REVISTA Mundi
Engenharia, Tecnologia e Gestão
INSTITUTO FEDERAL Paraná

A PROTEÇÃO DE DADOS PESSOAIS NO CONTEXTO DA REDE ELÉTRICA INTELIGENTE

DATA PROTECTION IN THE SMART GRID CONTEXT

Matheus F. Machado [1]

Décio Estevão do Nascimento [2]

Keiko Veronica Ono Fonseca [3]

Resumo: 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. Assim, o objetivo geral deste artigo é discutir a proteção de dados pessoais no contexto da Rede Elétrica Inteligente. Trata-se de pesquisa de natureza aplicada e, quanto aos seus objetivos, descritiva, utilizando procedimentos de pesquisa documental e bibliográfica. Os resultados apontam para a necessidade de se considerar os riscos à proteção de dados pessoais desde a concepção do sistema, quando são mais simples e baratos de serem mitigados, até sua implementação com a finalidade de proteção do direito à privacidade.

Palavras-chave: Rede Elétrica Inteligente. Dados Pessoais. Privacidade.

Abstract: 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. Therefore, the purpose of this article is to discuss personal data protection in the Smart Grid context. The research is applied in its nature and descriptive in its purposes, using methods of bibliographic and documentary research. The results point to the need of considering personal data protection risks since the design of the system, when they are cheaper and simpler to be solved, until its implementation with the aim of protecting the right of privacy.

Keywords: Smart Grid. Personal Data. Privacy.

[1] Mestre, Universidade Tecnológica Federal do Paraná, mc77res@tuta.io
[2] Doutor, UTFPR, decio@utfpr.edu.br
[3] Doutora, UTFPR, keiko@utfpr.edu.br

1 INTRODUÇÃO

O desenvolvimento da Rede Elétrica Inteligente (REI), *Smart Grid* (*SG*), 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 REI 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).

Os fluxos bidirecionais de informação se dão utilizando medidores eletrônicos, *Smart Meters* (*SM*), instalados nas Unidades Consumidoras (UC). Segurança e privacidade serão fatores essenciais ao desenvolvimento e aceitação pública dos medidores eletrônicos *(SM)* (EFTHYMIOU; KALOGRIDIS, 2010; MINAMIZAKI *et al*., 2013). Preocupações de privacidade relativas ao uso de *SM* decorrem do fato de que na medição detalhada de uso realizada em curtos intervalos de tempo é possível a inferência sobre diversos aspectos da UC apenas pela análise dos dados de consumo (PARSON *et al*., 2012).

Este trabalho é parte da investigação conduzida por um consórcio internacional para a execução do projeto SecureCloud (SECURECLOUD, 2017). O projeto visa o desenvolvimento de tecnologias de processamento seguro de grandes volumes de dados em nuvens não confiáveis. Os casos de uso propostos para a demonstração da arquitetura SecureCloud são de Smart Grids.

2 DESENVOLVIMENTO

Nesta seção serão apresentados conceitos sobre dados pessoais e sua definição na legislação brasileira, sobre a Rede Elétrica Inteligente e de que maneira sua operação se relaciona com o uso de dados pessoais.

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 conceituar a REI e dados pessoais, por meio de levantamento bibliográfico e documental sobre o tema.

2.1 Dados pessoais

Com a mudança na dinâmica econômica global os dados pessoais tomaram posição central na vida em sociedade (DONEDA, 2011). O primeiro artigo da Lei nº 13.709 de 14 de agosto 2018, Lei Geral de Proteção de Dados Pessoais (LGPDP), indica que a tutela legal sobre o tratamento de dados pessoais tem "o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural" (BRASIL, 2018). Ainda que a terminologia legislativa trate da "proteção de dados pessoais", sua finalidade não se exerce sobre os dados, mas sim sobre seus titulares (DONEDA, 2010).

Conceituar dados pessoais não é tarefa simples, mas essencial para a definição de aplicabilidade de eventual Lei que pretenda protege-los. A LGPDP definiu dados pessoais como "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018). Tal definição se justifica na medida em que cada vez mais é desnecessário que o registro identifique diretamente a pessoa para que ela ainda assim esteja sujeita aos efeitos do tratamento de seus dados (BIONI, 2015).

A legislação apresenta os dados sensíveis como uma subdivisão de dados pessoais que, pela sua natureza, mereceria maiores proteções. Dado sensível é definido no texto legal como:

> dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural (BRASIL, 2018).

Contudo, a conceituação de dado sensível tem dado espaço à tendência de se considerar sensível o tratamento que se realiza sobre os dados pessoais, a despeito de sua natureza. Esta tendência decorre da imprevisibilidade dos

efeitos causados ao titular simplesmente pela natureza do dado que é tratado (DONEDA, 2010).

A legislação também conceitua dado anonimizado como aquele “relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento” (BRASIL, 2018), não sendo considerados dados pessoais para os fins da LGPDP, excetuando-os de sua proteção. Uma vez publicizada, a informação não pode ser removida e, conforme se desenvolvem as técnicas de re-identificação e se multiplicam as bases de dados disponíveis, aumentam as chances de reversão de um dado considerado anônimo em dado pessoal (NARAYANAN; HUEY; FELTEN, 2016).

2.2 Rede Elétrica Inteligente (REI)

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). 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. Além das vantagens ambientais, espera-se que com a Rede Elétrica Inteligente a confiabilidade no sistema elétrico aumente significativamente (AMIN; WOLLENBERG, 2005; WEN *et al*., 2015).

A Plataforma de Tecnologia Europeia para Smart Grids define Rede Elétrica Inteligente (REI) 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, 2014, 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

Rede Elétrica Existente	***Smart Grid***
Medidores eletromecânicos	Medidores digitais
Fluxo unidirecional de comunicação	Fluxo bidirecional de comunicação
Geração centralizada	Geração distribuída
Hierárquica	Rede
Poucos sensores	Sensores espalhados
“Cega”	Automonitoramento
Restauração manual	Autorreparação
Falhas e apagões	Adaptativa e segregativa
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).

2.3 Dados pessoais na Rede Elétrica Inteligente (REI)

As redes elétricas tradicionais transmitem energia de um gerador central a muitos usuários, enquanto a Rede Elétrica Inteligente (REI) utiliza fluxos bidirecionais de energia e informação para criar uma rede avançada

automatizada e distribuída de entrega de energia (FANG *et al*., 2012). A geração de valor esperada com a REI advém da disponibilidade de uma nova gama de informações geradas pelo uso dos *smart meters* (*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). O uso das informações granulares sobre o consumo de energia é componente essencial para o sistema de resposta de demanda (LERNER; MULLIGAN, 2008) e necessário para as inovações pretendidas com a REI. 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.

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, quando se tenha realizado previamente a medição do conteúdo para referência (CARLUCCIO; BRINKHAUS, 2011; LAM; FUNG, 2007; 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).

Os dados de consumo energético podem sofrer diversos tipos de usos que tragam prejuízos aos titulares, como ladrões descobrindo padrões de ocupação e de uso de sistemas de alarmes ou usos comerciais como no direcionamento de publicidade (McKENNA; RICHARDSON; THOMSON, 2012; QUINN 2009) além dos prejuízos ainda não vislumbrados que possam ocorrer

com o desenvolvimento das tecnologias e combinação com outras bases de dados (BIONI, 2005; NARAYANAN; HUEY; FELTEN, 2016; QUINN, 2009). Considerar a privacidade desde a concepção do projeto permite que potenciais riscos sejam identificados no início e endereçados quando ainda são mais baratos e simples de corrigir (WRIGHT, 2012)

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. Por duas vezes em 2009 o senado bloqueou legislações que previam a implantação dos medidores eletrônicos por força da pressão social em torno da questão da privacidade. (CUIJPERS; KOOPS, 2013; HOENKAMP; HUITEMA; DE MOOR-VAN VUGT, 2011).

2.4 Discussão

Atualmente os dados pessoais têm grande relevância social e podem trazer reflexos variados aos seus titulares, desde restrições creditícias até precificação variada sobre produtos e serviços (BIONI, 2015; DONEDA, 2010; DONEDA, 2011). Sua proteção é prevista em Lei e tem a finalidade de garantia de direitos fundamentais (BRASIL, 2018).

A operação da Rede Elétrica Inteligente (REI) depende do uso das informações de consumo energético advindas das Unidades Consumidoras (UC) (LERNER; MULLIGAN, 2008; QUINN, 2009). Estas informações de consumo podem identificar consumidores e seus comportamentos (CARLUCCIO; BRINKHAUS, 2011; LAM; FUNG, 2007; PARSON *et al*., 2012; WYNN, 2010). Se dados pessoais são “informação relacionada a pessoa natural identificada ou identificável” (BRASIL, 2018) e dados sensíveis são informações que por força de seu tratamento revelam aspectos considerados sensíveis sobre o sujeito, como aqueles referentes à saúde ou à vida sexual (BRASIL, 2018; DONEDA, 2010), conclui-se que informações sobre consumo

energético na Rede Elétrica Inteligente são dados pessoais e podem ser dados sensíveis a depender de seu tratamento.

Parte dos benefícios esperados com a implantação da REI dependem da participação ativa das unidades consumidoras no planejamento de seu consumo (EUROPEAN COMMISSION *et al.*, 2013; FANG *et al.*, 2012) além da necessidade da aceitação pública do sistema fortemente atrelada às garantias de segurança e privacidade que podem ser oferecidas (EFTHYMIOU; KALOGRIDIS, 2010; MINAMIZAKI *et al*., 2013). O caso da implantação dos *smart meters* na Holanda demonstra que a privacidade é fator de grande importância na aceitação do sistema e que, quando interesses técnicos e comercias se sobrepõem às garantias de direitos, podem ocorrer perdas de investimentos e atraso no desenvolvimento da Rede (CUIJPERS; KOOPS, 2013; HOENKAMP; HUITEMA; DE MOOR-VAN VUGT, 2011).

Soma-se a isto o fato de que, após divulgada, a informação não pode ser removida (NARAYANAN; HUEY; FELTEN, 2016), portanto, correções de privacidade posteriores, além de mais caras e complicadas (WRIGHT, 2012) podem não ser efetivas.

3 CONSIDERAÇÕES FINAIS

O objetivo deste artigo era o de discutir a proteção de dados pessoais no contexto da Rede Elétrica Inteligente (REI) como uma necessidade decorrente dos dados de consumo energético utilizados para sua operação.

Algumas abordagens têm sido estudadas para equacionar o uso de dados pessoais em Redes Elétricas Inteligentes. Efthymiou e Kalogridis (2010) propõem uma arquitetura de privacidade para REIs que envolve um serviço de terceiro garantidor (*escrow service*) para realizar a anonimazação dos dados. Rusitschka, Eger e Gerdes (2010) discutem o uso de computação em nuvem para dados de REIs destacando as vantagens da gerência distribuída de dados e processamento paralelo de informação em tempo real, porém alertando para a necessidade de se considerar os riscos adicionais à privacidade em decorrência do armazenamento e gerência da informação ser de responsabilidade do provedor de serviços. Como soluções são propostas

arquiteturas de dados de múltiplo gerenciamento e operações criptográficas para anonimização dos dados (RUSITSCHKA; EGER; GERDES, 2010).

Baek *et al*. (2015) propõem um framework de gerenciamento seguro, baseado em uma estrutura hierárquica de computação em nuvem e com criptografia baseada em identidade (*identity-based encryption*) para fornecer diferentes tipos de análise *big-data*, ao qual denominam "*Smart-Frame*".

Riella *et al*. (2018) discute um caso de uso do projeto SecureCloud que utiliza *hardware* específico para processamento seguro de dados (IntelSGX) e acesso baseado em função (*role-based access*) para assegurar que somente os dados necessários para a realização de determinada função sejam acessados.

Ferrag *et al*. (2016) realizam revisão de literatura de esquemas de privacidade para comunicação em Redes Elétricas Inteligentes; Leszczyna (2018) apresenta uma revisão completa de padrões de privacidade aplicáveis às REIs e Asghar *et al*. (2017) apresentam uma revisão de literatura sobre privacidade de dados em *Smart Meters* com uma visão geral, limitações e recomendações para pesquisas futuras.

Concluiu-se que as preocupações de privacidade podem prejudicar a adoção do sistema e acarretar perdas às companhias que desejem o desenvolvimento da REI. Os encaminhamentos apontam para as vantagens de se considerar a privacidade desde a concepção do sistema por permitir soluções de privacidade mais baratas, simples e efetivas, aumentando a possibilidade de aceitação social do sistema.

4 AGRADECIMENTOS

Este trabalho recebeu financiamento do programa da União Europeia de pesquisa e inovação Horizon 2020 sob os acordos de bolsa 690111 (SecureCloud) and MCTIC /RNP Brazil (ACT 2549). Os autores também agradecem ao Programa de Pós-Graduação em Planejamento e Governança Pública da Universidade Tecnológica Federal do Paraná.

REFERÊNCIAS

AMIN, S. Massoud; WOLLENBERG, B. F. Toward a smart grid: power delivery for the 21st century. **IEEE Power and Energy Magazine**, [s. l.], v. 3, n. 5, p. 34–41, 2005.

ASGHAR, Muhammad Rizwan et al. Smart Meter Data Privacy: A Survey. **IEEE Communications Surveys & Tutorials**, [s. l.], v. 19, n. 4, p. 2820–2835, 2017.

BAEK, Joonsang et al. A Secure Cloud Computing Based Framework for Big Data Information Management of Smart Grid. **Cloud Computing, IEEE Transactions on**, [s. l.], v. 3, n. 2, p. 233–244, 2015.

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.

BIONI, Bruno Ricardo. **Xeque-Mate, o tripé da proteção de dados pessoais no jogo de xadrez das iniciativas legislativas no Brasil**. São Paulo: GPoPAI/USP. 2015

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.

CARVALHO, Priscila. Smart Metering Deployment in Brazil. **Energy Procedia**, Sustainability in Energy and Buildings: Proceedings of the 7th International Conference SEB-15. [s. l.], v. 83, Sustainability in Energy and Buildings: Proceedings of the 7th International Conference SEB-15, p. 360–369, 2015.

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>.

CUIJPERS, Colette; KOOPS, Bert-Jaap. Smart Metering and Privacy in Europe: Lessons from the Dutch Case. In: GUTWIRTH, Serge et al. (Eds.). **European Data Protection: Coming of Age**. Dordrecht: Springer Netherlands, 2013. p. 269–293.

DONEDA, Danilo. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia**. Brasília: Escola Nacional de Defesa do Consumidor. 2010.

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 ago. 2018.

EFTHYMIOU, Costas; KALOGRIDIS, Georgios. **Smart Grid Privacy via Anonymization of Smart Metering Data**. IEEE, 2010. Disponível em: <http://ieeexplore.ieee.org/document/5622050/>.

ETP Smart Grids. **The SmartGrids European Technology Platform**. 2006. Disponível em: <http://www.smartgrids.eu/ETPSmartGrids>. Acesso em: 05 jun. 2017.

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>.

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

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.

FERRAG, Mohamed Amine et al. A Survey on Privacy-preserving Schemes for Smart Grid Communications. **arXiv:1611.07722 [cs]**, [s. l.], 2016. Disponível em: <http://arxiv.org/abs/1611.07722>. Acesso em: 7 nov. 2018.

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

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>.

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.

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.

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.

NARAYANAN, Arvind; HUEY, Joanna; FELTEN, Edward W. A Precautionary Approach to Big Data Privacy. In: GUTWIRTH, Serge; LEENES, Ronald; DE HERT, Paul (Eds.). **Data Protection on the Move**. Dordrecht: Springer Netherlands, 2016. v. 24p. 357–385.

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

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.

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: ACM Press, 2018. Disponível em: <http://dl.acm.org/citation.cfm?doid=3195258.3195263>. Acesso em: 21 ago. 2018.

RUSITSCHKA, Sebnem; EGER, Kolja; GERDES, Christoph. Smart Grid Data Cloud: A Model for Utilizing Cloud Computing in the Smart Grid Domain. In: **First Ieee International Conference On Smart Grid Communications**, 2010, Gaithersburg, MD, USA. Disponível em: <http://ieeexplore.ieee.org/document/5622089/>. Acesso em: 25 out. 2018.

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.

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

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.

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.

Edição especial – I Encontro Nacional Interdisciplinar em Ciência, Tecnologia e Sociedade (ENICTS 2019)

Enviado em: 14 mai. 2020

Aceito em: 05 jul. 2020

Editor responsável: Mateus das Neves Gomes