dados do sujeito, que determina o nível técnico apropriado e os controles organizacionais para sua proteção (CNIL, 2015). A AIPD pode auxiliar na utilização de bases de dados que sejam capazes de oferecer conhecimento valioso, mesmo quando previamente pudessem representar ameaça à privacidade. A AIPD permite que riscos à privacidade, atuais ou potenciais, sejam levantados no início do projeto e endereçados quando ainda são mais baratos e simples de corrigir (STEWART, 1996; WRIGHT, 2012).

Outro benefício esperado é o aumento da transparência e da confiabilidade na entidade que processa os dados. Para Flaherty (2000, n.p., tradução nossa):

> De maneira simplificada, uma avaliação do impacto sobre a privacidade procura apresentar, tão detalhadamente quanto requerido para promover o entendimento necessário, os componentes essenciais de qualquer sistema de informação pessoal ou qualquer sistema que contenha quantidades significantes de informações pessoais.

O processo de AIPD deve ser conduzido pelo controlador dos dados e se beneficia da consultoria com todos os *stakeholders* envolvidos e *experts* que possam oferecer visões variadas sobre as ameaças e contramedidas. A consulta com

especialistas auxilia também na categorização dos riscos para orientar a prioridade das ações (ICO, 2018).

2.4.1 AIPD na legislação

O Art. 5º da LGPD traz as definições adotadas na Lei e conceitua em seu inciso XVII (BRASIL, 2018):

> relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco.

A própria definição do relatório sinaliza que o processo de AIPD não é exclusivamente sobre privacidade; apesar de se concentrar em proteção de dados pessoais, o processo objetiva proteger as liberdades civis e os direitos fundamentais. Fica a cargo da ANPD requerer o referido relatório de impacto à proteção de dados pessoais (RIPD). Quando da criação da LGPD os artigos que previam a criação da ANPD foram vetados por vício de iniciativa e, no mesmo ano, foi proposta a Medida Provisória nº 869 pelo governo Temer para superar este impedimento e estabelecer a criação da Agência. A MP nº 869 é convertida em Projeto de Lei de Conversão nº 7/2019 (PLC Nº. 7) pelo Senado e em 8 de julho de 2019 é convertida na Lei nº 13.853, pelo governo que sucede o de Temer, e é criada a ANPD, com alguns vetos à MP e algumas alterações na LGPD (BRASIL, 2019).

Fica criada a ANPD sem aumento de despesa e como órgão da administração pública federal, integrada à Presidência da República, com assegurada autonomia técnica e decisória (BRASIL, 2019). O modelo da ANPD trazido na MP e aprovado na Lei é apontado como frágil por não ter independência financeira e ser parte integrante da Presidência da República, o que pode prejudicar sua função de garantidora de respeito à Lei pelo próprio Governo, ainda que transitório e com possibilidade de revisão em dois anos (LEORATTI, 2019).

O processo de construção da LGPD foi notadamente participativo e multisetorial, desde a consulta pública ao texto proposta pelo Ministério da Justiça até a elaboração da Medida Provisória 869/2018, de modo que os vetos da Presidência

foram tidos como uma desconsideração da vontade popular manifestada ao longo do processo legislativo (CDR, 2019; IDEC, 2019).

A legislação não nomeia qual processo leva ao referido relatório, contudo, define que, para atender aos princípios de Segurança (Art. 6º, VII) e Prevenção (Art. 6º, VIII), o controlador poderá implementar programa de governança de privacidade que, no mínimo (BRASIL, 2018, grifo nosso):

> Art. 50, § 2º, inciso I
> a) *demonstre* o comprometimento do controlador em adotar processos e políticas internas que assegurem *o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais*;
> b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta;
> c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados;
> d) estabeleça políticas e salvaguardas adequadas *com base em processo de avaliação sistemática de impactos e riscos à privacidade*;
> e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular;
> f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos;
> g) conte com planos de resposta a incidentes e remediação; e
> h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas;

Ainda que a ANPD eventualmente publique guias para um “processo de avaliação sistemática de impactos e riscos à privacidade” (BRASIL, 2018) sob nomenclatura distinta de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD), esta dissertação considera que a documentação referente aos processos de AIP e AIPD são suficientes para o atendimento dos objetivos da legislação e podem auxiliar no estabelecimento do referido programa de governança de privacidade. Uma AIPD pode se aplicar a uma atividade de processamento única ou um conjunto de atividades similares e de um produto de tecnologia (WP29, 2017). A LGPD deixa a cargo da ANPD o requerimento de produção de Relatório de Impacto à Proteção de Dados (BRASIL, 2018), contudo, a GDPR prescreve que uma AIPD deve ser conduzida para operações que sejam prováveis de resultar em um elevado risco aos direitos e liberdades da pessoa natural, citando não-exaustivamente as seguintes situações (EUR-LEX, 2018, artigo 35º, nº 3):

> a) Avaliação sistemática e completa dos aspetos pessoais relacionados com pessoas singulares, baseada no tratamento automatizado, incluindo a definição de perfis, sendo com base nela adotadas decisões que produzem efeitos jurídicos relativamente à pessoa singular ou que a afetem significativamente de forma similar;
> b) Operações de tratamento em grande escala de categorias especiais de dados a que se refere o artigo 9º, nº 1, ou de dados pessoais relacionados com condenações penais e infrações a que se refere o artigo 10.o; ou
> c) Controlo sistemático de zonas acessíveis ao público em grande escala.

As categorias especiais de dados referidas no artigo 9º, nº 1 são aquelas nas quais o tratamento possa revelar informação sensível, como origem racial ou étnica, opiniões políticas ou o tratamento de dados genéticos e biométricos (EUR-LEX, 2018). A análise do Article 29 Working Party cita também, como exemplos de operações que requerem AIPD, o processamento de informações genéticas por um hospital, a criação de uma base nacional de proteção ao crédito, ou o reconhecimento automático de placas de carros (WP29, 2017). O ICO (2018) aponta o uso de tecnologias inovadoras como inteligência artificial, veículos autônomos e sistemas inteligentes de transporte como exemplos de processamento que requerem AIPD. O órgão inclui os dados processados por *Smart Meters* na categoria de criação de perfis em larga escala, motivo pelo qual a atividade requer condução prévia de AIPD (ICO, 2018).

Os motivos que podem levar uma organização a realizar uma AIPD são: identificar e gerenciar riscos; evitar custos desnecessários; evitar soluções inadequadas; evitar a perda de confiança e reputação; orientar a estratégia de comunicação da organização; e cumprir requerimentos legais (ICO, 2009). Quanto a natureza dos riscos, a AIPD pode avaliar aqueles (STEWART, 2002, p. 25, tradução nossa):

> - que surgem de uma nova tecnologia ou da convergência de tecnologias existentes
> - onde uma tecnologia conhecida que invada a privacidade será usada em novas circunstâncias
> - em uma grande empreitada ou alteração de prática com efeitos significativos para a privacidade

Ainda não é claro como a ANPD exercerá suas atribuições, contudo, pela análise de documentação relativa à aplicação da GDPR e do próprio processo de AIPD, defende-se que a implantação da Rede Elétrica Inteligente é caso de requisição de avaliação sistemática dos possíveis impactos à proteção de dados pessoais nos termos da LGPD.

A privacidade é obtida por meio de um conjunto de boas práticas e regulações, não decorre simplesmente de uma ou outra implementação técnica, portanto é necessário que o processo se dê de maneira holística e contemple todos os *stakeholders.* Ao realizar uma AIPD a organização não busca somente proteger sua reputação, garantir *compliance* e evitar gastos com litigância, mas especialmente garantir a privacidade e as melhores práticas no tratamento dos dados pessoais e como consequência evitar para si reflexos negativos da concretização de um risco. A condução da AIPD permite verificar os riscos e contrapô-los aos benefícios esperados com a publicização ou o tratamento dos dados, sendo que o objetivo é excluí-los ou minimizá-los a um nível aceitável sem diminuir os benefícios (GREEN *et al*., 2017).

2.5 COMPUTAÇÃO EM NUVEM (*CLOUD COMPUTING*)

Neste estudo se adota o conceito de computação em nuvem oferecido pelo Instituto Nacional de Padrões e Tecnologia dos Estados Unidos (US National Institute for Standards and Technology – NIST) (MELL; GRANCE, 2011, tradução nossa):

> Computação em nuvem é um modelo para permitir acesso onipresente, conveniente e por demanda por rede a um conjunto compartilhado de recursos computacionais configuráveis (*e.g.*, redes, servidores, armazenamento, aplicações e serviços) que possam ser rapidamente providos e lançados com mínimo esforço de gerência ou interação com o provedor de serviços.

Há várias definições para computação em nuvem, mas o conceito central é o de computação utilitária (*utility-computing*) que tem como vantagens a possibilidade de o usuário consumir recursos conforme sua demanda e se valer de uma variedade de fornecedores no mercado para otimizar custos e acessar melhores serviços (CREESE; GOLDSMITH; HOPKINS, 2013).

A definição mais utilizada de nuvem lista cinco características essenciais, três modelos de serviço e quatro modelos de implantação (MELL; GRANCE, 2011, tradução nossa).

2.5.1 Características essenciais

a) Auto-serviço por demanda (*on-demand self-service*): Um cliente pode prover capacidades computacionais de acordo com suas necessidades e sem a necessidade de intervenção do fornecedor (MELL; GRANCE, 2011, tradução nossa);

b) Acesso amplo pela rede (*broad network access*): Os recursos e capacidades podem ser acessados pela rede, permitindo que o consumidor não dependa de localidade ou capacidade de hardware local (*e.g.* acesso por meio de *smartphones*) (MELL; GRANCE, 2011, tradução nossa);

c) Compartilhamento de recursos (*resource pooling*): Armazenamento, poder de processamento, memória e largura de banda são dinamicamente atribuídos e reatribuídos de acordo com a demanda do consumidor, criando um modelo de “múltiplos locatários” (*multi-tenant*) (MELL; GRANCE, 2011, tradução nossa);

d) Rápida elasticidade (*rapid elasticity)*: As capacidades computacionais podem aumentar ou diminuir rapidamente em função da demanda, em alguns casos automaticamente. Da perspectiva do consumidor, os recursos estão disponíveis em qualquer quantidade a qualquer momento (MELL; GRANCE, 2011, tradução nossa);

e) Serviço medido (*measured service*): O uso dos recursos é monitorado e utilizado para cobrar o consumidor apenas pelo que foi utilizado (MELL; GRANCE, 2011, tradução nossa).

2.5.2 Modelos de serviço

a) *Software* como serviço (*Software as a Service – SaaS*): O consumidor utiliza as aplicações do provedor executando em uma infraestrutura de nuvem. O consumidor não administra ou controla a infraestrutura e as capacidades da

aplicação, exceto por possíveis configurações de usuário limitadas (MELL; GRANCE, 2011, tradução nossa);

b) Plataforma como serviço (*Platform as a Service – PaaS*): O consumidor controla a aplicação que será executada na infraestrutura de nuvem, mas não administra ou controla os recursos subjacentes, como redes, servidores, armazenamento e sistema operacional, com a exceção da possibilidade de configurações para o ambiente de hospedagem da aplicação (MELL; GRANCE, 2011, tradução nossa);

c) Infraestrutura como serviço (*Infrastructure as a Service – IaaS*): O consumidor pode prover processamento, armazenamento, conexão e outros recursos computacionais e pode executar *software* arbitrariamente, como sistemas operacionais e aplicações. O consumidor não administra ou controla a infraestrutura subjacente, exceto alguns componentes de rede como o *firewall* do hospedeiro (MELL; GRANCE, 2011, tradução nossa).

2.5.3 Modelos de implantação (*Deployment models*)

a) Nuvem privada (*Private cloud*): A infraestrutura de nuvem é utilizada exclusivamente por uma organização, composta de vários consumidores (unidades de negócios). As responsabilidades por controle e administração da infraestrutura pode ficar a cargo da própria organização, terceiro ou uma combinação de ambos. A estrutura pode estar localizada nas dependências do cliente ou não (MELL; GRANCE, 2011, tradução nossa);

b) Nuvem comunitária (*Community cloud*): A infraestrutura de nuvem é utilizada exclusivamente por um grupo de consumidores que se beneficiam da união para atingir objetivos similares, como por exemplo requisitos de segurança ou de *compliance*. A operação e propriedade pode ser responsabilidade de uma ou mais organizações, terceiros ou uma combinação destes e a infraestrutura pode estar nas dependências do cliente ou não (MELL; GRANCE, 2011, tradução nossa);

c) Nuvem pública (*Public cloud*): A infraestrutura de nuvem é ofertada ao público geral. Os recursos são compartilhados pelos usuários por meio de virtualização e são propriedade administrada e operada pelo provedor, que pode ser um negócio, uma entidade acadêmica, uma organização governamental ou uma combinação destes. A infraestrutura é localizada nas dependências do provedor de nuvem (MELL; GRANCE, 2011, tradução nossa);

d) Nuvem híbrida (*Hybrid cloud*): A infraestrutura de nuvem é uma combinação dos modelos de implantação que são interconectados para permitir um fluxo de trabalho integrado (MELL; GRANCE, 2011, tradução nossa).

2.5.4 Desafios da computação em nuvem

Tradicionalmente, modelos de segurança definem primeiramente o perímetro de segurança dentro do qual há controle sobre recursos e informações sensíveis podem ser armazenadas e processadas, como é o caso do limite estabelecido pelo *firewall* da empresa. Estas barreiras se tornam difíceis de estabelecer em nuvens públicas ou híbridas nas quais a informação é armazenada e processada fora de áreas de confiança (CREESE; GOLDSMITH; HOPKINS, 2013; PEARSON; BENAMEUR, 2011). Ainda que um modelo de nuvem privada resolva alguns dos problemas de segurança física e ofereça maior confidencialidade e controle (M'RHAOAURH et al., 2018), algumas ameaças decorrem das próprias características essenciais de computação em nuvem (GROBAUER; WALLOSCHEK; STOCKER, 2011). O acesso amplo pela rede se aplica aos consumidores, mas também a possíveis agentes maliciosos, portanto as medidas para controle de acesso e detecção de intrusão devem estar presentes em qualquer implantação de computação em nuvem.

Nuvens privadas são mais caras e nuvens públicas é a implantação mais difundida pela relação custo-benefício. O custo é menor, mas a infraestrutura e os recursos são propriedade administrada e operada pelo provedor de serviço de nuvem, causando preocupações quanto ao processamento de informações pessoais fora do perímetro de segurança da organização (CREESE; GOLDSMITH; HOPKINS, 2013).

Alguns problemas de privacidade são consequência de problemas de segurança, como acesso não-autorizado à informação, contudo, Pearson e Benameur (2011) destacam quatro problemas de privacidade para computação em nuvem:

a) Falta de controle pelo usuário: Ao utilizar o modelo de *SaaS*, por exemplo, o usuário confia no provedor do serviço para armazenar e processar seus dados de uma certa forma, com pouca ou nenhuma capacidade de checar tais suposições;
b) Uso secundário não autorizado: Alguns usos secundários podem fazer parte do acordo de prestação de serviço, por exemplo para fins de direcionamento de publicidade, contudo, o usuário não tem a capacidade de obrigar apenas os usos contratados ou impedir usos posteriores;
c) Proliferação e fluxo internacional de informações: É característica do modelo de nuvem replicar informações, seja para otimizar a entrega de conteúdo ou atingir redundância em *backups*. Estas múltiplas versões da informação podem se encontrar em jurisdições com proteção legal inferior, com acesso facilitado às autoridades ou pode não ser deletada em conjunto com outras cópias. Esta característica dificulta o atendimento às legislações de proteção de dados, eventualmente de mais de uma jurisdição simultaneamente e aumenta a necessidade de procedimentos efetivos para governança nas organizações.
d) Provimento dinâmico: a natureza dinâmica da nuvem faz com que seja difícil de definir, na prática ou contratualmente, quais partes estão responsáveis pelo tratamento e garantia dos dados. Não é claro que os subcontratantes do provedor de nuvem possam claramente definidos e responsabilizados, nem qual a situação dos direitos sobre os dados em caso de aquisição, fusão ou falência do provedor.

A superação destes desafios requer uma ação integrada e dinâmica de monitoramento de segurança e práticas de governança. Os desafios da computação em nuvem se somam aos próprios desafios da *SG*, na medida em que a implantação desta utilizará computação em nuvem para operar. A metodologia de pesquisa considerou os dois contextos integradamente para a revisão de literatura que pudesse subsidiar o processo de AIPD.

3 METODOLOGIA DA PESQUISA

Neste capítulo serão detalhados os procedimentos metodológicos empreendidos no desenvolvimento desta pesquisa. O objetivo geral desta dissertação é propor um conjunto de medidas de proteção de dados pessoais que precisariam ser consideradas no planejamento e operação de *Smart Grid* utilizando computação em nuvem.

O processo de AIPD é geral e reprodutível (NIST, 2014a), assim, pode auxiliar no direcionamento da investigação de ameaças à privacidade em uma variedade de contextos e sistemas. Por ser geral, o processo conduzido nesta pesquisa foi subsidiado pela metodologia de *Advanced Cloud Privacy Threat Modeling* (*CPTM*) apresentada por Gholami *et al*. (2016) para a definição de requisitos de privacidade, identificação de ameaças e proposição de contramedidas no ambiente de nuvem. Para a seleção da bibliografia foram utilizados procedimentos de Revisão Bibliográfica Sistemática (CONFORTO; AMARAL; SILVA, 2011) e bibliométricos (ENSSLIN; ENSSLIN; PINTO, 2013), enquanto para a análise do *corpus* levantado utilizou-se Análise de Conteúdo (BARDIN, 2011).

As ações de coleta de material aqui descritas ocorreram no mês de julho de 2018 e foram possíveis graças ao uso remoto via CAFe (Comunidade Acadêmica Federada) que permite o acesso completo ao Portal de Periódicos da Capes. O Portal conta atualmente com mais de 53 mil periódicos com texto completo e 129 bases referenciais. A escolha pelo portal se deu por ser possível realizar a pesquisa pelos termos definidos (*string* de busca) simultaneamente em bases como Scopus, Web of Science, ProQuest, Clarivate Analytics e permitir o salvamento de múltiplas referências para posterior análise (CAPES, 2018).

3.1 O PROCESSO DE AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS (AIPD)

As discussões e resultados desta dissertação serão apresentados de acordo com o processo de AIPD apresentado pela Autoridade de Proteção de Dados do Reino Unido, o Information Commissioner’s Office (ICO). O órgão publicou um manual para a condução do processo de Avaliação de Impacto à Privacidade (ICO, 2007), posteriormente revisado e expandido para um Código de Prática de AIP (ICO, 2014)

que, após a entrada em vigor da GDPR, foi reeditado para conter as recomendações necessárias à AIPD, com foco em responsabilização e proteção por *design* (ICO, 2018). O guia para a condução de AIPD foi eleito por ser mais recente e alinhado à terminologia empregada na legislação nacional e europeia, contudo, conforme discutido anteriormente, os processos de AIP e AIPD são similares e muitas vezes tratados indistintamente (DE HERT, 2012; WP29, 2017).

O processo é descrito como um ciclo de atividades que devem ocorrer desde as fases iniciais de planejamento do projeto e seguirem até sua execução. Os passos apresentados são (ICO, 2018, tradução nossa):

1. Identificar a necessidade de uma AIPD;
2. Descrever o processamento dos dados;
3. Considerar consultoria;
4. Avaliar a necessidade e proporcionalidade;
5. Identificar e avaliar os riscos;
6. Identificar medidas para mitigar risco;
7. Aprovar e registrar os resultados da AIPD;
8. Integrar os resultados da AIP ao plano do projeto;
9. Manter sob revisão.

Neste estudo, o processo de AIPD será conduzido com o apoio de metodologia de modelagem de ameaças de privacidade para ambiente de nuvem, proposta por Gholami *et al*. (2016) e descrita nos próximos itens. A opção pelo auxílio de metodologia específica para a modelagem de ameaças de privacidade em ambiente de nuvem contribui principalmente com os passos 4, 5 e 6 do processo de AIPD.

3.2 *ADVANCED CLOUD PRIVACY THREAT MODELING* (*CPTM*)

A metodologia escolhida para a modelagem de ameaças foi a apresentada por Gholami *et al*. (2016) especificamente para identificar ameaças à privacidade no uso de computação em nuvem. Os autores propõem esta metodologia como uma extensão da *Cloud Privacy Threat Modeling* (*CPTM*) apresentada em 2013 (GHOLAMI *et al*., 2014) inicialmente com foco na legislação europeia e posteriormente alterada para acomodar outros requisitos legais (GHOLAMI *et al*., 2016).

O uso da metodologia de modelagem de ameaças no ambiente de nuvem foi escolhido para subsidiar a condução do processo de AIPD por sistematizar os (1) Requisitos de Privacidade (RP_i, no qual i corresponde ao número do item) de acordo

com *compliance* regulatório e nos estágios iniciais dos projetos. Estes requisitos são então transferidos à fase de *Design* onde ocorrem as atividades de (2) Especificação do ambiente de nuvem; (3) Identificação de ameaças à privacidade (A_i); (4) Avaliação de risco e (5) Mitigação de ameaças pela proposição de contramedidas (*countermeasures*) (C_i). Esta metodologia contribui especialmente para as etapas 4, 5 e 6 do processo de AIPD por ser específica ao contexto analisado e tem seus passos detalhados a seguir (GHOLAMI *et al*., 2016):

3.2.1 *Compliance* regulatório de privacidade

Neste passo da *Advanced CPTM* são listados os requisitos de privacidade. Os autores apresentam a metodologia considerando princípios da GDPR e argumentam que a metodologia é flexível para considerar os requisitos de privacidade de outras legislações (GHOLAMI et al., 2016). A legislação brasileira foi escolhida para centrar esta dissertação, portanto os requisitos de privacidade foram extraídos dos princípios que devem ser observados para o processamento de dados pessoais de acordo com a LGPD. Cada Requisito de Privacidade ($RP_{1\text{-}10}$) foi listado e enumerado de acordo com os princípios contidos no artigo 6º da LGPD, “I – Finalidade; II – Adequação; III – Necessidade; IV – Livre acesso; V – Qualidade dos dados; VI – Transparência; VII – Segurança; VIII – Prevenção; IX – Não discriminação; X – Responsabilização e prestação de contas” (BRASIL, 2018). Pela identificação dos princípios para processamento de dados da LGPD com os RP, as propostas de contramedidas (C) às ameaças encontradas (A) buscarão *compliance* com a legislação nacional.

3.2.2 Especificação de ambiente de nuvem

Serviços de computação em nuvem são apresentados em diferentes modalidades (MELL; GRANCE, 2011), com características distintas de ameaças e superfície de ataque. A definição do ambiente no qual o projeto será implementado é essencial para a definição de atores e responsabilidades no sistema e quais medidas de mitigação de risco são mais indicadas. Por exemplo um projeto que utilize exclusivamente nuvem do tipo *Software as a Service* (*SaaS*) deve focar as análises em ameaças no nível das aplicações de software, enquanto para o tipo *Infrastructure*

as a Service (*IaaS*) seria benéfico priorizar os aspectos de *hardware*, rede e armazenamento (GHOLAMI *et al*., 2016).

3.2.3 Identificação de ameaças à privacidade

Nesta etapa serão identificadas as ameaças (A) aos Requisitos de Privacidade (RP) selecionados na etapa anterior. Para esta etapa e as seguintes (Avaliação de risco e Mitigação de ameaças) serão utilizadas as contribuições sistematizadas pela Análise de Conteúdo (AC) (BARDIN, 2011) realizada no *corpus* bibliográfico obtido pela pesquisa bibliométrica descrita nos itens 3.5 e 3.3 desta dissertação, respectivamente. As ameaças serão numeradas segundo a convenção $A_{i,j}$ na qual $_i$ indica o RP correspondente e $_j$ o número da ameaça, assim a ameaça $A_{4,3}$ refere-se à terceira ameaça identificada contra o quarto requisito (RP_4).

3.2.4 Avaliação de risco

Para a avaliação dos riscos, Gholami *et al*. (2016) e a metodologia eleita para a AIPD (ICO, 2018) indicam a consulta com especialistas e participantes no desenvolvimento do sistema. Os *stakeholders* envolvidos no projeto avaliam as ameaças com relação à probabilidade de ocorrência e efeitos esperados, auxiliando na priorização das ações de mitigação (GHOLAMI *et al*., 2016). Nesta dissertação esta consulta não foi realizada e é uma das limitações da pesquisa, contudo, buscou-se suplementar esta ausência através da abrangência na revisão sistemática de literatura.

3.2.5 Mitigação de ameaças

Neste passo são propostas as contramedidas (*countermeasures*) para endereçar as ameaças encontradas na etapa anterior. Sua nomenclatura segue a mesma regra anterior, assim, a contramedida $C_{4,3}$ se refere à medida indicada contra a ameaça $A_{4,3}$. As considerações obtidas nesta etapa, baseadas na AC descrita no item 3.5, integrarão o processo de AIPD, que prescreve ações similares, mas menos específicas ao caso analisado.

3.3 LEVANTAMENTO BIBLIOMÉTRICO

A coleta dos dados secundários, fundada em material científico já elaborado, permite uma análise ampla do tema de pesquisa (GIL, 2009). Para este trabalho a etapa de coleta de dados baseada no levantamento bibliométrico forneceu material para a compreensão do estado da arte sobre privacidade em *Smart Grids* com foco em boas práticas e metodologias de gerenciamento de informações. A grande disponibilidade de artigos científicos e bancos de dados bibliográficos faz com que a escolha dos trabalhos, mais adequados à fundamentação da pesquisa, seja facilitada por uma sistematização que possibilite a identificação os principais trabalhos científicos aderentes à pesquisa em meio a uma grande quantidade de produção acadêmica nacional e internacional.

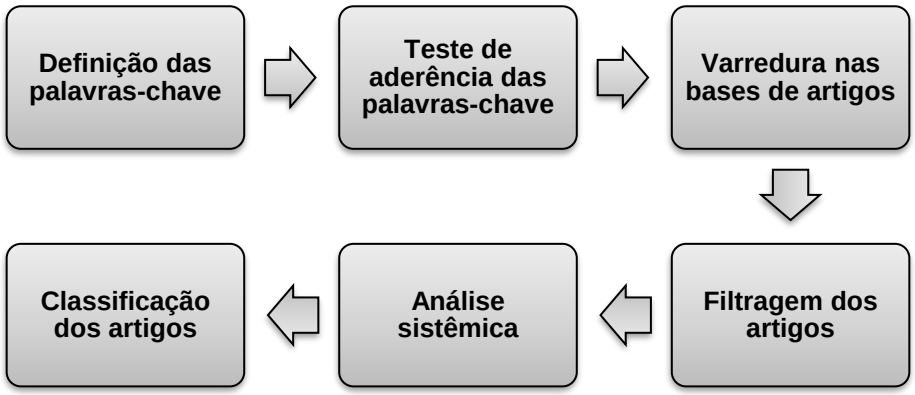
A utilização de métodos com maior rigor científico na revisão bibliográfica sistemática pode levar a melhores resultados, menos erros e diminuir o viés do pesquisador (CONFORTO; AMARAL; SILVA, 2011). Frequentemente utilizada em pesquisas na área da medicina, a revisão bibliográfica sistemática tem aplicabilidade em outras áreas de conhecimento, como a análise de políticas públicas, por integrar e analisar eficientemente uma grande quantidade de informação, auxiliando na tomada de decisões (CONFORTO; AMARAL; SILVA, 2011).

O levantamento bibliográfico deste trabalho deu-se por meio de levantamento bibliométrico, com contribuições da metodologia apresentada por Ensslin, Ensslin e Pinto (2013). A análise sistemática sobre o levantamento permite constatar o estado da arte da produção científica sobre o tema, identificar eventuais lacunas e dotar de validade científica o corpus bibliográfico final utilizado como base para o trabalho.

A análise bibliométrica considera quantitativamente parâmetros como número de citações e periódicos mais relevantes para definir o conjunto de artigos a serem utilizados (portfólio bibliográfico) (ENSSLIN; ENSSLIN; PINTO, 2013). A preferência pela utilização de métodos quantitativos na bibliometria contribui para a objetividade da seleção de literatura (ARAÚJO, 2006).

Este levantamento bibliométrico ocorreu de acordo com as seguintes etapas: (i) Definição das palavras-chave; (ii) Teste de aderência das palavras-chave; (iii) Varredura nas bases de artigos; (iv) Filtragem dos artigos; (v) Análise sistêmica; e (vi) Classificação dos artigos.

Figura 1 - Etapas da pesquisa bibliométrica



Fonte: Autoria própria (2019)

Para a identificação do tema e adaptação das recomendações e resultados ao contexto nacional realizou-se levantamento bibliográfico preliminar exclusivamente em português, conforme demonstra-se na seção seguinte.

3.3.1 Levantamento bibliográfico preliminar

Primeiramente busca-se identificar o tratamento do tema no contexto nacional. A pesquisa foi realizada utilizando-se a *string* de busca **"Avaliação * Impacto * Privacidade"** nos buscadores Google Acadêmico e Portal de Periódicos Capes. A utilização dos operadores de truncamento se deu para que os resultados contemplassem as variações de preposição utilizadas na tradução do nome do processo (Avaliação de Impacto de Privacidade; A de I sobre P; A de I na P, etc). Buscou-se também pela *string* **"relatório * impacto * proteção de dados *"** por ser a terminologia adotada pela Lei Geral de Proteção de Dados Pessoais ("relatório de impacto à proteção de dados pessoais") (BRASIL, 2018).

Tabela 1 - Levantamento bibliográfico preliminar

String de busca	Periódicos Capes	Google Acadêmico
"Avaliação * Impacto * Privacidade"	0	7
"relatório * impacto * proteção de dados *"	0	0

Fonte: Autoria própria (2019)

Os resultados da Tabela 1 demonstram que há pouca literatura nacional sobre o tema. Entre os sete resultados encontrados no buscador Google Acadêmico, o único que possui citações (2 citações) é uma tese de pós-graduação que trata de consentimento e privacidade em bases de dados de saúde e apenas menciona o processo por duas vezes, sem descrevê-lo ou aprofundar-se sobre sua condução (SILVA, 2012).

Dois dos resultados encontrados são trabalhos de Portugal que tratam sobre a legislação protetiva europeia, a GDPR (LOPES; OLIVEIRA, 2018; RAPOSO, 2018) e não contam com citações reconhecidas pelo buscador. Por não descreverem o processo, apenas mencioná-lo, também não foram incluídos ao portfólio de análise.

Um dos trabalhos encontrados foi uma dissertação de mestrado em gestão de redes de telecomunicações (MACHADO, 2016) e, apesar de tratar de *Smart Grid*, foca em seus aspectos de segurança cibernética, apenas mencionando o processo de AIP, motivo pelo qual também foi descartado.

O resultado que ao menos descreve o processo é um trabalho de graduação sobre recomendações de segurança para o desenvolvimento de web services para a administração pública federal (RIBEIRO; NIYAMA, 2016). O trabalho descreve brevemente o processo utilizando documentação de referência do NIST, que já figura no corpus documental utilizado no presente trabalho, motivo pelo qual também foi descartado.

Os dois resultados restantes tratam sobre o direito de estar só e o direito ao esquecimento na perspectiva da legislação europeia (SILVEIRA; MARQUES, 2016) e sobre a necessidade de uma lei específica de proteção de dados pessoais no ordenamento jurídico brasileiro (HOSTERT, 2018) e mencionam o processo quando discorrem sobre a GDPR.

Constata-se por meio deste levantamento preliminar que o processo de Avaliação de Impacto à Privacidade é pouco estudado pela literatura nacional. A recém aprovação da Lei nº 13.709 de 2018, a Lei Geral de Proteção de Dados Pessoais (LGPD) deve alterar este panorama na medida em que faculta à Autoridade Nacional de Proteção de Dados o requerimento de relatório de impacto à proteção de dados pessoais ao controlador de dados em seu artigo 38 (BRASIL, 2018).

Este trabalho objetiva propor um conjunto de medidas de proteção de dados pessoais que precisariam ser consideradas no planejamento e operação de *Smart*

Grid utilizando computação em nuvem. Neste sentido foram definidas as seguintes palavras-chave para a continuação do levantamento bibliográfico preliminar: "*Smart Grid*"; "*cloud*"; "*secure cloud*"; "*untrusted cloud*" "*Privacy Impact Assessment*"; "*by design*" e "*best practices*" com os resultados dispostos na Tabela 2.

Tabela 2 - Levantamento bibliográfico preliminar (continuação)

String de busca	Periódicos Capes	Google Acadêmico
"privacy impact assessment" AND *"smart grid"* AND *"by design"*	5	158
"privacy impact assessment" AND *"smart grid"* AND *"cloud"* AND *"by design"*	0	87
"privacy impact assessment" AND *"smart grid"* AND *"untrusted cloud"* AND *"by design"*	0	0
"privacy impact assessment" AND *"smart grid"* AND *"secure cloud"* AND *"by design"*	0	3
"privacy impact assessment" AND *"smart grid"* AND *"cloud"* AND *"by design"* AND *"best practices"*	0	55
"privacy impact assessment" AND *"smart grid"* AND *"secure cloud"* AND *"by design"* AND *"best practices"*	0	3

Fonte: Autoria própria (2019)

Nota-se que há literatura que aborda os temas estudados na presente dissertação, contudo, há mais resultados que abordam os conceitos separadamente, sem necessariamente interligá-los ou apresentar guias sobre procedimentos. As seções seguintes descrevem a metodologia utilizada para o levantamento bibliográfico, a classificação dos conceitos e a análise de conteúdo para tratamento dos dados e prosseguimento da pesquisa.

3.3.2 Seleção do portfólio bibliográfico

Nesta fase do levantamento bibliométrico, os autores levantam uma gama de artigos relacionados ao tema de pesquisa, alinhados com sua percepção e inscritos nas delimitações impostas (ENSSLIN; ENSSLIN; PINTO, 2013). Os critérios de inclusão e exclusão de artigos, bem como os procedimentos empreendidos para sua coleta, serão tratados a seguir.

3.3.2.1 Seleção do Banco de Artigos Bruto

Para o levantamento do material que integrará o Banco de Artigos Bruto, primeiramente define-se os eixos de pesquisa alinhados à percepção dos pesquisadores sobre o tema (ENSSLIN; ENSSLIN; PINTO, 2013). Este trabalho busca propor um conjunto de práticas de gestão da informação e de tecnologias, para companhias de energia operando *Smart Grid* utilizando nuvens, que permitam o uso de dados das Unidades Consumidoras sem invasão à privacidade.

O primeiro eixo delimita o contexto do presente trabalho, a *Smart Grid*, incluindo os *Smart Meters*, peças chaves em sua implantação e desenvolvimento. O segundo eixo buscará elencar práticas de gerenciamento de privacidade enquanto o terceiro eixo foca especificamente no processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD) e no conceito de *Privacy by Design* em *Smart Grid*. O quarto eixo busca compreender o uso de *cloud* no contexto de *Smart Grid* com foco nos aspectos de privacidade e segurança.

Definidos os eixos de pesquisa, a etapa de formação do Banco de Artigos Bruto se deu por meio das fases de (a) definição das palavras-chave e *strings* de busca; (b) teste de aderência das palavras-chave; e (c) varredura nas bases de artigos otimizada pelo uso de operadores *booleanos*.

a) Definição de palavras-chave e s*trings* de busca

Iniciou-se a seleção dos artigos pela definição das palavras-chave e *strings* de busca para cada um dos eixos apresentados (CONFORTO; AMARAL; SILVA, 2011; ENSSLIN; ENSSLIN; PINTO, 2013;). Buscou-se utilizar palavras-chave em inglês por ser o principal idioma de indexação nas bases de dados (RUTHES; DA SILVA, 2015) e para contemplar possíveis variações dos termos em diferentes traduções. A busca atinge artigos publicados em outros idiomas, inclusive em português, que contenham o título, resumo ou palavras-chave em inglês (RUTHES; DA SILVA, 2015).

Para o primeiro eixo, relacionado à *Smart Grid*, foram definidas as seguintes palavras-chave para submissão ao teste de aderência: (i) *Smart Grid Privacy* ; (ii) *Smart Grid Data Privacy*; (iii) *Smart Grid Data Protection*; (iv) *Smart Grid Data Security*; (v) *Smart Meter Privacy*; (vi) *Smart Meter Data Privacy*; (vii*) Smart Meter Data*

Protection; (viii) *Smart Meter Data Security*; (ix) *Advanced Metering Infrastructure Privacy*; (x) *Advanced Metering Infrastructure Data Privacy*; (xi) *Advanced Metering Infrastructure Data Protection*; (xii) *Advanced Metering Infrastructure Data Security* (Grupo 1 de palavras-chave).

O segundo eixo relaciona-se ao objetivo de propor práticas para o gerenciamento de privacidade, com esta finalidade foram definidas as seguintes palavras-chave: (i) *Impact Assessment*; (ii) *Risk Assessment*; (iii) *Risk Management*; (iv) *Information Management* (v) *Framework*; (vi) *Guidelines*; e (vii) *Best-practices* (viii) *Template* (Grupo 2 de palavras-chave).

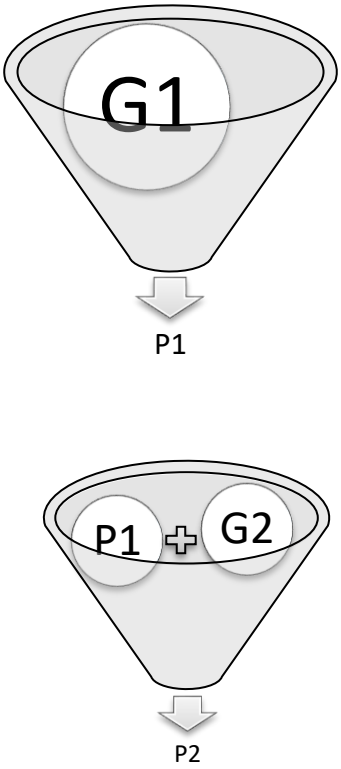
O terceiro eixo busca levantar material bibliográfico sobre o processo de Avaliação do Impacto à Privacidade e os conceitos de Privacidade por Desenho e Privacidade por Padrão no contexto de Smart Grid. Assim, foram definidas as palavras-chave (i) *Privacy Impact Assessment*; (ii) *Data Protection Impact Assessment*; (iii) *Data Privacy Impact Assessment*; (iv) *Privacy by Design*; e (v) *Privacy by Default*.

O quarto eixo levantará bibliografia sobre o uso de *cloud* em *Smart Grids* com foco em privacidade e segurança, utilizando as palavras-chave de contexto validadas do Grupo 1 em conjunto com a combinação de palavras-chave: (i) "*Secure Cloud*" OR "*Cloud Privacy*" OR "*Untrusted Cloud*" e (ii) "*Privacy*" OR "*Security*" OR "*Availability*" OR "*Trust*" OR "*by Design*".

b) Teste de Aderência das Palavras-chave

Os testes de aderência das palavras-chave foram realizados primeiramente com as palavras-chave do Grupo 1 isoladamente buscando identificar sua representatividade (R%) no total de artigos encontrados. Definidas as palavras-chave representativas (P1) realizou-se o teste de aderência para as palavras-chave do Grupo 2 em cruzamento com as palavras-chave validadas anteriormente (P1 x G2) conforme demonstra a Figura 2:

Figura 2 - Teste de Aderência das Palavras-chave dos grupos 1 e 2.



Fonte: Autoria própria (2019)

Realizou-se a pesquisa para cada um dos termos do Grupo 1 de palavras-chave no portal de periódicos CAPES e no buscador Google Acadêmico. A única restrição utilizada nesta etapa da pesquisa foi a limitação a periódicos revisados por pares no portal Capes. Optou-se por não restringir a busca por uma ou outra base específica pelo interesse particular em resultados multidisciplinares para o portfólio bibliográfico. Os resultados encontram-se dispostos na Tabela 3.

Tabela 3 - Teste de Aderência das Palavras-chave do grupo 1

Grupo 1 de palavras-chave		Periódicos Capes	R%	Google Acadêmico	R%
Smart Grid	*Privacy*	63	55,75%	946	56,44%
	Data Privacy	7	6,19%	54	3,22%
	Data Protection	0	0%	14	0,83%
	Data Security	0	0%	23	1,37%
Smart Meter	*Privacy*	33	29,20%	504	30,07%
	Data Privacy	9	7,96%	105	6,26%
	Data Protection	0	0%	4	0,23%
	Data Security	0	0%	15	0,89%
Advanced Metering Infrastructure	*Privacy*	0	0%	6	0,35%
	Data Privacy	1	0,88%	5	0,29%
	Data Protection	0	0%	0	0%
	Data Security	0	0%	0	0%
Total c/ duplicados		**113**	**100%**	**1676**	**100%**

Fonte: Autoria própria (2019)

Os testes de aderência para as palavras-chave do Grupo 1 demonstraram que, ainda que caracterizem pesquisas de temática similar, o termo "*Smart Grid*" é significativamente mais usual que "*Advanced Metering Infrastructure*". Além disto, os qualificadores "*Privacy*" e "*Data Privacy*" retornaram mais resultados que os qualificadores "*Data Protection*" e "*Data Security*". Assim, foram validadas pelo teste de aderência as palavras-chave **(i) "*Smart Grid Privacy*"; (ii) "*Smart Meter Privacy*"; e (iii) "*Smart Meter Data Privacy*"** (Palavras-chave P1).

Devido à utilização das palavras-chave do Grupo 2 ser extensa em diversas áreas de estudos, seu teste de aderência se deu em combinação com as palavras-chave validadas no grupo 1 (P1). O resultado encontra-se na Tabela 4:

Tabela 4 - Teste de Aderência das Palavras-chave do grupo 2

Palavras-chave P1	Grupo 2 de palavras-chave	Periódicos Capes	R%	Google Acadêmico	R%
"Smart Grid Privacy" OR *"Smart Meter Privacy"* OR *"Smart Meter Data Privacy"*	*Impact Assessment*	3	2,47%	104	5,42%
	Risk Assessment	0	0%	95	4,95%
	Risk Management	4	3,30%	73	3,80%
	Information Management	10	8,26%	100	5,21%
	Framework	64	52,89%	954	49,76%
	Guidelines	29	23,96%	398	20,76%
	Best-practices	8	6,61%	117	6,10%
	Template	3	2,47%	76	3,96%
Total c/ duplicados		**121**	**100%**	**1917**	**100%**

Fonte: Autoria própria (2019)

Os resultados demonstram que os descritores "*Framework*" e "*Guidelines*" retornaram a maior quantidade de produção científica. No portal Capes a terceira palavra-chave mais representativa foi "*Information Management*" enquanto no Google Acadêmico foi o termo "*Best-Practices*". Desta maneira, validou-se pelo teste de aderência as seguintes palavras-chave para o Grupo 2: **(i) "*Framework*"; (ii) "*Guidelines*"; (iii) "*Information Management*";** e **(iv) "*Best-Practices*".**

O Grupo 3 de palavras-chave, por procurar levantar processos e conceitos de nome específico, removeu os qualificadores "*Privacy*" e "*Data*" das palavras-chave de contexto do Grupo 1 para levantar os materiais que contivessem especificamente os termos desejados. Os resultados são os dispostos na Tabela 5.

Tabela 5 - Teste de Aderência das Palavras-chave do grupo 3

Grupo 1 de palavras-chave	Grupo 3 de palavras-chave	Periódicos Capes	R%	Google	R%
"Smart Grid" OR "Smart Meter" OR "Advanced Metering Infrastructure"	*Privacy Impact Assessment*	30	45,45%	325	22,21%
	Data Protection Impact Assessment	12	18,18%	182	12,44%
	Data Privacy Impact Assessment	0	0%	5	0,34%
	Privacy by Design	19	28,78%	839	57,34%
	Privacy by Default	5	7,57%	112	7,65%
Total c/ duplicados		**66**	**100%**	**1463**	**100%**

Fonte: Autoria própria (2019)

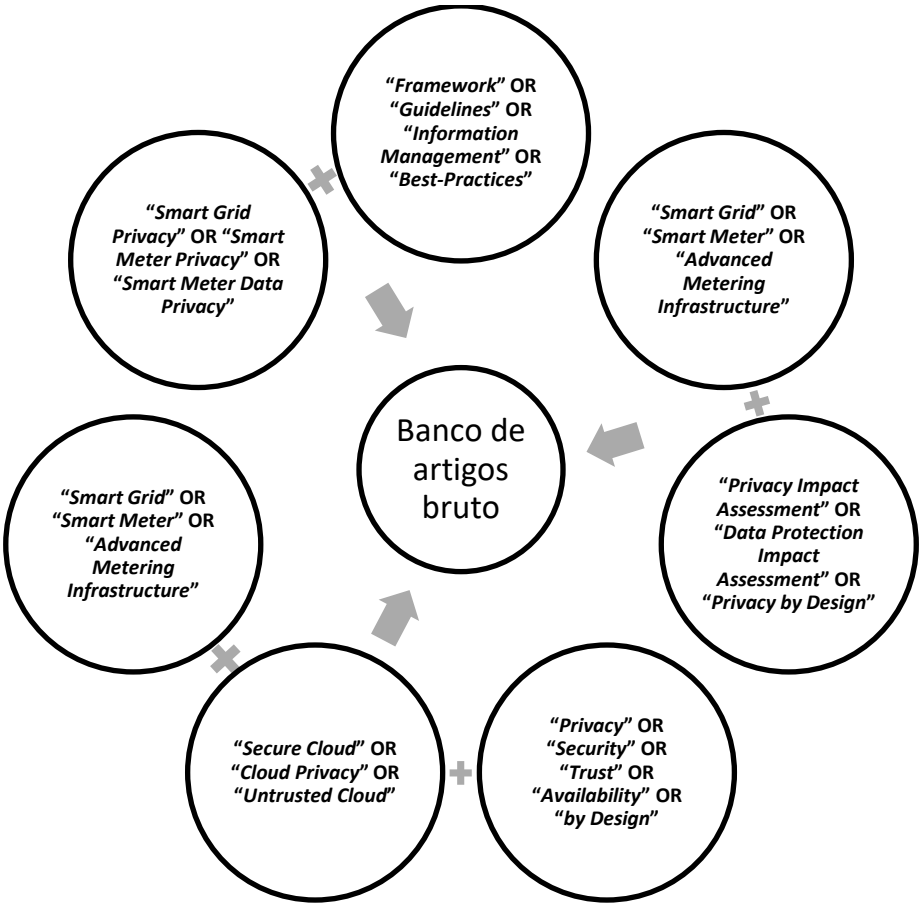
Nota-se que entre os processos pesquisados, o de Avaliação do Impacto à Privacidade é o que conta com maior produção acadêmica, contudo os termos Avaliação de Impacto à Proteção de Dados também são representativos nos resultados. Conforme mencionado anteriormente, os dois processos serão tratados indistintamente nesta dissertação. Entre os conceitos, o de Privacidade por *Design* é abordado por uma quantidade maior de material que o de Privacidade por Padrão. Assim, o teste de aderência para as palavras-chave do Grupo 3 resultou na adoção dos seguintes termos: **(i) "*Privacy Impact Assessment*"; (ii) "*Data Protection Impact Assessment*";** e **(iii) "*Privacy by Design*"** (Palavras-chave P3).

Para o quarto eixo definiu-se a *string* de busca que contivesse as palavras-chave de contexto P1 em combinação com as palavras-chave: (i) "*Secure Cloud*"; (ii) "*Cloud Privacy*"; e (iii) "*Untrusted Cloud*" em conjunto com os qualificadores: (i) "*Privacy*"; (ii) "*Security*"; (iii) "*Availability*"; (iv) "*Trust*"; e (v) "*by Design*", resultando na seguinte *string* de busca: **("*Smart Grid*" OR "*Smart Meter*" OR "*Advanced Metering Infrastructure*") AND ("*Secure Cloud*" OR "*Cloud Privacy*" OR "*Untrusted Cloud*") AND ("*Privacy*" OR "*Security*" OR "*Trust*" OR "*by Design*")**

Desse modo, o levantamento validado pelo teste de aderência para o Banco de Artigos Bruto se dará pelas seguintes *strings* de busca: **(i) ("*Smart Grid Privacy*" OR "*Smart Meter Privacy*" OR "*Smart Meter Data Privacy*") AND ("*Framework*" OR "*Guidelines*" OR "*Information Management*" OR "*Best-Practices*")**; **(ii) ("*Smart Grid*" OR "*Smart Meter*" OR "*Advanced Metering Infrastructure*") AND ("*Privacy Impact Assessment*" OR "*Data Protection Impact Assessment*" OR "*Privacy by Design*");** e **(iii) ("*Smart Grid*" OR "*Smart Meter*" OR "*Advanced***

***Metering Infrastructure*”) AND (“*Secure Cloud*” OR “*Cloud Privacy*” OR “*Untrusted Cloud*”) AND (“*Privacy*” OR “*Security*” OR “*Trust*” OR “*Availability*” OR “*by Design*”)** conforme ilustrado pela Figura 3.

Figura 3 - Formação do banco de artigos bruto



Fonte: Autoria própria (2019)

Concluída esta etapa obteve-se o banco de artigos bruto com um total de 187 referências que foram submetidas às próximas análises.

3.3.2.2 Filtragem dos artigos

Nesta etapa é realizada a filtragem dos artigos obtidos na etapa anterior. Os resultados obtidos até esta etapa resultaram no banco de artigos bruto que ainda conta com artigos duplicados e potencialmente sem alinhamento com o tema. Para esta etapa do processo são considerados: (a) a presença de artigos duplicados; (b) o

alinhamento dos títulos e resumos dos artigos com o tema; e (c) o reconhecimento científico dos artigos (ENSSLIN; ENSSLIN; PINTO, 2013).

Os resultados obtidos após a varredura das bases indexadas no Portal Capes foram exportados por meio de ferramenta própria do site e importadas para o *software* gerenciador de referências Zotero, totalizando 187 itens. Após a importação dos artigos foram removidos os itens duplicados, resultando em um total de 152 artigos para a análise de alinhamento de: (i) títulos e subtítulos; (ii) resumos; e (iii) palavras-chave (RUTHES; DA SILVA, 2015).

Realizada esta análise, foram excluídos 54 artigos considerados não alinhados à pesquisa, alguns por tratarem o tema apenas tangencialmente ou outros por tratarem de situações ou tecnologias específicas sem reprodutibilidade ou generalização imediata para o escopo desta dissertação. Um total de 72 artigos foram considerados alinhados à pesquisa e passaram a compor o **Portfólio de Interesse**. Outros 26 artigos foram considerados de interesse, porém sem alinhamento direto, tendo sido agrupados no **Portfólio Complementar**.

3.3.2.3 Análise Sistêmica

Obtido o Banco de Artigos Bruto não Repetidos, composto pelo Portfólio de Interesse e pelo Portfólio Complementar, inicia-se a fase de análise bibliométrica para verificar a representatividade e o reconhecimento científico do material levantado. Tais artigos foram exportados do *software* Zotero para uma tabela no formato CSV com a finalidade de serem tabulados e ordenados em relação ao seu grau de reconhecimento científico. Como métrica de reconhecimento científico utilizou-se o número de citações de cada artigo no site Google Acadêmico (ENSSLIN; ENSSLIN; PINTO, 2013).

Para os dois portfólios obtidos, estipulou-se que serão representativas 90% das citações, contudo, cumpre ressaltar que artigos de autoria recente podem ainda não ter tido seu reconhecimento confirmado, motivo pelo qual não serão excluídos por este critério (Critério 1). Assim, os artigos menos citados, mas publicados nos dois últimos anos continuarão no processo de filtragem. Os critérios de decisão sobre a inclusão de artigos recentes foram os seguintes: O artigo é de algum dos autores mais citados? (Critério 2); O artigo é de algum dos autores do *corpus* estático? (Critério 3); O artigo cita os autores mais citados ou do *corpus* estático? (Critério 4).

Realizada tal filtragem, foram excluídos do Portfólio de Interesse 17 artigos, resultando em um Portfólio de Análise (PA) de 55 artigos. A mesma filtragem realizada no Portfólio Complementar levou à exclusão de 7 artigos, resultando em um Portfólio Complementar de 19 artigos. Para fins didáticos as tabelas contendo todas as referências do Portfólio de Análise e do Portfólio Complementar encontram-se nos Apêndices 1 e 2, respectivamente.

Em vista do objetivo geral deste trabalho, propor um conjunto de medidas de proteção de dados pessoais que precisariam ser consideradas no planejamento e operação de *Smart Grid* utilizando computação em nuvem, o levantamento bibliográfico fundado em análise bibliométrica fornecerá subsídios suficientes para a condução do processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD). O processo será apoiado pela metodologia de Advanced CPTM (GHOLAMI *et al*., 2016) para posterior obtenção do relatório de impacto à proteção de dados pessoais. O relatório é o produto do processo de AIPD e conterá as recomendações e práticas mais disseminadas na literatura. A próxima etapa desta seção de metodologia descreverá a técnica de Análise de Conteúdo empreendida para informar os processos de AIPD e de modelagem de ameaças.

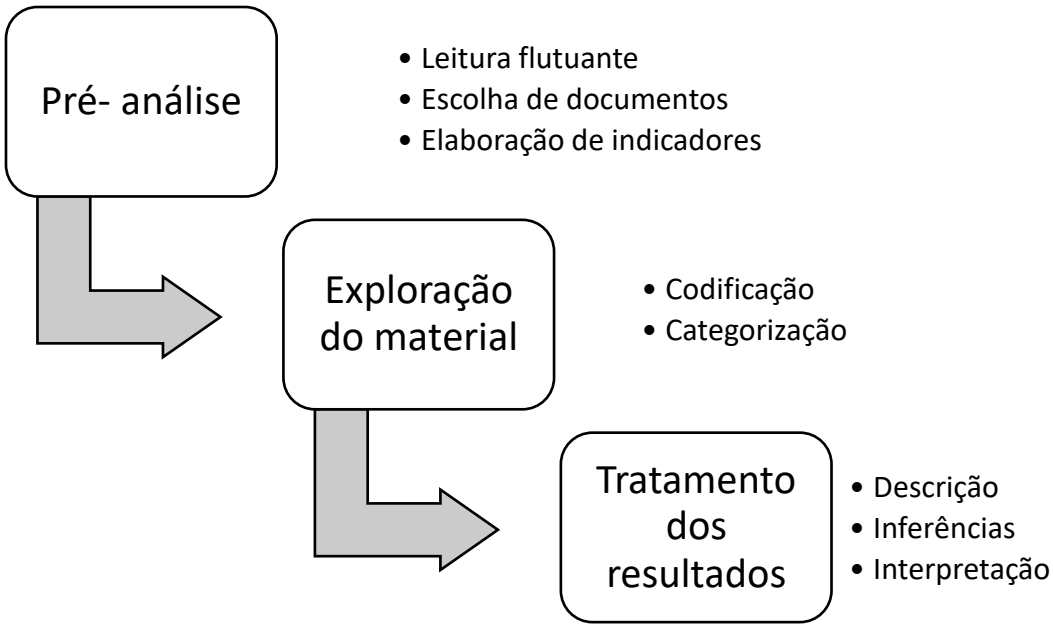
3.4 ANÁLISE DE CONTEÚDO

Obtidos os materiais que darão suporte à pesquisa por meio das etapas anteriores de levantamento bibliográfico, parte-se à análise do portfólio bibliográfico. As técnicas utilizadas foram as de Análise de Conteúdo conforme propostas por Bardin (2011), que trata de método empírico e envolve tanto procedimentos quantitativos, como na contagem de palavras e frequência de incidência de temas, quanto procedimentos qualitativos, na identificação de referenciais e características no elemento analisado (BARDIN, 2011).

O processo da análise de conteúdo pode ser dividido em três fases gerais (BARDIN, 2011): 1) pré-análise, 2) exploração do material e 3) tratamento dos resultados, inferência e interpretação. A fase inicial compreende organização do material e realização de leitura flutuante para a seleção dos materiais alinhados à pesquisa, além da definição inicial de indicadores. A segunda fase ocorre pela exploração do material selecionado utilizando-se de codificação para a marcação do material e posterior categorização, definindo as Categorias de Contexto, Categorias

de Análise, Unidades de Registro e Unidades de Contexto. A última etapa contempla o desenvolvimento das inferências, a análise dos resultados em si. As etapas do processo encontram-se sintetizadas na Figura 6.

Figura 4 - Fases da Análise de Conteúdo



Fonte: Adaptado de Bardin (2011)

As etapas realizadas nesta dissertação serão descritas nas próximas seções.

3.4.1 Pré-análise

Nesta etapa o material é organizado e selecionado. Esta fase da análise de conteúdo abrange a leitura flutuante, a escolha dos documentos e a elaboração de indicadores. Bardin (2011) ressalta que a escolha dos dados analisados deve atender aos critérios de exaustividade, representatividade, homogeneidade e pertinência. No presente trabalho estes procedimentos ocorreram nas etapas de seleção do portfólio bibliográfico e encontram-se dispostos na seção 3.3 Pesquisa bibliométrica. Foram atendidos os critérios estabelecidos acima na seleção do portfólio bibliográfico pela realização dos testes de aderência das palavras-chave com foco na exaustividade e representatividade dos resultados bem como pelo uso de técnicas bibliométricas para complementar a seleção e satisfazer os critérios de homogeneidade e pertinência.

3.4.2 Exploração do material

Para a exploração do material é realizada sua categorização em conjuntos progressivamente mais restritivos e específicos contendo materiais com características comuns. Esta fase é definida como “operação de classificação de elementos constitutivos de um conjunto por diferenciação e, em seguida, por reagrupamento segundo gênero (analogia), com critérios previamente definidos” (BARDIN, 2011, p. 147).

Essa autora subdivide as categorias em 4 grupos progressivamente excludentes: 1) Categorias de Contexto: mais amplas e relacionadas aos objetivos de pesquisa; 2) Categorias de Análise: divisão das categorias de contexto e indicativas dos elementos a serem analisados; 3) Unidades de Registro: palavras que explicam a categoria de análise; e 4) Unidades de Contexto: parágrafo ou fragmento que explica a unidade de registro (BARDIN, 2011).

As categorias de contexto foram definidas com base nos objetivos da pesquisa e nos resultados da revisão de literatura, tendo sido as seguintes: a) *Privacy by Design*, b) Ameaças à privacidade e c) Contramedidas. Tais categorias informaram o reagrupamento do material obtido e possibilitaram a primeira definição das Categorias de Análise. Inicialmente as Categorias de Análise foram definidas qualitativamente pela leitura dos textos e identificação de agrupamentos temáticos. A distribuição dos textos do Portfólio de Análise nas categorias de contexto foi a seguinte:

a) *Privacy by Design*: 12 referências

b) Ameaças à privacidade: 17 referências

c) Contramedidas: 26 referências

Os materiais foram reagrupados com o auxílio do *software* Zotero e novamente analisados, desta vez em cada conjunto, para a definição das categorias de análise e posteriormente das unidades de registro e de contexto.

Utilizou-se o recurso de contagem de palavras para cada um dos grupos de textos das categorias de contexto iniciais na expectativa de definir as categorias de

análise apoiando-se também em critérios quantitativos, contudo, os resultados não foram significativos. Por exemplo, para o grupo de textos da categoria de contexto "*Privacy by Design*" as palavras mais recorrentes foram, respectivamente "*data*" (2,17% do total); "*privacy*" (1,79%) e "*smart*" (0,9%), que se mostram pouco úteis na definição de categorias de análise. Mesmo quando excluídas as palavras genéricas mais repetidas, as palavras seguintes continuavam pouco significativas, conforme pode ser constatado no ANEXO 1. Assim, procedeu-se à nova análise qualitativa para a categorização final dos textos.

3.4.3 Definição das Categorias de Análise finais

Em função do objetivo geral deste trabalho, propor um conjunto de medidas de proteção de dados pessoais que precisariam ser consideradas no planejamento e operação de *Smart Grid* utilizando computação em nuvem, definiu-se que as categorias de contexto a serem exploradas seriam I) *Privacy by Design* e II) *Smart Grid*.

Inicialmente a categoria de contexto *Privacy by Design* seria subdividida em 7 categorias de análise referentes aos seus 7 princípios fundacionais (CAVOUKIAN, 2010a), contudo, conforme apresentado na seção de fundamentação teórica sobre o tema, os princípios apresentados oferecem uma visão pouco aplicável do conceito, sob o ponto de vista de desenvolvimento de sistemas. De acordo com Gurses, Troncoso e Diaz (2015), o que deve nortear a aplicabilidade do conceito de *Privacy by Design*, além do sentido geral de prevenção, é a busca pela minimização de dados, no estado da arte em que puder ser obtida, o que levou à definição das categorias de análise "Preventiva" e "Minimização de dados". A prevenção em *PbD* tem a função de evitar a concretização do risco e garantir direitos da personalidade (CAVOUKIAN; POLONETSKY; WOLF, 2010), assim, definiu-se também a categoria de análise "Respeito ao usuário" para o contexto de *PbD*. Desta forma, as categorias de análise definidas para a primeira categoria de contexto foram: a) Preventiva; b) Minimização de dados e c) Respeito ao usuário.

A categoria de análise "Preventiva" contempla as unidades de registro: "Evitar concretização do risco", que é o objetivo da tomada de medidas previamente, preferencialmente antes de danos ocorrerem (VAN DIJK; GELLERT; ROMMETVEIT,

2016) e “No planejamento”, que é o momento no qual a tomada de medidas deve ocorrer para ser mais eficaz (CAVOUKIAN; POLONETSKY; WOLF, 2010).

A minimização de dados pode ser obtida por meio de limitação de coleta, especificação de necessidade, de-identificação (anonimização) e criptografia (GURSES; TRONCOSO; DIAZ, 2015), tendo sido estas as unidades de registro para a categoria de análise “Minimização de Dados”.

O “respeito ao usuário” sintetiza o objetivo de garantia de direitos que possuem os princípios de *PbD* e foi dividida em “proteção de dados” que deve ser assegurada ao usuário, parte mais frágil da relação (MANTELERO, 2014) e “por padrão”, partindo do pressuposto que a proteção deva ser garantida mesmo sob inércia do usuário (ROMANOU, 2018).

No contexto de *Smart Grid* é interesse desta dissertação investigar o uso de computação em nuvem para a condução do processo de AIPD que leve em consideração as características particulares do meio. A função de *Smart Metering* é também eleita como categoria de análise por serem os perfis de consumo energético a maior fonte das preocupações de privacidade no sistema, além da categoria que trata da principal característica diferenciadora da *Smart Grid* para a Rede Elétrica tradicional, o fluxo bidirecional de informação e energia. Logo, para a segunda categoria de contexto foram definidas as seguintes categorias de análise: a) Bidirecional; b) *Cloud* e c) *Smart metering*. O fluxo bidirecional de “informação e energia” (unidade de registro) é uma das características essenciais da *SG* (PARVEZ *et al.,* 2016) e condição que permite o “gerenciamento da demanda” (unidade de registro), pela alocação de cargas e pela conscientização do usuário (WEN et al., 2015).

Para a categoria de análise “Cloud” escolheu-se como unidades de registro características essenciais do modelo, que trazem vantagens e riscos simultaneamente. Foram elas: “Onipresente” (ubiquitous) pelo fato de que a localização física dos servidores da nuvem não é essencial, devido a sua outra característica de Acesso amplo pela rede (MELL; GRANCE, 2011) o consumidor pode acessar as informações de qualquer servidor em qualquer localidade. Ao mesmo tempo, o controlador de dados pode estar em qualquer localidade, sujeito a uma variedade de leis (TENE, 2011); “Escalável”, devido à capacidade que o modelo de computação em nuvem tem de expandir sua alocação de recursos rapidamente de acordo com a necessidade (BAEK et al., 2015), levando aos problemas de

“Proliferação de dados”, quando a informação possa ser replicada diversas vezes, escapando à capacidade de controle do contratante e impedindo que ele possa saber com precisão qual ou quais entidades estão responsáveis pelas suas informações (CAVOUKIAN; POLONETSKY; WOLF, 2010).

Na categoria de análise “*Smart metering*” a primeira unidade de registro definida foi “Classificação/ *profiling*” que é a preocupação sobre o mau uso das informações de consumo energético para inferências e criação de perfis de consumidores de forma discriminatória (MANTELERO, 2016). Os riscos sobre os “usos secundários” também estão presentes e decorrem do desrespeito aos princípios de Finalidade, Adequação e Necessidade (BRASIL, 2018). É possível associar o conjunto de dados de consumo energético a técnicas de *Big Data* e obter inferências que se distanciam do propósito da coleta (MANTELERO, 2016).

A localização do *SM* no interior da Unidade Consumidora (UC) gera preocupação quanto à “fronteira do lar” que pode ocorrer na medida em que pode revelar comportamentos do interior da UC, tida como inviolável (MCNEIL, 2011). As limitações técnicas dos *SM* são um fato que deve ser considerado no planejamento do sistema (RIAL; DANEZIS, 2011), de modo que uma sugestão de solução não deve incorrer em realização de computações complexas no âmbito do medidor.

O Quadro 3 demonstra a categorização final obtida e traz exemplos de Unidades de Contexto para as Unidades de Registro definidas.

Quadro 3 - Definição das Categorias de Análise, Unidades de Registro e Contexto finais

(Continua)

CATEGORIAS DE CONTEXTO	CATEGORIAS DE ANÁLISE	UNIDADES DE REGISTRO	UNIDADES DE CONTEXTO (tradução e grifos nossos)
Privacy by Design	**Preventiva**	Evitar concretização do risco	AIPDs ocuparão uma posição central conforme são encarregadas de descobrir ("avaliar") os riscos à privacidade, proteção de dados e liberdades fundamentais, **quanto antes possível no planejamento e execução** de um projeto que envolva o processamento de dados pessoais, **preferencialmente antes que qualquer dano ocorra** (VAN DIJK; GELLERT; ROMMETVEIT, 2016).
		No planejamento	**Aqueles que falham** em vislumbrar requerimentos de privacidade **no começo do desenvolvimento** de tecnologias, práticas de negócios ou espaços físicos e infraestrutura **terão menor probabilidade de oferecer proteção completa**, a despeito da presença de outros elementos (CAVOUKIAN; POLONETSKY; WOLF, 2010)
	Minimização de dados	Limitação de coleta / necessidade	**As seguintes características** do sistema holandês de medição inteligente **não se mostraram necessárias em uma sociedade democrática**: a geração e transmissão de leituras a cada quinze minutos ou a cada hora; a leitura diária para os gerentes da rede e fornecedores; e a implantação obrigatória dos medidores inteligentes em todas as casas (CUIJPERS; KOOPS, 2013)
		De-identificação	De modo geral, **os métodos para de-identificar informações pessoais incluem pseudonimização, agregação, redução de dados, supressão de dados e ocultação de dados**. **Contudo**, não é fácil de seguramente proteger informações pessoais nas informações de medição da Rede Elétrica Inteligente (REI) **apenas com estes métodos** (LEE et al., 2018).
		Criptografia	**Criptogradia dos dados** na REI, do medidor à companhia de energia é uma ferramenta útil na prevenção de invasões, preservando assim a confidencialidade da informação (BARI et al., 2014).
	Respeito ao usuário	Proteção de dados	Autoridades de proteção de dados, e não consumidores, têm o conhecimento tecnológico para avaliar os riscos associados ao processamento dos dados e podem adotar medidas legais para endereçá-los. [...] A sugestão não é mudar o modelo tradicional de proteção de dados, mas remodela-lo com relação ao contexto de *Big Data* e outros contextos nos quais a assimetria na negociação das informações drasticamente reduz a autodeterminação dos usuários (MANTELERO, 2014).
		Por padrão	Usuários ou consumidores **devem estar protegidos sem nenhuma outra ação de sua parte**. Deste modo, mesmo menores de idade ou indivíduos que não estão familiarizados o suficiente com tecnologia podem estar previamente protegidos (ROMANOU, 2018).

(Conclusão)

CATEGORIAS DE CONTEXTO	CATEGORIAS DE ANÁLISE	UNIDADES DE REGISTRO	UNIDADES DE CONTEXTO
Smart Grid	**Bidirecional**	Energia / Informação	A Rede Elétrica Inteligente é o sistema moderno de energia elétrica utilizando um sistema inovador de comunicação e distribuição para entregar eletricidade ao usuário final com melhora no monitoramento, controle e eficiência. Uma característica anunciada da REI é a **interação entre suas entidades utilizando comunicação bidirecional** (PARVEZ et al., 2016).
		Gerenciamento de demanda	A ideia geral de controle de demanda é ainda muito similar ao paradigma tradicional, que envolve diretamente controlar as "cargas interrompíveis" ou **estimular os consumidores a alterarem seu uso de energia por meio da variação nos preços da eletricidade** (WEN et al., 2015).
	Cloud	Onipresente (ubiquitous)	Com o aumento da computação em nuvem e a proliferação de aplicativos móveis e *online*, não somente a identidade mas também a localização dos controladores de dados se torna indeterminada (TENE, 2011)
		Escalável	Ao empregarmos computação em nuvem em REIs, não somente endereçamos o problema de gerenciamento de grandes quantidades de informação como também oferecemos uma plataforma de alta economia de custos e energia. Isto se dá pois 1) **o *framework* pode ser escalado rapidamente para lidar com as mudanças de processamento de informações** e 2) pode oferecer alta utilização de recursos computacionais (BAEK et al., 2015)
		Data proliferation	**Proliferação de informações,** controles fracos e supervisão insuficiente destas informações **pode levar a invasões sem precedentes da privacidade do consumidor.** (CAVOUKIAN; POLONETSKY; WOLF, 2010)
	Smart metering	Classificação / Profiling	O uso de informações pessoais e análises de *big data* para apoiar decisões excede as fronteiras da dimensão individual e assume uma dimensão coletiva, com consequências potencialmente danosas para alguns grupos. Neste sentido, preconceito pode resultar não somente de riscos conhecidos relacionados à privacidade (ex. uso ilegítimo de informações pessoais, segurança da informação) mas também de **formas discriminatórias e invasivas de processamento de dados** (MANTELERO, 2016).
		Usos secundários	Análises de *big data* possibilitam a inferência de **informações preditivas** de uma grande quantidade de dados para obter conhecimento mais aprofundado sobre indivíduos e grupos, **que podem não necessariamente estar relacionadas ao propósito inicial da coleta dos dados** (MANTELERO, 2016).
		Limitações técnicas dos *SM*	Medidores precisam ser baratos e como resultado têm **banda e conexão limitadas**. Eles oferecem uma **interface de usuário limitada** que não pode entregar informações sobre o uso de energia, dicas de eficiência ou o detalhamento da conta (RIAL; DANEZIS, 2011).
		Fronteira do lar	A informação gerada pelos medidores inteligentes cria preocupações individuais de privacidade devido ao consumo de energia da unidade consumidora, particularmente quando medido quase em tempo real e relacionado à sua fonte, **revela uma quantidade alarmante de informações sobre a vida e o comportamento dentro do lar** (MCNEIL, 2011).

Fonte: Autoria própria (2019)

Esta categorização foi utilizada para subsidiar a condução do processo de AIPD bem como as etapas de modelagem de ameaças em computação em nuvem. O processo de AIPD foi conduzido com o objetivo de atender os requisitos da legislação nacional e promover os conceitos de *Privacy by Design*, os quais foram sintetizados e incluídos na Análise de Conteúdo.

4 APRESENTAÇÃO E DISCUSSÃO DOS RESULTADOS

Valendo-se do material documental, *corpus* estático e *corpus* dinâmico, este último obtido por meio de levantamento bibliográfico descrito no Capítulo 3 - METODOLOGIA DA PESQUISA, foi conduzido um processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD) em *Smart Grid* (*SG*) para se obter um conjunto de medidas de proteção de dados que considerem a privacidade na concepção do projeto e em suas múltiplas dimensões.

O processo se deu em linhas gerais pois a natureza de uma AIPD requer que a pessoa ou organização responsável por sua condução, o controlador, tenha o conhecimento de todos os fluxos informacionais e processos internos. Este trabalho não se configura como estudo de caso, portanto, o processo se deu sobre um modelo conceitual de *Smart Grid* que foi estabelecido em função dos Requisitos de Privacidade elencados na modelagem de ameaças, conforme descrito no item 3.2.2 Especificação de ambiente de nuvem da seção de Metodologia da Pesquisa.

A Resolução Normativa nº 502 da Aneel prevê que procedimentos e tecnologias devem ser adotados para garantir a segurança dos dados trafegados e das informações de caráter pessoal oriundas das Unidades Consumidoras (ANEEL, 2012) conforme discutido no item 2.3.2 Aspectos regulatórios de *Smart Grid* (*SG*). Contudo, a Resolução não especifica quais técnicas ou procedimentos deverão ser adotados para a garantia da segurança dos dados. A ausência de medidas educacionais ou comunicação de benefícios, somada à dependência de escolha do consumidor para o uso de *smart meters* em sua casa, gera dúvidas quanto ao desenvolvimento do sistema no Brasil (CARVALHO, 2015).

A ausência de framework impossibilita a criação de um modelo de negócios para os atores envolvidos em *Smart Grid* e indica ser o primeiro ponto que deve ser considerado pelos Ministérios responsáveis, seguido pelo estabelecimento de políticas públicas federais definindo a implantação e considerando a multiplicidade de agentes de mercado, sob pena de prejudicar a interoperabilidade da rede (CARVALHO, 2015).

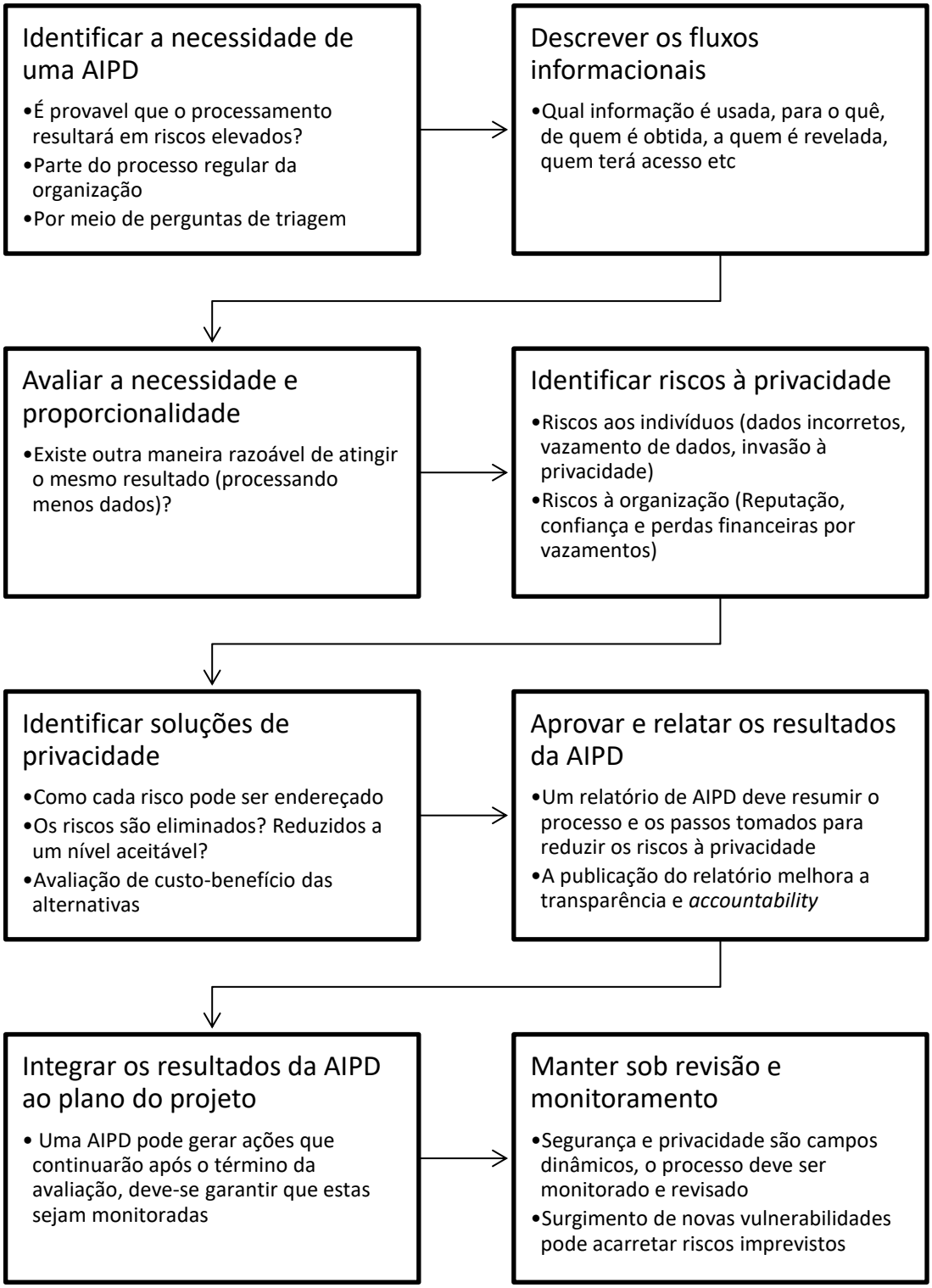
O relatório de impacto à proteção de dados pessoais, produto da AIPD, apresenta os resultados encontrados e contém a resposta à pergunta de pesquisa, propondo um conjunto de medidas de proteção de dados pessoais que precisariam

ser consideradas no planejamento e operação de *Smart Grid* utilizando computação em nuvem.

4.1 CONDUÇÃO DA AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS

Uma Avaliação de Impacto à Proteção de Dados Pessoais é um processo para analisar as atividades de processamento de dados sistematicamente e extensivamente para auxiliar o controlador a identificar e minimizar os riscos à proteção de dados (ICO,2018) e é discutido mais detalhadamente na seção 2.2 AVALIAÇÃO DE IMPACTO À PROTEÇÃO DE DADOS PESSOAIS desta dissertação. Com base em documentação produzida pelo Article29 Working Party da União Europeia (WP29, 2017) e pelo Information Commissioner's Office do Reino Unido (ICO, 2014, 2018), o processo de Avaliação de Impacto à Proteção de Dados Pessoais (AIPD) é representado na Figura 5.

Figura 5 - Etapas do processo de Avaliação de Impacto à Proteção de Dados Pessoais



Fonte: Adaptado de WP29 (2017) e ICO (2014, 2018)

O primeiro passo para a realização de uma AIPD é identificar a necessidade de realização do processo. Na seção seguinte foi iniciado o processo utilizando-se as

contribuições da Análise de Conteúdo e da revisão de literatura para responder às questões que norteiam sua condução.

4.1.1 Identificar a necessidade de uma AIPD

A organização pode já ter em seu processo regular de projetos o requerimento de condução de uma AIPD, contudo, quando não exista tal previsão é possível identificar a necessidade do processo através de algumas perguntas de triagem. As perguntas de triagem aqui utilizadas para determinar a necessidade de uma AIPD são (ICO, 2014, p.33, tradução nossa):

- O projeto envolve a coleta de novas informações sobre indivíduos?
- O projeto obrigará indivíduos a fornecerem informações sobre si?
- A informação sobre indivíduos será revelada a organizações ou pessoas que não a acessavam previamente?
- A informação será utilizada com propósito diferente do atual?
- O projeto envolve o uso de novas tecnologias que podem ser percebidas como invasivas à privacidade?
- O projeto resultará em tomada de decisões ou ações contra indivíduos de maneira que os impacte significativamente?
- A informação sobre indivíduos é de um tipo sensível, provável de levantar preocupações de privacidade?
- O projeto requererá o contato com indivíduos de modos que podem ser tidos como invasivos?

Os objetivos do projeto, bem como suas vantagens à organização e aos indivíduos devem ser explicitados, e em caso de resposta positiva a pelo menos uma das perguntas de triagem em função dos objetivos esperados recomenda-se a condução de uma AIPD.

A revisão de literatura identificou, na documentação produzida pelo ICO (2018), o processamento de dados por *Smart Meter* como uma espécie da categoria de criação de perfis em larga escala que, nas regras da GDPR, obrigam à condução do processo. Não há na legislação brasileira circunstâncias que indiquem a obrigatoriedade de condução de avaliação sistemática de riscos à proteção de dados pessoais, contudo, depreende-se da literatura que tal processo é necessário, considerando-se as perguntas de triagem expostas previamente.

O material identificado na Análise de Conteúdo para a definição das categorias de análise para a categoria de contexto *Smart Grid* oferece resposta

afirmativa a todas as perguntas de triagem, portanto, conclui-se que é recomendada a condução de AIPD para a implantação de *Smart Grid*.

Pela AC conduzida previamente, nota-se que no contexto de *Smart metering* a criação de perfis comportamentais, combinação com técnicas de *big data* e reuso dos dados para propósitos distintos dos coletados (MANTELERO, 2016) responde afirmativamente às perguntas: “A informação será utilizada com propósito diferente do atual?” e “O projeto envolve o uso de novas tecnologias que podem ser percebidas como invasivas à privacidade?”. Já a pergunta “A informação sobre indivíduos é de um tipo sensível, provável de levantar preocupações de privacidade?” também possui resposta afirmativa derivada das preocupações de invasão do lar (MCNEIL, 2011) e da possibilidade de invasão à privacidade decorrente da proliferação dos dados de *SM* (CAVOUKIAN; POLONETSKY; WOLF, 2010).

Além do material que informou as unidades de registro “*Profiling*” e “Usos secundários” na categoria de análise “*Smart metering*”, mais diretamente relacionado ao aumento da coleta de informações possivelmente pessoais, o material que informa a categoria de análise “*Cloud*” oferece resposta afirmativa à pergunta “A informação sobre indivíduos será revelada a organizações ou pessoas que não a acessavam previamente?” pela característica de onipresença da computação em nuvem o controlador de dados muitas vezes é indeterminado (TENE, 2011) e reforça a conclusão de que a implantação da *SG* deve ser precedida por uma AIPD.

Tendo sido considerado necessário, as próximas seções prosseguiram com o processo de AIPD com o auxílio de etapas da metodologia de modelagem de ameaças de privacidade em nuvem.

4.1.2 Requisitos de privacidade (RP)

A definição dos requisitos de privacidade (RP) é parte da condução do processo de modelagem de ameaças utilizado (*Advanced Cloud Privacy Threat Modeling*) e informa o desenvolvimento do sistema com privacidade desde a concepção.

Os requisitos de privacidade foram selecionados da LGPD e são os princípios de observância obrigatória para o tratamento de dados pessoais no país. A escolha pela legislação brasileira como fonte para os requisitos de privacidade pretende contribuir com os estudos sobre a recente legislação e ao mesmo tempo prover

recomendações que sirvam também como forma de *compliance* legal. Os RP serão numerados de 1 a 10 e correspondem a cada inciso do artigo 6º da LGPD (BRASIL, 2018):

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - segurança: utilização de medidas 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 difusão;
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Estes Requisitos de Privacidade (RP) foram contra os quais as Ameaças (A) foram identificadas e os que as Contramedidas (C) buscaram proteger.

4.1.3 Descrever os fluxos informacionais

Esta etapa relaciona-se à etapa descrita na metodologia no item 3.2.2 Especificação de ambiente de nuvem e leva em consideração as recomendações dos dois processos.

Em uma AIPD executada sobre um projeto real, os fluxos de dados devem ser descritos da maneira mais detalhada possível, indicando qual informação é utilizada, com qual função, coletada de quem, revelada a quem, passível de acesso por quem,

armazenada por quanto tempo e deletada quando (ICO, 2018). Ressalta-se que o modelo de dados SecureCloud aqui disposto é teórico e proposto para investigar o planejamento de *SG* como possível caso de aplicação do processo de AIPD. Esta dissertação não se configura como estudo de caso.

O modelo de dados SecureCloud é composto pelos seguintes atores:

(I) Unidade Consumidora: O sujeito de dados. O *Smart Meter* localiza-se em suas dependências e relata informação o suficiente para prover ao consumidor o valor correto de sua conta de consumo;

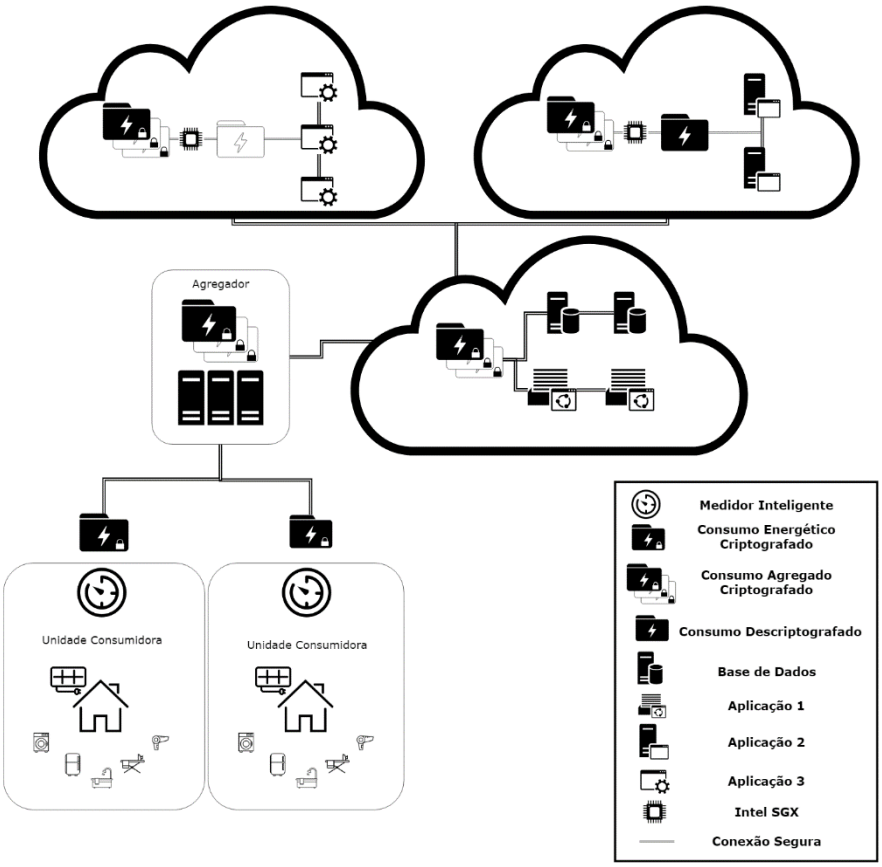
(II) *Smart Meter* inviolável: O *SM* não pode ser violado e tem a capacidade de criptografar e assinar digitalmente a informação de consumo;

(III) Agregador: O controlador de dados. O sistema responsável por coletar e agregar os dados provenientes dos *SM* e pelas operações da rede, como gerenciamento de demanda. Segurança, controle e administração podem ser responsabilidade da Companhia de Energia ou serem compartilhadas com terceiro.

(IV) A nuvem: O processador de dados. Modalidade de serviço *Infrastructure as a Service* contratada em nuvens públicas. Este modelo de serviço é requisito para que o hardware responsável pelas operações criptográficas (IntelSGX) possa ser acessado. A depender da aplicação desejada, a administração e controle podem ser de responsabilidade da Companhia de Energia ou de subcontratado que acessa estritamente o mínimo de informação necessário para realizar suas funções.

O *SM* (II) mede o consumo da Unidade Consumidora (I) e transmite somente a informação necessária ao Agregador (III) que pode armazenar, processar e/ou transmitir essa informação à nuvem (IV) para subsequente processamento. O consumo detalhado é criptografado no nível do *SM* (II) e somente descriptografada se/quando necessário, pela aplicação desejada na região de execução protegida do processador, em servidor acessível na nuvem (IV), conforme Figura 6.

Figura 6 - Modelo de fluxo de dados SecureCloud



Fonte: Autoria própria (2019)

4.1.4 Avaliar a necessidade e proporcionalidade

Nesta etapa o controlador deve se guiar pelo objetivo que pretende atingir, sem se prender à implementação que espera executar, assim, com foco na finalidade do projeto, deve ser identificada a alternativa de implementação que ofereça menos riscos à proteção de dados. Conforme exposto ao longo deste trabalho, o foco da implementação de *Privacy by Design* deve ser o de minimização de dados (GURSES; TRONCOSO; DIAZ, 2015), uma das categorias de análise da categoria de contexto *PbD*, da qual os princípios de Limitação de coleta e estrita necessidade decorrem.

A decisão de reverter a obrigatoriedade de instalação dos *smart meters* na Holanda considerou que os envios de informações aos administradores da rede em intervalos de 25, 60 minutos e 24 horas, além da obrigatoriedade de instalação dos *smart meters* não eram necessários ou excediam a necessidade (CUIJPERS; KOOPS, 2013). No mesmo sentido, Rial e Danezis (2011) argumentam que é falsa a alegação que um equilíbrio deve ser encontrado entre a necessária invasão dos *smart*

meters e o benefício social da *Smart Grid* ao demonstrarem modelo que não revela informações pessoais e cumpre as funções de preço dinâmico. A diferença do modelo proposto pelos autores para o modelo SecureCloud reside no âmbito em que ocorrem as computações de privacidade.

Conforme consta da Unidade de Registro “Limitações técnicas dos SM” os *SM* não possuem grandes capacidades computacionais, assim os autores propõem que o medidor forneça a informação de consumo criptografada e assinada para que a computação ocorra em dispositivo do cliente, diminuindo as preocupações relativas à transmissão de informação sensível para fora do domínio da UC (RIAL; DANEZIS, 2011). No modelo SecureCloud, o *SM* fornece a informação de consumo criptografada e assinada e a computação de privacidade ocorre no ambiente seguro do processador na nuvem, dispensando a necessidade de que o consumidor tenha acesso a algum dispositivo computacional. Este modelo possui a desvantagem de enviar informações potencialmente privadas (ainda que criptografadas) para servidor remoto, contudo, a AIPD conduzida busca mitigar este risco ao estabelecer controles de acesso enquanto o sistema SecureCloud busca assegurar a execução de operações sensíveis apenas nos enclaves protegidos.

Conclui-se portanto que, implementações do sistema de *SG* no modelo “coletar primeiro, processar depois”, ou seja, uma implementação em que os dados de consumo energético granulares saem do domínio da UC e são processados em alguma outra circunstância, mesmo que por “terceiro garantidor”, utilizando técnicas de anonimização e criptografia, violaria os princípios da legislação brasileira de Finalidade, Adequação e Necessidade, respectivamente os Requisitos de Privacidade $RP_{1,2,3}$.

4.1.5 Identificar ameaças à privacidade

Nesta etapa as ameaças aos Requisitos de Privacidade foram analisadas e geraram as ameaças que receberam a notação $A_{i,j}$ na qual i corresponde ao número do RP e j ao número da ameaça. Desse modo, por exemplo, a ameaça $A_{1,2}$ é a segunda ameaça encontrada contra o princípio RP_1, finalidade.

Os requisitos de privacidade foram extraídos dos princípios que devem ser observados para o tratamento de dados pessoais no Brasil, contidos na LGPD e as ameaças identificadas no conjunto da Análise de Conteúdo descrita anteriormente:

a) RP_1 Finalidade – ameaças contra este requisito de privacidade são as que buscam usos secundários dos dados, desrespeitando a finalidade da coleta.

$A_{1,1}$: A companhia de energia elétrica (CEE) oferece acesso ao conjunto de dados dos *SM* a terceiro com finalidade de marketing;

$A_{1,2}$: A CEE, considerando o conjunto de dados como anonimizado, realiza acordo de compartilhamento de dados com terceiro que, em posse de outros conjuntos de dados utiliza técnicas de *Big data* para reidentificar os sujeitos de dados e seus comportamentos (BARI et al., 2014; LIU et al., 2017; MANTELERO, 2016).

b) RP_2 Adequação – Ameaças contra este requisito ocorrem quando o tratamento de dados busca inferências além das estabelecidas no contexto da coleta, fugindo ao uso consentido

$A_{2,1}$: A CEE alega que processa os dados para fins operacionais, por meio da análise de dados granulares que revelam perfil comportamental dos sujeitos.

c) RP_3 Necessidade – Ações que coletam ou processam dados excessivos em relação ao objetivo esperado

$A_{3,1}$: A CEE recebe e armazena perfis de consumo energético detalhados e “abertos” (*plaintext*) (GE et al., 2018; RIAL; DANEZIS, 2011);

$A_{3,2}$: A CEE associa informações de localização com perfis de consumo;

$A_{3,3}$: A CEE processa consumo detalhado identificado para fornecer a conta (RIAL; DANEZIS, 2011).

d) RP_4 Livre Acesso – Ações que obstam o acesso facilitado e gratuito à auto informação

$A_{4,1}$: A CEE demora a responder a uma requisição de acesso do titular e/ou fornece um conjunto de dados incompleto.

e) RP_5 Qualidade dos dados – Ações ou omissões que acarretem armazenamento de dados incorretos ou incompletos

$A_{5,1}$: A CEE não registra uma alteração cadastral e fornece uma chave privada a alguém que não o sujeito de dados (FAN; GONG, 2013; PARVEZ et al., 2016);

$A_{5,2}$: A CEE não registra uma alteração cadastral e realiza decisão automatizada sobre dados incorretos (JAIN; GYANCHANDANI; KHARE, 2016).

f) RP_6 Transparência – Omissões em divulgar os usos e processamento de dados que estão sendo realizados

$A_{6,1}$: A CEE não informa o consumidor sobre o processamento realizado sobre seus dados;

$A_{6,2}$: A CEE não informa, ou não consegue determinar, com quais entidades os dados do consumidor são compartilhados (CAVOUKIAN; POLONETSKY; WOLF, 2010).

g) RP_7 Segurança – Ações ineficazes ou omissões que levem à exposição dos dados

$A_{7,1}$: Um agente malicioso obtém acesso a credenciais baixas e consegue escalar privilégios pelo sistema, acessando dados pessoais;

$A_{7,2}$: Um agente malicioso se passa pela CEE e convence o consumidor a lhe fornecer informação privada;

$A_{7,3}$: Um terceiro com acesso ao sistema consegue escalar privilégios e acessar dados pessoais;

$A_{7,4}$: Uma vulnerabilidade expõe uma base de dados à internet e a extração dos dados passa desapercebida.

h) RP_8 Prevenção – Omissão de tomada de ações para evitar a ocorrência do dano

$A_{8,1}$: A CEE espera por um incidente de segurança para agir;

$A_{8,2}$: A CEE implementa sistemas que coletam primeiro e processam depois, adicionando privacidade posteriormente por componentes acessórios e mecanismos de acesso e controle.

i) RP_9 Não discriminação – Ações de tomadas de decisão (automatizada ou não) de modo discriminatório contra os sujeitos de dados

$A_{9,1}$: A CEE cobra tarifas diferentes com base na localização onde o consumo acontece.

j) RP_{10} Responsabilização – Ações ou omissões que impeçam a apuração de responsabilidade por incidentes

$A_{10,1}$: O fluxo de dados e as medidas protetivas não são documentadas;
$A_{10,2}$: O sistema não fornece registros (*logs*).

As ameaças (A) identificadas contra os requisitos de privacidade (RP) serviram para informar a sugestão de contramedidas (C) para solucioná-las.

4.1.6 Identificar as soluções de privacidade

Nesta etapa foram sugeridas as contramedidas (C) que buscam endereçar as ameaças identificadas na etapa anterior. Está contida aqui a resposta à pergunta de pesquisa: “quais medidas de proteção de dados pessoais precisariam ser consideradas no planejamento e operação de Smart Grid utilizando computação em nuvem?”. A maneira como se chegou a este resultado pretende que as medidas propostas atendam aos requisitos legais por serem pautadas pelos princípios da legislação, facilitando *compliance* e ao mesmo tempo culminem em um sistema que atenda aos critérios de *PbD*. As recomendações foram extraídas da AC e do *corpus* estático do estudo. As contramedidas foram identificadas com suas correspondentes ameaças, assim, a contramedida $C_{1,2}$ busca solucionar a ameaça $A_{1,2}$.

a) $C_{1,1}$: Devido ao princípio legal da finalidade (BRASIL, 2018) a CEE deve processar os dados de acordo com seus propósitos, nos quais não se inclui direcionamento de propaganda.

$C_{1,2}$: Conjuntos de dados verdadeiramente anonimizados são difíceis de se obter. Realizar simulações de ataques aos conjuntos de dados para determinar sua resistência à reidentificação para tomar uma decisão informada sobre se ou como os dados devem ser compartilhados (BARI et al., 2014; LIU et al., 2017; MANTELERO, 2016).

b) $C_{2,1}$: Estabelecer processos que primeiramente determinam a finalidade do uso dos dados e posteriormente a melhor maneira de obtê-la, valendo-se da minimização dos dados (GURSES; TRONCOSO; DIAZ, 2015) e adequação ao propósito (BRASIL, 2018);

c) $C_{3,1}$: Estabelecer processos para a de-identificação na fonte e não armazenar informações abertas (*plaintext*), além de estabelecer processos para a deleção regular dos dados;

$C_{3,2}$: Ainda pelos princípios de Adequação e Finalidade (BRASIL, 2018), não correlacionar os dados para obter informações pessoais;

$C_{3,3}$: Planejar o sistema para operar sem a necessidade de acesso a perfis detalhados de consumo (KELBERT et al., 2017; RIAL; DANEZIS, 2011; RIELLA et al., 2018)

d) $C_{4,1}$: Estabelecer processos para responder a requisições dos usuários: documentar todos os fluxos de dados (ICO, 2018) e os processamentos empreendidos. Estabelecer maneira automatizada de preparação deste conjunto de dados para atender às disposições legais conforme Art 9º da LGPD, que indica que as informações prestadas ao titular devem ser facilitadas, claras, adequadas e que contenham a finalidade específica do tratamento, a forma e a duração do tratamento, a identificação do controlador, informações de contato do controlador, informações sobre o uso compartilhado de dados pelo controlador, responsabilidades dos agentes que realizarão o tratamento e os direitos do titular (BRASIL, 2018). Quando não haja no sistema um plano de dados pré-estabelecido, dificilmente a empresa conseguirá atender aos requisitos legais dada a amplitude da obrigação. A condução e documentação de uma AIPD prepara e atende os requisitos de acesso (ICO, 2018; WP29, 2017) e sua integração auxilia na manutenção de um programa de governança de privacidade nos termos da LGPD (BRASIL, 2018) além de contribuir com a transparência da organização.

e) $C_{5,1}$: Estabelecer processos que sinalizem alteração de versão nas informações;

$C_{5,2}$: Atestar a qualidade dos dados antes de utilizá-los como fonte para decisões automatizadas. Dados enviesados, incompletos, incorretos podem gerar decisões prejudiciais aos sujeitos (JAIN; GYANCHANDANI; KHARE, 2016).

f) $C_{6,1}$: Publicar documentação clara e transparente sobre o uso, guarda e processamento de dados no sistema (WRIGHT, 2012);

$C_{6,2}$: Documentar todas as entidades envolvidas na cadeia de dados e sua responsabilização. O processo de AIPD pode auxiliar na obtenção de transparência pela organização e em sua própria condução define todos os fluxos de dados e atores envolvidos (PIATKOWSKA *et al*., 2017), facilitando a preparação desta documentação.

g) $C_{7,1}$: Implementar controle de acesso e segmentação de responsabilidades no qual uma credencial comprometida não acarrete um sistema comprometido (BAEK *et al*., 2015; BARI *et al*., 2014);

$C_{7,2}$: Documentar e publicar as interações legítimas e esperadas com o consumidor. Oferecer um canal para que o consumidor possa validar a alegações que sejam feitas pela CEE (Linha para verificar se o operador alegando estar a serviço da CEE efetivamente a representa). Não estabelecer comportamentos legítimos que possam ser abusados por agentes maliciosos (nunca pedir informações ou senhas aos consumidores);

$C_{7,3}$: Permitir acesso a sistemas internos apenas a instituições avaliadas e verificadas; estabelecer sistemas de gerenciamento de identidades que delegue o mínimo de acesso necessário a cada agente (RIAL; DANEZIS, 2011).

$C_{7,4}$: Monitorar o acesso e a extração de dados nos sistemas. Definir conjuntos de dados que ofereçam maior risco ou piores consequências em decorrência do vazamento e intensificar monitoramento.

h) $C_{8,1}$: Em respeito ao princípio da Prevenção (BRASIL, 2018) tomar medidas protetivas antes de incidentes.

$C_{8,2}$: Em respeito aos princípios de Finalidade, Adequação e Necessidade (BRASIL, 2018) não coletar informações excedentes ao uso pretendido. Para o atendimento aos conceitos de *PbD*, buscar sempre a minimização dos dados (GURSES; TRONCOSO; DIAZ, 2015). Privacidade contratual (*by policy*) não é recomendada, mesmo quando as políticas sejam seguidas à risca, caso haja um incidente de segurança o dano ocorrerá.

i) $C_{9,1}$: Implementar sistemas que de-identificam na fonte;

j) $C_{10,1}$: Alinhado ao princípio de Transparência (BRASIL, 2018), documentar e publicar as medidas tomadas para a proteção de dados;

$C_{10,2}$: Ativar registros (*logs*) para facilitar a apuração de incidentes e responsabilização.

O Quadro 4 apresenta os requisitos de privacidade e suas respectivas ameaças e contramedidas:

Quadro 4 - Requisitos de privacidade, Ameaças e Contramedidas

(Continua)

Requisito de Privacidade	Ameaça	Contramedida
RP_1 Finalidade	$A_{1,1}$: A companhia de energia elétrica (CEE) oferece acesso ao conjunto de dados dos *SM* a terceiro com finalidade de marketing;	$C_{1,1}$: Devido ao princípio legal da finalidade a CEE deve processar os dados de acordo com seus propósitos, dentre os quais não se inclui direcionamento de propaganda.
	$A_{1,2}$: A CEE, considerando o conjunto de dados como anonimizado, realiza acordo de compartilhamento de dados com terceiro que, em posse de outros conjuntos de dados utiliza técnicas de *Big data* para reidentificar os sujeitos de dados e seus comportamentos	$C_{1,2}$: Conjuntos de dados verdadeiramente anonimizados são difíceis de se obter. Realizar simulações de ataques aos conjuntos de dados para determinar sua resistência à reidentificação para tomar uma decisão informada sobre se ou como os dados devem ser compartilhados
RP_2 - Adequação	$A_{2,1}$: A CEE alega que processa os dados para fins operacionais, por meio da análise de dados granulares que revelam perfil comportamental dos sujeitos.	$C_{2,1}$: Estabelecer processos que primeiramente determinam a finalidade do uso dos dados e posteriormente a melhor maneira de obtê-la, valendo-se da minimização dos dados
RP_3 - Necessidade	$A_{3,1}$: A CEE recebe e armazena perfis de consumo energético detalhados e "abertos" (*plaintext*)	$C_{3,1}$: Estabelecer processos para a de-identificação na fonte e não armazenar informações abertas (*plaintext*), além de estabelecer processos para a deleção regular dos dados
	$A_{3,2}$: A CEE associa informações de localização com perfis de consumo	$C_{3,2}$: Ainda pelos princípios de Adequação e Finalidade, não correlacionar os dados para obter informações pessoais
	$A_{3,3}$: A CEE processa consumo detalhado identificado para fornecer a conta	$C_{3,3}$: Planejar o sistema para operar sem a necessidade de acesso a perfis detalhados de consumo
RP_4 Livre Acesso	$A_{4,1}$: A CEE demora a responder a uma requisição de acesso do titular e/ou fornece um conjunto de dados incompleto	$C_{4,1}$: Estabelecer processos para responder a requisições dos usuários: documentar todos os fluxos de dados e os processamentos empreendidos

(Conclusão)

Requisito de privacidade	Ameaça	Contramedida
RP_5 Qualidade dos dados	$A_{5,1}$: A CEE não registra uma alteração cadastral e fornece uma chave privada a alguém que não o sujeito de dados	$C_{5,1}$: Estabelecer processos que sinalizem alteração de versão nas informações
	$A_{5,2}$: A CEE não registra uma alteração cadastral e realiza decisão automatizada sobre dados incorretos	$C_{5,2}$: Atestar a qualidade dos dados antes de utilizá-los como fonte para decisões automatizadas. Dados enviesados, incompletos, incorretos podem gerar decisões prejudiciais aos sujeitos
RP_6 Transparência	$A_{6,1}$: A CEE não informa o consumidor sobre o processamento realizado sobre seus dados	$C_{6,1}$: Publicar documentação clara e transparente sobre o uso, guarda e processamento de dados no sistema
	$A_{6,2}$: A CEE não informa, ou não consegue determinar, com quais entidades os dados do consumidor são compartilhados	$C_{6,2}$: Documentar todas as entidades envolvidas na cadeia de dados e sua responsabilização
RP_7 Segurança	$A_{7,1}$: Um agente malicioso obtém acesso a credenciais baixas e consegue escalar privilégios pelo sistema, acessando dados pessoais	$C_{7,1}$: Implementar controle de acesso e segmentação de responsabilidades no qual uma credencial comprometida não acarrete um sistema comprometido
	$A_{7,2}$: Um agente malicioso se passa pela CEE e convence o consumidor a lhe fornecer informação privada	$C_{7,2}$: Documentar e publicar as interações legítimas e esperadas com o consumidor
	$A_{7,3}$: Um terceiro com acesso ao sistema consegue escalar privilégios e acessar dados pessoais	$C_{7,3}$: Permitir acesso a sistemas internos apenas a instituições avaliadas e verificadas; estabelecer sistemas de gerenciamento de identidades que delegue o mínimo de acesso necessário a cada agente
	$A_{7,4}$: Uma vulnerabilidade expõe uma base de dados à internet e a extração dos dados passa desapercebida	$C_{7,4}$: Monitorar o acesso e a extração de dados nos sistemas. Definir conjuntos de dados que ofereçam maior risco ou piores consequências em decorrência do vazamento e intensificar monitoramento
RP_8 Prevenção	$A_{8,1}$: A CEE espera por um incidente de segurança para agir	$C_{8,1}$: Em respeito ao princípio da Prevenção (LGPD) tomar medidas protetivas antes de incidentes
	$A_{8,2}$: A CEE implementa sistemas que coletam primeiro e processam depois, adicionando privacidade posteriormente por componentes acessórios e mecanismos de acesso e controle	$C_{8,2}$: Em respeito aos princípios de Finalidade, Adequação e Necessidade (LGPD) não coletar informações excedentes ao uso pretendido. Privacidade contratual (*by policy*) não é recomendada, mesmo quando as políticas sejam seguidas à risca, caso haja um incidente de segurança o dano ocorrerá.
RP_9 Não discriminação	$A_{9,1}$: A CEE cobra tarifas diferentes com base na localização onde o consumo acontece	$C_{9,1}$: Implementar sistemas que de-identificam na fonte
RP_{10} Responsabilização	$A_{10,1}$: O fluxo de dados e as medidas protetivas não são documentadas	$C_{10,1}$: Alinhado ao princípio de Transparência (LGPD), documentar e publicar as medidas tomadas para a proteção de dados
	$A_{10,2}$: O sistema não fornece registros (*logs*)	$C_{10,2}$: Ativar registros (*logs*) para facilitar a apuração de incidentes e responsabilização

Fonte: Autoria própria (2019)

Estas contramedidas buscam solucionar as ameaças de privacidade identificadas ao longo dos processos de AIPD e *Advanced Cloud Privacy Threat Modeling*. Os princípios de privacidade contidos na LGPD foram convertidos em requisitos de privacidade do sistema e as ameaças a estes requisitos foram levantadas com apoio de Análise de Conteúdo. As medidas de proteção de dados apresentadas (contramedidas) valeram-se dos resultados da Análise de Conteúdo e das informações obtidas pelo *corpus* estático da pesquisa. As medidas objetivaram promover os conceitos de *Privacy by Design* na engenharia do sistema, principalmente pela busca de minimização dos dados, pela ausência de coleta, de-identificação na fonte, deleção programada e especificação de propósito (GURSES; TRONCOSO; DIAZ, 2015).

5 CONSIDERAÇÕES FINAIS

O objetivo geral desta pesquisa era de propor um conjunto de medidas de proteção de dados pessoais que precisariam ser consideradas no planejamento e operação de *Smart Grid* utilizando computação em nuvem. Esse resultado se encontra sintetizado no Quadro 4 (p.91-92)

Quanto aos objetivos específicos, o processo de AIPD foi caracterizado na seção 2.4 Avaliação de Impacto à Proteção de Dados Pessoais, os aspectos relevantes do conjunto de princípios de *Privacy by Design* foram discutidos na seção 2.2 Privacy by Design – PbD e utilizados como norteadores das recomendações. O uso de *cloud* segura para *Smart Grid* é o que se obtém com a adoção das medidas protetivas que respondem à pergunta de pesquisa. Os princípios de PbD são importantes para que o sistema possa proteger efetivamente os dados pessoais, o que dificilmente ocorre quando a privacidade é considerada como acessório a um sistema heterogêneo e interoperável.

O uso de computação em nuvem introduz novos atores e riscos a qualquer sistema, e foram apontadas práticas que levam tais riscos em consideração. Importante ressaltar que a alternativa ao uso de computação em nuvem, ou seja, a implantação e gerenciamento dos próprios servidores não implica por si só na extinção dos riscos identificados, fazendo surgir uma outra série de riscos relacionados à capacidade da organização de gerenciar e proteger sua rede e seus servidores.

A condução de AIPD antes da execução do projeto permite que o sistema seja planejado para a minimização dos riscos em todas as etapas, principiando pela minimização da coleta até a limitação de acesso aos mínimos privilégios necessários na operação em nuvem.

As medidas apresentadas aqui pretendem ser abrangentes e objetivam a garantia de direitos. Mesmo que o estudo tenha sido sobre um sistema hipotético, há diversas indicações que podem ser aplicadas ao desenvolvimento real de uma *SG* que utilize computação em nuvem para operar. Além disso, os princípios gerais que orientaram a proposta das medidas podem ser aplicados a diversos sistemas e elevar sua capacidade de proteção de dados. Para isto, é preciso que sejam estabelecidos claramente os objetivos do sistema e exaustivamente sejam procuradas alternativas de implementação orientadas para estes princípios (minimização de dados e

segurança). É possível que a implementação direta e simplista seja a que traga consigo os maiores riscos, o que não quer dizer que a proteção deva ser complexa.

Os cenários de segurança e privacidade são dinâmicos, com novas técnicas de ataque e re-identificação surgindo constantemente. Uma organização que conduza uma AIPD no planejamento de um sistema tem muito mais chances de proteção eficaz do que uma que o faça após o sistema implantado, mas em nenhum dos casos é dispensado o monitoramento e acompanhamento. O ritmo da pesquisa acadêmica é diferente do ritmo de publicação de vulnerabilidades técnicas, estas muito mais frequentes, indicando que o monitoramento deve acompanhar múltiplas fontes de informação

Com a multiplicação e interconexão de diversos sensores no espaço físico nossa existência passa a ser cada vez mais quantificada e monitorada. Esse conjunto de informações pode traçar um perfil muito completo sobre nossos comportamentos e os prejuízos ao desenvolvimento da personalidade, individualmente e socialmente têm efeitos deferidos no tempo. Ao mesmo tempo, a falta de cuidados no momento da implantação dos sistemas dificulta, muitas vezes inviabiliza, sua correção posterior. Privacidade é fácil “de errar”; é fácil acreditar que um conjunto de dados está anonimizado e não oferece riscos ou considerar que o sistema está suficientemente protegido, além da existência de incentivos econômicos para o aumento e intensificação da coleta de dados.

Contra esse cenário, apenas a legislação é insuficiente. O estabelecimento de medidas punitivas na legislação visa a desencorajar comportamentos que possam gerar danos, mas questiona-se em que medida isso é eficaz contra o aparato de monitoramento instalado e em expansão. O reconhecimento do sujeito de dados como parte vulnerável na relação auxilia na resolução de conflitos, contudo, é preciso que a busca pelo direito à proteção de dados seja mais do que um desejo de nicho. Se/quando esta vontade se tornar um anseio social generalizado é possível que as organizações internalizem processos protetivos desde a concepção de produtos.

A comunicação da importância da privacidade não é simples, esbarrando em argumentos como “não tenho nada a esconder” e sendo difícil oferecer expectativas positivas em um cenário de vigilância já instaurado: “qual o problema com *Smart Meters* se eu já uso *Alexa/Cortana/Google Home* em casa?”. A comoditização dos dados pessoais, por vezes apresentada como cenário vantajoso por supor contrapartida financeira por uma coleta que já é realizada, é arriscada e não oferece

diminuição dos danos aos direitos fundamentais e ao desenvolvimento da personalidade, provavelmente multiplicando-os pelos variados usos de dados sob a justificativa do “consentimento”.

Há uma sinalização de que as empresas têm considerado a proteção à privacidade como um diferenciador em seus produtos, algumas destacando especificamente esta vantagem em sua publicidade. É possível também que a demanda mercadológica promova uma mudança para que o respeito à privacidade seja o padrão mínimo dos produtos, em oposição à um artigo de luxo reservado àqueles que possam pagar por este diferencial.

Uma AIPD malconduzida pode passar a falsa sensação de segurança e aprovar medidas que não reduzam as ameaças do sistema. O processo ainda não conta com recomendações oficiais no país, mas espera-se que logo a ANPD possa oferecer guias e requisitos mínimos para que o processo não seja utilizado apenas como autorizador de qualquer prática sob o selo de privacidade.

Uma limitação deste estudo reside na ausência de consulta com especialistas, recomendada tanto na metodologia de AIPD como na de modelagem de ameaças. Buscou-se suprir esta falta com levantamento abrangente da literatura, contudo, um especialista com experiência prática na área poderia auxiliar na transformação das ameaças encontradas em uma matriz de risco para orientar a melhor alocação de recursos na implantação das medidas sugeridas, além de constatar sua viabilidade prática.

Como sugestão de trabalhos futuros, seria interessante a validação das metodologias utilizadas como subsidiárias à condução do processo de AIPD, tanto no levantamento das fontes para identificação ampla de ameaças quanto na proposição de soluções pela sistematização através de Análise de Conteúdo. A opção por estas metodologias buscou dotar de maior especificidade o processo que é útil, porém abrangente e genérico para se adequar a diversos objetos de análise. Trabalhos futuros podem buscar investigar os limites de aplicabilidade do processo de AIPD. Outra questão que segue sem fechamento é sobre o que quer dizer exatamente *Privacy by Design*, também apontada como um conceito genérico. Nesta dissertação optou-se por uma visão que buscava implementá-la na engenharia de sistemas pela busca da minimização dos dados. Possivelmente sua adaptação para outros contextos pode revelar outros requisitos do conceito que não tenham sido capturados aqui.

REFERÊNCIAS

AGÊNCIA NACIONAL DE ENERGIA ELÉTRICA – ANEEL. **Resolução Normativa nº 502/2012**. Disponível em: <http://www.aneel.gov.br/cedoc/ren2012502.pdf>. Acesso em: 08 jun. 2018.

ARAÚJO, Carlos A. A. Bibliometria: evolução histórica e questões atuais. **Em Questão.** v. 12, n. 1, p. 11–32, 2006.

BAEK, Joonsang *et al*. **A secure cloud computing based framework for big data information management of smart grid.** IEEE transactions on cloud computing 3, no. 2 (2015): 233-244. p. 11, 2015.

BARDIN, Lawrence. **Análise de conteúdo**. São Paulo: Edições 70, 2011.

BARI, Ataul *et al*. Challenges in the Smart Grid Applications: An Overview. **International Journal of Distributed Sensor Networks**, [s. l.], v. 2014, n. 2, 2014.

BASTOS, Celso Ribeiro. **Curso de direito constitucional**. 21. ed. São Paulo: Saraiva, 2000.

BENNETT, C. **In Defense of Privacy: The Concept and the Regime.** *Surveillance and Society*, 8(4): 486–496. 2011.

BIONI, Bruno Ricardo. **Xeque-Mate: o tripé de proteção de dados pessoais no xadrez das iniciativas legislativas no Brasil**. São Paulo, 2015. Disponível em: https://gpopai.usp.br/wordpress/wpcontent/uploads/2016/07/XEQUE_MATE_INTERATIVO2.pdf. Acesso em: 08 de jun. 2017.

BIONI, Bruno Ricardo. **Proteção de dados pessoais: a função e os limites do consentimento**. Rio de Janeiro: Forense, 2019.

BIRMAN, K. P.; GANESH, L.; RENESSE, R. V. Running smart grid control software on cloud computing architectures. In **Proceedings of the Workshop on Computational Needs for the Next Generation Electric Grid**, p. 1–33, 2011.

BRANDEIS, Louis; WARREN, Samuel. **The right to privacy**. Harvard Law Review, vol. IV, no. 5, 1890.

BRASIL. Constituição (1988). **Constituição da República Federativa do Brasil**. Brasília: Senado, 1988.

BRASIL. **Lei n. 13.709** de 14 de ago. de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/Lei/L13709.htm >. Acesso em: 16 ago. 2018.

BRASIL. **Lei n. 13.853** de 8 de jul. de 2019. Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências. Disponível em: <

http://www.planalto.gov.br/ccivil_03/_ato2019-2022/2019/Lei/L13853.htm >. Acesso em: 10 ago. 2019.

BROOKS, Sean et al. **An introduction to privacy engineering and risk management in federal systems**. Gaithersburg, MD: National Institute of Standards and Technology, 2017. Disponível em: <https://nvlpubs.nist.gov/nistpubs/ir/2017/NIST.IR.8062.pdf>. Acesso em: 24 out. 2018.

BOAG, Annan. **Myki incident- lessons for organisations.** Office of the Victorian Information Commissioner, 2019. Disponível em: <https://ovic.vic.gov.au/blog/myki-incident-lessons-for-organisations/>. Acesso em: 16 ago. 2019.

BOILLAT, Philippe, e MORTEN Kjaerum. **Handbook on European data protection law**. *European Union Agency for Fundamental Rights.–2014.–199 p*, 2014.

CARLUCCIO, Dario; BRINKHAUS, Stephan. Smart Hacking For Privacy. In: **28C3 Behind Enemy Lines**, 2011. Berlin, Alemanha. Disponível em: <http://mirror.fem-net.de/CCC/28C3/mp4-h264-HQ/28c3-4754-en-smart_hacking_for_privacy_h264.mp4>. Acesso em: 20 maio 2018.

CAVOUKIAN, Ann. **Privacy by Design - The 7 Foundational Principles** - Implementation and Mapping of Fair Information Practices. Take the challenge. Information and privacy commissioner of Ontario, Canada, [s. l.], p. 10, 2010a.

CAVOUKIAN, Ann. Privacy by design: the definitive workshop. A foreword by Ann Cavoukian, Ph.D. **Identity in the Information Society**, [s. l.], v. 3, n. 2, p. 247–251, 2010b.

CAVOUKIAN, Ann; POLONETSKY, Jules; WOLF, Christopher. SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation. **Identity in the Information Society**, [s. l.], v. 3, n. 2, p. 275–294, 2010.

CDR. Coalizão Direitos na Rede. **Presidente da República desrespeita acordos firmados no processo legislativo e fragiliza entidade guardiã de dados pessoais**. 2019. Disponível em: <https://direitosnarede.org.br/seus_dados_sao_voce/2019/07/09/cdr-repudia-os-vetos-na-lei-que-cria-anpd.html>. Acesso em: 18 ago. 2019.

CLARKE, R. Privacy impact assessment: Its origins and development. **Computer Law & Security Review**, v. 25, n. 2, p. 123–135, 2009.

CNIL. Commission Nationale de l'Informatique et des Libertés. **Privacy Impact Assessment – Methodology.** Paris, 2015. Disponível em: <https://www.cnil.fr/sites/default/files/typo/document/CNIL-PIA-1-Methodology.pdf>. Acesso em: 10 maio 2018.

CONFORTO, Edivandro Carlos; AMARAL, Daniel Capaldo; SILVA, Sérgio Luis da. Roteiro para revisão bibliográfica sistemática: aplicação no desenvolvimento de

produtos e gerenciamento de projetos. In: **8º Congresso Brasileiro de Gestão e Desenvolvimento de Produto (CBGDP)**, 2011, Porto Alegre. Anais do Congresso. Porto Alegre: [s.e.], 2011. p. 1 – 12.

COORDENAÇÃO DE APERFEIÇOAMENTO DE PESSOAL DE NÍVEL SUPERIOR – CAPES. **Periódicos Capes: institucional.** 2018. Disponível em:<http://www.periodicos.capes.gov.br/index.php?option=com_pinstitucional&mn=69>. Acesso em: 03 jun. 2018.

CREESE, S., GOLDSMITH, M., & HOPKINS, P. (2013). Inadequacies of current risk controls for the cloud. In ***Privacy and Security for Cloud Computing*** (pp. 235-255). Springer, London.

DONEDA, Danilo. A Proteção Dos Dados Pessoais Como Um Direito Fundamental. **Espaço Jurídico Journal Of Law**, v.12, nº 2, p. 91-108, 2011. Disponível em: <http://editora.unoesc.edu.br/index.php/espacojuridico/article/view/1315>. Acesso em: 10 mai. 2018.

DONEDA, Danilo. **O que está em jogo com a nova Autoridade Nacional de Proteção de Dados**, 2018. Disponível em: <https://www.jota.info/opiniao-e-analise/artigos/o-que-esta-em-jogo-com-a-nova-autoridade-nacional-de-protecao-de-dados-13082018>. Acesso em: 14 ago. 2018.

DWORK, Cynthia. A Firm Foundation for Private Data Analysis. **Communications of the ACM**, [s. l.], 2011. Disponível em: <https://www.microsoft.com/en-us/research/publication/a-firm-foundation-for-private-data-analysis/>. Acesso em: 19 jun. 2018.

EFTHYMIOU, Costas; KALOGRIDIS, Georgios. **Smart Grid Privacy via Anonymization of Smart Metering Data**. IEEE, 2010. Disponível em: <http://ieeexplore.ieee.org/document/5622050/>. Acesso em: 21 mai. 2018.
ETP Smart Grids. **The SmartGrids European Technology Platform**. 2006. Disponível em: <http://www.smartgrids.eu/ETPSmartGrids>. Acesso em: 05 jun. 2017.

ENSSLIN, Leonardo; ENSSLIN, Sandra Rolim; PINTO, Hugo de Moraes. Processo de investigação e análise bibliométrica: avaliação da qualidade dos serviços bancários. **Revista de Administração Contemporânea**, v. 17, n. 3, p. 325–349, 2013.

EUR-LEX. **Regulation (EU) 2016/679 of the European Parliament and of the Council.** Disponível em: <http://data.europa.eu/eli/reg/2016/679/oj>. Acesso em: 22 jun. 2018.

EUROPEAN COMMISSION *et al*. **Smart grid projects in Europe: lessons learned and current developments : 2012 update.** Luxembourg: Publications Office of the European Union, 2013. Disponível em: <http://dx.publications.europa.eu/10.2790/82707>. Acesso em: 25 jun. 2018.

FAN, Xinxin; GONG, Guang. Security Challenges in Smart-Grid Metering and Control Systems. **Technology Innovation Management Review**, [s. l.], v. 3, n. 7, p. 42–49, 2013.

FANG, Xi *et al*. Smart Grid — **The New and Improved Power Grid: A Survey**. IEEE Communications Surveys & Tutorials, [s. l.], v. 14, n. 4, p. 944–980, 2012.

FARHANGI, H. **The path of the smart grid**. IEEE Power and Energy Magazine, [s. l.], v. 8, n. 1, p. 18–28, 2010.

FLAHERTY, David. **Privacy Impact Assessment - An Essential Tool for Data Protection**. Disponível em: <https://aspe.hhs.gov/privacy-impact-assessment-essential-tool-data-protection>. Acesso em: 23 nov. 2017.

GE, Shanshan et al. FGDA: Fine-grained data analysis in privacy-preserving smart grid communications. **Peer-to-Peer Networking and Applications**, [s. l.], v. 11, n. 5, p. 966–978, 2018.

GHOLAMI, Ali; LAURE, Erwin. Advanced Cloud Privacy Threat Modeling. In: **Sixth International Conference on Computer Science and Information Technology**. : Academy & Industry Research Collaboration Center (AIRCC), 2016. Disponível em: <http://www.airccj.org/CSCP/vol6/csit64820.pdf>. Acesso em: 11 maio. 2018.

GHOLAMI, Ali et al. Design and Implementation of the Advanced Cloud Privacy Threat Modeling. **International Journal of Network Security & Its Applications**, [s. l.], v. 8, n. 2, p. 103–122, 2016.

GIL, Antonio Carlos. **Como elaborar projetos de pesquisa**. São Paulo: Atlas, 2010.

GROBAUER, B.; WALLOSCHEK, T.; STOCKER, E. Understanding Cloud Computing Vulnerabilities. **IEEE Security Privacy**, [s. l.], v. 9, n. 2, p. 50–57, 2011.

GUIMARAES, Lucas Noura. The Dichotomy between Smart Metering and the Protection of Consumer's Personal Data in Brazilian Law. **Brazilian Journal of Public Policy**, [s. l.], v. 7, p. 275, 2017.

GUIMÓN, Pablo. **Cambridge Analytica, empresa pivô no escândalo do Facebook, é fechada**. 2018. Disponível em: <https://brasil.elpais.com/brasil/2018/05/02/internacional/1525285885_691249.html>. Acesso em: 06 jul. 2018.

GURSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia. **Engineering Privacy by Design**. p. 25, 2015.

GREEN, B. Z.; CUNNINGHAM, G.; EKBLAW, A.; *et al*. **Open Data Privacy**. 2017. Disponível em: <https://dash.harvard.edu/handle/1/30340010>. Acesso em: 15 nov. 2017.

D. HAGGERTY, RICHARD V. ERICSON, Kevin. The surveillant assemblage. **British Journal of Sociology**, v. 51, n. 4, p. 605–622, 2000.

HAYES, B. **Cloud computing**. Communications of the ACM, 51(7):9 –11, 2008

HES, R.; BORKING, J., 1998. **Privacy Enhancing Technologies**: the path to anonymity. *ISBN*, *90*(74087), p.12.

HOENKAMP, Robin; HUITEMA, George; DE MOOR-VAN VUGT, Adrienne. **The Neglected Consumer: The Case of the Smart Meter Rollout in the Netherlands**. Rochester, NY: Social Science Research Network, 2011. Disponível em: <https://papers.ssrn.com/abstract=2061668>. Acesso em: 9 ago. 2018.

ICO (Information Commissioner's Office). **Privacy Impact Assessment Handbook.** 2009. Disponível em: <www.adls.ac.uk/wp-content/uploads/2011/08/PIA-handbook.pdf>. Acesso em: 23 nov. 2017.

ICO (Information Commissioner's Office). **Conducting privacy impact assessments code of practice**. v. 1.0. Technical report, UK, 2014. Disponível em: <https://ico.org.uk/media/for-organisations/documents/1595/pia-code-of-practice.pdf>. Acesso em: 23 nov. 2017.

ICO (Information Commissioner's Office). **Data Protection Impact Assessments (DPIAs)**. v. 1.0.77 Technical report, UK, 2018. Disponível em: <https://ico.org.uk/media/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/data-protection-impact-assessments-dpias-1-0.pdf> Acesso em: 20 jun. 2019.

IDEC. **Após pressão da sociedade, Senado aprova Lei de Dados Pessoais**. 2018. Disponível em: <https://idec.org.br/noticia/apos-pressao-da-sociedade-senado-aprova-lei-de-dados-pessoais>. Acesso em: 10 ago. 2018.

IDEC. **Idec pede derrubada dos vetos de MPs que atingem consumidores**. 2019. Disponível em: <https://idec.org.br/noticia/idec-pede-derrubada-dos-vetos-de-mps-que-atingem-consumidores>. Acesso em: 27 ago. 2019.

IEEE STANDARDS COMMITTEE *et al*. IEEE guide for smart grid interoperability of energy technology and information technology operation with the electric power system (EPS), end-use applications and loads. New York, N.Y.: Institute of Electrical and Electronics Engineers, 2011. Disponível em: <http://ieeexplore.ieee.org/servlet/opac?punumber=6018237>. Acesso em: 22 mai. 2018.

JAIN, Priyank; GYANCHANDANI, Manasi; KHARE, Nilay. Big data privacy: a technological perspective and review. **Journal of Big Data**, [s. l.], v. 3, n. 1, p. 1–25, 2016.

KAFKA, Franz. O processo. Tradução de Torrieri Guimarães – São Paulo: Abril Cultural, 1979.

KING, Nancy J.; JESSEN, Pernille Wegener. For privacy's sake: Consumer "opt outs" for smart meters. **Computer Law & Security Review**, [s. l.], v. 30, n. 5, p. 530–539, 2014.

KUMAR, Ravinder; KUMAR, Anil. NOVEL RISK ASSESSMENT FRAMEWORK FOR SMART GRID. **International Journal of Advanced Research in Computer Science**, [s. l.], v. 8, n. 7, 2017. Disponível em: <http://search.proquest.com/docview/1931129536/>. Acesso em: 06 jul. 2018.

LACTEC. **Participação no Paraná Smart Energy**, 2015. Disponível em: <http://www.lactec.org.br/menu-noticias/participacao-no-parana-smart-energy/>. Acesso em: 10 ago. 2018.

LAFER, Celso. **A reconstrução dos direitos humanos:** um diálogo com o pensamento de Hannah Arendt. Companhia das Letras, 1991

LAM, H. Y.; FUNG, G. S. K. **A Novel Method to Construct Taxonomy of Electrical Appliances Based on Load Signatures**. IEEE Transactions on Consumer Electronics, [s. l.], v. 53, n. 2, p. 9, 2007.

LEORATTI, Alexandre. **Problemas estruturais e insegurança dificultam formação da ANPD**. 2019. Disponível em: <https://www.jota.info/legislativo/problemas-estruturais-anpd-09072019>. Acesso em: 18 ago. 2019.

LERNER, Jack I.; MULLIGAN, Deirdre K. **Taking the Long View on the Fourth Amendment: Stored Records and the Sanctity of the Home**. Stan. Tech. L. Rev. 3. 2008.

LESZCZYNA, Rafał. Cybersecurity and privacy in standards for smart grids – A comprehensive survey. **Computer Standards & Interfaces**, [s. l.], v. 56, p. 62–73, 2018.

LINE, Maria B. Why securing smart grids is not just a straightforward consultancy exercise: Securing smart grids-not just a plain consultancy exercise. **Security and Communication Networks**, v. 7, n. 1, p. 160–174, 2014.

LIU, Qin et al. Preface: Security and privacy in big data clouds. **Future Generation Computer Systems**, [s. l.], v. 72, p. 206–207, 2017.

LOPES, Isabel Maria; OLIVEIRA, Pedro. **Aplicabilidade do Regulamento Geral sobre Proteção de Dados em Clínicas de Saúde.** Revista Ibérica de Sistemas e Tecnologias de Informação E15 (2018): 118-129.

LYON, D. **The Surveillance Society**, 2001. Buckingham: Open University Press.

LYON, D. **Surveillance as Social Sorting: Privacy, Risk and Automated Discrimination.** Florence: Taylor and Francis, 2005. Disponível em: <http://public.eblib.com/choice/publicfullrecord.aspx?p=240591>. Acesso em: 16 ago. 2018.

MANTELERO, Alessandro. The future of consumer data protection in the E.U. Re-thinking the “notice and consent” paradigm in the new era of predictive analytics. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, v. 30, n. 6, p. 643–660, 2014.

MANTELERO, Alessandro. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, v. 32, n. 2, p. 238–255, 2016.

MÁRMOL, Félix *et al*. **Do not snoop my habits: preserving privacy in the smart grid**. IEEE Communications Magazine, [s. l.], v. 50, n. 5, p. 166–172, 2012.

MCDANIEL, Patrick; MCLAUGHLIN, Stephen. Security and Privacy Challenges in the Smart Grid. **IEEE Security & Privacy Magazine**, [s. l.], v. 7, n. 3, p. 75–77, 2009.

MCNEIL, Sonia K. Privacy and the modern grid. **Harvard Journal of Law & Technology**, [s. l.], v. 25, n. 1, p. 199, 2011.

MCQUAY, Terry; CAVOUKIAN, Ann. A pragmatic approach to privacy risk optimization: privacy by design for business practices. **Identity in the Information Society**, [s. l.], v. 3, n. 2, p. 379–396, 2010.

MCKENNA, Eoghan; RICHARDSON, Ian; THOMSON, Murray. **Smart meter data: Balancing consumer privacy concerns with legitimate applications**. Energy Policy, [s. l.], v. 41, p. 807–814, 2012.

MINAMIZAKI, Gislaine Midori *et al*. **Data security issues on metering systems of energy consumption in Brazil**. ESPAÇO ENERGIA, [s. l.], n. 18, p. 11, 2013.

MOREIRA, Bruno. **Falta de regulação entrava Smart Grid no país**. 2015. Disponível em: <https://www.osetoreletrico.com.br/falta-de-regulacao-entrava-smart-grid-no-pais/>. Acesso em: 11 ago. 2018.

M’RHAOAURH, Ibtissam et al. Challenges of cloud computing use: A systematic literature review. **MATEC Web of Conferences**, [s. l.], v. 200, p. 00007, 2018.

NARAYANAN, Arvind; SHMATIKOV, Vitaly. Myths and Fallacies of “Personally Identifiable Information”. **Commun. ACM**, [s. l.], v. 53, n. 6, p. 24–26, 2010.

NIST. **Guidelines for Smart Grid Cybersecurity**. 2014a. Disponível em: <http://dx.doi.org/10.6028/NIST.IR.7628r1>. Acesso em: 18 nov. 2017.

NIST. **NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0**. National Institute of Standards and Technology, 2014b. Disponível em: <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1108r3.pdf>. Acesso em: 24 mai. 2018.

OECD. **Manual de Frascati**. Gráfica de Coimbra: Coimbra, 2007.

OLEJNIK, Lukasz. **On privacy impact assessment and leaking data of millions of users**. 2019. Disponível em: <http://blog.lukaszolejnik.com/on-privacy-impact-assessment-and-leaking-data-of-millions-of-users/>. Acesso em: 16 ago. 2019.

OVIC. Office of the Victorian Information Commissioner. **Report of investigation:** disclosure of myki travel information. Disponível em: <https://ovic.vic.gov.au/wp-content/uploads/2019/08/Report-of-investigation_disclosure-of-myki-travel-information.pdf>. Acesso em: 16 ago. 2019.

PARANÁ. Decreto n. 8842, de 04 de set. de 2013. **Dispõe sobre a criação do Projeto Smart Energy Paraná e dá outras providências - SETI**, Curitiba, PR, set. 2013.

PARSON, Oliver *et al*. **Non-Intrusive Load Monitoring Using Prior Models of General Appliance Types**. Proceedings of the Twenty-Sixth AAAI Conference on Artificial Intelligence, [s. l.], p. 7, 2012.

PARK, Chan-Kook; KIM, Hyun-Jae; KIM, Yang-Soo. A study of factors enhancing smart grid consumer engagement. **Energy Policy**, [s. l.], v. 72, n. C, p. 211–218, 2014.

PARVEZ, Imtiaz et al. Securing Metering Infrastructure of Smart Grid: A Machine Learning and Localization Based Key Management Approach. **Energies**, [s. l.], v. 9, n. 9, p. 691, 2016.

PAYÃO, Felipe. **Vazamento da Netshoes continua e totaliza dados de 2,5 milhões de clientes.** 2018. Disponível em: <https://www.tecmundo.com.br/seguranca/129428-vazamento-netshoes-continua-totaliza-dados-2-5-milhoes-clientes.htm>. Acesso em: 06 jul. 2018.

PEARSON, Siani; BENAMEUR, Azzedine. Privacy, Security and Trust Issues Arising from Cloud Computing. 2011, In**: 2ND IEEE International Conference On Cloud Computing Technology And Science**, CLOUDCOM 2010.

PIATKOWSKA, Ewa et al. Tool support for data protection impact assessment in the smart grid. **e & i Elektrotechnik und Informationstechnik**, [s. l.], v. 134, n. 1, p. 26–29, 2017.

QUINN, Elias Leake. **Privacy and the New Energy Infrastructure**. Rochester, NY: Social Science Research Network, 2009. Disponível em: <https://papers.ssrn.com/abstract=1370731>. Acesso em: 24 mai. 2018.

RAPOSO, Jorge Nunes. **Guia Prático do Regulamento Geral sobre a Protecção de Dados**. Leya, 2018.

RIAL, Alfredo; DANEZIS, George. Privacy-Preserving Smart Metering. **Proceedings of the 2011 ACM Workshop on Privacy in the Electronic Society**, [s. l.], p. 12, 2011.

RIBEIRO, Rodolfo Augusto Mota; NIYAMA Yuiti Oki. **"Guia de recomendações de segurança para o desenvolvimento de web services para a administração pública federal."** (2016).

RIELLA, Rodrigo J. et al. Securing Smart Metering applications in Untrusted Clouds with the SecureCloud Platform. In: **PROCEEDINGS OF THE 1ST WORKSHOP ON PRIVACY BY DESIGN IN DISTRIBUTED SYSTEMS** - W-P2DS'18 2018, Porto, Portugal. In: THE 1ST WORKSHOP. Porto, Portugal: ACM Press, 2018. Disponível em: <http://dl.acm.org/citation.cfm?doid=3195258.3195263>. Acesso em: 15 ago. 2018.

ROMANOU, Anna. The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, [s. l.], v. 34, n. 1, p. 99–110, 2018.

RUBIN, Netanel. On Smart Cities, Smart Energy, And Dumb Security. In: **33C3 Works for Me**, 2016. Berlin, Alemanha. Disponível em: <https://media.ccc.de/v/33c3-8272-on_smart_cities_smart_energy_and_dumb_security>. Acesso em: 20 nov. 2017.

RUBINSTEIN, Ira; GOOD, Nathan. **Privacy by Design: A Counterfactual Analysis of Google and Facebook Privacy Incidents**. Rochester, NY: Social Science Research Network, 2012. Disponível em: <https://papers.ssrn.com/abstract=2128146>. Acesso em: 10 ago. 2018.

RUSITSCHKA, S; EGER, K; GERDES, C. Smart grid data cloud: A model for utilizing cloud computing in the smart grid domain. In **Proceedings of the 1st International Conference on Smart Grid Communications (SmartGridComm)**, p. 483–488, 2010

RUTHES, Sidarta; SILVA, Christian L. da. O uso de estudos prospectivos na análise de políticas públicas: uma análise bibliométrica. In: **XVI ALTEC Congresso da Associação Latino-Iberoamericana de Gestão de Tecnologia**. 2015. p. 1-19.

SCANDARIATO, Riccardo; WUYTS, Kim; JOOSEN, Wouter. A descriptive study of Microsoft's threat modeling technique. **Requirements Engineering**, [s. l.], v. 20, n. 2, p. 163–180, 2015.

SECURECLOUD. Project Overview. **H2020 - SecureCloud**. Disponível em: <https://www.securecloudproject.eu/project-overview/>. Acesso em: 23 nov. 2017.

SETO, Yoichi. Application of Privacy Impact Assessment in the Smart City. **Electronics and Communications in Japan**, [s. l.], v. 98, n. 2, p. 52–61, 2015.

SILVA, M. **"Linkage de bases de dados identificadas em saúde: consentimento, privacidade e segurança da informação."** Rio de Janeiro (RJ): Universidade Federal do Rio de Janeiro (2012).

SOLOVE, Daniel J. **Conceptualizing Privacy**. 2002. Disponível em: <http://scholarship.law.berkeley.edu/californialawreview/vol90/iss4/2>. Acesso em: 18 jun. 2018.

STEWART, B. **Privacy impact assessments**. Privacy Law & Policy Reporter(4):61–4. Disponível em: <http://www.austlii.edu.au/au/journals/PLPR/1996/39.html>. Acesso em: 20 maio 2018

STEWART, B. Privacy impact assessment: some approaches, issues and examples. **Assistant Commissioners Office of the Privacy Commissioner, New Zealand**, 2002. Disponível em: <http://jeb.cerps.org.tw/files/JEB2002-009.pdf>. Acesso em: 23 nov. 2017.

SWEET, Ken. Equifax: 2.5 million more Americans may be affected by hack. 2017. Disponível em: <http://www.chicagotribune.com/business/ct-biz-equifax-2-5-million-more-americans-story.html>. Acesso em: 6 out. 2017.

TANCOCK, D., PEARSON, S., & CHARLESWORTH, A. (2013). A privacy impact assessment tool for cloud computing**.** In ***Privacy and security for Cloud computing*** (pp. 73-123). Springer, London.

TENE, Omer. Privacy: The new generations. **International Data Privacy Law**, [s. l.], v. 1, n. 1, p. 15–22, 2011.
VAN DIJK, Niels; GELLERT, Raphaël; ROMMETVEIT, Kjetil. A risk to a right? Beyond data protection risk assessments. **Computer Law & Security Review: The International Journal of Technology Law and Practice**, [s. l.], v. 32, n. 2, p. 286–306, 2016.

VAN LIESHOUT, Marc *et al*. **Privacy by Design: an alternative to existing practice in safeguarding privacy**. Info v. 13, n. 6, p. 55–68, 2011.

WALDMAN, Ari Ezra. **Privacy's Law of Design**. Rochester, NY: Social Science Research Network, 2018. Disponível em: <https://papers.ssrn.com/abstract=3263000>. Acesso em: 25 out. 2018.

WATERS, G. (2006). **Conquering advanced metering cost and risk**. Electric Energy T&D Magazine, 10:22–25.

WEN, Miles H. F. *et al*. A survey on smart grid communication system. **APSIPA Transactions on Signal and Information Processing**, [s. l.], v. 4, 2015. Disponível em: <http://www.journals.cambridge.org/abstract_S2048770315000098>. Acesso em: 25 jul. 2018.

WP29. Article 29 Working Party. **Guidelines on Data Protection Impact Assessment (DPIA) and determining whether processing is "likely to result in a high risk" for the purposes of Regulation 2016/679**. 2017. Disponível em: <https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=611236>. Acesso em: 9 ago. 2019.

WRIGHT, D. The state of the art in privacy impact assessment. **Computer Law & Security Review**, v. 28, n. 1, p. 54–61, 2012.

WYNN, Gerard. Privacy concerns challenge smart grid rollout. **Reuters**, 25. jun. 2010. Disponível em: <https://www.reuters.com/article/energy-smart/privacy-concerns-challenge-smart-grid-rollout-idUSLDE65N2CI20100625>. Acesso em: 20 nov. 2017.

APÊNDICE 1 – PORTFÓLIO DE ANÁLISE

Publication Year	Author	Title	Publication Title	ISSN	Citations
2014	Yan, Zheng; Zhang, Peng; Vasilakos, Athanasios V.	A survey on trust management for Internet of Things	Journal of Network and Computer Applications	1084-8045	403
2012	Rong, Chunming; Nguyen, Son T.; Jaatun, Martin Gilje	Beyond lightning: A survey on security challenges in cloud computing	Computers and Electrical Engineering	0045-7906	306
2010	Cavoukian, Ann; Polonetsky, Jules; Wolf, Christopher	SmartPrivacy for the Smart Grid: embedding privacy into the design of electricity conservation	Identity in the Information Society	1876-0678	180
2017	Sivarajah, Uthayasankar; Kamal, Muhammad Mustafa; Irani, Zahir; Weerakkody, Vishanth	Critical analysis of Big Data challenges and analytical methods	Journal of Business Research	0148-2963	159
2011	Rajagopalan, S. Raj; Sankar, Lalitha; Mohajer, Soheil; Poor, H. Vincent	Smart Meter Privacy: A Utility-Privacy Framework			146
2013	Sankar, L.; Rajagopalan, S. R.; Mohajer, S.; Poor, H. V.	Smart Meter Privacy: A Theoretical Framework	Smart Grid, IEEE Transactions on	1949-3053	143
2015	Baek, Joonsang; Vu, Quang Hieu; Liu, Joseph K.; Huang, Xinyi; Xiang, Yang	A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid	Cloud Computing, IEEE Transactions on	2168-7161	132
2014	Bari, Ataul; Jiang, Jin; Saad, Walid; Jaekel, Arunita	Challenges in the Smart Grid Applications: An Overview	International Journal of Distributed Sensor Networks	1550-1329	67
2011	Tene, Omer	Privacy: The new generations	International Data Privacy Law	2044-3994	64
2014	Park, Chan-Kook; Kim, Hyun-Jae; Kim, Yang-Soo	A study of factors enhancing smart grid consumer engagement	Energy Policy	0301-4215	48
2016	Jain, Priyank; Gyanchandani, Manasi; Khare, Nilay	Big data privacy: a technological perspective and review	Journal of Big Data	2196-1115	45
2014	Park, Namje; Kim, Marie	Implementation of load management application system using smart grid privacy policy in energy	Cluster Computing	1386-7857	39

		management service environment			
2011	McNeil, Sonia K.	Privacy and the modern grid	Harvard Journal of Law & Technology	0897-3393	37
2013	Zeadally, Sherali; Pathan, Al-Sakib; Alcaraz, Cristina; Badra, Mohamad	Towards Privacy Protection in Smart Grid	Wireless Personal Communications	0929-6212	34
2013	Fan, Xinxin; Gong, Guang	Security Challenges in Smart-Grid Metering and Control Systems	Technology Innovation Management Review	1927-0321	24
2013	Gómez Mármol, Félix; Sorge, Christoph; Petrlic, Ronald; Ugus, Osman; Westhoff, Dirk; Martínez Pérez, Gregorio	Privacy-enhanced architecture for smart metering	International Journal of Information Security	16155262	23
2014	Mantelero, Alessandro	The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics	Computer Law & Security Review: The International Journal of Technology Law and Practice	0267-3649	22
2014	Brown, Ian	Britain's smart meter programme: a case study in privacy by design.(The Future of Data Protection: Collapse or Revival?)	International Review of Law, Computers & Technology	1360-0869	21
2016	Benhamouda, Fabrice; Joye, Marc; Libert, Benoît	A New Framework for Privacy-Preserving Aggregation of Time-Series Data	ACM Transactions on Information and System Security (TISSEC)	1094-9224	20
2016	Mantelero, Alessandro	Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection	Computer Law & Security Review: The International Journal of Technology Law and Practice	0267-3649	19
2016	Shakil, Kashish; Alam, Mansaf	Recent Developments in Cloud Based Systems: State of Art	International Journal of Computer Science and Information Security	19475500	17

2015	Piggin, Richard	Are industrial control systems ready for the cloud?	International Journal of Critical Infrastructure Protection	1874-5482	16
2017	Munshi, Amr A.; Mohamed, Yasser A.-R. I.	Big data framework for analytics in smart grids	Electric Power Systems Research	0378-7796	15
2015	Huang, Shuang; Zhou, Chun-Jie; Yang, Shuang-Hua; Qin, Yuan-Qing	Cyber-physical system security for networked industrial processes	International Journal of Automation and Computing	1476-8186	13
2018	Wang, Tian; Zhou, Jiyuan; Huang, Minzhe; Bhuiyan, Md zakirul alam; Liu, Anfeng; Xu, Wenzheng; Xie, Mande	Fog-based storage technology to fight with cyber threat	Future Generation Computer Systems	0167-739X	10
2017	Mai, Vu; Khalil, Ibrahim	Design and implementation of a secure cloud-based billing model for smart meters as an Internet of things using homomorphic cryptography	Future Generation Computer Systems	0167-739X	10
2017	Kaur, Jaideep; Kaur, Kamaljit	Internet of Things: A Review on Technologies, Architecture, Challenges, Applications, Future Trends	International Journal of Computer Network and Information Security	20749090	10
2016	Barbosa, Pedro; Brito, Andrey; Almeida, Hyggo	A Technique to provide differential privacy for appliance usage in smart metering	Information Sciences	0020-0255	10
2018	Huang, Qinlong; Wang, Licheng; Yang, Yixian	DECENT: Secure and fine-grained data access control with policy updating for constrained IoT devices	World Wide Web	1386-145X	9
2016	van Dijk, Niels; Gellert, Raphaël; Rommetveit, Kjetil	A risk to a right? Beyond data protection risk assessments	Computer Law & Security Review: The International Journal of Technology Law and Practice	0267-3649	9
2014	King, Nancy J.; Jessen, Pernille W.	Smart metering systems and data sharing: why getting a smart meter should also mean getting strong information privacy	International Journal of Law and Information Technology	0967-0769	8

		controls to manage data sharing			
2015	Seto, Yoichi	Application of Privacy Impact Assessment in the Smart City	Electronics and Communications in Japan	1942-9533	8
2015	Wen, Miles; Leung, Ka-Cheong; Li, Victor; He, Xingze; Kuo, C-C	A survey on smart grid communication system	APSIPA Transactions on Signal and Information Processing	2048-7703	7
2016	Parvez, Imtiaz; Sarwat, Arif; Wei, Longfei; Sundararajan, Aditya	Securing Metering Infrastructure of Smart Grid: A Machine Learning and Localization Based Key Management Approach	Energies	1996-1073	7
2018	Romanou, Anna	The necessity of the implementation of Privacy by Design in sectors where data protection concerns arise	Computer Law & Security Review: The International Journal of Technology Law and Practice	0267-3649	6
2017	Mylrea, Michael	Smart energy-internet-of-things opportunities require smart treatment of legal, privacy and cybersecurity challenges	The Journal of World Energy Law & Business	1754-9957	5
2017	Ferrag, Mohamed	EPEC: an efficient privacy-preserving energy consumption scheme for smart grid communications	Telecommunication Systems	10184864	3
2018	Leszczyna, Rafał	Cybersecurity and privacy in standards for smart grids – A comprehensive survey	Computer Standards & Interfaces	0920-5489	3
2018	Lee, Donghyeok; Park, Namje; Kim, Geonwoo; Jin, Seunghun	De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment	Peer-To-Peer Networking and Applications	19366442	2
2016	Alcón, Jose; López, Lourdes; Martínez, Jose-Fernan; Cifuentes, Gregorio	Trust and Privacy Solutions Based on Holistic Service Requirements	Sensors	1424-8220	2
2018	Sani, Abubakar Sadiq; Yuan, Dong; Jin, Jiong; Gao, Longxiang; Yu, Shui; Dong, Zhao Yang	Cyber security framework for Internet of Things-based Energy Internet	Future Generation Computer Systems	0167-739X	1

2017	Liu, Qin; Srinivasan, Avinash; Hu, Jiankun; Wang, Guojun	Preface: Security and privacy in big data clouds	Future Generation Computer Systems	0167-739X	1
2016	BARTHOLOMEW, ANDREW	THE SMART GRID IN MASSACHUSETTS: A PROPOSAL FOR A CONSUMER DATA PRIVACY POLICY.	Boston College Environmental Affairs Law Review	1907034	0
2018	Ge, Shanshan; Zeng, Peng; Lu, Rongxing; Choo, Kim-Kwang	FGDA: Fine-grained data analysis in privacy-preserving smart grid communications	Peer-to-Peer Networking and Applications	1936-6442	0
2018	Yang, Junjie; Huang, Gengqiang; Wei, Chunjuan	Privacy-aware electricity scheduling for home energy management system	Peer-to-Peer Networking and Applications	1936-6442	0
2018	Tudor, Valentin; Almgren, Magnus; Papatriantafilou, Marina	The influence of dataset characteristics on privacy preserving methods in the advanced metering infrastructure	Computers & Security	0167-4048	0
2018	Rial, Alfredo; Danezis, George; Kohlweiss, Markulf	Privacy-preserving smart metering revisited	International Journal of Information Security	1615-5262	0
2017	Zhang, Lei; Zhang, Jing	EPPRD: An Efficient Privacy-Preserving Power Requirement and Distribution Aggregation Scheme for a Smart Grid	Sensors	14248220	0
2017	Piatkowska, Ewa; Bajraktari, Agron; Chhajed, Dharini; Smith, Paul	Tool support for data protection impact assessment in the smart grid	e & i Elektrotechnik und Informationstechnik	0932-383X	0
2017	Kumar, Ravinder; Kumar, Anil	NOVEL RISK ASSESSMENT FRAMEWORK FOR SMART GRID	International Journal of Advanced Research in Computer Science	9765697	0
2018	Miao, Yinbin; Ma, Jianfeng; Liu, Ximeng; Liu, Zhiquan; Zhang, Junwei; Wei, Fushan	DOAS: Efficient data owner authorized search over encrypted cloud data	Peer-to-Peer Networking and Applications	1936-6442	0
2018	Silva, Leandro; Barbosa, Pedro; Marinho, Rodolfo; Brito, Andrey	Security and privacy aware data aggregation on cloud computing	Journal of Internet Services and Applications	1867-4828	0
2018	Li, Wenting; Shen,	Breaking Three Remote user Authentication	Journal of Signal	1939-8018	0

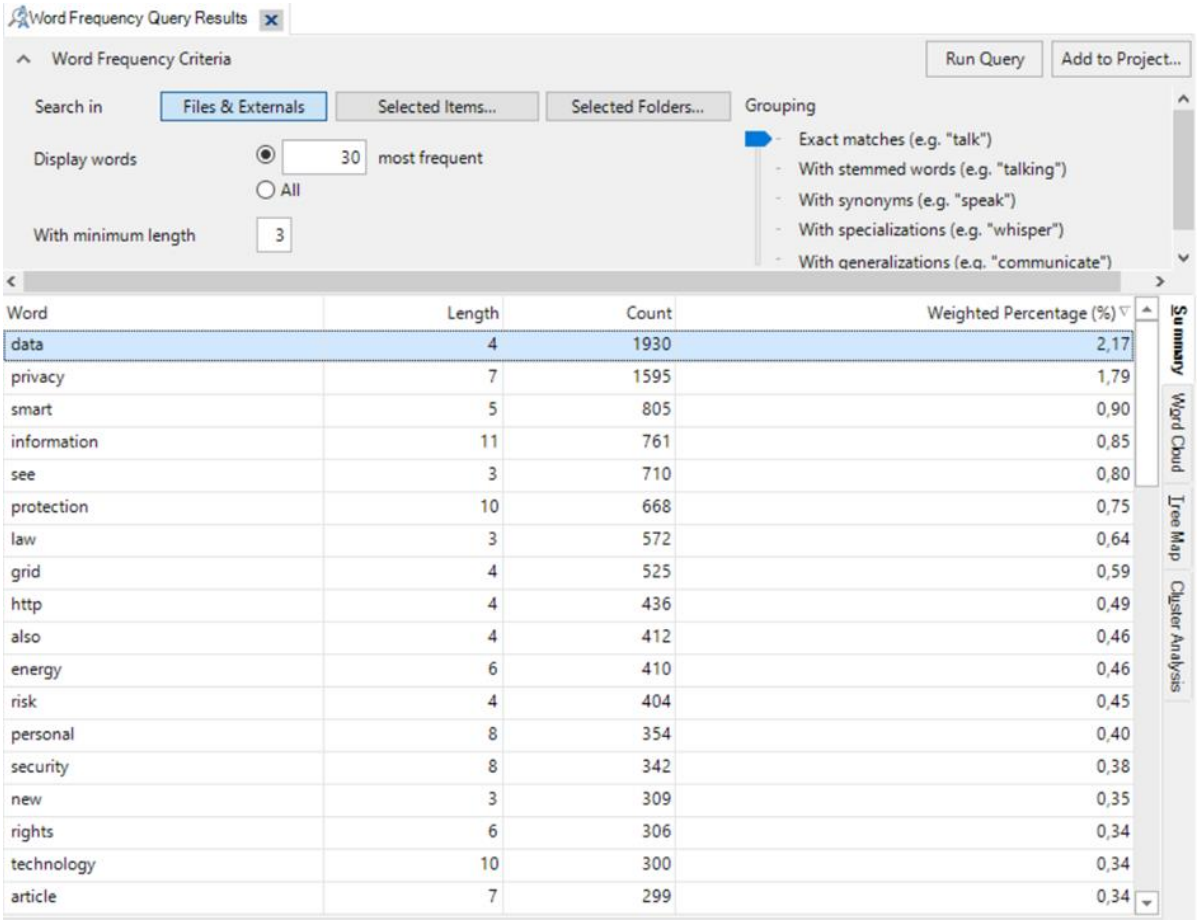
	Yaosheng; Wang, Ping	Systems for Mobile Devices	Processing Systems		
2017	Li, Ji; Wei, Jianghong; Liu, Wenfen; Hu, Xuexian	PMDP: A Framework for Preserving Multiparty Data Privacy in Cloud Computing.(Research Article)	Security and Communicatio n Networks	1939-0114	0
2018	Oztemel, Ercan	Literature review of Industry 4.0 and related technologies	Journal of Intelligent Manufacturing	9565515	0

APÊNDICE 2 – PORTFÓLIO DE INTERESSE

Publication Year	Author	Title	Publication Title	ISSN	Citations
2014	Barbato, Antimo; Capone, Antonio	Optimization Models and Methods for Demand-Side Management of Residential Users: A Survey	Energies	1996-1073	78
2016	Han, Wenlin; Xiao, Yang	Privacy preservation for V2G networks in smart grid: A survey	Computer Communications	0140-3664	37
2017	Molina-Solana, Miguel; Ros, María; Ruiz, M. Dolores; Gómez-Romero, Juan; Martin-Bautista, M.J.	Data science for building energy management: A review	Renewable and Sustainable Energy Reviews	1364-0321	37
2014	Hess, David J.	Smart meters and public acceptance: comparative analysis and governance implications.	Health, Risk & Society	13698575	30
2017	Zhou, Shan; Brown, Marilyn A.	Smart meter deployment in Europe: A comparative case study on the impacts of national policy schemes	Journal of Cleaner Production	0959-6526	23
2014	Mantelero, Alessandro	The future of consumer data protection in the E.U. Re-thinking the "notice and consent" paradigm in the new era of predictive analytics	Computer Law & Security Review: The International Journal of Technology Law and Practice	0267-3649	22
2015	Asri, Satin; Pranggono, Bernardi	Impact of Distributed Denial-of-Service Attack on Advanced Metering Infrastructure	Wireless Personal Communications	0929-6212	19
2018	Jiang, Rong; Lu, Rongxing; Choo, Kim-Kwang Raymond	Achieving high performance and privacy-preserving query over encrypted multidimensional big metering data	Future Generation Computer Systems	0167-739X	19
2016	Park, Namje	Mutual Authentication Scheme in Secure Internet of Things Technology for Comfortable Lifestyle	Sensors	1424-8220	15
2017	Khan, Zaheer; Pervez, Zeeshan; Abbasi, Abdul Ghafoor	Towards a secure service provisioning framework in a Smart city environment	Future Generation Computer Systems	0167-739X	12

2017	Khan, Saad; Parkinson, Simon; Qin, Yongrui	Fog computing security: a review of current applications and security solutions	Journal of Cloud Computing	2192-113X	10
2018	Wang, Huaqun; He, Debiao; Sun, Yanfei; Kumar, Neeraj; Choo, Kim-Kwang Raymond	PAT: A precise reward scheme achieving anonymity and traceability for crowdcomputing in public clouds	Future Generation Computer Systems	0167-739X	7
2018	Peters, Derek; Axsen, Jonn; Mallett, Alexandra	The role of environmental framing in socio-political acceptance of smart grid: The case of British Columbia, Canada	Renewable and Sustainable Energy Reviews	1364-0321	5
2016	Rodrigues, Rowena	The future of privacy certification in Europe: an exploration of options under article 42 of the GDPR.	International Review of Law, Computers & Technology	13600869	3
2017	Raab, Charles; Szekely, Ivan	Data protection authorities and information technology	Computer Law & Security Review: The International Journal of Technology Law and Practice	0267-3649	3
2018	Lee, Donghyeok; Park, Namje; Kim, Geonwoo; Jin, Seunghun	De-identification of metering data for smart grid personal security in intelligent CCTV-based P2P cloud computing environment	Peer-To-Peer Networking and Applications	19366442	2
2017	Warkentin, Merrill; Goel, Sanjay; Menard, Philip	Shared Benefits and Information Privacy: What Determines Smart Meter Technology Adoption?	Journal of the Association for Information Systems	15369323	1
2018	Heartfield, Ryan; Loukas, George; Budimir, Sanja; Bezemskij, Anatolij; Fontaine, Johnny R.J.; Filippoupolitis, Avgoustinos; Roesch, Etienne	A taxonomy of cyber-physical threats and impact in the smart home	Computers & Security	0167-4048	0
2018	Liu, Qun-Ying; Tian, Guiyun; Gao, Bin; Fagen, Li	AKAIoTs: authenticated key agreement for Internet of Things	Wireless Networks	10220038	0

ANEXO 1 – FREQUÊNCIA DE PALAVRAS PARA O GRUPO DE TEXTOS DE PBD



Word	Length	Count	Weighted Percentage (%)
data	4	1930	2,17
privacy	7	1595	1,79
smart	5	805	0,90
information	11	761	0,85
see	3	710	0,80
protection	10	668	0,75
law	3	572	0,64
grid	4	525	0,59
http	4	436	0,49
also	4	412	0,46
energy	6	410	0,46
risk	4	404	0,45
personal	8	354	0,40
security	8	342	0,38
new	3	309	0,35
rights	6	306	0,34
technology	10	300	0,34
article	7	299	0,34