WooCommerce e LGPD: Uma análise de uso e conformidade

Camila Pinheiro Alves da Costa, Oldrado José Teixeira Junior, Wellington de Araujo Morete, Nilson Mori Lazarin

[1]Bacharelado em Sistemas de Informação – Centro Federal de Educação Tecnológica Celso Suckow da Fonseca (Cefet/RJ) – Nova Friburgo, RJ – Brazil

{camilapadacosta,oldradojunior,welllington.morete,nilsonmori}@gmail.com

Abstract. *This paper presents an analysis of WooCommerce's compliance with the General Law on Personal Data Protection (LGPD), Brazilian law that regulates the personal data processing. This study aims to check if the open-source e-commerce plugin for WordPress is according to the LGPD.Therefore, an analysis is performed on e-commerce sites to assess the use of the plug-in and its versions. By the end, an analysis of compliance and versions is presented.*

Resumo. *Esse artigo apresenta uma análise da conformidade do WooCommerce com a Lei Geral de Proteção de Dados (LGPD), lei brasileira que dispõe sobre o tratamento de dados pessoais. O objetivo deste trabalho é averiguar se o plugin open source de e-commerce do WordPress está aderente com a LGPD. É realizada uma análise em sites de e-commerce para avaliar o uso do plugin e versão. Ao final é apresentada uma análise sobre aderência e versionamento.*

1. Introdução

A Lei Geral de Proteção de Dados (LGPD) traz um novo aspecto para a Segurança da Informação com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade. Desde que foi anunciada, vem impactando o comércio eletrônico, visto que não havia nenhuma legislação brasileira específica para proteção de dados pessoais e algumas das principais medidas para adequação, segundo [Herdy 2020] são: *"evidenciar o motivo pelo qual os dados estão sendo coletados; ter o consentimento dos clientes para a utilização dos seus dados; possibilitar que os consumidores alterem ou excluam seus dados assim que desejarem"*.

O Woocommerce, *plugin* do Wordpress, é a terceira plataforma mais popular de *e-commerce* no Brasil e possui 28% de participação de mercado em todo o mundo [BuiltWith Pty Ltd 2020]. O objetivo deste trabalho é avaliar se o WooCommerce está em conformidade com a LGPD e a partir de qual versão, além de apresentar um panorama de conformidade realizado através de uma pesquisa com milhares de sites de comércio eletrônico.

2. Trabalhos Relacionados

O trabalho de [Carvalho et al. 2019] discute os desafios de transparência associados e oriundos da LGPD no aspecto de Tecnologia da Informação (TI) em Sistemas de Informação (SI) e apresenta uma agenda de pesquisa sobre o tema. O trabalho de [Nakamura et al. 2019] apresenta uma metodologia de avaliação de risco e segurança para suportar as empresas no atendimento dos requisitos de segurança demandados pela LGPD

e, de acordo com os autores, no Brasil ocorrerá um movimento semelhante às empresas europeias que ainda estão em processo de adequação ao GDPR, apesar desta lei já estar em vigor na Europa desde 2018. O trabalho de [Raposo et al. 2019] apresenta uma revisão sistematizada sobre artigos que englobam a LGPD e conclui que: *"nenhuma discussão foi mencionada sobre a aplicabilidade nas empresas e como elas devem se regulamentar"*, além de que *"a comunidade acadêmica deve se preocupar como vai afetar o Brasil e as estratégias que teremos de entrar em compliance com a LGPD"*.

Os trabalhos citados abordam aspectos importantes da LGPD, entretanto nenhum trata especificamente de sua aplicação em uma plataforma de comércio eletrônico, como é o caso do WooCommerce.

3. Análise de Conformidade

A fim de realizar a análise, foi necessária a criação de uma loja virtual para avaliar se estaria aderente à LGPD. Para isso foi instalado a versão 5.3.3 do WordPress e o plugin WooCommerce na versão 4.7.0.

Segundo [Elia 2018], o WordPress passou a trazer mais enfoque a privacidade e segurança de dados para seus usuários na versão 4.9.6 e as novas funcionalidades foram: Visitantes não conectados a uma conta têm a opção de gravar seu nome, endereço de e-mail e site em um cookie no navegador; Página de política de privacidade; Possibilidade de exclusão e exportação dos dados ao se receber uma solicitação do cliente.

A análise de conformidade foi realizada através de um estudo de caso em que quatro clientes fictícios realizam compras na loja virtual. A seguir são listadas as possíveis ações e motivos da exclusão ou da não exclusão dos dados do cliente.

- Ações possíveis
    1. Se cadastrar na loja, realizar uma compra e não solicitar exclusão de dados;
    2. Se cadastrar na loja, realizar uma compra e, por insatisfação, decidir cancelar a compra e solicitar exclusão de dados;
    3. Se cadastrar na loja, realizar uma compra e solicitar informações sobre quais de seus dados estão sendo tratados;
    4. Se cadastrar na loja, e após isso, solicitar a exclusão de todos os seus dados.
- Motivos possíveis
    1. Os dados pessoais necessários para tratamento e controle do pedido foram mantidos, conforme previsto no art. 16, inciso I, da LGPD;
    2. Como não há pedidos relacionados ao cliente, seus dados foram apagados totalmente.

Usuário	Ação	Acesso aos Dados	Dados excluídos	Motivo
João Woo	1	Sim	Não	-
Maria Woo	2	Sim	Não	1
Matheus Woo	3	Sim	Não	-
Wellington Woo	4	Sim	Sim	2

Tabela 1. Resultados da análise realizada na loja virtual.

Na tabela 1 são apresentados os resultados do estudo de caso. Constatou-se que, no que diz respeito ao tratamento de dados, o WooCommerce mantém os dados do cliente

enquanto o fluxo de compra não foi finalizado. Através de uma solicitação, o cliente pode pedir a retirada completa de seus dados da base de dados, salvo casos mantidos pela lei, cumprimento de obrigação legal ou regulatória pelo controlador.

4. Panorama da conformidade

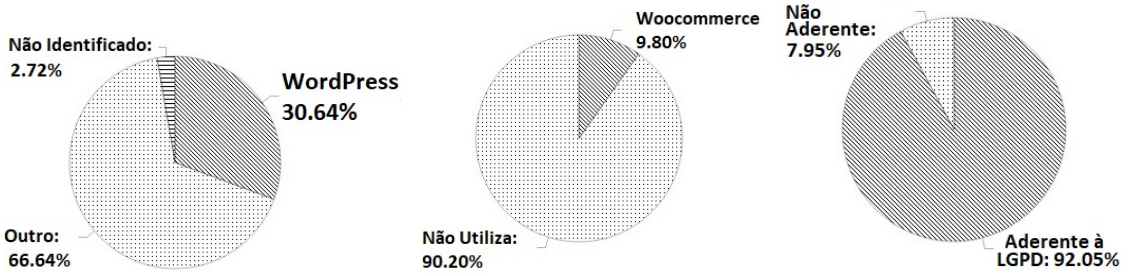
Para obtermos um panorama do uso do WooCommerce, foi utilizada a ferramenta WPScan, que é um verificador de segurança WordPress de caixa preta escrito para profissionais de segurança e mantenedores de blog testarem a segurança de seus sites. O *WPScan Vulnerability Database*, fonte de dados do WPScan, usa identificadores CVE (*Common Vulnerabilities and Exposures*) para permitir que os usuários cruzem as vulnerabilidades com diferentes ferramentas e bancos de dados de vulnerabilidade [Broad and Bindner 2014].

A realização da pesquisa foi dividida em 3 etapas descritas a seguir:

1. Buscou-se uma lista de sites de *e-commerce*, para tal utilizado o arquivo *domains* da categoria *ecommerce* do URLBlacklist[1], um projeto de catalogação de sites. Apesar da lista obtida ser a nível internacional, ela é válida para a análise, uma vez que ao realizar o tratamento de dados de brasileiros os controladores internacionais estão sujeitos à LGPD, conforme previsto no art. 33, inciso VI.
2. Utilizando o Kali Linux, submetemos a lista ao WPScan, através do script:

```
#! /bin/sh
while read DOM; do
    wpscan -e ap --url $DOM -o $DOM.json -f json
done < domains
```

3. Analisamos os resultados obtidos.



(a) Analisados **(b)** Woocommerce **(c)** Aderência

Figura 1. Resultados obtidos através do WPScan.

Do total de 147.604 domínios obtidos na lista, 79.935 foram descartados, por não resolverem via consulta DNS. Foram analisados 67.669 domínios válidos, dos quais foi possível identificar que 21.315 utilizam WordPress, 46.354 utilizam outro sistema e não foi possível identificar o sistema utilizado em 1.895 domínios, conforme Figura 1a. Do total de 21.315 domínios que utilizam WordPress como gerenciador, foi identificado que 2.089 utilizam o plugin WooCommerce e 19.226 não utilizam, conforme Figura 1b. Na Figura 1c observa-se que do total de 2.089 domínios que utilizam o WooCommerce, 1.923 estão aderentes à LGPD, pois utilizam versão do WordPress superior à 4.9.6, e que 166 domínios não estavam aderentes à LGPD.

[1]https://web.archive.org/web/20170724071845/http://urlblacklist.com/

Foi possível identificar a versão do WordPress em 6.158 domínios, dos quais 84,2% estão aderentes à LGPD, conforme a Tabela 2.

Versão	**<4.5**	**4.6**	**4.7**	**4.8**	**4.9**	**5**	**5.1**	**5.2**	**5.3**	**5.4**	**5.5**	**5.6**
Uso	3,4%	0.8%	2%	1.5%	8.1%	1.9%	2,3%	4.9%	6.4%	10.4%	26.2%	32.1%
	Não Aderente					**Aderente**						

Tabela 2. Resultado do panorama de conformidade do WordPress com a LGPD.

5. Conclusão

Através do estudo de caso realizado percebeu-se que o WordPress está em conformidade com a lei brasileira, mas apenas para usuários com a versão 4.9.6 ou superior. De acordo com o panorama de conformidade apresentado, verificou-se que 30,64% dos domínios analisados utilizam WordPress, que o plugin WooCommerce está presente em 9,8% dos que utilizam WordPress e que 92,05% dos domínios que utilizam WooCommerce para comércio eletrônico estão aderentes à LGPD.

Por fim, conclui-se que mesmo com os desafios da implantação da LGPD em lojas virtuais, as mesmas podem ser beneficiadas, já que a lei traz uma visão mais segura para o cliente onde o mesmo pode saber a finalidade do tratamento de seus dados, dando uma maior credibilidade e transparência para os e-commerces.

Referências

Broad, J. and Bindner, A. (2014). *Hacking com Kali Linux: Técnicas práticas para testes de invasão*. Novatec Editora Ltda, São Paulo.

BuiltWith Pty Ltd (2020). eCommerce technologies Web Usage Distribution on the Entire Internet. Disponível em: https://trends.builtwith.com/shop/traffic/Entire-Internet. Acessado em 30/12/2020.

Carvalho, L., Oliveira, J., Cappelli, C., and Majer, V. (2019). Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais. In *Anais do VII Workshop de Transparência em Sistemas*, pages 21–30, Porto Alegre, RS, Brasil. SBC. ISSN: 2595-6140 event-place: Belém.

Elia, F. (2018). WordPress 4.9.8 – Atualização de manutenção. Disponível em: https://br.wordpress.org/tag/4-9/. Acessado em: 19/11/2020.

Herdy, S. (2020). Entenda o impacto da LGPD na transformação digital. Disponível em: https://www.ecommercebrasil.com.br/artigos/o-impacto-da-lgpd-na-transformacao-digital/ Acessado em: 24/10/2020.

Nakamura, E., Filho, J. R. F., and Ide, M. C. (2019). Metodologia de Avaliação de Riscos e Medidas de Segurança na Proteção de Dados Pessoais. In *Anais do V Workshop de Regulação, Avaliação da Conformidade e Certificação de Segurança*, pages 11–16, Porto Alegre, RS, Brasil. SBC.

Raposo, C., Melo de Lima, H., Junior, W., Silva, P., and Barros, E. (2019). LGPD - LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS EM TECNOLOGIA DA INFORMAÇÃO: Revisão Sistemática. *RACE - Revista de Administração do Cesmac*, v.4, 2019.