NÚCLEO INTERDISCIPLINAR DE PESQUISA

UNIDESC
Centro Universitário de Desenvolvimento do Centro-Oeste

Curso de Sistemas de Informação Artigo Original

A aplicação da Lei Geral de Proteção de Dados em privacidade e segurança, a partir da sua inicialização nas empresas de tecnologia da informação no Distrito Federal

The application of the General Data Protection Law in privacy and security, from its initialization in information technology companies in the Federal District

André Ricardo Matos dos Santos[2], Carlos Henrique Sucupira Reis[1], Maria Eduarda Alves Siqueira Fernandes[1]
1 Alunos do Curso de Sistemas de Informação
2 Professor do Curso de Sistemas de Informação

RESUMO

O presente trabalho tem como objetivo principal evidenciar a atuação da **LGPD** (Lei geral de proteção de dados) nas empresas que utilizam a tecnologia da informação como principal meio de segurança nos serviços e produtos fornecidos, ou seja, apresentar como o surgimento da **LGPD** afetou as grandes e pequenas empresas, tendo foco em como as mesmas utilizam da **tecnologia** para agregar valor aos serviços prestados. Os dados foram coletados através de pesquisas, artigos, relatórios de segurança, situações que envolvem a privacidade do usuário, fatos históricos, análises de gráficos dentre outras evidências abordadas ao decorrer da elaboração do trabalho. A partir das informações obtidas foi imposto que a segurança dos dados privados e públicos se tornou uma prioridade para organizações que se propõem a respeitar o contexto geral da lei, provendo assim **segurança e confiabilidade** a todo e qualquer processo que envolva a utilização de **dados** privados, cujas permissões para uso devem ser apresentadas de forma coesa para o usuário/cliente dos serviços providos pela empresa, o principal foco das pesquisas foi para empresas que atuam principalmente no Distrito Federal e utilizam da **LGPD** em seus processos.

Palavras-Chave: LGPD; Tecnologia; Segurança e Confiabilidade; Dados.

ABSTRACT

The main objective of this work is to highlight the performance of the **LGPD** (General Data Protection Law) in companies that use information technology as the main means of security in the services and products provided, that is, to present how the emergence of the **LGPD** affected the large and small companies, focusing on how they use **technology** to add value to the services provided, data were collected through surveys, articles, security reports, situations involving user privacy, historical facts, analysis of graphs, among others. other evidence addressed during the preparation of the work. From the information obtained, it was imposed that the security of private and public data has become a priority for organizations that intend to respect the general context of the law, thus providing **security and reliability** to any and all processes that involve the use of private **data**, whose permissions for use must be presented in a cohesive way to the user/customer of the services provided by the company, the main focus of the research was on companies that operate mainly in the Federal District and use the **LGPD** in their processes.

Keywords: LGPD; Technology; Security and Reliability; Data.

Contato: carloshenriquecacau@gmail.com; eduarda.alves.siqueira.fernandes@gmail.com

INTRODUÇÃO

Com o avançar das décadas a tecnologia evoluiu e junto a ela o conceito de proteção e segurança, se tornando cada vez mais uma preocupação pras empresas que usam de tecnologia para sua prestação de serviços assim forjando meios de solucionar problemas e evitar situações de risco, e em meio a esse cenário surgiu o conceito da Lei Geral de Proteção de dados e com ela uma nova era de mecanismos que buscam melhorar a forma como se lida com informações vitais para o cotidiano empresarial.

As análises de estudiosos e especialistas da área comprovam que as leis de proteção de dados são extremamente essenciais para que vazamentos e ataques a informações privadas sejam evitados, e evidenciando como um determinado vazamento de dados pode afetar uma empresa ou uma pessoa individual, como, por exemplo, uma perda de dados bancários ou possíveis invasores externos tomam conhecimento de senhas e de números que um cliente possui, e por meio destes realiza operações visando próprio sem a ciência do cliente detentor dos dados. Com a implementação da internet das coisas e do conceito de Big Data força que todos estejam totalmente conectados num mundo tecnologicamente avançado, onde compras e serviços estão hoje presentes num contexto onde é obrigatório a produção de dados, dados esses que são utilizados para a navegação da internet Estes dados são uma importância crucial para as empresas e portanto devem possuir e devida segurança, afinal tais informações são basicamente o que movimenta os serviços e a importância geral de uma sociedade que consome serviços tecnológicos.

> Em uma sociedade da Informação e do conhecimento os dados são coletados, processados e, em seguida, seus resultados são aplicados em ambientes específicos do mundo real. Essa informação, considerada por muitos autores, como o principal patrimônio, de uma organização, está sujeita a problemas com relação a Segurança da Informação, dentre eles, o acesso não autorizado. (SANTANA; DUARTE, 2021).

Este trabalho se apoiará em artigos e documentos de empresas, e visando como a aplicabilidade da LGPD propõem resultados para tais empresas. Por meio de estudos e pesquisa também será evidenciado propostas e mecanismos para efetivação de soluções de LGPD em ambientes empresariais, ou seja, projetos e empresas que prestam serviços voltados para a Lei Geral de Proteção de Dados propondo soluções e aplicações para o mercado. Neste trabalho, buscamos responder à seguinte questão: como funciona a aplicação da lei geral de proteção de dados em privacidade e segurança, a partir da sua inicialização nas empresas de tecnologia da informação no Distrito Federal?

MATERIAIS E MÉTODOS

A metodologia de investigação adotada para suportar o desenvolvimento deste projeto foi a metodologia do tipo descritivo/documental, abordando as formas teóricas de implementação da Lei Geral de Proteção de Dados (LGPD) nas empresas de tecnologia no Distrito Federal. Analisando dados e estatísticas que comprovem a sua aplicação e efetividade. Utilizando informações já existentes e também de um conjunto de opiniões e pontos de vista de diversas pesquisas acadêmicas. A pesquisa documental recorre a fontes mais diversificadas e dispersas, sem tratamento analítico, tais como: tabelas estatísticas, jornais, revistas, relatórios, documentos oficiais, cartas, filmes, fotografias, pinturas, tapeçarias, relatórios de empresas, vídeos de programas de televisão, etc. (FONSECA, 2002, p. 32).

De tal modo, a pesquisa se caracteriza também como uma pesquisa de cunho exploratório, pois segundo Cervo e Bervian (1983) uma característica importante da pesquisa exploratório consiste no aprofundamento de conceitos preliminares de temáticas não contemplada de modo satisfatório anteriormente, e por tanto determinada pesquisa pode promover maior conhecimento sobre o tema explorado.

Será usado o método de pesquisa bibliográfica para a aquisição de dados para a caracterização da pesquisa, segundo Gil (1999), a pesquisa bibliográfica é desenvolvida mediante material já elaborado, principalmente livros e artigos científicos. Portanto será pesquisado obras já documentadas e evidenciadas sobre o tema abordado.

O recorte temporal pega como base, pesquisas elaboradas no período de 2018 até 2021, evidenciando como a LGPD está atuando após sua elaboração e como era antes de ser efetivada na sociedade. Os dados e as aplicações serão abordados em um capítulo à parte juntamente com as documentações das empresas estudadas.

FUNDAMENTAÇÃO TEÓRICA

ORIGEM DA LGPD

Com as transformações advindas da grande revolução tecnológica do início do século XXI as grandes empresas tiveram suas grandes cargas de dados de milhares de clientes e usuários de seus serviços ampliadas exponencialmente. Estes dados possuem uma importância extrema para as empresas e portanto deve possuir e devida segurança,

afinal tais informações são basicamente o que movimenta os serviços e a importância geral de uma sociedade que consome serviços tecnológicos.

“Inspirada na lei europeia de proteção de dados, conhecida como General Data Protection Regulation (GDPR), a Lei Geral de Proteção de Dados (LGPD) tem como objetivo proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas.”(GARCIA; ROCHA; p.16, 2020)

“Inicialmente, a lei foi sancionada com a *vacatio legis* de dezoito meses, entrando em vigor em fevereiro de 2020. Entretanto, com a revogação do artigo 65, dada pela lei n° 13.853, de julho de 2019, foi estabelecido novo prazo para que a LGPD entrasse em vigor, em agosto de 2020. Ocorre que o ano de 2020 vem sendo marcado por incertezas e preocupações, tanto para o governo, quanto para as demais entidades públicas e privadas, em decorrência da atual situação de pandemia que o mundo enfrenta.”(MOTTA, p.24, 2020)

A LGPD nos apresenta um direito difuso, visando entregar isonomia a todos os que se acolhem em seus braços, a coibir a usurpação de dados diante dos avanços tecnológicos em um cenário de criminalidade virtual.

MOTIVAÇÕES PARA O USO DA LGPD

No mundo inteiro tem-se ampliado golpes, numa evolução de mecanismos para subtrair de outras vantagens e privilégios. Incorporou-se ao cotidiano dos crimes presenciais e ataques físicos essa nova modalidade. Um novo empreendimento de uma facção sem rosto.

Roubo de dados como CPF, informações de contas bancárias, invasão de WhatsApp, Facebook, Instagram, entre outras redes sociais. E na missão de assegurar proteção e direitos, a segurança pública cria metodologias, demanda por políticas públicas e conscientização coletiva para alinhar o que é direito ao que é dever. Entre este e aquele, existe uma linha tênua que beira a proximidade e a desordem.

As análises de estudiosos e especialistas da área comprovam que as leis de proteção de dados são extremamente essenciais para que vazamentos e ataques a informações privadas sejam evitados, e evidenciando como um determinado vazamento de dados pode afetar uma empresa ou uma pessoa individual, como, por exemplo, uma perda de dados bancários ou possíveis invasores externos tomam conhecimento de senhas e de números que um cliente possui, e por meio destes realiza operações visando próprio sem a ciência do cliente detentor dos dados.

“Em uma sociedade da informação e do conhecimento os dados são coletados, processados e, em seguida, seus resultados são aplicados em ambientes específicos do mundo real. Essa informação, considerada por muitos autores como o principal patrimônio de uma organização, está sujeita a problemas com relação à Segurança da Informação, dentre eles, o acesso não autorizado.”(SANTANA; DUARTE, 2021)

É de ciência geral que vazamento de informações é um fenômeno que nenhum indivíduo quer que ocorra, pois os danos podem ser avassaladores. A única forma de proteger tais informações é com políticas de proteção equivalentes à gravidade de um possível vazamento, portanto empresas devem possuir níveis de segurança altos e atuais para suas bases de dados.

Boas práticas de segurança de dados são recomendados há mais de 20 anos, porém como não era uma exigência, mas apenas uma recomendação, poucas empresas faziam uso dessas recomendações, afinal isso envolve custos com pessoal, tecnologia (POHLMANN, 2020). Apenas com a chegada de novos avanços na tecnologia onde as pessoas começaram a efetuar todo o tipo de ação por meio tecnológicos as preocupações para com a segurança tiveram a devida atenção, pois a credibilidade de meios virtuais foi colocada à prova com a grande massa de pessoas utilizando dos mesmos para efetuar ações do cotidiano.

E agora estamos numa transição muito importante da LGPD que é como ela está sendo efetivada na atualidade, agora que sua importância está de fato colocada à prova como ela está mudando as organizações e suas visões com a segurança de dados.

EFETIVIDADE NO MERCADO

Após a implementação da LGPD se tornar um critério importante para as empresas, os primeiros resultados começaram a aparecer, e com eles a LGPD começou a apresentar seus efeitos. Muitas empresas e organizações que tiveram experiências com a lei afirmaram que ela é efetiva e demonstra para todos os colaboradores como deve ser tratado as informações dos usuários de forma correta.

Apesar da efetividade da lei, ela é um assunto recente para a maioria das empresas, ou seja, por mais que seja um tema importante, muitas delas têm receios para mudar suas táticas e protocolos.

“Considerando que a LGPD entrou em vigor recentemente, empresas de diferentes setores e órgãos públicos ainda estão enfrentando desafios para adequarem seus sistemas de software em conformidade com a legislação vigente. Garantir a conformidade le-

gal visa evitar sanções administrativas sejam aplicadas pela autoridade nacional de proteção de dados.” (ALVES; NEVES, 2021)

RESULTADOS e DISCUSSÃO

Ao analisar artigos e pesquisas entre 2018 e 2021 de aproximadamente 20 pesquisadores, como France Bellanger, Robbert E Crossier, Victtor Henrique, Pedro Lima e outros autores de estudos voltados ao surgimento e implementação da LGPD, foi constatado diversos casos e fatos que iram compor os resultados e discussões desta pesquisa. Esta pesquisa seguirá uma ordem de fluxo semelhante a uma linha do tempo, referenciando os estados da legislação, ou seja, seu passado, presente e futuro, começando em como surgiram os primeiros conceitos de proteção de dados neste século.

Na modernidade é vital o uso de mecanismos para obtenção de dados, pois que mesmo as empresas possuem uma boa parcela de clientes procurando os serviços da empresa e dessa forma fornecendo seus dados pessoais para os recursos oferecidos, a captação de novos clientes é fundamental para o crescimento de qualquer empresa, ou seja, novos dados precisam ser obtidos e apurados de forma a qual a empresa possa tirar os proveitos necessários para seu consumo.

Em uma sociedade da informação e do conhecimento os dados são coletados, processados e, em seguida, seus resultados são aplicados em ambientes específicos do mundo real. Essa informação, considerada por muitos autores como o principal patrimônio de uma organização, está sujeita a problemas com relação à Segurança da Informação, dentre eles, o acesso não autorizado.(SANTANA; DUARTE, 2021)

Métodos de busca são variados, alguns envolvem a comunicação direta e simples com os clientes, seja por ligação telefônica ou entrevista intrapessoal, nesses métodos os clientes possuem a liberdade de fornecer informações ou não para quem os está perguntando, caso o cliente se interesse pelo produto ou serviço prestado pela empresa, o responsável pela interação pedirá os dados com o consentimento dos clientes para que estas informações sejam usadas. Este cenário é o mais direto para obtenção de dados, entretanto ele é incompatível com a grande necessidade quantitativa de dados que uma empresa precisa para ter seus lucros em uma vantagem competitiva para com suas concorrentes, e a partir disso novos mecanismos de captação são utilizados, existem muitos tipos de mecanismos e cada um atua de um jeito próprio para o benefício da empresa, a

melhor forma de explicar como funciona essa competição é exemplificar como as maiores empresas do mundo lidam com obtenção de dados.

Grandes empresas que trabalham com a internet, possuem vários serviços gratuitos e pagos para os clientes, serviços esses variados e específicos para cada tipo de interesse, um bom exemplo desses serviços é o uso do Google para pesquisas casuais. Tais pesquisas, sendo elas relacionadas ao perfil do usuário ou não, carregam com elas uma bateria de informações sobre quem efetua as pesquisas.

“A pesquisa sobre preocupações com privacidade de informações é claramente importante para pesquisadores de Sistemas de informação e normalmente procura explicar diferenças nos níveis de preocupação com privacidade ou explorar os efeitos de preocupações com privacidade em várias variáveis dependentes, como a disposição de fornecer informações pessoais ou a disposição de realizar transações on-line. As preocupações com a privacidade na Internet representam as percepções dos indivíduos sobre o que acontece com as informações que eles fornecem através da Internet” (DINEV; HART 2006).

O conceito de informação é algo amplo e extremamente abrangente, a definição mais simples é dada como uma reunião ou conjunto de dados e conhecimentos organizados, que possam constituir referências sobre um determinado acontecimento, fato ou fenômeno. Esses dados quando relacionados a pessoas, são muitas vezes características ou definições importantes de como um indivíduo se parece ou se comporta, tais informações são vitais para que esse indivíduo esteja de certa forma existindo na sociedade, um forte exemplo disso é o CPF e o RG, tais dados estão atrelados diretamente a pessoa e definem quem ela é, e qual o papel dela na sociedade, seja uma pessoa regular, uma pessoa com deficiência, pobre, rico ou mesmo se ela já cometeu algum delito.

A informação é um conjunto de dados com significados distintos e diversos valores tanto para indivíduos e empresas privadas, quanto para entidades governamentais (PIERSON, 2009; ZAMOISKY, 2014; CAPONI, 2015).

Ao longo do tempo os dados pessoais tornaram-se um ativo da modernidade. Empresas captam milhões de dados de seus usuários, dados esses essenciais para a longevidade da empresa sendo a captação e utilização de dados pessoais um dos grandes focos de grandes empresas como Google, Microsoft, Apple entre outras famosas pelo meio tecnológico, entretanto os meios privados não são os únicos que possuem a necessidade de dados pessoais, visto que organizações governamentais são as que criam tais dados e

os usam para identificar os indivíduos que habitam em sua jurisdição, tais órgãos tendem a catalogar tudo aquilo que está sobre seus direitos, como locais, equipamentos, capital, espaços geográficos e outros milhões de registros de tudo aquilo julgado importante para o funcionamento de um órgão, desta forma criando uma grande base de dados onde os principais dados são pessoas. O mesmo conceito envolve as empresas de tecnologia, visto que informações de clientes ou usuário é praticamente o responsável pelo funcionamento de uma organização.

Segundo o matemático e empresário britânico Clive Humby “Dados são o novo petróleo”, tal frase é uma perfeita metáfora de como a era digital trata seus recursos mais valiosos, visto que há algumas décadas atrás o foco de grandes empresas era adquirir material bruto, algo tangível e precioso, agora o bem mais valioso de uma empresa são as informações de seus clientes. Entretanto, Humbly trabalha ainda mais a metáfora quando diz: “Os dados são o novo petróleo. É valioso, mas, se não for refinado, não pode ser usado (...), portanto, os dados devem ser divididos, analisados para que tenham valor”, ou seja, o petróleo deve ser refinado para que tenha valor, e os dados precisam receber um tratamento correto para estarem prontos para exercer sua função. Isso indica que a riqueza não está na quantidade de dados em si, mas na gestão capaz de organizá-los, e extrair descobertas que transformam a realidade das empresas.

O desafio quando se trata de dados é qualificar e cruzar informações criando padrões de cenários específicos para o benefício da empresa, a partir de uma grande massa de dados. Visto que a quantidade de dados é limitada apenas pela necessidade de cada pessoa no mundo, e levando em consideração que cada indivíduo possui diversas necessidades, pode se dizer por fim que a quantidade de dados existentes no mundo é infinita, portanto localizar aqueles dados que são de fato importantes para a empresa é a verdadeira razão pela qual existem tantos ramos e áreas de estudo envolvendo medidas e projetos referentes a captação de dados , soluções essas que desencadearam um problema extremamente grave para a sociedade deste século e dos séculos vindouros, problema este definido como a segurança de dados.

A privacidade da informação pode ser definida de várias maneiras. Enquanto Clarke (1999) afirma que “a privacidade é muitas vezes pensada como um direito moral ou um direito legal”, muitos pesquisadores sugeriram que a privacidade é a capacidade de controlar informações sobre si mesmo (Bélanger 2002).

Quais os limites de uma empresa para concluir seus objetivos e até onde ela iria para conseguir mais dados e consequentemente mais capital? As empresas de tecnologia que dependem de dados para sobreviver estão cada vez mais desesperadas para conse-

guir seu meio de sustento, seja ela da área social, empresarial ou contábil, os dados devem estar presentes na sua rotina de trabalho.

Porém os dados pessoais de uma pessoa não devem estar simplesmente abertos para qualquer indivíduo ou organização que os procure, os dados devem ser adquiridos de forma meticulosa e segura pois existe uma linha tênue entre a necessidade de acesso a dados pessoais para o negócio das empresas de tecnologia e as limitações impostas pela legislação.

Com a implementação da internet das coisas e do conceito de Big Data força que todos estejam totalmente conectados num mundo tecnologicamente avançado, onde compras e serviços estão hoje presentes num contexto onde é obrigatório a produção de dados, dados esses que são utilizados para a navegação da internet.

Isso causa uma falta de privacidade, forçando os usuários a terem sua intimidade exposta para os acessos de empresas prestadoras de serviços e produtos, o risco desses vazamentos prevê um problema na segurança da informação de não só cidadãos comuns, mas de diversos âmbitos privados e públicos criando uma brecha para quebra de vários serviços primários para a vida em sociedade.

No mundo inteiro tem-se ampliado golpes, numa evolução de mecanismos para subtrair de outras vantagens e privilégios. Incorporou-se ao cotidiano dos crimes presenciais e ataques físicos essa nova modalidade. Um novo empreendimento de uma facção sem rosto.

Roubo de dados como CPF, informações de contas bancárias, invasão de WhatsApp, Facebook, Instagram, entre outras redes sociais. E na missão de assegurar proteção e direitos, a segurança pública cria metodologias, demanda por políticas públicas e conscientização coletiva para alinhar o que é direito ao que é dever. Entre este e aquele, existe uma linha tênue que beira a proximidade e a desordem.

Para entender o risco e a gravidade dos problemas causados por fraquezas nos sistemas de segurança, é estudado por especialistas falhas que resultaram em grandes desastres na segurança de dados de empresas e órgãos públicos, são exemplos as seguintes falhas de segurança relatadas.

Em maio de 2011, um hacker conseguiu acessar o computador pessoal da atriz Carolina Dieckmann, acessando 36 fotos pessoais de cunho íntimo. De acordo com as fontes, o invasor exigiu R $10 mil para não publicar as fotos. A atriz recusou a exigência e acabou tendo suas fotos divulgadas na internet. Com esse acontecimento ocorreu uma

discussão popular sobre a criminalização desse tipo de prática, que ainda foi excessivamente fomentada pela mídia.

Em junho de 2012, o LinkedIn foi vítima de uma invasão que expôs os dados pessoais de mais de aproximadamente 117 milhões de usuários. Além de permitir o acesso às senhas, o vazamento expôs dados pessoais como endereço de e-mail e nome de usuários.

Em dezembro de 2020, mais de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ou como beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança do Ministério da Saúde. As informações incluem nome completo, CPF, endereço e telefone, elas deveriam estar protegidas por login e senha, porém havia uma vulnerabilidade no código da plataforma que permitia que qualquer usuário consultasse o banco de dados.

Em janeiro de 2021, a Autoridade Nacional de Proteção de Dados (ANPD) fez uma requisição para que a Polícia Federal iniciasse uma investigação para apurar o vazamento de dados de aproximadamente 223 milhões de brasileiros números esse maior que a população do país, pois esse vazamento incluiu dados de pessoas falecidas esse vazamento foi identificado pela empresa PSafe. O vazamento incluía nome completo, fotos, endereço, renda mensal e CPF, entre outras informações pessoais, essas até mesmo de pessoas mortas. Até hoje, não se sabe qual é a fonte das informações. A principal suspeita é que haja mais de uma fonte e que os dados tenham sido agregados durante anos.

Em janeiro de 2022, foi divulgado um incidente ao qual resultou no vazamento de dados que estavam vinculados a chaves PIX que estavam sob a guarda e a responsabilidade da empresa Acesso Soluções de Pagamento. Os dados de 160.147 chaves acabaram por ser expostos. As informações como nome completo, CPF, instituição, número da agência e conta foram expostas. O fato ocorreu entre 3 e 5 de dezembro de 2022. Apesar deste vazamento, uma nota do Banco Central confirmou que não foram expostos dados sensíveis, como senhas, extratos ou outras informações sob sigilo bancário.

Em dezembro de 2020, mais de 243 milhões de brasileiros cadastrados no Sistema Único de Saúde (SUS) ou como beneficiários de planos de saúde ficaram expostos na internet por falhas de segurança do Ministério da Saúde. As informações incluem nome completo, CPF, endereço e telefone, elas deveriam estar protegidas por login e senha, porém havia uma vulnerabilidade no código da plataforma que permitia que qualquer usuário consultasse o banco de dados.

Esses vazamentos são uns dos principais causadores de questionamentos sobre como a tecnologia deveria ser mantida sob estrito controle, visto que a segurança da informação não necessariamente é algo físico como um cadeado trancado, portanto, o cidadão comum entende que todo e qualquer meio tecnológico como frágil e não confiável. Essa discussão não é nova e vem se mantendo por um bom tempo, desde o grande marco da tecnologia da informação no começo deste século o medo e a insegurança para com a tecnologia se alastra na mente daqueles que a usam no seu dia a dia. E foi nesse contexto que surgiu as primeiras menções a criação de uma lei que proteja os dados que são usados nesses processos.

Segundo BELANGER (2011) A privacidade da informação refere-se ao desejo dos indivíduos de controlar ou ter alguma influência sobre os dados sobre si mesmos. Os avanços na tecnologia da informação levantaram preocupações sobre a privacidade da informação e seus impactos, e motivaram os pesquisadores de Sistemas de Informação a explorar questões de privacidade da informação, incluindo soluções técnicas para lidar com essas preocupações.

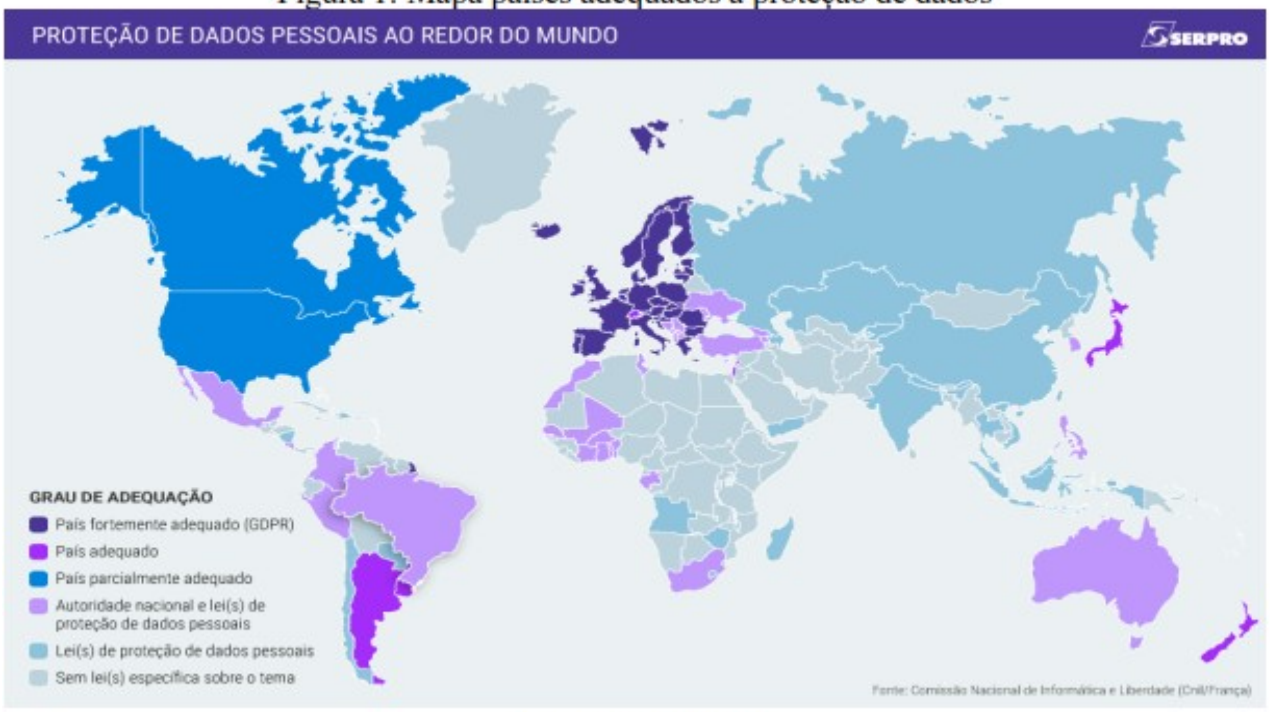
A General Data Protection Regulation, ou GDPR, foi criada para regular a proteção dos dados dos cidadãos de países da União Europeia, sendo idealizada no ano de 2012, mas liberada apenas em 2016. Com a implementação da lei em meados de 2018, iniciou-se a fiscalização em relação à GDPR em todos os tipos de empresas e organizações que armazenam e utilizam dados dos cidadãos europeus.

O regulamento foi criado graças a uma crescente exigência popular, as críticas e discussões foram causadas por insegurança para com informações como identidade, endereço, opiniões e características biológicas às organizações.

Visto a infinidade de conteúdos disponíveis, as empresas devem ser as responsáveis pela segurança dessas informações, para que as mesmas defendem esses dados de intrusos e elementos mal-intencionados. A GDPR aparece como uma proteção da população europeia, de maneira a garantir que a proteção de dados e a segurança sejam direi-

tos das pessoas.

Figura 1: Mapa países adequados a proteção de dados



Fonte: SERPRO (2020).

A legislação estabelece regras às organizações de diversos tipos e portes, Dessa forma a coleta, o processamento e o armazenamento dos dados são regulamentados, o que contribui para resguardar a privacidade dos cidadãos.

Com as transformações advindas da grande revolução tecnológica do início do século XXI, as grandes empresas atuantes em território brasilero tiveram suas grandes cargas de dados de milhares de clientes e usuários de seus serviços ampliadas exponencialmente. Estes dados possuem uma importância extrema para as empresas e portanto deve possuir e devida segurança, afinal tais informações são basicamente o que movimenta os serviços e a importância geral de uma sociedade que consome serviços tecnológicos.

“Inspirada na lei europeia de proteção de dados, conhecida como General Data Protection Regulation (GDPR), a Lei Geral de Proteção de Dados (LGPD) tem como objetivo proteger dados pessoais de pessoas naturais, ou seja, pessoas físicas.”(GARCIA; ROCHA; p.16, 2020)

Inicialmente, a lei foi sancionada com a *vacatio legis* de dezoito meses, entrando em vigor em fevereiro de 2020. Entretanto, com a revogação do artigo 65, dada pela lei n° 13.853, de julho de 2019, foi estabelecido novo prazo para que a LGPD entrasse em vigor, em agosto de 2020. Ocorre que o ano de 2020 vem sendo marcado por incertezas e preocupações, tanto para o governo, quanto para as demais entidades públicas e priva-

das, em decorrência da atual situação de pandemia que o mundo enfrenta.(MOTTA, p.24, 2020)

A nova lei prevê em seu teor 9 hipóteses que tornam legais os tratamentos de dados:

1) Consentimento

A primeira base legal disposta no artigo 7º da LGPD é o consentimento, sendo ele uma autorização expressa, livre, inequívoca, destacada e informada do titular para o tratamento de seus dados pessoais para uma finalidade determinada. Isso simplifica que, revogada a autorização, a sua empresa não poderá mais lidar com essas informações.

2) Cumprimento de Obrigação Legal ou Regulatória pelo Controlador

Definida como o cumprimento de obrigação legal ou regulatória pelo gestor, quando a empresa precisa da informação para cumprir alguma lei ou norma, o dado pode ser usado para esse fim, independentemente de consentimento do titular.

3) Execução de Contrato

Se o dado pessoal for necessário para que a empresa possa executar o contrato ou procedimentos preliminares relacionados ao contrato do qual seja parte o titular, a pedido do titular dos dados, o tratamento também é permitido pela LGPD.

4) Exercício de Direitos em Processos

A LGPD também prevê a possibilidade de as empresas utilizarem dados pessoais para o exercício regular de direitos em processos judiciais, administrativos ou arbitrários.

5) Interesses Legítimos do Controlador ou de Terceiro

O tratamento de dados pessoais pode se realizar quando necessário para atender aos interesses legítimos do Gestor ou de terceiros, exceto no caso de prevalecer em direitos e liberdades fundamentais do titular que exijam a proteção das informações.

6) Proteção da Vida ou da Incolumidade Física

A LGPD também permite o trabalho de dados pessoais que tenham como objetivo proteger a vida ou a incolumidade física do titular dos dados ou de terceiros.

7) Tutela da Saúde

Essa permissão prevê que as informações pessoais podem ser trabalhadas exclusivamente em procedimentos realizados por profissionais de saúde, serviços de saúde ou autoridades sanitárias.

8) Proteção ao Crédito

A Lei Geral de Proteção de Dados propõe que os dados pessoais podem ser tratados nos casos em que o objetivo for a proteção do crédito, contanto que as regras deste tema sejam seguidas.

9) Demais Bases Legais

Mesmo que as outras 8 situações desta lei sejam as mais utilizadas, existem outras 2 (duas) hipóteses que também permitem o tratamento dos dados sendo elas:

• Execução de Políticas Públicas: Administração Pública pode realizar o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em lei ou respaldadas em contratos, convênios ou instrumentos congêneres;

• Estudos por Órgão de Pesquisa: Órgãos de pesquisa podem realizar estudos, garantindo, sempre que possível, a anonimização dos dados pessoais.

As análises de estudiosos e especialistas da área comprovam que as leis de proteção de dados são extremamente essenciais para que vazamentos e ataques a informações privadas sejam evitados, e evidenciando como um determinado vazamento de dados pode afetar uma empresa ou uma pessoa individual, como, por exemplo, uma perda de dados bancários ou possíveis invasores externos tomam conhecimento de senhas e de números que um cliente possui, e por meio destes realiza operações visando próprio sem a ciência do cliente detentor dos dados.

“Em uma sociedade da informação e do conhecimento os dados são coletados, processados e, em seguida, seus resultados são aplicados em ambientes específicos do mundo real. Essa informação, considerada por muitos autores como o principal patrimônio de uma organização, está sujeita a problemas com relação à Segurança da Informação, dentre eles, o acesso não autorizado.”(SANTANA; DUARTE, 2021)

É de ciência geral que vazamento de informações é um fenômeno que nenhum indivíduo quer que ocorra, pois os danos podem ser avassaladores. A única forma de proteger tais informações é com políticas de proteção equivalentes à gravidade de um possível vazamento, portanto empresas devem possuir níveis de segurança altos e atuais para suas bases de dados.

Boas práticas de segurança de dados são recomendados há mais de 20 anos, porém como não era uma exigência, mas apenas uma recomendação, poucas empresas faziam uso dessas recomendações, afinal isso envolve custos com pessoal, tecnologia (POHLMANN, 2020). Apenas com a chegada de novos avanços na tecnologia onde as pessoas começaram a efetuar todo o tipo de ação por meio tecnológicos as preocupações para com a segurança tiveram a devida atenção, pois a credibilidade de meios virtuais foi colocada à prova com a grande massa de pessoas utilizando dos mesmos para efetuar ações do cotidiano.

E agora estamos numa transição muito importante da LGPD que é como ela está sendo efetivada na atualidade, agora que sua importância está de fato colocada à prova como ela está mudando as organizações e suas visões com a segurança de dados.

A LGPD forçou então, as empresas a mudarem os métodos que fornecem a elas os dados que as mesmas precisavam para sua prestação de serviços se tornando um critério importante para as empresas, os primeiros resultados começaram a aparecer, e com eles a LGPD começou a apresentar seus efeitos. Muitas empresas e organizações que tiveram experiências com a lei afirmaram que ela é efetiva e demonstra para todos os colaboradores como deve ser tratado as informações dos usuários de forma correta.

Apesar da efetividade da lei, ela é um assunto recente para a maioria das empresas, ou seja, por mais que seja um tema importante, muitas delas têm receios para mudar suas táticas e protocolos.

“Considerando que a LGPD entrou em vigor recentemente, empresas de diferentes setores e órgãos públicos ainda estão enfrentando desafios para adequarem seus sistemas de software em conformidade com a legislação vigente. Garantir a conformidade legal visa evitar sanções administrativas sejam aplicadas pela autoridade nacional de proteção de dados.” (ALVES; NEVES, 2021)

A área de marketing é a que mais sofre com as limitações da LGDP visto que muitas das formas de se conectar com os ditos novos clientes são barradas pela LGPD, principalmente quanto às ações no mundo digital. Uma empresa voltada para tecnologia da informação deve tomar muito cuidado para caminhar de acordo com a lei e realizar apenas operações legais, que também inclui a área de marketing digital.

Transformar os bancos de dados em ambientes mais seguros, por exemplo, é uma das atribuições de uma empresa de TI. Os usuários da internet, estão sob proteção da lei, e qualquer vazamento de dados é responsabilidade da empresa portadora dessas informações. Conseguir recuperar os dados coletados e/ou excluí-los quando necessário são ações fundamentais da TI, quando falamos em LGPD.

Algumas das ações que colocam as empresas dentro da legalidade, usando as normas da LGPD:

- Adaptar os canais de comunicação com os clientes, ainda mais aqueles que coletam quaisquer tipo de informações.
- Ter certeza de que todos os dados coletados foram autorizados pelos donos originais.

- Desenvolver métodos de gerenciamento de pedidos dos donos dos dados. Isso facilita na hora de atender a todos, quando necessário.
- Criar um plano de segurança da informação objetivando a proteção de dados pessoais.

Uma das grandes ferramentas de obtenção de dados é a utilização de arquivos criados pelos sites que você visita, os chamados cookies. Criados para facilitar sua experiência on-line salvando dados de navegação.

As organizações normalmente mostram conformidade sobre os cookies, observando se eles cumprem com os requisitos da LGPD, dentre eles o consentimento livre, claro e transparente com as configurações do navegador, medições de audiência e rastreadores.

A lei é uma oportunidade para os profissionais que já estavam realizando esse trabalho de forma padrão dentro das empresas, porque vão ser extremamente valorizados, quanto para os prestadores de serviço que não trabalham em uma empresa específica e vão ter uma demanda muito maior.

E é nesse contexto que as empresas de tecnologia da informação do Distrito Federal se destacam perante as aplicações da LGPD, proporcionando uma grande quantidade de serviços e produtos relacionados à segurança da informação. Algumas empresas se especializaram em criar soluções e produtos. A Segurança da informação, se fundamenta em 3 bases de atuação: a confidencialidade, integridade e disponibilidade. A confidencialidade é a garantia de que a informação esteja disponível apenas para pessoas autorizadas.

“A integridade assegura que os dados estejam em sua integridade e totalidade durante todo o seu ciclo de vida. A disponibilidade garante que os dados estejam disponíveis a qualquer momento, sem interrupções” (STALLINGS, 2015).

“Uma política de segurança é padronizada como um conjunto de normas e diretrizes baseadas em técnicas como a ISO/IEC 2005, ao qual uma instituição deve seguir para garantia e segurança de seus recursos e informações” (VARGAS, 2020).

A segurança da informação precisa determinar o que pode ser feito com as informações, padrões, entradas de informação, verificações de acesso de informações, acessos internos ou externos, meios para fazer a transmissão e acesso de informações vitais. A política deve padronizar os detalhes e requisitos de seu respectivo mecanismo, para que uma política de segurança possa ser efetiva em uma empresa ela precisa de ter o su-

porte de todas as áreas envolvidas na empresa, a implementação de uma política de segurança força uma grande mudança cultural na empresa se tornando essencial que tenha uma preparação com todos os colaboradores, ou seja, todos devem ser integrados nas novas políticas através de reuniões, treinamentos e comunicados.

De acordo com o artigo 48 da Lei nº 13.709/18 (Lei Geral de Proteção de Dados), o controlador tem o dever de comunicar à autoridade nacional e ao titular qualquer incidente de segurança que possa acarretar risco aos titulares, devendo ser feita em prazo razoável.

A cultura de uma organização é moldada com base em um sistema de regras e criações próprias de mecanismos de segurança, sendo que a maioria das empresas do Distrito Federal tendem a se portar de forma mais consciente para com seus conceitos de privacidade e segurança pois está localizada no centro de uma nação e também por ser responsável por grande parte da gestão nacional tanto em âmbito gerencial quanto político. As empresas sediadas no Distrito Federal sofreram após a implementação da LGPD, tiveram duas opções de inovação do uso da lei, a primeira e mudar os conceitos culturais da empresa, criando métodos para lidar com as novas tecnologias, ou seja, novos conceitos, novas normas, novos sistemas de segurança como biometria, senhas rotatórias, domínios para acesso de funcionários, cuidados com clientes e usuários que possam ter acesso às informações vitais da empresa, dentre outros modos de lidar com a proteção dos dados. A segunda forma é terceirizar o sistema de proteção da sua organização, requisitando uma prestadora de serviços especializada em soluções LGDP como por exemplo, a criação de software específico para a proteção dos dados de pequenas e grandes empresas, essas soluções carregam os conceitos de privacidade e segurança em cada linha de código, fornecendo ao cliente uma série de ferramentas responsáveis pela proteção de informações vitais da empresa, algumas dessas funcionalidades incluem, proteções contra invasões, ransomwares, evita o roubo de informações, protege contra ataques de hackers e impede o vazamento de dados.

“É recomendado a revisão jurídica e atualização das cláusulas de contratos com parceiros e fornecedores que realizam algum tipo de tratamento de dados, principalmente fornecedores de soluções em nuvem, e-mail marketing e mídias sociais, a responsabilidade por qualquer infração ou incidente de vazamento de dados será do controlador e operador. Muitas empresas não possuem uma estrutura para efetuar uma revisão, nesses casos a contratação de uma empresa de consultoria jurídica poderá auxiliar nesse processo.” (LIMA; 2020)

Durante o desenvolvimento do trabalho foi evidenciado a importância de uma política de segurança com os mais diversos tipos de profissionais para que se possa garantir a segurança dos dados, além da equipe ter conhecimentos sobre a LGPD. A complexidade da implantação de novos padrões em organizações que já possuem uma cultura rígida por parte de seus colaboradores pode dificultar a adesão. Ao longo da análise foi identificado a necessidade da revisão constante dos processos internos e externos da empresa, e em alguns casos será necessário ajustes simples, em outros casos ajustes de grande impacto. Empresas que já possuem boas práticas de governança implantadas em seus processos, têm menor impacto com a agregação da lei e portanto facilita as novas regras e mudanças do cotidiano. A colaboração de todos os funcionários e integração dos setores da empresa poderá diminuir a dificuldade dessa viabilização. A nomeação de um encarregado de proteção de dados é uma boa forma de facilitar o processo de implementação da LGPD, investimento em cursos de capacitação, certificações serão essenciais para que o mesmo seja efetivo e confiável em seu trabalho.

Como resultado do trabalho efetuado, foi mapeado o conjunto de informações e dados da LGPD que propõe soluções para auxiliar empresas, evidenciar situações de risco, descrever propostas de melhorias e informar estudantes e profissionais das características específicas da implementação da LGPD. Foi definido quais as limitações e quais são suas falhas, foi evidenciado causas para quebras de segurança e análises propostas de softwares voltados para criação de normas ou sistemas que visam aplicar conceitos da lei, foi demonstrado como as empresas no Distrito Federal lidam com todas essas afirmações e de que forma elas podem ser influenciadas pelos conceitos abordados.

É viável para uma organização que não possui uma estrutura organizacional edificada com as normas padrões da LGPD requisitar serviços externos para auxiliar na implementação de processos de segurança na empresa. Portanto a LGPD passou de uma lei de segurança para um conceito presente constantemente no mercado de tecnologia, ou seja, toda e qualquer empresa utilizadora de dados deve estar de acordo com os padrões especificados pela legislação, e uma empresa que atua fora dessas normas corre o risco de ser alvo de quebras de segurança, ou mesmo ser cassada pela justiça, por estar fora das normas estabelecidas em lei.

CONSIDERAÇÕES FINAIS

Dados possuem uma importância extrema para as empresas e com isso a segurança se tornou um dos maiores problemas quando se pensa em meios tecnológicos e como

proteger os dados, a segurança deve ser sempre prioridade para empresas que usam de tecnologia como meio principal de renda, deve existir o respeito a integridade daqueles que são os alvos das empresas. Desta forma a LGPD aborda todo tipo de método usado para tratar os dados e também aponta suas exceções.

Quando aplicada em empresas de tecnologia da informação, a lei geral de proteção de dados atua como um padrão tanto para segurança da empresa, como para proteção dos dados de clientes e usuários que têm relações com os serviços e produtos da organização. A LGPD propõe uma forma de adaptar os costumes da empresa para uma realidade corporativa onde os dados, mesmo sendo o recurso mais importante da empresa, deve ser tratado como mais sensível. As empresas do Distrito Federal obtiveram êxito na implementação e na utilização da lei de forma correta e objetiva, mostrando inclusive novas soluções para questões de segurança, colocando no mercado soluções, serviços e produtos relacionados à LGPD.

O matemático londrino Clive Humby, discursou uma frase que mostra a real importância dos países adotarem leis de proteção de dados: “data is the a new oil”, ou seja, dados são o novo petróleo. A atualidade é um ciclo vicioso de venda de dados pessoais, onde bancos de dados de empresas valem muito dinheiro. A lei tem o objetivo de padronizar essa prática, que coloca em risco a privacidade das pessoas.

Neste projeto, tentamos apresentar os principais pontos da Lei Geral de Proteção de Dados, e seus impactos na relação entre relações de tratamento de dados pessoais e todos aqueles que coletam e usam de alguma forma esses dados. A lei foi redigida de forma brilhante, e mesmo com alguns pontos controversos, o impacto inicial com a efetivação da lei em âmbito comercial foi tratado com muito cuidado perante os dados pessoais por aqueles que coletam e tratam esses dados.

REFERÊNCIAS

BÉLANGER, France. CROSSIER, Robert E. **Privacy in the digital age: a review of information privacy research in information systems**. MIS Quarterly, vol 35. 2011.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018, dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet)

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas (UNIFAFIBE)**, v. 8, n. 2, p. 197-231, 2020.

CARVALHO, Luiz et al. Desafios de Transparência pela Lei Geral de Proteção de Dados Pessoais.In: Anais do VII Workshop de Transparência em Sistemas.SBC, 2019. p. 21-30

CLARKE, Roger. Internet privacy concerns confirm the case for intervention. **Communications of the ACM**, v. 42, n. 2, p. 60-67, 1999..

DELOITTE. 2007. “Enterprise@Risk: 2007 Privacy & Data Protection Survey,” http://www.deloitte.-com/dtt/cda/doc/content/us_risk_s%26P_2007%20Privacy10Dec2007final.pdf; recuperado em 16 de janeiro de 2008.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD): guia de implantação**. Editora Blucher, 2020.

MADDEN, Mary; SMITH, Aaron W.; VITAK, **Jessica. Digital footprints**: Online identity management and search in the age of transparency. 2007.

MENDES, Michele da Mota. **A Nova Lei Geral de Proteção de Dados Pessoais: Principais Aplicações da Lei sob a ótica da Ciência da Informação nas Organizações no Brasil**. 2020. Trabalho de Conclusão de Curso.

LIMA, Victtor Henrique. LGPD **Análise dos impactos da implementação em ambientes corporativos**: Estudo de caso. 2020.

RAMOS, Pedro. A regulação de proteção de dados e seu impacto para a publicidade online: um guia para a LGPD. **Publicado em**, v. 16, n. 07, p. 17, 2019.

ALCÂNTARA, CLAYTON DEODORO GONÇALVES DE. Impactos da Lei Geral de Proteção de Dados nas relações de trabalho. 2021.

FERNANDES, Leticia Queiroz. IMPACTOS DA LGPD NAS EMPRESAS. In: **ENGENHARIAS, EXATAS E TECNOLOGIAS**. 2021.

PACHECO, Juliana. A proteção de dados pessoais amparada pela LGPD: **um estudo sobre os impactos causados no marketing digital**. 2022.

ALMEIDA, Siderly do Carmo Dahle de; SOARES, Tania Aparecida. Os impactos da Lei Geral de Proteção de Dados-LGPD no cenário digital. **Perspectivas em Ciência da Informação**, v. 27, p. 26-45, 2022.

DA ROCHA MAGRI, Marli. LEI GERAL DE PROTEÇÃO DE DADOS: PRINCIPAIS ASPECTOS E IMPACTOS DE SUA VIGÊNCIA. **Anais UniCathedral-Eventos**, n. 1, 2020.