Processando o Saber
eISSN 2179-5150
FATEC Praia Grande · fatecpg.edu.br/revista
submetido: Jan/2021 · **aceito**: Mar/2021 · **publicado**: Jun/2021

A segurança da informação de encontro às conformidades da LGPD

Information security against GDPL compliance

Denise Lemes Fernandes Neves
Fatec Praia Grande
denise.neves@fatec.sp.gov.br

Guilherme Cintra Pavani
Fatec Praia Grande
guilherme.pavani@fatec.sp.gov.br

Rafael Marcos Sales
Fatec Praia Grande
rafael.sales3@fatec.sp.gov.br

Tatiana Schmitz de Almeida Lopes
Fatec Praia Grande
tatiana@fatecpg.com.br

RESUMO

A contínua expansão dos negócios gera diariamente uma enorme massa de dados, com informações pessoais e organizacionais, públicas ou privadas. Sobre essa massa há uma grande necessidade de atenção e cuidados, pois nela transita qualquer tipo de informação como fotos, vídeos, relatórios médicos, policiais e judiciais, dados que devem ser mantidos sob sigilo. Com o intuito de proteger tais informações, a Lei Geral de Proteção de Dados (LGPD) coíbe o compartilhamento e a troca de informações pessoais ou institucionais para a manipulação no âmbito empresarial. A garantia da segurança dos dados fica sob a responsabilidade das empresas que realizam a coleta. Este artigo investiga, através do método exploratório, como o tratamento de dados da LGPD pode estar em conformidade com o plano de segurança de informação (PSI) de uma empresa.

PALAVRAS-CHAVE: LGPD. Segurança da Informação. Sistemas de Informação.

ABSTRACT

The continuous expansion of business generates a huge mass of data on a daily basis, with personal and organizational information, public or private. About this mass there is an enormous need for attention and care, as any type of information, such as photos, videos, medical reports, police, judicial reports and information that must be kept confidential. In order to protect such information, the General Data Protection Law (LGPD) prohibits the sharing and exchange of personal or institutional information for manipulation in the business environment. The guarantee of data security is under the responsibility of the companies that collect it. This article investigates, through the exploratory method, how the treatment of LGPD data can be in accordance with a company's information security plan).

KEY-WORDS: *GDPL. Security. Information systems.*

INTRODUÇÃO

Conforme o Dicionário Aurélio, a palavra "lex." significa Lei – uma regra obrigatória, um preceito, uma norma, criada para estabelecer deveres e direitos a serem obedecidos. Toda e qualquer legislação é conceituada para determinar regras para sua sociedade, porém, em todos os cenários há sempre a presença de anomia[1].

Na Europa está em vigor a "Lei que Regulamenta o Tráfego de Dados e a Proteção dos Mesmos" ((EU)2016/679), que influenciou a lei brasileira.

A Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709/2018, foi sancionada somente em 18 de agosto de 2018, alterando a lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), que foi criada com o intuito de direcionar o tratamento de dados no Brasil. O tratamento de dados é todo o processo que deve ser feito com um dado, desde o momento que ele é coletado e colocado em um Banco de Dados, permanecendo até o momento que é excluído.

Segundo RAPÔSO, et al. (2019), o surgimento da globalização bem como a expansão da *internet*, trouxe grande quantidade de dados gerados a cada minuto em inúmeras transações comerciais e ou sociais, demonstrando a necessidade de definição de parâmetros em forma de lei, para que haja total responsabilidade na conduta desta relação, necessitando de normatizações para a segurança da informação.

Ainda segundo RAPÔSO (2019):

> Com a globalização e o desenvolvimento de novas tecnologias desenvolve uma competição cada vez mais voraz entre as empresas, desenvolvendo questionamentos sobre a segurança das informações corporativas e de seus clientes. As empresas e até o estado estão cada vez mais vulneráveis à espionagem ou de ataques de Hackers como evidenciado as divulgações e áudios de empresas e dos principais poderes do Brasil.

A responsabilidade das empresas para tratar a coleta e a armazenagem de dados pode ser apoiada nos três pilares da segurança da informação: confidencialidade, integridade e disponibilidade, conhecida com tríade CIA, focando a proteção à privacidade online, a liberdade de expressão e a segurança da informação de pessoas naturais (PEIXOTO, 2020).

Em cumprimento da LGPD, as empresas que coletam e manipulam dados, precisam garantir a segurança contra as ameaças e os possíveis vazamentos de seus locais de

[1]Anomia é um conceito que se refere ao **estado social de ausência de regras e normas**, onde os indivíduos desconsideram o controle social que rege determinada sociedade. Acesso em: <https://www.significados.com.br/anomia>, 27 de fevereiro de 2021.

armazenamento. Os cuidados com a segurança da informação nas organizações são tratados, normalmente, em uma política de segurança interna.

Este artigo traz uma pesquisa exploratória para corroborar a hipótese de que a segurança da informação é o principal desafio das empresas a se adequarem à Lei de Proteção de Dados, podendo reavaliar e adaptar as suas diretrizes e normas internas de segurança.

1. A RELEVÂNCIA DOS DADOS SENSÍVEIS DAS PESSOAS NATURAIS

De acordo com o órgão Federal Brasileiro SERPRO[2], dados sensíveis revelam origem racial ou étnica, convicções religiosas ou filosóficas, opiniões políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde e escolha sexual de cada pessoa.

Outro ponto para os dados naturais que são considerados tão críticos quanto os dados sensíveis são os relacionados a crianças e adolescentes, que conforme a lei, os responsáveis legais devem autorizar de forma inequívoca o conteúdo da utilização desses dados.

Os dados sensíveis estão inseridos nos dados naturais, que devem receber a conformidade da nova Lei de Proteção de Dados, sancionada em 18/09/2020.

Conforme LIEM & PETROPOULOS (2020), a relevância e o valor das informações das pessoas naturais vêm crescendo exponencialmente e tornando-se um ativo altamente negociável, com crescente valor de mercado que é muito disputado.

A *internet* passou a ser utilizada para invadir a privacidade alheia e espionar pessoas físicas e jurídicas, além da prática de ofensas e crimes pela rede, ignorando possíveis punições, e conforme a Lei Geral de Proteção de Dados (LGPD), o proprietário dos dados terá o direito de processar qualquer conduta ofensiva ou a utilização de seus dados como ativo comercial.

Isto significa que se houver discriminação através de comentário, fala, sugestão de forma direta ou indireta e que seja depreciativa, pela *internet*, a LGPD garante com base no Artigo II da Lei supracitada, que disciplina o uso da internet no Brasil e que determina, em seu Parágrafo II, a preservação dos direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais, punição na forma da lei.

Devemos lembrar que os direitos humanos estão diretamente ligados ao entendimento de ordenamento jurídico e se a internet passar a ser vista e utilizada como um meio para a

[2] SERPRO, serviço Federal de Processamento de Dados, criada em 1964, Disponível em: <https://serpro.gov.br> Acesso em 28/03/2021.

propagação de conteúdo, dados pessoais e demais informações, então é necessária a proteção dos direitos fundamentais e humanos em seu ambiente.

Em documento público, a Academia Brasileira de Direito do Estado (ABDET) fez a seguinte análise da legislação:

> Na sociedade atual, mergulhada no âmbito digital, é possível considerar que a personalidade e cidadania da pessoa humana também são moldadas pelo uso da internet: por esse meio a pessoa se expressa, busca informações, se relaciona. O ambiente virtual, tanto quanto o real, deve se submeter à proteção dos direitos humanos, de forma mais abrangente possível, respeitando o princípio do não retrocesso. (ABDET,2015, p.2)

A constante evolução tecnológica, obriga as empresas a buscar cada vez mais novas formas de obter informações sobre seus clientes, procurando por estratégias inovadoras e assim dominar o mercado de produtos, permitindo negociações pelo acúmulo de informações de cada usuário, que são eles: dado identificado[3], dado identificável[4] e dados sensíveis[5], de forma direta ou indireta, possibilitando a identificação das tendências para cada setor, inclusive o da segurança da informação. (SILVEIRA, AVELINO & SOUZA, 2016).

O ramo que busca negociar o acúmulo de informações que as empresas armazenam é uma atividade nova, e por esse motivo, ainda é muito difícil comprovar que elas estejam realmente comercializando os dados de seus clientes.

Para VARELLA (2019), os dados devem receber tratamento no momento da recepção pelas empresas, objetivando caso a caso, analisando-se o tipo e a quantidade coletadas, pois apenas o acesso autorizado às informações é essencial ao titular delas.

Um caso que esteve em voga nos noticiários (REVISTA ÉPOCA (2018), envolveu o *Facebook*, que admitiu vazamento de dados de seus clientes, porém alegaram falha no sistema e não uma real comercialização dos dados.

A robustez da lei definirá processos de conduta às instituições, que devem seguir e assim garantir a proteção total e completa dos dados que armazenam.

Conforme o TRIBUNAL DE CONTAS DA UNIÃO (2007), preservar a integridade, confidencialidade e autenticidade das informações manipuladas por qualquer modo, deve receber a garantia do cumprimento da lei, para que não haja vazamentos acidentais e ou propositais, garantindo que apenas pessoas autorizadas tenham acesso às informações, não permitindo a criação de um novo produto comercial.

[3] identificado - nome, RG, CPF e diversos outros dados.
[4] identificável - Nº de cartão de crédito, IP de computador, empresa que trabalha entre outros.
[5] sensíveis - Na nova legislação, são determinados por: origem étnica ou racial, crença religiosa, filiação sindical, direcionamento político, orientação sexual, dados genéticos ou biométricos e informações sobre a saúde.

2. A LEI DE PROTEÇÃO DE DADOS (LGPD)

A Lei Geral de Proteção de dados (LGPD) foi criada com base no regulamento europeu ((EU)2016/679) e do conselho da União Europeia de 27 de abril de 2016, mais conhecido como: Regulamento Geral sobre a Proteção de Dados (RGPD), obrigando inclusive gigantes como o *Facebook* e *Google*, a mudar seus meios de coleta e tratamento de dados (ASSIS E MENDES, 2020).

Demorou mais de dois anos, entre a definição da LGPD e sua aplicação por parte das instituições. Esse espaço de tempo foi dado para que as empresas se adequassem e assim estivessem aptas a cumprirem a nova lei.

A LGPD[6] regulamenta o modo como as informações pessoais de cada pessoa natural deverão receber tratamento pelas empresas privadas ou públicas, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados pessoais. Por isso, não importa qual o segmento do negócio, se trata de dados pessoais de clientes, logo a empresa terá que se adequar à legislação.

A lei diz que, por tratamento de dados, entende-se toda operação realizada com dados pessoais, que são referenciadas pela coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração.

De acordo com a LGPD, em seus art. 37 ao 41, alguns papéis de responsabilidade devem garantir a conformidade na aplicabilidade, conforme itens abaixo:

a. CONTROLADOR: pessoa natural ou jurídica, de direito público ou privada a quem compete decisões referentes ao tratamento de dados pessoais;
b. OPERADOR: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador;
c. ENCARREGADO OU D.P.O.: pessoa indicada pelo Controlador e Operador para atuar como canal de comunicação entre o Controlador, os titulares de dados e a Autoridade Nacional de Proteção de Dados (ANPD), que é um órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento da Lei no Brasil.

[6] Planalto. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm.> Acesso em 26/02/2021.

A adequação à Lei deve seguir práticas que estão sendo implementadas pelas empresas, que se utilizarão do mapeamento dos dados, levantando os dados que possuem – pessoais ou não - e como esses dados foram adquiridos. Com o mapeamento feito, deverá ser analisado o que necessita de ajuste nos seus procedimentos internos para ficar em conformidade com a Lei. Aqui é recomendado uma análise dos tipos de riscos e gravidade aos quais a empresa está exposta.

De acordo com o seu modelo de negócio, o plano de ação define em qual das bases legais sua empresa vai se encaixar para ter legitimidade para tratar os dados pessoais. O plano de ação pode se ajustar ao plano de segurança ou mesmo à política de segurança da empresa, se houver.

A próxima fase é a implementação, através do plano de ação e que com um cronograma de execução, indicará a política de segurança da empresa. É fundamental que todas as áreas da empresa estejam engajadas, mas a área da Tecnologia da Informação (TI) será envolvida diretamente para a execução. Toda a empresa deverá estar ciente das novas práticas a respeito da proteção de dados. Portanto, documentos de termos de responsabilidade e políticas de segurança deverão ser divulgados e compartilhados por toda a empresa.

Os negócios são dinâmicos e estão sempre mudando, desta forma o próximo estágio é a revisão, com testes periódicos e adequações conforme o surgimento de inconsistências e para tal o monitoramento se torna a prática mais importante para seguir em conformidade com as mudanças na empresa e com a Lei.

A Autoridade Nacional de Proteção de Dados (ANPD)[7] divulgou no final de janeiro de 2021, seu primeiro ato normativo, no Diário Oficial da União. Trata-se da agenda regulatória da ANPD para o biênio 2021-2022, na qual aponta os temas prioritários a serem enfrentados em resoluções. Divulgou-se os instrumentos para funcionamento próprio – um regimento interno e o planejamento estratégico até 2023 – as primeiras resoluções, previstas ainda para o primeiro semestre deste 2021, envolvem regras para pequenas e médias empresas, metodologia de multas, comunicação de incidentes e elaboração dos relatórios de impacto.

[7] ANPD, Autoridade Nacional de proteção de Dados. Disponível em: < https://www.gov.br/anpd/pt-br > Acesso em 26/02/2021.

4. A SEGURANÇA DA INFORMAÇÃO

Segundo Campos (2007), a informação é elemento essencial para todos os processos de negócio da organização. A definição para a segurança da informação está diretamente ligada em proteger dados de propriedade das organizações e ou sob sua guarda, podendo ser de pessoa física e jurídica, nas quais requerem esforços para garantir a mitigação de riscos e a continuidade das operações. O ato em aplicar a segurança da informação a qualquer tipo de dado, está envolvido em utilizar processos de governança empresarial, que envolva recursos humanos, de infraestrutura e lógicos (computacionais).

A garantia em receber reconhecimento em sua organização, está em demonstrar que os dados fundamentais das pessoas naturais estão sendo manipulados dentro da norma da lei estabelecida e assim construir uma imagem de sucesso.

Cabral (2019) diz que o responsável pelo tratamento dos dados das pessoas naturais, deve priorizar a privacidade dessas informações, observando e cumprindo a lei, garantindo a transparência na manipulação, cumprindo o ciclo da coleta, tratamento, compartilhamento, armazenamento e descarte, e assim, estabelecendo harmonia entre as partes.

Conforme Campos (2007), todo o sistema de segurança da informação objetiva diminuir os riscos que os incidentes de segurança da informação possam representar para a organização. O risco é baseado em dois principais pilares: a probabilidade de ocorrência do incidente e o impacto que o incidente causaria para a organização.

Conforme relatos da empresa Axur[8]**,** no dia 20 de janeiro de 2021, indica que desenvolvedores, enquanto criavam a versão *mobile* do aplicativo do Banco *Scotiabank,* tiveram o código-fonte distribuído via *GitHub*. Por deixarem o acesso ao repositório de forma pública, por descuido, os dados ficaram expostos por meses e foram identificados por um pesquisador. Estavam lá credenciais de acesso, documentações e partes sensíveis do código. O conteúdo foi removido, mas um dia depois, a imprensa já havia liberado todas as informações e os clientes do banco estavam muito preocupados, pensando no que poderia acontecer com seus dados. Afinal, suas informações mais sensíveis estavam na base vazada.

[8]Descubra vazamentos de dados em sua empresa, antes que seja tarde. Disponível em: <https://axur.com/pt/lgpd/?utm_source=adwords&utm_term=lgpd&utm_campaign=Axur+%7C+Search+%7C+2020+%7C+LGPD&utm_medium=ppc&hsa_mt=b&hsa_ad=431222974962&hsa_net=adwords&hsa_src=g&hsa_kw=lgpd&hsa_tgt=kwd-350057729515&hsa_cam=9197105996&hsa_acc=2507947540&hsa_ver=3&hsa_grp=93147865117&gclid=CjwKCAjwwMn1BRAUEiwAZ_jnEpyQ9ylcN1i_2iVydhEbRyqu7yTpQr4lJJBF3VzUTZEYqG3WrUlZvxoCFvsQAvD_BwE.> Acesso em 20/01/2021.

Outro relato da mesma empresa acima citada, Axur, no dia 20 de janeiro de 2021, trata de nova exposição de dados ocorrida na *Dark Web*. Após o constrangimento de ter que anunciar publicamente a exposição de dados de mais de três milhões de clientes, a empresa acreditou que não haveria mais problemas, pois a brecha já havia sido fechada. Enganou-se, pesquisadores identificaram um anúncio com a venda da base de dados em dois formatos diferentes, sendo feita em fóruns da *Dark Web*. Os registros de nome, endereço, preferências de compra e senhas criptografadas em *HASH* estavam novamente na mídia. Como o time interno não estava monitorando esses fóruns na *Dark Web*, a imprensa foi mais rápida na divulgação – e só depois o time de segurança da empresa tomou conhecimento. Mais uma vez, a empresa teve que se pronunciar e novamente, o medo e a preocupação caíram sobre os usuários, que acreditavam estar tudo solucionado.

Um terceiro caso real que ocorreu recentemente e vem causando muita preocupação a muitas pessoas no Brasil: o vazamento de dados de mais de 220 milhões de pessoas. Baseado na notícia de Felipe Ventura no site Tecnoblog[9], na semana do dia 22 de janeiro de 2021.

Foi publicada uma informação de um vazamento de informação enorme que expôs dados pessoais como o CPF de mais de 220 milhões de pessoas. A equipe do Tecnoblog descobriu que a situação é ainda mais grave do que se previa porque além dos dados que estão disponíveis de graça na internet, existe um outro arquivo ainda maior que possui muitas outras informações sensíveis além do CPF como: salário, score de créditos, endereço, fotos etc.

Mesmo com todas as suspeitas voltadas para o Serasa Experian, sua equipe declarou ao Tecnoblog que foi realizada uma análise profunda nas bases de dados e foi concluído que o Serasa não é a fonte dos dados vazados, que não existe nenhuma correspondência entre os campos das pastas que foram vazadas com os campos existentes nas bases de dados onde as informações são armazenadas, além de não possuírem alguns dos tipos de dados vazados na web, os dados que estão sendo atribuídos ao Serasa não correspondem aos dados armazenados nos arquivos da empresa.

O objetivo dos fraudadores é a busca de dados que as corporações detêm em seus bancos de dados, para conseguirem dados básicos de pessoas físicas ou jurídicas. Em poder das informações, criminosos conseguem se passar pelos verdadeiros proprietários dos documentos e assim efetuar quaisquer tipos de ilícitos, como compras, abrir empresas, conseguir empréstimos, trazendo para os verdadeiros donos dos dados, enormes prejuízos.

[9] https://tecnoblog.net/404838/exclusivo-vazamento-que-expos-220-milhoes-de-brasileiros-e-pior-do-que-se-pensava/. Acesso 27/02/2021

Conforme Agostinelli (2018), a lei atribui as responsabilidades de competência a quem realmente deve e no caso de violação serão atribuídas sanções administrativas e punições por ressarcimentos ao dano causado.

Os incidentes de segurança, quando tratados, precisam ser analisados pelas organizações ao ponto de gerar informações que possibilitarão identificar quais são mais recorrentes e os que geram maiores impactos CAMPOS (2007). Alguns incidentes mais graves poderão acabar em um tribunal. Para que as ações sejam sustentadas em um julgamento, é necessário que existam e que sejam coletadas evidências que irão proteger a empresa ou identificar alguma negligência.

A evidência pode ser fortalecida por uma trilha forte e confiável de informações ao longo de um período significativo e uma política de segurança poderá ajudar a organização na coleta dessas informações.

4.1 POLÍTICA DE SEGURANÇA DA INFORMAÇÃO

Segundo Campos (2007), estabelecer um sistema de gestão de segurança da informação é dar vida própria para a segurança da informação dentro da empresa.

Grande parte das organizações, mesmo antes da LGPD, aplicam algumas ações para diminuir vulnerabilidade de seus sistemas, através de uma Política de Segurança da Informação (PSI). A política é um conjunto de normas e procedimentos que regulam o comportamento das pessoas que se relacionam com a organização no que se refere ao tratamento da informação. Os esforços realizados na implementação de controles de segurança da informação são acompanhados de investimentos, sendo necessário um tempo de adequação. A política de segurança da informação deve ser um documento simples e de fácil entendimento, pois será lida por todos os colaboradores da organização.

O principal objetivo da política é estabelecer um padrão de comportamento que seja conhecido por todos na organização e que sirva de base para decisões da alta administração. Outro benefício é que as pessoas saberão como se comportar em diversas situações dentro da organização, o que diminui incidentes de segurança da informação e aumenta a produtividade.

O sistema de segurança de informação precisa ser planejado, implementado, monitorado e melhorado continuamente. O ciclo inicia-se no planejamento, passa pela implementação, monitoramento, melhoria e transforma-se em um ciclo de evolução contínua, garantindo adaptabilidade necessária ao sistema nos ambientes dinâmicos das organizações modernas.

Campos (2007) revela que a área da Tecnologia da Informação é, na maioria dos casos, aquela que inicia o processo de implantação de um sistema de gestão de segurança da informação, pois é a área mais afetada pelas normas de segurança, e talvez a que tenha maior consciência da necessidade de um sistema de segurança que garanta as informações que ele gerencia.

Porém, para a adequação do negócio a LGPD será necessário a contribuição das outras áreas que darão suporte a implementação da lei como a área Jurídica, área de Recursos Humanos, a área da Gestão da Qualidade, entre outras. É recomendado que a empresa crie um escritório específico para manter a segurança da informação em sua estrutura organizacional. A empresa deve estar juridicamente bem embasada, demonstrando a existência de uma Política Interna de Segurança de Dados e, ao mesmo tempo, precisa conhecer e saber explicar o uso das tecnologias e processos produtivos que revelam o cuidado adequado quando o assunto é a necessidade de proteção ao risco de vazamento de dados.

Se houver uma mudança na estratégia da organização que represente alteração nos processos, mudanças tecnológicas e pessoas, surgindo ameaças novas para os ativos já existentes, a visão de riscos da segurança precisa ser reavaliada e adaptada as normas internas e a lei, ocorrendo alterações na política de segurança da empresa.

A LGPD e a Política de Segurança da Informação (PSI) explicita para toda as pessoas que acessam e usam a informação, qual é a filosofia da organização sobre esse recurso (FONTES,2006), visando assegurar que toda informação da empresa e de seus clientes esteja protegida contra mau uso e possíveis perdas.

5. CONSIDERAÇÕES FINAIS

Este artigo corrobora com as organizações que possuem uma boa política de segurança da informação e assim estão mais próximas da conformidade com a LGPD e observa que as que não possuem uma política de segurança devem começar o quanto antes a definirem uma.

A política de segurança de uma empresa é um conjunto de regras, normas e procedimentos que determina qual deve ser o comportamento das pessoas que se relacionam com a organização no que se refere o tratamento da informação. Não é um documento independente com regras de conduta desconectadas, mas um documento em continuidade de regras, normas e leis já existentes.

A Lei Geral de Proteção de Dados foi criada com o intuito de proteger os dados de qualquer pessoa, impedindo que empresas comercializem ou manipulem dados pessoais, dentro ou fora do país. Podendo o cidadão, quando sentir seus direitos violados, acionar a justiça, impedindo que os detentores dos dados continuem manipulando dados pessoais de forma irregular, causando danos e prejuízos para usuários, que são os proprietários das informações.

O artigo 48 da Lei 13.709/18 (LGPD) que elenca as ações que devem ser observadas de imediato pela empresa em caso de vazamento de dados, determina, de forma impositiva, que o controlador dos dados deve comunicar à autoridade nacional e aos titulares dos dados, imediatamente, o evento que possa colocar em risco direitos individuais. O controlador é um papel de responsabilidade que faz parte da equipe de segurança de uma empresa, em conformidade da lei. Portanto, faz parte do plano de segurança da empresa.

Visando o lado das empresas, aquelas que já possuem maturidade com um plano de segurança e investimentos na estrutura de segurança dos dados coletados no seu negócio, terão menos desafios e investimentos a se adequarem à LGPD.

Uma forma eficiente das empresas demonstrarem boa-fé com o tratamento dos dados são com condutas implementadas em uma boa política de segurança interna, sem punições pela falta de conformidades, quando a Lei efetivamente for cobrada pelos órgãos competentes, no final do ano de 2021.

REFERÊNCIAS

ASSIS E MENDES. **Histórico das Leis de Proteção de Dados e da Privacidade na Internet**. Direito Digital, Empresarial e Proteção de Dados, 2020. Disponível em: < https://assisemendes.com.br/historico-protecao-de-dados/ >. Acesso em: 07 de dezembro de 2020.

BAPTISTA LUZ. **Dia Internacional da Proteção de Dados**, 2019. Disponível em: < https://baptistaluz.com.br/espacostartup/28-01-dia-internacional-da-protecao-de-dados/ >. Acesso em: 12 de dezembro de 2020.

BARBOSA, D. **8 ferramentas de adequação à Lei Geral de Proteção de Dados (LGPD)**. *We Live Security*, 2020. Disponível em: < https://www.welivesecurity.com/br/2020/09/22/8-ferramentas-de-adequacao-a-lei-geral-de-protecao-de-dados-lgpd/> Acesso em: 31 de outubro de 2020.

BRASIL. LEI Nº 12.965, DE 23 DE ABRIL DE 2014. **Marco Civil Da Internet**. Brasília, 23 abr. 2014. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm >. Acesso em: 05 outubro 2019.

BRASIL. LEI Nº 13.709, DE 14 DE AGOSTO DE 2018. **Lei Geral de Proteção de Dados Pessoais**. Brasília, 14 ago. 2018. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm >. Acesso em: 05 outubro 2019.

CAMPOS, A. **Sistema de Segurança da informação**. 2 ed. Ed. Florianopolis: Visual Books, 2007.

COELHO, Gabriela **Deputado propõe que entrada em vigor da LGPD seja adiada.** Disponível em: < https://www.conjur.com.br/2019-out-31/deputado-propoe-entrada-vigor-lgpd-seja-adiada > Acesso em 20 de novembro de 2019.

Comentários ao Marco Civil da Internet ABDET – Academia Brasileira de Direito do Estado. Disponível em: < https://abdet.com.br/site/wp-content/uploads/2015/02/MCI-ABDET.pdf >. Acesso em: 07 outubro 2019.

Em que "estágio" estamos? Confira o mapa da proteção de dados pessoais no mundo. Disponível em: < https://www.serpro.gov.br/lgpd/menu/a-lgpd/mapa-da-protecao-de-dados-pessoais >. Acesso em: 21 set. 2019.

FONTES, Eduardo. **Segurança da informação:** o usuário faz a diferença. São Paulo: Saraiva, 2006.

Lei 13.709/2018: Lei Geral de Proteção de Dados Pessoais Disponível em: < https://www.dizerodireito.com.br/2018/08/lei-137092018-lei-geral-de-protecao-de.html?m=1&fbclid=IwAR2Kusjw1aucpdBtCBDyoK2rWDCZSEi42ZH8MzoqzT4dggaNLR0DCiAFb_Q >. Acesso em: 10 out. 2019.

LIEM, Cassandra; PETROPOULOS, Georgios. **The economic value of personal data for online platforms, firms and consumers**, 14 de janeiro de 2016. Disponível em: < http://bruegel.org/2016/01/the-economic-value-of-personal-data-for-online-platforms-firms-and-consumers/#_ftnref6 > Acesso em: 11 de outubro de 2020.

MACEDO, Fausto. **LGPD entenda o que é a lei geral de proteção de dados pessoais.** Disponível em: < https://politica.estadao.com.br/blogs/fausto-macedo/lgpd-entenda-o-que-e-a-lei-geral-de-protecao-de-dados-pessoais/ >. Acesso em: 10 set. 2019.

MACHADO, José Mauro Decoussau; DOS SANTOS, Matheus Chucri; PARANHOS, Mario Cosac Oliveira. **LGPD E GDPR:** Uma análise comparativa entre as legislações. Disponível em: < http://www.pinheironeto.com.br/publicacoes/lgpd-e-gdpr-uma-analise-comparativa-entre-as-legislacoes >. Acesso em: 20 nov. 2019.

PEIXOTO, A. S. **Lei de Proteção de Dados:** entenda em 13 pontos! Politize, 2020. Democracia Digital. Disponível em: < https://www.politize.com.br/lei-de-protecao-de-dados/#:~:text=A%20LGPD%20complementa%20o%20escopo,da%20seguran%C3%A7a%20das%20informa%C3%A7%C3%B5es%20pessoais >. Acesso em: 28 de novembro de 2020.

RAPÔSO, Cláudio Filipe Lima et al. **LGPD-Lei Geral de Proteção de Dados Pessoais em Tecnologia da Informação:** Revisão Sistemática. RACE-Revista de Administração do Cesmac, v. 4, p. 58-67, 2019

SERPRO.DADOS SENSÍVEIS. **O que são dados sensíveis, de acordo com a LGPD**. Disponível em:< https://www.serpro.gov.br/lgpd/menu/protecao-de-dados/dados-sensiveis-lgpd> Acesso em; 28 de março de 2021.

SILVEIRA, Sergio Amadeu; AVELINO, Rodolfo; SOUZA, Joyce. **A privacidade e o mercado de dados pessoais| *Privacy and the Market of personal data***. Liinc em Revista, v. 12, n. 2, 2016.

SOPRANA, Paula. **O que é a GDPR, a lei de proteção de dados europeia, e por que ela importa.** Disponível em: < https://gizmodo.uol.com.br/lei-proteca-dados-gdpr/ > Acesso em: 20 nov. 2019.

TRIBUNAL DE CONTAS DA UNIÃO. **Boas práticas em segurança da informação**. 2. ed. Brasília: TCU, Secretaria de Fiscalização de Tecnologia da Informação, 2007. Disponível em: <https://portal.tcu.gov.br/lumis/portal/file/fileDownload.jsp?fileId=8A8182A24D6E86A4014D72AC823F5491&inline=1 >. Acesso em: 03 de dezembro de 2020.

UNIÃO EUROPEIA. REGULAMENTO (UE) 2016/679 DO PARLAMENTO EUROPEU E DO CONSELHO de 27 de abril de 2016. **Regulamento Geral sobre a Proteção de Dados**. Bruxelas, em 27 de abril de 2016. Disponível em: < https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679&from=PT > Acesso em: 06 set. 2019.

VARELA, L. **TUDO sobre a Lei Geral de Proteção de Dados (LGPD)**, 2019. Compugraf. Disponível em: < https://www.compugraf.com.br/tudo-sobre-a-lei-geral-de-protecao-de-dados-lgpd/ >. Acesso em: 07 de novembro de 2020.