UNI PROCESSUS centro universitário

ISSN: 2675-6595

RESENHA

Revista Processus Multidisciplinar

Página da revista:
https://periodicos.processus.com.br/index.php/multi/index

Resenha do artigo intitulado "O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD"[1]

Review of the article "The principle of security in the era of ciber-attacks: an analysis based on the protective scope of the LGPD"

ARK: 44123/multi.v6i11.1398

Recebido: 08/12/2024 | Aceito: 28/03/2024 | Publicado *on-line*: 24/04/2025

Patrícia de Souza Falcão Oliveira[2]
https://orcid.org/0009-0007-4212-9397
http://lattes.cnpq.br/4909075934246350
UniProcessus – Centro Universitário Processus, DF, Brasil
E-mail: patty.fallcao@gmail.com

Resumo

Esta é uma resenha do artigo intitulado "O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD". Este artigo é de autoria de Haide Maria Hupffer e Gabriel Cemin Petry. O artigo aqui resenhado foi publicado no periódico "Revista CNJ", no Vol. 07, edição n. 01, jan.-jun., 2023.

Palavras-chave: Princípio da Segurança. LGPD. Incidentes de Segurança. Proteção de Dados.

Abstract

This is a review of the article entitled "The principle of security in the age of cyberattacks: an analysis based on the protective scope of the LGPD". This article is authored by Haide Maria Hupffer and Gabriel Cemin Petry. The article reviewed here was published in the periodical "Magazine of CNJ", in Vol. 07, edition n. 01, Jan.-Jun., 2023.

Keywords: *Security Principle. LGPD. Security Incidents. Data Protection.*

Resenha

O presente texto, em forma de resenha, analisa o artigo intitulado "O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD". Este artigo é de autoria de Haide Maria Hupffer e Gabriel Cemin Petry e foi publicado no periódico "Revista CNJ", no Vol. 07, edição n. 01, jan.-jun., 2023.

[1] Resenha de aproveitamento da disciplina *TC* (Trabalho de Curso), do curso *Bacharelado em Direito*, do *Centro Universitário Processus – UniProcessus*, sob a orientação dos professores *Jonas Rodrigo Gonçalves* e *Danilo da Costa*. A revisão linguística foi realizada por Vanessa Fagundes de Souza Leite.
[2] Graduanda em Direito pelo Centro Universitário Processus – UniProcessus.

A reflexão e a experiência deste artigo contribuem para a análise dos temas propostos.

A primeira autora deste artigo, Haide Maria Hupffer, pós-doutora e doutora em Direito pela UNISINOS é pesquisadora no Programa de Pós-Graduação em Qualidade Ambiental e no curso de Direito da Universidade Feevale, líder do Grupo de Pesquisa CNPq/Feevale Direito e Desenvolvimento e líder do Projeto de Pesquisa FAPERGS, Inteligência Artificial e Sociedade de Algoritmos: regulação, riscos discriminatórios, governança e responsabilidades. Currículo disponível em: http://lattes.cnpq.br/4950629941533824.

O segundo autor**,** Gabriel Cemin Petry, bolsista do CNPq, graduando em Direito pela Universidade Feevalee é integrante do Grupo de Pesquisa CNPq/Feevale: Direito e Desenvolvimento do Projeto de Pesquisa CNPq/Feevale, Inteligência Artificial para um Futuro Sustentável: Desafios Jurídicos e Éticos. Currículo disponível em: http://lattes.cnpq.br/ 5313877171706309

Este artigo é dividido em: resumo, palavras-chave, *abstract*, *keywords*, introdução, ameaças invisíveis: a recorrente problemática dos incidentes de segurança e ataques cibernéticos na atualidade, instrumentos ao dispor do atacante: a necessária atenção aos malwares e técnicas de engenharia social, fundamentalidade do princípio da segurança para proteção de dados pessoais no contexto da LGPD, instituído pela Lei 13.709/2018 (BRASIL, 2018).

No resumo, os autores explicam que os ataques cibernéticos se tornaram uma grande ameaça e, de forma crescente, vem causando danos à sociedade e ao Estado. Desta forma, o artigo traz o princípio da segurança presente na Lei nº 13.709, de 14 de agosto de 2018 (BRASIL, 2018), através do método dedutivo, utilizando a pesquisa bibliográfica e documental para garantia de seus direitos.

No tema desta resenha, “o princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD”, instituído pela Lei 13.709/2018 (BRASIL, 2018), foi discutido o problema da segurança com o avanço das novas tecnologias e seus inúmeros benefícios de serviços oferecidos no ambiente digital e o potencial risco de ataques às organizações públicas e à sociedade. O artigo partiu da hipótese que os ataques cibernéticos podem ter alvos variados, conforme motivação que ensejou a invasão virtual.

O objetivo geral aqui firmado é ressaltar o papel da segurança, pautado no diploma legal, consoante Lei 13.709/2018 (BRASIL, 2018), para proteção de dados pessoais, evitando, assim, a ocorrência de incidentes de segurança desta modalidade.

A temática da pesquisa contou com a justificativa de que o estudo é relevante, uma vez que destaca a importância das “medidas técnicas e administrativas voltadas a garantir a funcionalidade de sistemas e proteção dos titulares de dados, garantindo-lhes seus direitos, desde a concepção até a execução das atividades.”

A metodologia utilizada é de forma qualitativa e exploratória, elaborada a partir do método dedutivo, com utilização de pesquisa bibliográfica e documental.

Os autores, diligentemente, ressaltam que o avanço e a exposição na rede atraem ameaças de ataques cibernéticos e impacto para organizações e sociedade. Os ciberataques têm objetivos variados, dependendo do que motivou a invasão (HUPFFER; PETRY, 2023, p. 85).

E a forma empregada pelos hackers é diversa e exige atenção dos técnicos da área de proteção da informação. O número de ataques vem crescendo e, por isso, a problemática é considerável em escala mundial (HUPFFER; PETRY, 2023, p. 85).

Neste cenário, o estudo teve como objetivo apurar a importância da segurança no contexto da Lei Geral de Proteção de Dados Pessoais (LGPD), nº 13.709/2018 (BRASIL, 2018). A investigação desenvolveu-se em exploratória e qualitativa, utilizando o método dedutivo (HUPFFER; PETRY, 2023, p. 86).

A análise, relatada no artigo, está dividida em três tópicos. O primeiro traz informações sobre os incidentes de segurança e ataques cibernéticos. No segundo, a explanação é sobre "malwares" e técnicas de engenharia social que demonstram as vulnerabilidades e são incluídas reflexões sobre a fundamentalidade do princípio da segurança para proteção de dados pessoais no cenário da Lei 13.709/2018 (BRASIL, 2018) (HUPFFER; PETRY, 2023, p. 86).

De forma contundente, os autores consideram que os ataques cibernéticos, como *ransomware*, oportunizam a atuação de associações criminosas contra organizações e empresas. Os ataques buscam benefícios materiais sobre constrição de dados e interrupção de atividades, tornando-se verdadeiras ferramentas de guerra (HUPFFER; PETRY, 2023, p. 86).

Os autores, cuidadosamente, ressaltam que o foco é a obtenção de um viés político e a guerra avança no mundo virtual, uma vez que estamos diante da inclusão de uma dimensão de guerra, em que as técnicas ofensivas agora incluem o ciberespaço. A prevenção e o fortalecimento de alvos prováveis podem revelar medidas eficazes para o monitoramento e a reação a incidentes. Os incidentes de segurança podem ser classificados como crimes cibernéticos (HUPFFER; PETRY, 2023, p. 86).

No ano de 2021, "The Harris Poll" (2022, p. 04) liderou a pesquisa que aponta o Brasil como líder global em ciberataques. O relatório indica que a prevalência da vida virtual criou um terreno fértil para hackers e essa situação cresceu com a pandemia de COVID-19, forçando o aumento de projetos de transição digital (HUPFFER; PETRY, 2023, p. 88).

Hupffer e Petry (2023, p. 88) foram precisos e verdadeiros ao identificar que os incidentes de segurança nos mercados digitais podem gerar danos de difícil reparação e limitar diretos dos usuários.

A Resolução do CNJ nº 396, de 7 de junho de 2021 (CNJ, 2021), criou a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ), pois o desconhecimento e a falta de cuidado podem ter consequências desastrosas para as organizações, as autarquias, os estados e as pessoas (HUPFFER; PETRY, 2023, p. 88).

O *malware* explora vulnerabilidades, bloqueia o sistema e exige o resgate para a recuperação dos dados. Técnicas de engenharia social podem ser utilizadas para obrigar as vítimas a informarem dados importantes ou sigilosos. Assim, exploram o fator mais fraco da ligação mais fraca da segurança com a informação que é o fator humano, pois o indivíduo pode introduzir vulnerabilidades e desencorajar as medidas de monitoramento (HUPFFER; PETRY, 2023, p. 90).

O artigo esclarece, conforme pontua Wolfgang Hoffmann-Riem (2021, p. 116), que é fundamental assegurar a funcionalidade de sistemas e frequentemente monitorá-los (HUPFFER; PETRY, 2023, p. 91).

Os autores afirmam, com sabedoria, que o dever de segurança é conceituado no diploma legal de proteção de dados da Lei nº 13.709/2018 (BRASIL, 2018). Além disso, outras legislações relevantes para o contexto de proteção de dados incluem o Código de Defesa do Consumidor, instituído pela Lei nº 8.078, de 11 de setembro de 1990 (BRASIL, 1990), o Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014 (BRASIL, 2014), a Lei do Cadastro Positivo, Lei 12.414, de 9 de junho de 2011

(BRASIL, 2011) e a Lei de Acesso à Informação, Lei nº 12.527, de 18 de novembro de 2011 (BRASIL, 2011), que juntas contribuem para a proteção de dados. E nesse contexto, o Código de Defesa do Consumidor, Lei nº 8.078, de 11 de setembro de 1990 (BRASIL, 1990) garante a utilização segura e adequada do produto ou serviço adquirido (HUPFFER; PETRY, 2023, p. 91-92).

Para Hupffer e Petry (2023, p. 92), é necessária uma ação em conjunto entre os setores público e privado para aprimorar a política vigente de proteção ao consumidor digital e reduzir os riscos. Além do cumprimento da legislação vigente sobre segurança da informação, é importante seguir as normas de padronização existentes para que cada organização aplique boas práticas em proteção de dados.

O princípio da responsabilização ética e legal, bem como a prestação de contas, combina um raciocínio jurídico voltado à restauração e à prevenção. Assim, o princípio da segurança equivale à utilização de medidas técnicas e administrativas apropriadas para proteger os dados pessoais contra acessos não autorizados e situações acidentais (HUPFFER; PETRY, 2023, p. 93).

De forma literata, os autores citam a importante contribuição do Conselho Nacional de Justiça, que instituiu a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Além disso, o Conselho Nacional de Justiça também criou o Centro de Prevenção, Tratamento e Resposta a Incidentes Cibernéticos do Poder Judiciário (CPTRIC-PJ) (HUPFFER; PETRY, 2023, p. 93).

Hupffer e Petry (2023, p. 93) exemplificam que, nesse mesmo viés, o CNJ criou o Provimento nº 74, de 31 de julho de 2018 (CNJ, 2018), para que os serviços oferecidos pelos cartórios sejam garantidos à segurança de dados. Este documento estabelece preceitos de segurança técnica e administrativa, baseados na disponibilidade, integridade e confidencialidade.

Com efeito, o artigo 46 da Lei 13.709/2018 (BRASIL, 2018) determina que as medidas preventivas deverão ser observadas desde a criação do produto ou do serviço até a entrega e execução. Assim, a organização ficará responsável por implementar medidas de segurança para ataques ou vazamentos de dados. E os agentes não responderão pelos danos causados no tratamento que forem comprovados e não realizaram a segurança de dados (HUPFFER; PETRY, 2023, p. 94-95).

A Lei 13.709/2018 (BRASIL, 2018) atribui ao responsável pelo manuseio de dados uma série de medidas de proteção e segurança. Por isso, a obrigação de segurança visa garantir o direito à autonomia informativa dos titulares dos dados. (HUPFFER; PETRY, 2023, p. 95).

Conforme supracitado no texto, ataques de hackers podem ter os mais diversos interesses e motivações e o modo pelo qual o atacante se aproveita é amplo, desafiando os profissionais da segurança da informação. Essa recorrência de ataques pode estar ligada a atos de negligência ou imprudência (HUPFFER; PETRY, 2023, p. 95).

Posto isto, como forma de simplificar, Haide Maria e Gabriel (2023, p. 96) informam que o tratamento de dados atrai os efeitos regulamentários da Lei 13.709/2018 (BRASIL, 2018), e trazem, de forma imperativa, a atenção às informações constantes da lei. Além disso, deve-se observar as normas de padronização existentes e os parâmetros de segurança das entidades competentes.

Por fim, os autores salientam que os deveres de segurança instituídos pela Lei 13.709/2018 (BRASIL, 2018) devem ser considerados, desde a criação até a completa execução da operação, sob pena de envolvimento pelos danos ocorridos em razão da violação de segurança (HUPFFER; PETRY, 2023, p. 96).

Referências

BRASIL. **Constituição Federal**. Brasília: Centro Gráfico do Senado Federal, 1988. Disponível em: <https://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm> Acesso em 12 ago. 2024.

BRASIL. **Lei n.8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Disponível em: < https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm> Acesso em: 10 ago. 2024.

BRASIL. **Lei n.12.414**, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12414.htm> Acesso em: 10 ago. 2024.

BRASIL. **Lei n.12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º , no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112, de 11 de dezembro de 1990; revoga a Lei nº 11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm> Acesso em: 10 ago. 2024.

BRASIL. **Lei n.12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm> Acesso em: 10 ago. 2024.

BRASIL. **Lei n.13.709**, de 14 de agosto de 2018. Institui a Lei Geral de Proteção de Dados Pessoais (LGPD). Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em: 10 ago. 2024.

CNJ, Conselho Nacional de Justiça. **Provimento n. 74**, de 31 de julho de 2018. Dispõe sobre padrões mínimos de tecnologia da informação para a segurança, integridade e disponibilidade de dados para a continuidade da atividade pelos serviços notariais e de registro do Brasil e dá outras providências. Disponível em: <https://atos.cnj.jus.br/atos/detalhar/2637> Acesso em: 10 ago. 2024.

CNJ, Conselho Nacional de Justiça. **Resolução n. 396**, de 7 de junho de 2021. Institui a Estratégia Nacional de Segurança Cibernética do Poder Judiciário (ENSEC-PJ). Disponível em: < https://atos.cnj.jus.br/atos/detalhar/3975> Acesso em: 12 ago. 2024.

GONÇALVES, Jonas Rodrigo. Como elaborar uma resenha de um artigo acadêmico ou científico. **Revista JRG de Estudos Acadêmicos**. Vol. 3, n. 7, p. 95–107, 2020.

DOI: 10.5281/zenodo.3969652. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/41>. Acesso em: 14 ago. 2024.

GONÇALVES, Jonas Rodrigo. Como escrever um artigo de revisão de literatura. **Revista JRG de Estudos Acadêmicos**. Vol. 2, n. 5, p. 29–55, 2019. DOI: 10.5281/zenodo.4319105. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/122>. Acesso em: 14 ago. 2024.

GONÇALVES, Jonas Rodrigo. Como fazer um projeto de pesquisa de um artigo de revisão de literatura. **Revista JRG de Estudos Acadêmicos**. Vol. 2, n. 5, p. 01–28, 2019. DOI: 10.5281/zenodo.4319102. Disponível em: <http://revistajrg.com/index.php/jrg/article/view/121>. Acesso em: 14 ago. 2024.

GONÇALVES, Jonas Rodrigo. Escolha do tema de trabalho de curso na graduação em Direito. **Revista Coleta Científica**. Vol. 5, n. 9, p. 88–118, 2021. DOI: 10.5281/zenodo.5150811. Disponível em: <http://portalcoleta.com.br/index.php/rcc/article/view/58>. Acesso em: 14 ago. 2024.

HUPFFER, Haide Maria; PETRY, Gabriel Cemin. O princípio da segurança na era dos ciberataques: uma análise a partir do escopo protetivo da LGPD. **Revista CNJ.** Vol. 7, n.1, jan.-jun., 2023. Disponível em: <https://www.cnj.jus.br/ojs/revista-cnj/article/view/445>. Acesso em: 14 ago. 2024.

THE HARRIS POLL. 2022 **Cyber Safety Insights Report.** 2022. Disponível em: https://www.nortonlifelock.com/us/en/ newsroom/press-kits/2022-norton-cyber-safetyinsights-re- port-special-release-online-creeping/. Acesso em: 14 ago. 2024.