Lei Geral de Proteção de Dados: Desafios técnicos enfrentados por microempresas e empresas de pequeno porte

Gabriela Rodrigues Tristão, Fatec Antônio Russo - São Caetano do Sul,
gabriela.tristao@fatec.sp.gov.br

Mayara Camargo Firmino, Fatec Antônio Russo - São Caetano do Sul,
mayara.firmino@fatec.sp.gov.br

Priscilla Amado Kozara, Fatec Antônio Russo - São Caetano do Sul,
priscilla.kozara@fatec.sp.gov.br

William Lopes Moreira, Fatec Antônio Russo - São Caetano do Sul,
william.moreira8@fatec.sp.gov.br

Estefânia Angelico Pianoski Arata, Fatec Antônio Russo - São Caetano do Sul,
estefania.arata@fatec.sp.gov.br

Resumo

Atualmente existe uma grande preocupação com a proteção dos dados pessoais. É comum telejornais noticiarem vazamentos de dados de empresas. Isso acontece porque não havia instrumentos legais que exigissem que as empresas trabalhassem de forma mais ativa para protegê-las. O objetivo deste trabalho é realizar um panorama sobre a nova lei de proteção de dados, de maneira a dissertar como microempresas e empresas de pequeno porte irão se adequar, e as consequências financeiras e sanções que as organizações estão sujeitas a sofrer caso descumpra a legislação. A metodologia utilizada para esse artigo tem como base a pesquisa bibliográfica, através da análise de informações já publicadas por profissionais.

Palavras-chave: LGPD. Empresas. Segurança da Informação. Adequação.

Abstract

Currently, there is a great concern of each citizen with the protection of their personal data. It is common to see news on the news and on the internet about data leaks from companies. This is because there were no legal instruments that required companies to work more actively to protect them. The objective of this work is to provide an overview of the new data protection law, in order to discuss how micro and small businesses will fit in, and the financial consequences and sanctions that organizations are subject to incur if they fail to comply with the law. The methodology used for this article is based on bibliographical research, through the analysis of information already published by professionals.

Keywords: LGPD. Companies. Information Security. Adequacy

1 Introdução

Em 2018, foi sancionada a Lei Geral de Proteção de Dados (LGPD) com objetivo de salvaguardar direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (LGPD, 2018). Sob outra vertente, a lei também ocasionou diversas discussões sobre os impactos financeiros e técnicos de sua correta implementação, principalmente em microempresas e empresas de pequeno porte que por vezes carecem de recursos para atender requisitos legais.

Diante do interesse nacional da legislação, empresas estarão sujeitas a responder perante ao titular de dados pessoais e ao poder público por eventual descumprimento de requisito legal. O artigo 52 prevê multa de até 2% do faturamento podendo chegar a até cinquenta milhões de reais por infração (LGPD, 2018).

Para implementação da lei empresas precisarão despender de ferramentas de segurança da informação, de pessoas com capacidade técnica para correta execução. Salienta-se que artigo 41 “caput” da lei também prevê a obrigatoriedade da empresa ter a figura do encarregado de proteção de dados, pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre os titulares e a Autoridade Nacional de Proteção, órgão fiscalizador da lei (LGPD, 2018).

Ocorre que embora a lei traga penalidades, a não conformidade com os requisitos exigidos é realidade de grande parte das empresas brasileiras, conforme dados apontados pela empresa Resultados Digitais em 2020.

Na atual conjuntura, em que o volume massivo de dados tratados pelas empresas ganharam altas proporções, adequar a empresa à LGPD é medida que precisa ser aplicada, nesse panorama, o existe o desafio de como conciliar a realidade técnica e econômica das empresas com o interesses da proteção de dados dos indivíduos.

Sendo assim, o presente artigo tem objetivo de discorrer acerca do contexto em que a lei geral de proteção de dados foi editada no país, demonstrar ferramentas aptas para o projeto de adequação, bem como apresentar o relatório da consulta pública realizada pelo Instituto de Tecnologia e Sociedade do Rio (ITS RIO).

2 Referencial Teórico

Com o advento do mundo *BIG DATA* que proporcionou massivo volume de informações, a proteção de dados e a segurança da informação passaram a ostentar posição de protagonismo empresarial, legislativo, social e econômico, considerando que a circulação de informações, principalmente em âmbito digital, se tornou atrativa para criminosos virtuais.

Corroborando Elba Lúcia de Carvalho Vieira (2021), doutoranda em Ciência da Informação pontua que o mundo imerso na tecnologia está repleto de ameaças digitais. Sequestro de informações, engenharia social, códigos maliciosos, funcionários despreparados, espionagem, crime cibernético cada vez mais sofisticado são exemplos de ameaçadas que podem causar sérios danos a uma organização.

Conforme dados apontados por (WEF, 2021 *apud* VIEIRA, 2021) o risco cibernético é um risco dominante para sociedade, visto que conforme relatório apresentado no Fórum Econômico Mundial, através do *The Global Risks Report* 2021, a falha de segurança

cibernética está entre os dez maiores riscos globais, um dos motivos essências para esse dado é o fato das medidas de segurança cibernética estarem obsoletas diante do surgimento de ferramentas sofisticadas capazes de ensejarem perdas financeiras, tensões geopolíticas ou instabilidades sociais.

Em consonância, a eminente escritora Viviane Nóbrega Maldonado (2021) leciona que o grande fluxo de dados notadamente na Europa contribuiu para edição da Diretiva 95/46 que trazia em seu escopo princípios, direitos e regras sobre a segurança da informação. Posteriormente este movimento protetivo ocasionou na criação do *General Data Protection Regulation (*GDPR).

Mencionado regulamento concorreu diretamente para a promulgação da Lei Geral de Proteção de Dados no cenário brasileiro.

Para Denise de Souza Luiz Francoski (2021) desembargadora do Tribunal de Justiça de Santa Catarina e encarregada pelo Tratamento de Dados Pessoais do TJSC, no Brasil, além da entrada em vigor da GDPR, outros fatores foram imprescindíveis para edição da LGPD, como o fato da crescente atividade econômica internacional, propagação das diversas redes sociais entre outras plataformas digitais as quais solicitam dados de titulares, nesse contexto a não regulamentação da proteção de dados pessoais poderia acarretar em isolamento comercial entre outros entraves econômicos para o Brasil.

Embora no Brasil a lei só tenha entrado em vigor em setembro de 2020, Andreia Saad e Antonio Hiunes (2020) sustentam que empresas parceiras de fornecedores e clientes internacionais já lidam com o tema privacidade pelo menos desde 2018, tendo em vista que em decorrência da GDPR se tornaram imprescindíveis exigências quanto ao cumprimento de obrigações basilares como segurança da informação e remoção de dados.

Dessa forma, conforme elucidado pelos autores, o tema Segurança da Informação e a influência de normas estrangeiras contribuíram para edição da Lei no Brasil, porém a grande questão em pauta é como implementar essa proteção adequada em micro e pequenos negócios.

3 Metodologia

A metodologia utilizada na elaboração deste artigo foi a de revisão bibliográfica, através de levantamento de fontes teóricas em livros, revistas, legislação, bem como sites que versam sobre o tema.

Adotou-se a análise e comparação de informações e dados sobre a Lei Geral de Proteção de Dados Pessoais e Segurança da Informação disponibilizados por profissionais da área jurídica e tecnológica atuantes com os mencionados temas.

4 Medidas Técnicas de Segurança para Adequação a Lei Geral de Proteção de Dados

Diante do capítulo VII da Lei Geral de Proteção de Dados (2018) que trata da segurança da informação e das boas práticas que devem ser tomadas pelos operadores dos dados e informações. Esse tópico baseia-se em medidas que pequenas e médias empresas devem

adotar para adequação e regulamentação perante a legislação.

Ao tratar de medidas técnicas para proteção dos dados, a Lei Geral de Proteção de Dados (2018) é clara nos termos do seu artigo 46, no qual informa que os responsáveis pelo tratamento das informações pessoais devem adotar medidas de segurança, técnicas e administrativas, a fim de proteger os dados pessoais de acessos não autorizados e de situações geradas por incidentes de segurança de forma acidentais ou ilícitas que acarrete destruição, perda, alteração, comunicação ou de qualquer forma que venha oferecer tratamento inadequado ou ilícito.

Em seu artigo 50, a Lei Geral Proteção de Dados (2018) informa que diante de suas atribuições e competências os responsáveis pelo tratamento dos dados devem formular regras de boas práticas e de governança a modo que estabeleçam condições, funcionamentos, procedimentos, normas de segurança, padrões técnicos, obrigações para todos que estiverem envolvidos nos processos, medidas educativas, monitoramento interno, mitigação de riscos envolvidos e todos e demais assuntos relacionados ao tratamento das informações.

Com esse referencial a lei nos direciona para as normas definidas pela ISO (*International Organization for Standardization*) em conjunto com a IEC (*International Electrotechnical Commission*), no qual a família de normas 27000 são direcionadas para gestão da segurança da informação. A norma técnica brasileira NBR ISO/IEC 27001 (2013) especifica os requisitos necessários para que seja criado, implantado, operado, monitorado, analisado, mantido e melhorado um Sistema de Gestão de Segurança da Informação (SGSI). Um SGSI fornece apoio para que incidentes de segurança sejam reduzidos, transferidos, evitados e aceitação do risco de forma consciente. Ao realizar a implantação de um SGSI, toda empresa tem como foco garantir que o pilar de segurança, definido pela NBR ISO/IEC 27001 (2013), seja atingido. Isso significa garantir que os dados sejam confidenciais, íntegros e disponíveis somente a quem possua direito de acesso a eles.

4.1 Ferramentas a serem usadas para adequação à Lei

Referencial de soluções técnicas que possuem como objetivo proteger os pilares de segurança. Muito deve-se debater com os gestores dessas empresas, equipe de tecnologia da informação e os responsáveis pela segurança da informação, para adoção de medidas que venham atender as devidas necessidades de forma eficaz, sejam com soluções pagas ou *softwares open source*.

Software Antivírus: Software de antivírus é uma ferramenta que tem como objetivo proteger os dispositivos dos usuários, computadores e celulares, de *malwares* indesejáveis. Possuir um software dessa natureza instalado é de extrema importância, devido os vários meios de contaminação existentes, como através da internet ou de mídias removíveis (SILVA, 2011).

Firewall: É uma ferramenta de rede que realiza filtragem as informações da rede, é a primeira proteção entre os dispositivos de uma rede interna com o restante da internet. Através de um firewall é possível controlar o que entra e sai de uma rede, realizar certos bloqueios relacionado a sites perigosos e evitar ataques remotos de *hackers* (SILVA, 2011).

Criptografia: É a técnica utilizada para que dados não sejam acessíveis e lidos por quem não tem direito de acesso a eles. Quando um dado é roubado, a criptografia impede que não seja facilmente descoberto seu conteúdo, isso nos diz quanto maior o nível de segurança é imposto na criptografia maior será a dificuldade em quebrá-la (NAKAMURA

e GEUS, 2007).

Rede Privada Virtual (VPN – *Virtual Private Network*): É uma ferramenta que permite efetuar acesso remoto de qualquer lugar que possua acesso à internet. Ela garante que um usuário possa acessar de forma segura e criptografada dados de onde quer que esteja. Durante o ano de 2020 com a pandemia mundial de coronavírus, muitas empresas necessitaram disponibilizar acesso remoto aos seus funcionários para darem continuidade a suas atividades de forma segura de suas casas. Sem o uso de VPN, muitas vulnerabilidades de invasões e ou intercepção de dados através da rede seriam explorados por hackers (NAKAMURA e GEUS, 2007).

Sistemas de Prevenção de Intrusões (IPS – *Intrusion Prevention System*): São sistemas que protegem e monitoram uma rede de forma continua e ativa, eles executam uma análise do tráfego de rede, e ao detectar tráfego suspeito e que não esteja de acordo, ele bloqueia a atividade. Impedindo ataques que podem ter ultrapassado a barreira do firewall (DOHERTY, 2008).

Sistemas de Detecção de Intrusões (IDS – *Intrusion Detection System*): Os sistemas de IDS trabalham de forma semelhante aos sistemas de IPS, focado em monitorar ambiente de tráfego de rede. Porém, eles não efetuam o bloqueio da atividade suspeita, geram um alerta para que os devidos administradores da rede e segurança tomem as devidas providências (DOHERTY, 2008).

Backups: Backups são cópias de segurança de arquivos e sistemas, eles geram proteção para dados que venham ser danificados ou perdidos, sejam por motivos não intencionais como desastres naturais ou por intencionais como os que salvos por um hacker. Ele é imprescindível para recuperação e restabelecimento de processos dentro de uma organização, pois realiza uma cópia de segurança dos seus dados (PRESTON, 2007).

Filtro de *SPAM*: *SPAM* é uma mensagem eletrônica indesejada que é enviada através de correio eletrônico. Os filtros de *SPAM* realizam uma triagem na qual separa os e-mails válidos de e-mails indesejáveis. Sendo o e-mail uma ferramenta indispensável no mundo corporativo, é um local de muitos ataques através de falsas mensagens, conhecidos como *phishing*, recebimento de arquivos infectados, entre outros. Um filtro de *SPAM* trabalha para que esse tipo de mensagem não chegue ao usuário final, reduzindo assim a probabilidade de ocorrências (FEBRE, 2005).

Prevenção de Perda de Dados (DLP – *Data Loss Prevention*): Uma ferramenta de sistema DLP auxilia na identificação, monitoração e proteção da perda de dados. Ele funciona através do monitoramento em tempo real, registros de *logs*, e demais políticas de segurança definidas para que acessos não autorizados não venha ocorrer, dados não sejam roubados, mal utilizados ou vazados por pessoas mal-intencionadas (ROEBUCK, 2011).

Sendo assim, conforme elucidado diversas são as ferramentas aptas a serem utilizadas no projeto de adequação à Lei Geral de Proteção de Dados, porém a grande preocupação que norteia autoridades do tema é como inserir ferramentas que demandam investimentos e conhecimento técnico na realidade de micro e pequenas empresas. Por esse motivo a lei em seu artigo 55-J, inciso XVIII prevê a necessidade da Autoridade Nacional de Proteção de Dados editar normas para tratamento diferenciado desse grupo (LGPD, 2018).

5 Tratamento Diferenciado para Microempresas e Empresas de Pequeno Porte

Inegável o papel de importância da Lei Geral de Proteção de Dados, porém, conforme demonstrado no tópico anterior, projeto de adequação demanda ferramentas de Segurança da Informação que por vezes carecem das possibilidades econômicas de micro e pequenas empresas.

Por esse motivo, a Lei Geral de Proteção de Dados (2018), em seu artigo 55-J, inciso XVIII, atribuiu como competência da Autoridade Nacional de Proteção de Dados a conduta de editar normas, orientações e procedimentos simplificados e diferenciados, inclusive quanto aos prazos, para que microempresas e empresas de pequeno porte.

Dados apontados por Resultados Digitais apud (LOUREIRO, 2020) mostram que em outubro apenas 4% dos pequenos negócios entrevistados afirmaram estar em conformidade com a lei. Por outro lado, 65% ainda estavam atuando em desacordo com os requisitos da norma. Para 20% das entrevistadas, a falta de ferramentas é fator dominante para a desconformidade com a lei. Elementos como falta de conhecimento técnico da equipe jurídica foi citado por 13%. Por fim, falta de recursos financeiros foi o fator alegado por 8% das entrevistadas para justificar a dissonância com a LGPD.

Nesse sentido, para começar a atender essa designação e ir ao encontro da realidade das empresas no país, a Autoridade Nacional de Proteção de Dados (ANPD), no dia 29 de janeiro de 2021 abriu Consulta Pública para coletar subsídios sobre a regulamentação da aplicação da Lei Geral de Proteção de Dados para microempresas e empresas de pequeno porte (ITS RIO, 2021).

O Instituto de Tecnologia & Sociedade do Rio (ITS RIO, 2021) participou da Consulta Pública, e em seu relatório elencou como Causa Raiz dos problemas regulatórios três vertentes, a saber: familiaridade com a cultura de proteção de dados; orçamento e recursos humanos insuficientes para implementar a LGPD; Realização de mapeamento de dados e análise de gaps e monitoramento contínuo de compliance .

Como solução para os problemas acima elencados, o ITS RIO (2021) sugere três nortes quais sejam: a conscientização e ferramentas simplificadas; mecanismos dedicados de auxílio e apoio e uso proporcional de mecanismos de sanção e fiscalização.

Conforme o Instituto ITS Rio (2021), o primeiro passo para adequação é a conscientização, dessa forma, cabe a ANPD promover eventos educativos e propor ferramentas simplificadas. Deve-se apresentar ferramentas que auxiliem diretamente o processo, e ter como influência diversas autoridades de proteção de dados de diferentes países, as quais proporcionam ferramentas para organizações: entender a lei e sua amplitude; realizar autoavaliação para verificar a compatibilidade; modelos de documentos, com instruções práticas de como usá-los e padronização de procedimentos.

Em decorrência da multa prevista na Lei Geral de Proteção de Dados também ser fator de preocupação, visto que prevê multa de até 2% do faturamento, a ITS Rio (2021) propôs em seu documento a proporcionalidade nas medidas sancionatórias para não impedir o funcionamento de serviços e negócios que estejam buscando cumprir com a regulação.

Dessa forma, apesar dos desafios técnicos que pequenas empresas enfrentam para o projeto de adequação, o diferencial competitivo e evidência para penas mais branda será a demonstração que dentre as possibilidades econômicas e técnicas, a organização adotou aquela que melhor represente as boas práticas.

6 Considerações finais

No atual mundo big data, em que massivo volume de dados pessoais estão em posse de empresas, tornou-se vital a proteção da privacidade dos indivíduos. Neste cenário, foi editada a Lei Geral de Proteção de Dados, inspirada pelo Regulamento Geral sobre Proteção de Dados (RGPD) a legislação busca regular o tratamento de dados, inclusive em meios digitais que venha ser realizado em território nacional. Com isso empresas precisarão de mecanismos de Segurança da informação aptas a proteger acessos não autorizados e o sigilo de informações.

Ademais cumpre salientar que o artigo 50 da Lei também a necessidade da formulação de boas práticas e governança, de modo a criar medidas educativas dentro da empresa, objetivando monitoramento interno e mitigação de riscos. Dessa forma, é necessário desenvolver um próprio SGSI que corrobora para garantir a segurança dos dados, por intermédio de ferramentas, normas de segurança, padrões técnicos e procedimentos correlatos e também a criação de camadas de segurança mais seguras.

Ocorre que o grande desafio que a Autoridade Nacional de Proteção de Dados (ANPD) enfrenta é como garantir a proteção de dados pessoais e ao mesmo tempo estipular um tratamento diferenciado para atender a realidade de técnica e econômica de micro e pequenas empresas.

O relatório do Instituto de Tecnologia & Sociedade do Rio apresentado à Consulta Pública em 2021 sugeriu três sugestões endereçamentos do problema, quais sejam: conscientização e ferramentas simplificados; mecanismos dedicados de auxílio e apoio e uso proporcional de mecanismos de sanção e fiscalização.

Dessa forma, resta evidente que empresas independente da capacidade técnica e condição econômica precisarão respeitar aos ditames da LGPD, porém a fim de resguardar o desenvolvimento social, econômico e o tratamento diferenciado previsto na lei, conforme a sugestão do ITS Rio, a ANPD poderá se valer de ações colaborativas para promover a cultura da proteção de dados, prestar suporte quanto as ferramentas nessas organizações de menor porte e aplicar sanções à luz do principio da proporcionalidade**.**

Referências

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. *NBR ISO/IEC 27001:2013. Tecnologia da informação — Técnicas de segurança — Sistemas de Gestão da Segurança da Informação — Requisitos.* 2013.

BRASIL. *Lei n.13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD).* Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em: 04 mai. 2021.

CARDOSO, Milena. *LGPD: Quais são os principais processos e informações que sua empresa precisa adequar para ficar em conformidade com a lei?*. Âmbito Jurídico. Disponível em: https://ambitojuridico.com.br/noticias/lgpd-quais-sao-os-principais-processos-e-informacoes-que-sua-empresa-precisa-adequar-para-ficar-em-conformidade-com-a-lei/. Acesso em: 24 mai. 2021.

DOHERTY, Jim; ANDERSON, Neil; MAGGIORA, Paul Della. *Cisco Networking Simplified.* 2. ed. Indianapolis: Cisco Press, 2008.

FABRE, Recímero César. *Métodos avançados para controle de Spam.* 2005. 81f. Dissertação (mestrado profissional) - Universidade Estadual de Campinas, Instituto de Computação, Campinas, SP. Disponível em: http://www.repositorio.unicamp.br/handle/REPOSIP/276356. Acesso em: 8 mai. 2021.

FRANCOSKI, Denise de Souza Luiz. *Aspectos práticos para a implementação da Lei Geral de Proteção de Dados Pessoais – LGPD nos Órgãos Públicos: O case do Tribunal de Justiça de Santa Catarina – TJSC*. In: ____. A Lei Geral de Proteção de Dados Pessoais: Aspectos práticos e teóricos relevantes no setor público e privado. 1ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2021.

ITS Rio. *Consulta Pública ANPD: Pequenas e médias empresas e startups*. Rio de Janeiro, 2021. Disponível em: https://itsrio.org/wp-content/uploads/2021/04/ConsultaPublica_PequenasMediasEmpresasStartups.pdf. Acesso em: 22 mai. 2021.

KISCHELEWSKI, Flávia Lubieska. *Startups, pequenas empresas e LGPD: o desafio da regulamentação*. Revista Consultor Jurídico. Disponível em: https://www.conjur.com.br/2021-fev-11/kischelewski-startups-pequenas-empresas-lgpd. Acesso em: 25 mai. 2021.

LOUREIRO, Rodrigo. *Falta de dinheiro e excesso de dúvidas afastam pequenas empresas da LGPD*. Exame, São Paulo, SP, out.2020. Disponível em: https://exame.com/tecnologia/falta-de-dinheiro-e-excesso-de-duvidas-afastam-pequenas-empresas-da-lgpd/. Acesso em: 24 mai. 2021.

MALDONADO, Viviane Nóbrega. Contextualização. In: Maldonado, Viviane Nóbrega. *LGPD Lei Geral de Proteção de Dados Pessoais Manual de Implementação*. São Paulo: Thomson Reuters Revista dos Tribunais, 2021.

NAKAMURA, Emilio Tissato; GEUS, Paulo Lício. *Segurança de Redes em Ambientes Corporativos.* São Paulo: Novatec Editora, 2007.

NERI, Alexandre Vinicius Rodrigues de Moura; LUNA, Henryque Resende. *A LGPD, por enquanto, é inexigível para pequenas empresas*. Revista Consultor Jurídico. Disponível em:https://www.conjur.com.br/2020-nov-03/neri-luna-lgpd-ainda-inexigivel-pequenas-empresas. Acesso em: 24 mai. 2021.

PRESTON, W. Curtis. *Backup and Recovery*. 1. ed. California: O'Reilly Media, 2007.

ROEBUCK, K. *Data loss prevention (DLP) - High-impact strategies*. Brisbane: Emereo Pty Limited, 2011.

SAAD, A; HIUNES,A. Ela,a *LGPD, vista pelas empresas: uma proposta de visão prática – e otimista*. In: DONEDA, D; MENDES, L.S; CUEVA, R.V.B. Lei Geral de Proteção de Dados (Lei n.13.709/2018). 1.ed. São Paulo: Thomson Reuters Revista dos Tribunais, 2020.

SILVA, Mário Gomes da. *Informática – Terminologia: Microsoft Windows Vista, Internet, Segurança, Microsoft Office Word 2007, Microsoft Office Excel 2007, Microsoft Office Access 2007, Microsoft PowerPoint 2007.* 3. ed. São Paulo: Érica, 2011.

VIEIRA, Elba Lúcia de Carvalho. *A proteção de dados desde a concepção (by design) e por padrão (by default)*.In: Maldonado, Viviane Nóbrega. LGPD Lei Geral de Proteção de Dados Pessoais Manual de Implementação. São Paulo: Thomson Reuters Revista dos Tribunais, 2021.