TEIDER, Josélio Jorge. TEIDER, Lucas Hinckel. BLANCHET, Luiz Alberto. Direito da energia e (ciber) terrorismo: A prevenção como necessário fator de desenvolvimento no setor energético. In: Revista Eletrônica do Curso de Direito do Centro Universitário UniOpet. Curitiba-PR. Ano XIII, n. 22, jan/jun 2020. ISSN 2175-7119.

DIREITO DA ENERGIA E (CIBER)TERRORISMO: A PREVENÇÃO COMO NECESSÁRIO FATOR DE DESENVOLVIMENTO NO SETOR ENERGÉTICO

ENERGY LAW AND (CYBER)TERRORISM: PREVENTION AS A NECESSARY DEVELOPMENT FACTOR IN THE ENERGY SECTOR

Josélio Jorge Teider[1]

Lucas Hinckel Teider[2]

Luiz Alberto Blanchet[3]

Resumo:

O objetivo do presente artigo científico constituía-se como evidenciar o risco de ciberterrorismo no setor energético e investigar quais seriam as medidas adequadas para prevenir ou responder adequadamente à esta circunstância. O método de pesquisa empregado foi o fenomenológico (descrevendo uma realidade tal qual ela é a partir de uma interpretação e onde o autor é reconhecidamente importante no processo de construção do conhecimento), com o procedimento de pesquisa monográfico e a técnica de pesquisa bibliográfica. A pesquisa resultou na compreensão da aproximação dos princípios do Direito da Energia com a prevenção do ciberterrorismo por meio de segurança cibernética, evidenciando tal risco (e suas prováveis consequências) e assumindo a imperiosidade de medidas de prevenção, monitoramento e resposta. Concluiu-se que, além da discussão acerca da importância e dos benefícios da energia, é igualmente necessária a contemplação dos riscos, notadamente o de ciberterrorismo, a fim de garantir o funcionamento das infraestruturas de geração, fornecimento e distribuição de energia. Em um cenário de ampla utilização e dependência tecnológica, atende aos princípios do Direito da Energia o estabelecimento de Programas de Integridade (Programas de *Compliance*) a fim de prevenir, monitorar ou responder adequadamente às possíveis circunstâncias de ciberterrorismo com o mapeamento de riscos, elaboração de documentos e implementação de controles, assegurando-se, desta maneira, o desenvolvimento do setor energético, do país, da sociedade e dos indivíduos.

Palavras-chave: Direito da Energia; Terrorismo; Ciberterrorismo; Prevenção; Desenvolvimento.

[1]Bacharel em Informática pela Universidade Federal do Paraná. Bacharel em Direito pelo Centro Universitário Curitiba. Especialista pelo MBA em Gestão Empresarial da FGV. Mestre em Direito pela Pontifícia Universidade Católica do Paraná. *E-mail*: joselio@cartacerta.com.br.

[2]Mestrando em Direito Econômico e Desenvolvimento pelo Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná (Curitiba-PR, Brasil). Bolsista do Programa de Excelência Acadêmica da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior (PROEX/CAPES). *E-mail*: lucas.teider@gmail.com.

[3] Doutor em Direito pela Universidade Federal do Paraná. Professor do Programa de Pós-Graduação em Direito da Pontifícia Universidade Católica do Paraná. Membro Catedrático da Academia Brasileira de Direito Constitucional. *E-mail*: blanchet@blanchet.adv.br.

***Abstract*:**

The purpose of this scientific article was to highlight the risk of cyberterrorism in the energy sector and to investigate what measures would be taken to prevent or respond to this circumstance. The research method employed was the phenomenological (describing a reality as it is from an interpretation and where the author is admittedly important in the process of knowledge construction), with the procedure of monographic research and a technique of bibliographic research. Research has resulted in an understanding of the approximation of the principles of Energy Law to the prevention of cyberterrorism through cybersecurity, highlighting the risk (and its likely consequences) and assuming the imperative of prevention, monitoring and response measures. It concluded that, in addition to discussing the importance and benefits of energy, it is also necessary to address risks, notably cyberterrorism, in order to ensure the operation of energy generation, supply and distribution infrastructures. In a scenario of widespread use and technological dependence, the establishment of Integrity Programs (Compliance Programs) meets the principles of Energy Law in order to prevent, monitor or respond to threats of potential cyberterrorism with risk assessment, elaboration of documents and implementation of controls, thereby ensuring the development of the energy sector, the country, society and individuals.

Keywords*:Energy law*; *Terrorism*; *Cyberterrorism*; *Prevention*; *Development*.

INTRODUÇÃO

Muito se estuda e se comenta acerca da importância das diversas fontes e meios de energia – o que não poderia ser diferente ante a sua indispensabilidade para as atividades globais e a dependência do ser humano (e demais seres vivos ou criações tecnológicas) das mais variadas matrizes energéticas, evidenciada de sobremaneira em tempos de dependência de (infra)estruturas digitais e virtuais.

Um estudo do Ministério de Minas e Energia da República Federativa do Brasil evidenciou que o consumo mundial de petróleo em 2016 foi de 96,6 Mbbl/d (milhões de barris de petróleo por dia), enquanto o consumo global de gás natural foi de 3.543 bilhões de m³ em 2016 e o de carvão mineral foi o de 3.732 Mtep (milhões de toneladas equivalentes de petróleo). Até o mencionado ano, a demanda total de energia no mundo foi de 13.729 Mtep (81,6% de combustíveis fósseis), sendo que "A matriz mundial de geração elétrica de 2016 contou com 38,5% de carvão mineral, 22,8% de gás, 4,0% de óleo, 10,6% de urânio, 16,2% de hidráulica e 7,9% de outras não especificadas. As fontes renováveis somaram 24,1%, dos quais, 3,9 pontos percentuais de eólica e 1,4 de solar" (MINISTÉRIO DE MINAS E ENERGIA, 2016).

De acordo com o Relatório *World Energy Outlook*, divulgado em 2018 pela *International Energy Agency* (*IEA*), organismo internacional integrante da Organização para a

Cooperação e Desenvolvimento Econômico (OCDE) e cuja missão é defender políticas que incrementem a confiabilidade, a acessibilidade e a sustentabilidade da energia – além de, instrumentalmente, fornecer análises e publicações fundamentadas naquele propósito – (INTERNATIONAL ENERGY AGENCY, 2019), o consumo de energia mundial deveria aumentar em 25% (vinte e cinco por cento) até 2040, muito em razão da demanda dos países considerados como em desenvolvimento, sendo que, atualmente, menos de 1 (um) bilhão de pessoas encontram-se sem acesso à eletricidade (INTERNATIONAL ENERGY AGENCY, 2018).

Igualmente comum é o debate sobre as vantagens das várias fontes e meios de energia, desde aqueles benefícios mais tradicionais (como o fato de proporcionar a sobrevivência das espécies e o desenvolvimento de diversas atividades públicas e econômicas essenciais) até aquelas vantagens desvendadas a partir de um maior espectro de modernidade (*v.g.* a inovação tecnológica que possibilita e estimula avanços e disrupções).

Inobstante a natural e necessária atenção à importância e aos benefícios da energia, é assimilação básica o fato de que, para que seja possível aproveitar as vantagens das matrizes energéticas, em primeiro lugar faz-se necessário o estabelecimento de uma estrutura robusta (em vários sentidos) que, fundamentalmente, coloque e mantenha em funcionamento as infraestruturas de produção e distribuição de energia. Neste ponto, é indispensável repisar o básico: sem a garantia de adequado funcionamento das instituições e plantas energéticas, não haverá consumo e fruição das vantagens e dos benefícios da energia.

Isto considerado, é imperiosa a discussão acerca dos riscos presentes no setor energético a fim de assegurar a continuidade no fornecimento de energia à população em geral para o desempenho de diversificadas atividades, bem como para garantir o desenvolvimento do país e buscar prevenir, monitorar ou ao menos responder adequadamente possíveis danos.

Um dos riscos evidenciados (porém ainda não adequadamente contemplado) no setor energético é o de (ciber)terrorismo, prática criminosa que, além de afetar o funcionamento da produção, distribuição e consumo de energia, acarretará profundo dano e extensão de efeito de desestabilização. Por se apresentar como um risco de altíssimo impacto (ainda que considerado como de baixa probabilidade), a sua consideração no âmbito do setor energético é medida necessária para assegurar o normal funcionamento e aproveitamento das pessoas, das instituições e do país, uma vez que, além de a energia cuidar-se de um bem comum de uso do povo, configura-se como essencial e indispensável para o atingimento dos objetivos fundamentais do Estado (VOLPI FILHO; ALVARENGA, 2008, p. 21).

1. DIREITO DA ENERGIA E (CIBER)TERRORISMO

O Direito da Energia se remonta às sociedades industriais do século XIX e ao início de uma sociedade baseada em uma específica fonte de energia dotada de larga escalabilidade (ao menos para os padrões de outrora): o vapor. Considerado, passo adiante, o conflito originário presente na matéria em questão de um dilema entre o direito de empreendedorismo da livre iniciativa (tendo-se em vista a crescente demanda) e o direito de propriedade (*v.g.* violações de passagens e de linhas de transmissões de energia), afirmou-se o Direito da Energia (notadamente aquele concernente à energia elétrica) com a natureza de Direito Público para promover a conexão entre o interesse público que se sobreporia às querelas particulares (SIMIONI, 2011, s. p.).

Tem-se, portanto, que o Direito da Energia "pretende disciplinar o aspecto [jurídico e] econômico, estudo e produção científica acerca da produção de energia (geração) e seu consumo junto ao ambiente social (transmissão, distribuição e consumo final)" (MARTINS; BLANCHET, 2013, p. 16).

Com uma evolução que se inicia entre o final do Império e a República Velha (1840 a 1934, aproximadamente) e apresenta uma segunda fase entre o Estado Novo e a segunda metade da década de 1990 (assumindo a energia uma conotação de interesse estratégico federal [NASCIMENTO NETO, 2017, p. 94]), um terceiro momento surgiu a partir das crises energéticas de 2001 no Brasil (NASCIMENTO NETO, 2017, p. 119), buscando-se melhores soluções para o modelo então posto.

Considerado o seu tratamento constitucional como serviço público (artigo 21, inciso XII, alínea "b", da Constituição da República Federativa do Brasil – CRFB[4]), inobstante suas

[4] "Art. 21. Compete à União: (...) XII – explorar, diretamente ou mediante autorização, concessão ou permissão: (...) b) os serviços e instalações de energia elétrica e o aproveitamento energético dos cursos de água, em articulação com os Estados onde se situam os potenciais hidroenergéticos (...)".

conexões com os fundamentos (artigo 1º da CRFB[5]) e os objetivos (artigo 3º da CRFB[6]) da República Federativa do Brasil (notadamente o de desenvolvimento nacional) e a promoção do desenvolvimento científico, da pesquisa, da capacitação científica e tecnológica e da inovação (artigo 218 da CRFB[7]) (BRASIL, 1988), subsiste até mesmo entendimento de que o acesso à energia [elétrica] no Brasil constituir-se-ia como direito fundamental social, ante a cláusula de abertura constitucional, o princípio da dignidade da pessoa humana e o núcleo essencial do mínimo existencial (ROSA, 2014, passim).

Inegável, portanto, o papel da energia para o desenvolvimento da nação, desde os aspectos mais básicos (como o fornecimento de energia para o desempenho das atividades comezinhas) até aqueles de maior importância e prestígio, relacionados com características de inovação e segurança nacional.

Verticalizando-se a temática, entre os princípios do Direito da Energia elenca-se "a tutela da não-interrupção do fornecimento regular de energia ao consumidor" ou a "segurança no aprovisionamento energético", que se traduz no planejamento (em sede de políticas públicas) sólido a ensejar a sustentabilidade (SIMIONI, 2011, s. p.).

Neste sentido, no âmbito da não-interrupção do fornecimento, muito se comenta acerca de uma "eficiência energética" (SIMIONI, 2011, s. p.) e de uma infraestrutura apta a comportar as demandas de produção, distribuição e fornecimento de energia; enquanto no aspecto da segurança debate-se a sustentabilidade muito em restritivos termos ambientais.

Sem desconsiderar a importância dos aspectos acima mencionados, quer-se abordar risco de interrupção e (possível) falha de segurança muito mais primária: o risco de ocorrência de (ciber)terrorismo, circunstância e ocorrência criminosa que por certo afetará o fornecimento regular de energia e romperá com os almejados ideários de segurança e sustentabilidade (em sentido amplo).

À esta guisa, cabe, portanto, conceituar "terrorismo". Neste ponto, em que pese um primeiro posicionamento doutrinário que entende pela impossibilidade de conceituação da espécie (CABETTE, 2017, p.99), na medida em que "qualquer tentativa de ser mais específico

[5] "Art. 1º. A República Federativa do Brasil, formada pela união indissolúvel dos Estados e Municípios e do Distrito Federal, constitui-se em Estado Democrático de Direito e tem como fundamentos: I – a soberania; II – a cidadania; III – a dignidade da pessoa humana; IV – os valores sociais do trabalho e da livre iniciativa; V – o pluralismo político (...)".

[6] "Art. 3º. Constituem objetivos fundamentais da República Federativa do Brasil: I – construir uma sociedade livre, justa e solidária; II – garantir o desenvolvimento nacional; III – erradicar a pobreza e a marginalização e reduzir as desigualdades sociais e regionais; IV – promover o bem de todos, sem preconceitos de origem, raça, sexo, cor, idade e quaisquer outras formas de discriminação".

[7] "Art. 218. O Estado promoverá e incentivará o desenvolvimento científico, a pesquisa, a capacitação científica e tecnológica e a inovação (...)".

está votada ao fracasso, pela simples razão de que não há um, mas muitos terrorismos diferentes" (LAQUEUR, 1999, p. 46), outra parcela compreende como necessário o estabelecimento de um conceito, ainda que não absoluto, eis que "a proliferação de definições contribui, obviamente, para a manipulação oportunista do termo, ao sabor dos interesses políticos de partidos, Estados e organizações internacionais" (MAGNOLI, 2008, p. 19).

A dificuldade semântica e a imprecisão terminológica afastam qualquer espécie de conceito absoluto e fechado de terrorismo. Contudo, algumas similitudes podem ser evidenciadas. A Sociologia define terrorismo como "a violência ou a ameaça de violência empregada por um indivíduo ou por um grupo de indivíduos como uma estratégia política" (CRETELLA NETO, 2008, p. 23). Cuello Calón define terrorismo como "a criação, mediante execução repetida de delitos, de um estado de alarme ou de terror na coletividade, ou em certos grupos sociais, para impor ou favorecer a difusão de determinadas doutrinas sociais e políticas" (SZNICK, 1993, p. 167). Em sentido mais prático, o *UK Prevention of Terrorist Act*, de 1976, define terrorismo como "o uso da violência para fins políticos [incluindo] qualquer uso da violência com o intuito de gerar medo no público ou numa secção do público", conforme o Dicionário de Pensamento Político (SCRUTON, 1996, p. 546).

Percebe-se, portanto, que elemento comum entre os conceitos de terrorismo se constitui como a provocação de temor e pânico social (consignada a etimologia da palavra advinda dos termos latinos "*terrere*" [tremer] e "*deterrere*" [amedrontar] [MAGNOLI, 2008, p. 20-21]). Não por outro motivo a legislação penal brasileira que aborda o delito de terrorismo, a saber, a Lei nº. 13.260, de 2016, tipifica a conduta, em seu artigo 2º, da seguinte e taxativa maneira:

> O terrorismo consiste na prática por um ou mais indivíduos dos atos previstos neste artigo, por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião, quando cometidos com a finalidade de provocar terror social ou generalizado, expondo a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública (BRASIL, 2016).

Denota-se, assim, do tipo legal de terrorismo na normativa brasileira a necessidade de presença de 4 (quatro) elementares indispensáveis e concomitantes para a configuração do crime de terorrismo: ato terrorista, motivação terrorista, finalidade terrorista e resultado. Atos são aqueles descritos no § 1º do artigo 2º da Lei[8] (com especial atenção do legislador ao

[8] "Art. 2. (...) § 1º. São atos de terrorismo: I – usar ou ameaçar usar, transportar, guardar, portar ou trazer consigo explosivos, gases tóxicos, venenos, conteúdos biológicos, químicos, nucleares ou outros meios capazes de causar danos ou promover destruição em massa; IV – sabotar o funcionamento ou apoderar-se, com violência, grave

atingimento de instalações públicas ou locais onde funcionem serviços públicos essenciais, tais como aqueles de geração ou transmissão de energia); motivação terrorista é aquela determinada "por razões de xenofobia, discriminação ou preconceito de raça, cor, etnia e religião"; finalidade terrorista deve ser a de "provocar terror social ou generalizado"; e o resultado caracteriza-se como a exposição "a perigo pessoa, patrimônio, a paz pública ou a incolumidade pública" (BRASIL, 2016).

Note-se que não necessariamente o terrorismo será marcado pela característica da violência física (ainda que assim possa se constituir a regra), denotada, de sobremaneira, a expansão das possibilidades de variações e perpetrações de atos terroristas com o desenvolvimento tecnológico (CABETTE, 2017, p. 100).

É justamente neste sentido que a figura do ciberterrorismo ganha destaque. Amplamente proporcionado pelos fenômenos da globalização e da evolução tecnológica, o ciberterrorismo nada mais é do que o terrorismo praticado no (ou por intermédio do) ambiente cibernético. Cuida-se, portanto, de "qualquer ato realizado através de tecnologias de informação que possam direta ou indiretamente causar terror ou gerar danos significativos a um grupo social ou político", realizados por intermédio, por exemplo, "da destruição do suporte tecnológico de qualquer de suas infraestruturas fundamentais" (SUBIJANA, 2008, p. 173).

Ressalte-se, ainda, o caráter exponencial do terrorismo no (ou pelo) ambiente cibernético, qual permite a perpetração de "significativos danos ou detrimentos sobre infraestruturas públicas ou serviços comunitários básicos" (SUBIJANA, 2008, p. 173), consignado, ainda, o fenômeno da Revolução 4.0, onde qualquer ação tem o potencial de apresentar maiores elementos de velocidade, amplitude, profundidade e impacto sistêmico na sociedade (SCHWAB, 2016, p. 189-194).

Não por outro motivo, como já mencionado, a Lei nº. 13.260/2016 contemplou, quando categorizando atos típicos de terrorismo, a possibilidade de atentados contra o funcionamento de instalações de geração ou transmissão de energia, considerado o inerente interesse de organizações (ciber)terroristas para a realização de sua estratégia comunicacional (FISHER; DUGAN, 2019, s. p.) de terror social. Evidencia-se, portanto, o risco neste sentido, sendo fundamentalmente necessária a consideração deste fator para a tomada de medidas

ameaça a pessoa ou servindo-se de mecanismos cibernéticos, do controle total ou parcial, ainda que de modo temporário, de meio de comunicação ou de transporte, de portos, aeroportos, estações ferroviárias ou rodoviárias, hospitais, casas de saúde, escolas, estádios esportivos, instalações públicas ou locais onde funcionem serviços públicos essenciais, instalações de geração ou transmissão de energia, instalações militares, instalações de exploração, refino e processamento de petróleo e gás e instituições bancárias e sua rede de atendimento; V – atentar contra a vida ou a integridade física de pessoa (...)".

adequadas de prevenção, monitoramento e resposta no sentido de assegurar o desenvolvimento do setor energético.

2. ORISCO DE CIBERTERRORISMO NO SETOR ENERGÉTICO

Entre os destacáveis benefícios da energia à população, de início encontram-se a sua criação, o seu fornecimento e a sua distribuição. Neste sentido e atualmente, virtualmente todos os seres humanos (e diversos outros seres vivos) são dependentes de alguma fonte de energia e não apenas para o desempenho de suas atividades biológicas básicas, mas, igualmente, para o aproveitamento de uma série de facilidades que a tecnologia proporcionou.

Ao passo que se incrementa a dependência de um produto ou de um serviço essencial, os focos de atividades e atentados terroristas observarão estas necessidades urgentes e valorosas – sobretudo aquelas desprotegidas, com base na Teoria da Oportunidade (FISHER; DUGAN, 2019, s. p.) – justamente em razão de o *telos* do terrorismo, seja ele cibernético ou não, constituir-se como provocar terror social e generalizado (medo e pânico).

Considerado o fato de que um atentado à uma planta de matriz energética possui um altíssimo potencial de impacto social desestabilizador, cujas consequências poderão ser exorbitantes ou imensuráveis, afigura-se como necessária a consideração deste risco, bem como a efetivação de seu tratamento de maneira adequada.

Em um primeiro momento, a preocupação principal poderia residir na tomada e cerco (físico) por organizações terroristas em locais de geração, distribuição e fornecimento de matrizes energéticas e energia, eis que, além de o ato servir como demonstração de poder e fator de intimidação, configura-se como rentável fonte de financiamento do terrorismo (hipótese na qual a organização terrorista mormente efetua cobranças às pessoas residentes nos arredores para uso e fruição de serviços já anteriormente disponibilizados), como ocorre, por exemplo, em campos petrolíferos e infraestruturas de represas e usinas elétricas no Iraque e na Síria, dominadas, na espécie, pelo Estado Islâmico (ISIL), a Frente Al-Nusrah e a Al-Qaeda (NAÇÕES UNIDAS, 2015).

Ocorre que o eventual controle de uma planta de matriz energética possui efeitos e repercussões locais (ainda que graves), além de ser facilmente detectado e, sequencialmente, combatido pelas estratégias estatais e bélicas tradicionais.

Inobstante esta problemática clássica relacionada ao terrorismo e o seu financiamento, casos concretos evidenciam a imperiosa observância do risco de ciberterrorismo no setor

energético, tendo-se em vista tentativas de invasões (ESTADO DE MINAS, 2018), constatações de fragilidades (GAZETA DO POVO, 2019) e mapeamento de "estado da arte" das organizações terroristas (CONJUR, 2004). O ciberterrorismo, que converge a amplitude do ciberespaço com os impactos do terrorismo, possui suas consequências amplificadas.

Subsistem, inclusive, reinvindicações no setor elétrico neste sentido, com exemplo da Associação Brasileira das Empresas de Transmissão de Energia Elétrica (ABRATE), que criou uma espécie de força-tarefa para discutir a questão da proteção de ciberataques),clamando por uma padronização no tratamento dos riscos a evitar a atual situação de exposição (CORREIO BRAZILIENSE, 2018); e o pedido da *Utilities Telecom & Technology Council* América Latina (*UTCAL*) à Agência Nacional de Energia Elétrica (ANEEL) para que o órgão regulador "autorize que parte do valor aplicado pelas empresas de geração, transmissão e distribuição de energia para pesquisa e desenvolvimento (P&D) seja usado em segurança de redes" (CORREIO BRAZILIENSE, 2018).

Estes clamores e a evidenciação da problemática apoiam-se em ocorrências já registradas, *v.g.*, um episódio de ciberataques registrado na Ucrânia em dezembro de 2015 (G1, 2017), onde mais de 700.000 (setecentas mil) pessoas ficaram sem energia, com preocupações de um novo ambiente de guerra (BBC, 2019); guerra virtual na Estônia (G1, 2007); e apagões no Brasil, em 2005 e 2007 e no Rio de Janeiro e no Espírito Santo, respectivamente, causando prejuízo à mais de 3.000.000 (três milhões) de pessoas (G1, 2009).

Além da preocupação com os impactos sociais e de Estado, o aspecto econômico também pode restar ampla e gravemente afetado: um estudo elaborado pelo Centro de Pesquisa e Desenvolvimento em Telecomunicações (CPqD) (e que nortearia proposta apresentada pela *UTCAL* à ANEEL para o desenvolvimento de um programa de segurança cibernética destinado ao setor de energia elétrica – o que uma vez mais evidencia a premência da questão) concluiu que o país pode perder até R$ 5milhões de reais em apenas 1 (um) minuto de interrupção de fornecimento de energia, sendo que, a cada hora, o prejuízo pode chegar a R$ 303,8 milhões e, em um dia inteiro sem o serviço, seriam perdidos R$ 7,29 bilhões. Estes dados integram o estudo "Impactos econômicos dos ataques cibernéticos no setor elétrico brasileiro e alternativas de mitigação" (VALOR ECONÔMICO, 2018).

Consignada a conexão entre os princípios do Direito da Energia (notadamente o da "tutela da não-interrupção do fornecimento regular de energia ao consumidor" ou o da "segurança no aprovisionamento energético") e a necessária prevenção à realidade do ciberterrorismo e, evidenciados, ainda, os possíveis danos aos quais as instituições estão

sujeitas, urge a necessidade de debater a questão do risco de segurança cibernética no setor energético.

Em um contexto de Sociedade de Informação – onde há cada vez mais a dependência da sociedade de tecnologias da informação e da comunicação e a sua utilização constitui-se como o padrão(CALVETY, 2002, p. 71) –,a segurança cibernética se demonstra como essencial na tentativa de garantir as propriedades de segurança e dos recursos dos usuários em face de riscos de segurança relevantes no ambiente cibernético (MUNK, 2015, p. 47).

Em sede de Segurança da Informação, 3 (três) pilares são de necessária observância na prevenção e contenção de ameaças: a confidencialidade, a integridade e a disponibilidade (TEIDER, 2019, p. 39). Enquanto a confidencialidade tem estreita relação com a privacidade, na guisa ora proposta a integridade e a disponibilidade figuram em plano central. Disponibilidade, neste contexto, significa a certeza de utilização e acesso quando se fizer necessário (TEIDER, 2019, p. 42). A característica da integridade, por sua vez, deve ser compreendida em leitura mais ampla e relacionada com as normativas técnicas, na assimilação de manter os ativos e serviços íntegros (inteiros, ilesos, intactos) (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005a).

À esta guisa, a segurança cibernética (neste ambiente das instituições do setor energético) deve se apoiar em arcabouço lastreado na resiliência e na preparação, fortemente conectada com a gestão de riscos e as melhores práticas de governança antecipatória e preventiva (MUNK, 2015, p. 46), sobretudo quando tratando-se de "infraestruturas críticas", quais sejam, aquelas que são vitais para o bem-estar e o adequado e regular funcionamento de uma sociedade ou nação, na medida em que qualquer perturbação poderá causar grave degradações operacionais e de prestações de serviços (essenciais) (NIEKERK; MAHARAJ, 2011, p. 101).

É fundamentalmente necessário, portanto, que, contemplado os riscos cibernéticos (notadamente o de ciberterrorismo) pelas instituições do setor energético, sejam tomadas atitudes concernentes à segurança cibernética integradas na governança corporativa com o fim de prevenir, monitorar ou responder adequadamente aos riscos e eventuais danos causados pela espécie.

3. MEDIDAS DE PREVENÇÃO, MONITORAMENTO E RESPOSTA COMO FATORES DE DESENVOLVIMENTO NO SETOR ENERGÉTICO

Considerada a evidência de riscos de potenciais danosos no setor energético, medida que se impõe é o estabelecimento de Programas de Integridade (consignado a amplitude e a adequação na espécie do termo de assegurar a inteireza das operações das instituições e a sua característica ilesa frente aos riscos) ou Programas de *Compliance* que visem prevenir, monitorar e/ou responder adequadamente as circunstâncias que se apresentarem.

Em que pese o termo *Compliance*, em um primeiro momento, significar meramente "cumprimento" (BLOCK, 2017, p. 15), entende-se que o conceito merece ser expandido para alcançar, além disso, a ética, a moral, a honestidade e a transparência, espraiando-se não apenas para o cotidiano operacional, mas igualmente possuindo abrangência para "todas as atitudes das pessoas" (GIOVANINI, 2014, p. 20). Neste sentido que se afirma que o *Compliance* deve transcender do mero imperativo hipotético (simples meio condicional e instrumental de cumprimento formal) para ser idealizado e executado como um imperativo categórico da integridade (em uma máxima replicável como parâmetro universal), desempenhando-se o certo por ser o certo a se desempenhar (KANT, 2007, p. 50-59).

Em simples termos, a implementação de um Programa de *Compliance* deve contemplar 3 (três) fases ou etapas: o mapeamento de riscos (*Compliance Risk Assesment*), a elaboração dos documentos e a implementação dos controles.

O mapeamento de riscos é "fundamental para o sucesso da organização" e para a efetividade do Programa de Integridade (GIOVANINI, 2014, p. 61 e 209). Aqui, é necessária a contemplação do "maior número de eventos incertos, no sentido de estabelecer uma dinâmica, após identificado, para a sua priorização, tratamento e controle" (CASTRO; ZILIOTTO, 2019, p. 143). Neste momento, com a colheita de diversos insumos informativos (a partir, *v. g.*, de revisão preliminar de documentos, da condução de entrevistas com diferentes atores das empresas, da análise de organogramas, de conflitos de interesses, de contratos e de diversos outros documentos, de produtos, serviços e/ou soluções da própria corporação e de processos e sistemas internos), será possível identificar a base normativa incidente (se existente), bem como reconhecer as matérias de interesse e os pontos sensíveis da instituição, elaborando-se o documento-base de um Programa de *Compliance*, qual seja, a Matriz de Riscos e Controles, definindo-se, também, as instâncias responsáveis (e em que medida) pelo cumprimento e os fluxos e os processos de conformidade.

Junto à Matriz de Riscos, componentes necessários são o risco *per se* considerado e descrito, a sua base normativa, os controles propostos (preventivos, de detecção ou de monitoramento e de resposta) e as evidências, não obstante o binômio "impacto x

probabilidade" (GIOVANINI, 2014, p. 214) que categorizará o impacto estimado do dano possível e a probabilidade de concretização do risco. Esta análise, além de possibilitar a criação do Programa de *Compliance*, igualmente facilita a sua revisão em sede de necessário aperfeiçoamento contínuo (GIOVANINI, 2014, p. 52).

Aqueles riscos que apresentem alto impacto ou alta probabilidade, ou ambos, deverão ser especialmente considerados e tratados. Referente à problemática do ciberterrorismo, ainda que a probabilidade possa se apresentar em níveis não tão altos (em que pese as reiteradas e cada vez mais comuns ocorrências e preocupações de ciberataques no Brasil e no mundo), o impacto certamente afigurar-se-ia como altíssimo, característica esta que torna imperioso o tratamento adequado e prioritário do risco em questão. Exemplificando-se o altíssimo impacto, rememora-se apagão no Brasil que afetou 18 (dezoito) Estados da Federação e 70.000.000 (setenta milhões de pessoas) em 11 de novembro de 2009 (UOL, 2019), oportunidade na qual houve a suspeita de ação de *hackers*, tendo esta hipótese sido analisada em audiência na Comissão de Ciência e Tecnologia, Comunicação e Informática da Câmara dos Deputados (CÂMARA DOS DEPUTADOS, 2009).

A segunda etapa (elaboração de documentos) representa a verdadeira consolidação material do Programa de Integridade, com a formalização escrita das condutas e dos procedimentos empenhados na prevenção, monitoramento e resposta dos riscos especificamente contemplados. Neste sentido, apesar de existir uma infinitude de possibilidades de documentos formais, ressalta-se a importância de uma Política Institucional de Segurança Cibernética (inclusive com plano de contingência e de continuidade de operações), com bases principiológicas e diretrizes gerais de atuação; e, por decorrência, um Manual de Procedimentos onde estará definida a efetiva e pormenorizada operacionalização da segurança cibernética.

A implementação dos controles, por sua vez, cuida-se do cumprimento do cumprimento, na medida em que efetivamente concretiza as medidas preventivas na atividade operacional da empresa, "colocando em prática os procedimentos criados" (GIOVANINI, 2014, p. 90). Os controles poderão ser formais (documentais), atitudinais (de condutas), procedimentais ou até mesmo físicos e de adaptações de *hardware*, *software* e de estrutura de arquitetura de informática, com o exemplo da atitude da Eletrosul (integrante da Eletrobras e com atuação de geração e transmissão de energia nos Estados do Mato Grosso do Sul e Região Sul) em separar as redes de telecomunicações da empresa, criando uma rede exclusiva para operação do sistema energético e apartada da linha de comunicação corporativa da instituição (CORREIO BRAZILIENSE, 2018).

Mais detidamente quanto aos aspectos técnicos de Segurança da Informação, de acordo com a norma ISO 27001, a adoção de um Sistema de Gestão de Segurança da Informação (SGSI) deve ser uma decisão estratégica da organização e a sua implementação deve se pautar nas necessidades e objetivos, requisitos de segurança, processos empregados e tamanho e estrutura da organização, sendo indispensável um modelo *PDCA* (*Plan*[estabelecimento do SGSI], *Do*[implementação e operação], *Check*[monitoramento e análise crítica de desempenho e resultados] *and Act*[manutenção e melhoria contínua relativa às ações preventivas e corretivas]) (ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS, 2005b). Em um ciclo contínuo de contexto da organização (a partir do mapeamento), liderança, planejamento, suporte, operação, avaliação de desempenho e melhorias (ISO 27001, 2019), a instituição poderá aproveitar de diversos benefícios, tais como, *e.g.*, a redução de possibilidade de falhas de segurança da informação; a minimização dos riscos e dos prejuízos diretos e indiretos; vantagem competitiva devido ao reconhecimento da norma; aumento de confiança de parceiros, clientes e público; método estruturado para atender às necessidades de conformidade; e redução de custos (TÜVRHEINLAND, 2019).

Tem-se, portanto, que os Programas de *Compliance* são mecanismos materialmente efetivos para a prevenção dos possíveis danos decorrentes do ciberterrorismo ou, em sentido complementar, afiguram-se como a mais adequada procedimentalização para prover as melhores respostas possíveis à eventos imprevisíveis ou inevitáveis e garantir o melhor funcionamento possível após a ocorrência destas circunstâncias (considerando-se que um Programa de Integridade não apenas é efetivo quando previne, mas também quando responde adequadamente aos eventos). Isto porque, executadas as fases do Programa de *Compliance*, com especial atenção à Matriz de Riscos e Controles e a sua escorreita observância e seguimento, a empresa poderá conhecer os riscos (sobretudo aqueles fático-circunstanciais e, igualmente e por exemplo, reputacionais) aos quais encontra-se exposta e procedimentalizar, executar e programar ações no intento de preveni-los, mitiga-los ou responde-los.

Em um contexto de sociedade de risco (BECK, 2011, passim), onde "age-se no presente a fim de evitar, ou ao menos mitigar, a concretização das ameaças previstas"(TAMBORLIN; SANTANA, 2015, p. 4), a gestão de riscos (verdadeiramente incutida como política corporativa [CASTRO; ZILIOTTO, 2019, p. 151])e o estabelecimento de uma Governança de Riscos no âmbito empresarial permitirão que a empresa "atinja seus objetivos de forma sustentável" (LEMOS, 2017, p. 456-457).

Em arremate, conhecendo os riscos aos quais está exposto, o setor energético poderá prevenir ou mitigar os eventuais danos e assegurar o adequado funcionamento da geração, transmissão e distribuição de energia, permitindo e concretizando, assim, desenvolvimento nos âmbitos do próprio setor, em termos relativos ao país na concretização dos objetivos e dos fundamentos constitucionais, à guisa social (consequentemente) e para todos os indivíduos usuários deste serviço essencial.

CONCLUSÕES

A importância e os benefícios da energia são amplamente comentados e, em um contexto de ampla dependência e de necessidade de consumo de matrizes energéticas, não poderia ser diferente. Contudo, para que seja possível aproveitar as vantagens da energia, é imperiosa análise no sentido de estabelecimento de uma estrutura robusta que coloque e mantenha em funcionamento as infraestruturas de geração, fornecimento e distribuição de energia. Neste sentido justifica-se a necessidade de contemplação dos riscos do setor energético, entre eles, o de ciberterrorismo.

No espectro do Direito da Energia, além das conexões com os fundamentos e os objetivos da República, entre os princípios da matéria vislumbra-se "a tutela de não-interrupção do fornecimento regular de energia" ou "a segurança no aprovisionamento energético" (SIMIONI, 2011, s. p.). À esta guisa, atos considerados como (ciber)terroristas, entendidos finalisticamente como aqueles cujo propósito seja o de causar temor e pânico social para a consecução de fins políticos (*lato sensu*), por certo observariam como interessante alvo instalações energéticas ante o altíssimo potencial de grave impacto e repercussão social de terror.

Em que pese as possibilidades de tomada e cerco físico por organizações terroristas de locais de geração, distribuição e fornecimento de energia em uma atuação clássica e tradicional, maior risco é evidenciado no ambiente cibernético (ciberterrorismo), tendo-se em vista, além da ampla conectividade e dependência da tecnologia, casos concretos de ciberataques tentados e consumados que registraram (ou registrariam) massivas perdas operacionais e financeiras, circunstâncias estas que ocasionaram reinvindicações das associações e empresas do setor energético a fim de clamarem por maior destinação de recursos e planejamento em matéria de

segurança cibernética, garantindo assim, de sobremaneira, a disponibilidade e a integridade das destas infraestruturas críticas.

Faz-se necessário, portanto, o estabelecimento de Programas de Integridade(Programas de *Compliance*) a fim de prevenir, monitorar ou responder adequadamente às possíveis circunstâncias de ciberterrorismo. Além da necessidade de considerar o *Compliance* como um imperativo categórico, instrumental e operacionalmente a implementação de um Programa de *Compliance* deve contemplar as fases de mapeamento de riscos, elaboração de documentos e implementação dos controles, atentando-se para os riscos de maior probabilidade ou de maior impacto (e ambos) para, após a formação de uma Matriz de Riscos e Controles, formalizar uma Política Institucional de Segurança Cibernética e Manual de Procedimentos, concretizando a efetividade do Programa com a consolidação dos controles.

Desta maneira, prevenindo-se os danos ou respondendo-os de maneira adequada e assegurando, assim, o adequado funcionamento da geração, transmissão e distribuição de energia, igualmente restará possibilitado e fomentado o desenvolvimento do próprio setor energético, bem como o do país, além do desenvolvimento em termos sociais e individuais aos usuários do serviço essencial de energia.

REFERÊNCIAS BIBLIOGRÁFICAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISSO/IEC 17799**: Tecnologia da informação — Técnicas de segurança — Código de prática para a gestão da segurança da informação. Rio de Janeiro, 2005a.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS (ABNT). **NBR ISO/IEC 27001**: – Sistemas de gestão de segurança da informação – Requisitos. Rio de Janeiro, 2005b.

BBC. **Como a energia elétrica se tornou o novo campo de batalha entre EUA e Rússia**, 2019. Sítio oficial da BBC Brasil. Disponível em: <https://www.bbc.com/portuguese/internacional-48691284>. Acesso em 17 set. 2019.

BECK, Ulrich. **Sociedade de risco**: rumo a uma outra modernidade. 2. ed. São Paulo: Editora 34, 2011.

BLOCK, Marcella. **Compliance e governança corporativa**: atualizado de acordo com a Lei Anti-corrupção Brasileira (Lei 12.846) e o Decreto-Lei 8.421/2015). Rio de Janeiro: Freitas Bastos, 2017.

BRASIL. **Constituição da República Federativa do Brasil de 1988**. Brasília: outubro de 1988.

BRASIL. **Lei nº. 13.260, de 16 de março de 2016**. Brasília: março de 2016.

CABETTE, Eduardo Luiz Santos. **Terrorismo**: Lei 13.260/16 Comentada. Rio de Janeiro: Freitas Bastos, 2017.

CALVETY, Myrian Dunn. **Information Age Conflicts**: A Study of the Information Revolution and a Changing Operating Environment. Master Thesis. Zurich Contributions to Security Policy and Conflict Analysis, Nr. 64 Zürich, Forschungsstelle für Sicherheitspolitik und Konfliktanalyse, 2002.

CÂMARA DOS DEPUTADOS. **Comissões vão se reunir para debater causas técnicas do apagão**. Disponível em: <https://www.camara.leg.br/noticias/135966-comissoes-vao-se-reunir-para-debater-causas-tecnicas-do-apagao/>. Publicado em 18 nov. 2009. Acesso em 13 jul. 2020.
CASTRO, Rodrigo Pironti Aguirre de; ZILIOTO, Mirela Miró. **Compliance nas contratações públicas**: exigências e critérios normativos. Belo Horizonte: Fórum, 2019.

CONJUR (Consultor Jurídico). **Al Qaeda está cada vez mais próxima do ciberterrorismo**, 2004. Sítio oficial do ConJur (Consultor Jurídico). Disponível em: <https://www.conjur.com.br/2004-ago-29/al_qaeda_cada_vez_proxima_ciberterrorismo>. Acesso em 17 set. 2019.

CORREIO BRAZILIENSE. **Sob ameaça de ciberataques, setor elétrico quer segurança**, 2018. Sítio oficial do Correio Braziliense. Disponível em: <https://www.correiobraziliense.com.br/app/noticia/economia/2018/04/05/internas_economia,671017/sob-ameaca-de-ciberataques-setor-eletrico-quer-seguranca.shtml>. Acesso em 17 set. 2019.

CRETELLA NETO, José. **Terrorismo internacional**: inimigo sem rosto – combatente sem pátria. Campinas: Millennium, 2008.

ESTADO DE MINAS. **Sob ameaça de ciberataques, setor elétrico quer segurança**, 2018. Sítio oficial do Jornal Estado de Minas. Disponível em: <https://www.em.com.br/app/noticia/economia/2018/04/05/internas_economia,949048/sob-ameaca-de-ciberataques-setor-eletrico-quer-seguranca.shtml>. Acesso em 17 set. 2019.

FISHER, Daren G.; DUGAN, Laura. Sociological and Criminological Explanations of Terrorism. *In*: CHENOWETH, Erica; ENGLISH, Richard; GOFAS, Andreas; KALYVAS, Stathis N. **The Oxford Handbook of Terrorism**. Oxford (Reino Unido): Oxford University Press, 2019.

G1. **Apagões em 2005 e 2007 foram causados por hackers, diz rede americana**. Sítio oficial do G1. Disponível em: <http://g1.globo.com/Noticias/Brasil/0,,MUL1374207-5598,00-APAGOES+EM+E+FORAM+CAUSADOS+POR+HACKERS+DIZ+REDE+AMERICANA.html>. Acesso em 13 jul. 2020.

G1. **Estônia protagoniza primeira guerra virtual**, 2007. Sítio oficial do G1. Disponível em: <http://g1.globo.com/Noticias/Tecnologia/0,,MUL45961-6174,00-ESTONIA+PROTAGONIZA+PRIMEIRA+GUERRA+VIRTUAL.html>. Acesso em 17 set. 2019.

G1. **Ucrânia tem segundo apagão elétrico causado por hackers**, 2017. Sítio oficial do G1. Disponível em: <http://g1.globo.com/tecnologia/blog/seguranca-digital/post/ucrania-tem-segundo-apagao-eletrico-causado-por-hackers.html>. Acesso em 17 set. 2019.

GAZETA DO POVO. **Rede de energia elétrica da Rússia é alvo fácil para hackers dos EUA**, 2019. Sítio oficial da Gazeta do Povo. Disponível em: <https://www.gazetadopovo.com.br/mundo/rede-de-energia-eletrica-da-russia-e-alvo-facil-para-hackers-dos-eua/>. Acesso em 17 set. 2019.

GIOVANINI, Wagner. **Compliance**: a excelência na prática. São Paulo: 2014.

INTERNATIONAL ENERGY AGENCY. Our Mission. In: Sítio oficial da International Energy Agency, 2019. Disponível em: <https://www.iea.org/about/ourmission/>. Acesso em: 16 set. 2019.

INTERNATIONAL ENERGY AGENCY. **World Energy Outlook**. Paris, 2018.

ISO 27001. **ISO 27001 – Sistema de Gestão de Segurança da Informação**. Sítio ISO 27001. Disponível em: <https://www.27001.pt/iso27001_3.html>. Acesso em 18 set. 2019.

KANT, Immanuel. **Fundamentação da Metafísica dos Costumes**. Lisboa (Portugal): Edições 70, 2007.

LAQUEUR, W.**The New Terrorism**: Fanaticism and the Arms of Mass Destruction. London: Phoenix, 1999.

LEMOS. Ricardo. Gerenciamento de Riscos Corporativos. In: LAMBOY, Christian Karl de [organizador]. **Manual de compliance**. São Paulo: Instituto ARC, 2017, p. 449-470.

MAGNOLI, Demétrio. **Terror global**. São Paulo: Publifolha, 2008.

MARTINS, Andre Luis Agner Machado; BLANCHET, Luiz Alberto. **Setor elétrico: regulação e sustentabilidade**. 2013. viii, 189 f. Dissertação (Mestrado) - Pontifícia Universidade Católica do Paraná, Curitiba, 2013 Disponível em: <http://www.biblioteca.pucpr.br/tede/tde_busca/arquivo.php?codArquivo=2473>. Acesso em: 16 set. 2019.

MINISTÉRIO DE MINAS E ENERGIA. **Energia no mundo**. Brasil, 2016. Disponível em: <http://www.mme.gov.br/documents/10584/3580498/14+-+Energia+no+Mundo+-+Matrizes+e+Indicadores+2017+-+anos+ref.+2015+-+16+%28PDF%29/60755215-705a-4e76-94ee-b27def639806;jsessionid=23A29A5505323A1DD0ED0E7D02E956E2.srv155>. Acesso em 16 set. 2019.

MUNK, Tine Hojsgaard.**Cyber Security in the European Region**: Antecipatory Governanceand Practice. 2015. Thesis (Doctor of Philosophy). University of Manchester, Manchester.

NASCIMENTO NETO, José Osório. **Políticas Públicas e Regulação Socioambiental**: energia e desenvolvimento em pauta. Curitiba: Íthala, 2017.

NIEKERK, Brett van; MAHARAJ, Manoj S. **Relevance of Information Warfare Models to Critical Infrastructure Protection**. Saldanha, Scientia Militaria, South African Journal of Military Studies, v. 39, n. 2, 2011.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS (ONU). **Conselho de Segurança aprova resolução para deter financiamento de terrorismo no Iraque e Síria**, 2015. Sítio oficial da Organização das Nações Unidas (ONU) Brasil. Disponível em: <https://nacoesunidas.org/conselho-de-seguranca-aprova-resolucao-para-deter-financiamento-de-terrorismo-no-iraque-e-siria/>. Acesso em 17 set. 2019.

ROSA, Taís Hemann da. **Direito fundamental social de acesso à energia elétrica**(apontamentos iniciais sobre a perspectiva brasileira). In: III Seminário Internacional de Ciências Sociais: Ciência Política buscando o Sul, São Borja, 2014. Anais do III Seminário Buscando o Sul, 2014. Disponível em: <http://cursos.unipampa.edu.br/cursos/cienciapolitica/files/2014/06/ACESSO-%C3%80-ENERGIA-EL%C3%89TRICA-evento-sb.pdf>. Acesso em: 16 set. 2019.

SCHWAB, Klaus. **A quarta revolução industrial** [eBook Kindle]. São Paulo: Edipro, 2016.

SCRUTON, R. Terrorism. *In*: SCRUTON, R.**A Dictionary of Political Thought**. 2ª ed. Londres: Macmillan, 1996.

SIMIONI, Rafael Lazzarotto. **Princípios do Direito da Energia**, 2011. Disponível em: <https://jus.com.br/artigos/19372/principios-do-direito-da-energia/1>. Acesso em: 16 set. 2019.

SUBIJANA, I. (2008): "**El ciberterrorismo**: Una perspectiva legal y judicial". Eguzkilore, 22, 169-187.

SZINICK, Valdir. **Comentários à Lei dos Crimes Hediondos**. 3ª ed. São Paulo: Leud, 1993.

TAMBORLIN, Fábio Augusto; SANTANA, Vinícius Cruz. Sociedade de risco e a democratização da gestão de riscos. In: GUARAGNI, Fábio André; BUSATO, Paulo César [coordenadores]; DAVID, Décio Franco [organizador]. **Compliance e direito penal**. São Paulo: Atlas, 2015, p. 3-16.

TEIDER, Josélio Jorge. **O direito à privacidade e a segurança da informação na era da vigilância digital** [recurso eletrônico]. Curitiba: FERNRIBS Artes e Editoração Eletrônica, 2019.

TÜVRHEILAND. **Segurança da informação ISO 27001**. Sítio oficial do TÜVRheiland. Disponível em: <https://www.tuv.com/portugal/pt/certifica%C3%A7%C3%A3o-de-acordo-com-a-iso-27001.html>. Acesso em 18 out. 2019.

UOL. **Ciberguerra - Internet será front de batalhas do futuro**, 2019. Sítio oficial do UOL. Disponível em: <https://vestibular.uol.com.br/resumo-das-disciplinas/atualidades/ciberguerra-internet-sera-front-de-batalhas-do-futuro.htm>. Acesso em 17 set. 2019.

VALOR ECONÔMICO. **Ataque pode custar R$ 7 bi diários ao setor elétrico**, 2018. Sítio oficial do Valor Econômico. Disponível em: <https://valor.globo.com/empresas/noticia/2018/04/19/ataque-pode-custar-r-7-bi-diarios-ao-setor-eletrico.ghtml>. Acesso em 17 set. 2019.

VOLPI FILHO, Clovis Alberto; ALVARENGA, Maria Amália Figueiredo Pereira. **Setor elétrico**. Curitiba: Juruá, 2008.