|  |  |
| --- | --- |
| |  | | --- | | Na Mídia  14/07/2022 | [LexLatin](https://br.lexlatin.com/reportagens/os-negocios-juridicos-no-setor-de-energia-contra-ataques-ciberneticos)  **Os negócios jurídicos no setor de energia contra ataques cibernéticos**  Área é especialmente vulnerável a esse tipo de vulnerabilidade em razão da complexidade de operações.  Luciano Teixeira    A regulação vem mudando no combate aos crimes cibernéticos no Brasil. Mas o ritmo das melhorias ainda corre abaixo da necessidade de prevenção e solução de ataques e golpes virtuais, especialmente para empresas do setor de infraestrutura energética. Crimes digitais como ransomware (que visa roubar dados ou bloquear máquinas em troca de resgate geralmente em bitcoin) já atingiram ao menos cinco gigantes do setor de energia nos últimos dois anos: Enel e Energisa em abril 2020, EDP e Light em junho de 2020, e Copel e Eletronuclear em fevereiro de 2021.  As ações criminosas não chegaram a afetar a distribuição ou o fornecimento de energia, mas vazaram dados e afetaram os sistemas administrativos das empresas, segundo dados da Agência Nacional de Energia Elétrica (Aneel).  De acordo com a União Internacional de Telecomunicações (ITU, na sigla em inglês), órgão da Organização das Nações Unidas (ONU) e que coordena esforços na área de segurança cibernética, o Brasil ocupava a 71ª colocação no índice de segurança cibernética em 2018, divulgado em 2019. O país foi o 2º no mundo que mais sofreu perdas econômicas de ataques cibernéticos. Segundo os dados da ITU, os prejuízos com ataques cibernéticos no Brasil ultrapassaram US$ 20 bilhões, atingido ao menos 70 milhões de brasileiros.  Com a melhora do ambiente legal e a entrada em vigor no país da LGPD, o Brasil passou para o 18º lugar no índice global de segurança cibernética em 2020, quando 193 países foram pesquisados, o que mostra como a criação de normas e regras contribui para aumentar a segurança.  Para um setor crítico de infraestrutura como o energético, a resolução 964 da Agência Nacional de Energia Elétrica (Aneel) prevê a adoção de normas, padrões e referências de boas práticas em segurança cibernética, além de identificação, proteção, diagnóstico, resposta e recuperação dos incidentes cibernéticos. A ideia é criar políticas de segurança compatíveis com o porte da empresa, a obrigatoriedade de as companhias comunicarem situações de crise em segurança cibernética, assim como o compartilhamento entre os agentes e o órgão regulador de ocorrências relevantes.  A norma também prevê procedimentos relacionados à gestão da segurança, como a segmentação de redes de operação da rede de TI e da Internet, ações de resposta rápida para contenção de incidentes, avaliação e tratamento de riscos.  Em sua Análise de Impacto Regulatório (AIR) sobre segurança cibernética no Setor Elétrico Brasileiro, a Aneel identificou três consequências principais relacionadas a um eventual incidente de segurança cibernética envolvendo agentes regulados do setor: eventual interrupção no suprimento de energia, a impossibilidade de realização de operações técnicas pelos agentes regulados e o possível extravio de dados.  O risco de continuidade da atividade essencial é um dos mais preocupantes e, na avaliação dos técnicos e advogados especializados ouvidos por LexLatin, não se trata de mero risco hipotético.  “A Resolução estabelece tanto medidas preventivas quanto reativas, a serem adotadas pelos agentes regulados em conexão com segurança cibernética. As medidas preventivas visam estabelecer parâmetros organizacionais e técnicos para a prevenção de riscos, e as reativas visam minimizar o impacto de incidentes que possam impactar o setor, tornando-o menos vulnerável a crimes cibernéticos”, explica Paulo Lilla,  sócio da área de Tecnologia, Proteção de Dados e Propriedade Intelectual do Lefosse Advogados.  De acordo com a resolução da Aneel, as empresas são responsáveis pela segurança das instalações e a continuidade da prestação do serviço e pelo ônus da adaptação de seus sistemas. Os gastos necessários para implantação dessas medidas poderão ser avaliados pela agência, para um eventual reconhecimento de custos nas tarifas.  "Com essas diretrizes criamos um ambiente de competição saudável no setor com uma maior segurança jurídica, transparência, com conceitos definidos e que prima pela gestão dos riscos e falhas de modo mais racional e coerente, preservando-se a confidencialidade e integridade das informações e prevendo regras de acessibilidade, bem como de continuidade dos negócios firmados”, avalia Bruno Guerra de Azevedo, sócio do SGMP Advogados.  A legislação, segundo os especialistas, permite uma atualização do ordenamento vigente, criando-se instrumentos específicos de combate aos cibercriminosos que possibilitam uma resposta mais eficiente aos delitos cometidos no âmbito digital.  **“Esse movimento de criar regras específicas para garantir a segurança cibernética começou por setores mais regulados, como o bancário e o de seguros, e agora chegou ao de energia. A tendência é que todos os setores se organizem, se regulem e criem boas práticas em relação à segurança, à exposição de dados, como incentivam a própria ANPD (Autoridade Nacional de Proteção de Dados) e a legislação”, diz Tatiana Campello, sócia da área de Energia do Demarest Advogados.**  Com a pandemia e o volume muito maior de informações transitando no ambiente online, a exposição de dados aumenta. Não só de dados pessoais, mas também de informações confidenciais das empresas que podem ser violadas e estão relacionadas à legislação de propriedade intelectual, explica Tatiana.  Quem não se adequar aos procedimentos exigidos para garantir ou fortalecer a proteção das informações processadas e transmitidas no setor elétrico pode ser autuado e receber as penalidades como preveem não apenas a legislação do setor elétrico, mas ainda toda a legislação que envolve o assunto segurança cibernética – desde as normas de Lei Geral de Proteção de Dados Pessoais (LGPD, Lei nº 13.709/2018), Marco Civil da Internet e do Código de Defesa do Consumidor.  Empresas e associações do setor de energia tiveram prazo até o início do mês para se adaptar às normas de segurança cibernética previstas na resolução 964, editada pela Aneel em dezembro de 2021.  A adequação é necessária para as concessionárias de energia, os permissionários e os agentes autorizados de serviços ou instalações de energia elétrica; além de entidades responsáveis pela operação do sistema, pela comercialização de energia elétrica ou até pela gestão de recursos provenientes de encargos do setor.  Para os advogados do setor alguns pontos merecem destaque. A Resolução prevê condutas focadas na prevenção, ao estipular, por exemplo, diretrizes para a atuação em segurança cibernética, conforme seu artigo 3º, bem como ao definir o escopo mínimo para as políticas de segurança de cada instituição ou agente, segundo estabelece seu artigo 4º”, afirma Vinícius Fochi, criminalista do Damiani Sociedade de Advogados.  Para ele, a norma é uma cartilha de como o setor deve se portar diante dos riscos relacionados a ataques cibernéticos.  A Resolução da Aneel também prevê diretrizes a serem tomadas nos casos de ataque cibernético de maior impacto, incluindo a análise da causa e das consequências e as ações de mitigação adotadas.  “Dentre as condutas, há a necessidade de os agentes notificarem a equipe de coordenação setorial designada sobre eventuais ataques e ameaças capazes de colocar em risco a segurança das instalações, das operações e dos serviços aos usuários, de acordo com o artigo 6º da Resolução. A legislação também prevê que o ônus pela segurança das instalações e a continuidade na prestação do serviço é de inteira responsabilidade dos agentes do setor, segundo o artigo 8º”, explica Mayra Mallofre Ribeiro Carrillo, criminalista, sócia de Damiani Sociedade de Advogados.  O setor de energia é especialmente vulnerável a esse tipo de ataque em razão da complexidade de suas operações. Para os analistas, a singularidade de operações como a geração ou distribuição de energia elétrica, que demandam infraestruturas físicas e tecnológicas variadas, apresenta muitos desafios em termos de cibersegurança.  “Sem dúvida alguma as novas regras contra crimes cibernéticos trazem mais segurança jurídica. O modelo regulatório e comercial do Setor Elétrico é baseado na separação e coexistência de um mundo físico e um mundo contratual. Sob o enfoque contratual, todas as operações de compra e venda de energia elétrica, as medições de geração e consumo e a contabilização e liquidação financeira do Mercado de Energia são feitos também por meio de programas computacionais e/ou plataformas eletrônicas de comercialização. Dessa forma, a instituição de alto padrão e diretrizes de segurança para evitar danos ou invasão aos sistemas, paralisações de operações e/ou acesso indevidos a dados das operações é imprescindível para a segurança jurídica, credibilidade e higidez das operações comerciais realizadas no Setor de Energia Elétrica”, avalia Raphael Gomes, sócio da área de Energia do Lefosse. | |
|  |