IMPACTOS DA LGPD NA TECNOLOGIA DA INFORMAÇÃO: DESAFIOS PARA OS PROFISSIONAIS DA ÁREA

IMPACTS OF LGPD ON INFORMATION TECHNOLOGY: CHALLENGES FOR PROFESSIONALS IN THE AREA

Ana Rita Akayama Kanagusku[1], Fatec Americana, ana.kanagusku@fatec.sp.gov.br
Marcus Vinícius Lahr[2], Fatec Americana, marcus.lahr@fatec.sp.gov.br

Resumo

O presente estudo investiga os grandes entraves que a LGPD traz para os profissionais da área de TI, por ser um projeto de privacidade, para que ocorra "*compliance*", muito mais que questões estruturais, demanda um trabalho de mudança cultural. O desafio maior para os profissionais da área é conciliar todas as questões humanas e de infraestrutura, para traçar um plano de ação que defina as prioridades para melhoria da gestão dos dados e ser capaz de criar uma boa cultura de governança, que vá além das soluções tecnológicas e implemente uma cultura de valorização das informações. A título de embasamento dos assuntos abordados, adotou-se uma combinação da metodologia de pesquisa bibliográfica com a pesquisa de campo. Um ponto relevante na análise dos resultados encontrados indica que para o processo de adequação à lei ser bem-sucedido, é primordial os profissionais da área de TI estarem solidamente preparados e muito bem inteirados do assunto.

Palavras-chave: LGPD, privacidade, governança.

Abstract

This study investigates the major obstacles that LGPD brings to IT professionals, as it is a privacy project, so that compliance occurs, much more than structural issues, it demands a work of cultural change. The biggest challenge for professionals in the area is to reconcile all human and infrastructure issues, to draw up an action plan that defines priorities for improving data management and being able to create a good culture of governance that goes beyond solutions technologies and implement a culture of valuing information. As a basis for the topics discussed, a combination of bibliographic research methodology with field research was adopted in this academic article. A relevant point in the analysis of the results found is that, in order to be successful in this process of compliance with the law, it is essential that professionals in the IT area are solidly prepared and very knowledgeable about the subject.

Keywords*: LGPD, privacy, governance.*

1. Introdução

A LGPD[3] traz uma demanda adicional aos responsáveis por tratamento de dados pessoais, a busca pela identificação de lacunas de segurança da informação e de privacidade foram intensificadas, havendo necessidade de melhorar as ferramentas existentes. Os controles para atendimento dos pilares de confidencialidade, integridade e disponibilidade precisam ser aprimorados para que haja uma diminuição dos riscos de segurança.

Além de uma boa infraestrutura de proteção de dados, outra vertente que requer atenção redobrada é o fator humano, em nossa era digital as informações estão cada vez mais valiosas e os riscos de vazamento aumentam em escala exponencial, porém, não existe uma cultura sedimentada de valorização das informações.

Nesse sentido, urge a conscientização dos colaboradores para um entendimento da importância dos dados e a responsabilidade necessária para tratar as informações. O processo de mudança inicia com treinamentos, campanhas, promover uma revisão e mapeamento dos processos, políticas de privacidade e segurança, contratos com terceiros, etc. É necessário um trabalho educativo de conscientização sobre como tratar informações pessoais de terceiros, uma boa prática é a promoção de palestras, cursos, elaboração de informativos, cartilhas e normas de tratamento de dados pessoais para que todos os colaboradores consigam cumprir o que a legislação exige.

A lei enfatiza o quesito transparência no tratamento dos dados, sendo assim, o papel da TI[4] é auxiliar a organização no entendimento dos dados em todo o processo: coleta, acesso, produção, classificação, utilização, controle, transmissão, distribuição, arquivamento, armazenamento, eliminação, reprodução, processamento, modificação e avaliação estão entre os principais tipos de tratativas.

Assim, o objeto do presente estudo é investigar os impactos que as diretrizes da Lei Geral de Proteção de Dados trazem para os profissionais de TI e como as mudanças por ela acarretadas serão processadas, de que maneira os desafios serão superados.

2. Referencial Teórico

Esta seção tem como objetivo apresentar o referencial teórico da pesquisa, fundamentar o conceito de privacidade e proteção de dados, contemplar os principais desafios da TI para atendimento à LGPD e as possíveis ferramentas que poderão ser utilizadas para adequação à referida lei.

2.1 Privacidade e Proteção de Dados

O sentido da palavra privacidade é muito abrangente e tem evoluído ao longo do tempo, as definições que encontram mais consenso são: algo restrito a poucos, sigiloso, protegido, confidencial ou íntimo, algo que se opõe ao público. Conforme afirma Zanini (2018, p. 58): “Depois da Revolução Francesa, quando os valores, a mentalidade e os costumes burgueses passaram paulatinamente a preponderar, dando espaço a um novo sistema de referência, que tinha a vida privada, a intimidade e o recato como fundamentos”.

Segundo Garcel, Moro, Souza Neto, Hippertt (2020, p. 05):

“O Direito à Privacidade é direito humano fundamental que proíbe a interferência do Estado na

vida privada, exceto nas hipóteses previstas em lei; envolve a inviolabilidade da intimidade, vida privada, honra, imagem, casa e do sigilo das telecomunicações".

O tema privacidade nunca esteve tão presente quanto nos dias atuais, é verdade também que nunca antes o mundo esteve tão conectado como agora, independentemente até de classe social e localidade. Como consequência, surgiu a necessidade de criação de leis e diretrizes para regulamentar o uso de todas essas informações disponibilizadas com tanta facilidade, um movimento reivindicando boas práticas para seu manuseio, começou timidamente na Alemanha na década de 1970, porém, só passou a ganhar força neste século, culminando no ano de 2012 com a idealização da "*General Data Protection Regulation*" (GDPR), ou Regulamento Geral de Proteção de Dados, porém, somente entrou em vigor em 2018. Trata-se de um conjunto de leis e regulamentos sobre a proteção de dados na União Europeia, na qual se inspirou a LGPD do Brasil.

No Brasil, a LGPD entrou em vigor em 18 de setembro de 2020, desde então passou a pertencer ao grupo de países que contam com uma legislação específica para a proteção de dados dos seus cidadãos. O cenário do século XXI apresenta inúmeros casos de uso indevido, comercialização e vazamento de dados; as regras da referida lei além de garantir a privacidade dos brasileiros, traz credibilidade para as relações comerciais com outros países.

O título deste tópico é "Privacidade e proteção de dados", qual é a relação entre eles? Pode-se dizer que estão intimamente interligados e fazem parte do mesmo assunto, um influenciando diretamente o outro.

Em um quadro comparativo para melhor entendimento, a privacidade é referente a tudo que diz respeito à vida particular de cada indivíduo. Já os dados, quando representam informações de uma pessoa, podem ser de caráter privado ou público. Porém, os dados que estão disponíveis na internet, grande parte é considerada de caráter público, mesmo assim, não está garantido o direito de livre uso dessas informações.

Analisando do ponto de vista da LGPD, de acordo com *"Privacy Tech"* (2022), o sigilo da informação é privado, mas os dados são públicos. A palavra de ordem é consentimento, pode ser dado o acesso à informação, desde que seja garantido que o seu tratamento (coleta, processamento e armazenamento), seguirá as regras ditadas na lei. Existe, portanto, uma obrigação de prestar contas sobre as práticas que estabelecem as normas de segurança e mitigação dos riscos que envolvem as informações pessoais de terceiros.

Segundo Carvalho e Pedrini (2019), não há como negar que essa era de tecnologia facilitou a vida dos seres humanos, é visível o quanto a sociedade modificou-se em razão das constantes modernizações trazidas pelo momento tecnológico vivenciado. Os celulares, computadores e muitos outros dispositivos eletrônicos com acesso à internet fazem com que informações em massa sejam processadas, os dados podem atingir escalas altíssimas em sua produção e alcance. Também, pode-se considerar que as pessoas estão vivendo uma era comunicacional, há busca maciça por notícias e o desejo de estar informado. Percebe-se que os instrumentos tecnológicos podem potencializar formação de conhecimento e disseminação de informações.

Quando se fala em conhecimento, constata-se que a Internet e seus produtos podem minimizar obstáculos do tempo e do espaço, proporcionando que o objeto envolvido alcance imediatamente um número bem expressivo de usuários. Já quando se fala em uma propagação

de informações, visualiza-se o espaço democrático em que estas são criadas e depois exibidas inúmeras vezes, sendo viralizadas em redes sociais, em que muitos podem acessar pelo próprio celular e até criar conteúdo a partir deste.

No entanto, essas facilidades de acesso que a Internet propicia, afloram por outro lado, um debate relacionado à vulnerabilidade dos dados disponibilizados.

Nesse sentido, Silva e Silva afirmam que

> Mas ao lado desse panorama de otimismo e de novas oportunidades também se revelam inéditos problemas e desafios decorrentes do grande fluxo informacional, especialmente quando as informações assumem a forma de dados pessoais e saem do controle do seu titular. Essa situação de vulnerabilidade tanto pode ocorrer quando os dados são espontaneamente disponibilizados nas interações sociais, como ocorre com publicações feitas em sites de redes sociais; nos casos em que são recolhidos pelo fornecedor para permitir a abertura de contas que garantirão o acesso a serviços e produtos ou nas situações de captura indevida por meio de algum programa espião. A pluralidade de formas de recolhimento de informações demonstra a complexidade do tema, pois mesmo o internauta mais cauteloso e com seletivas atuações no ambiente virtual não fica a salvo de sofrer ataques aos seus dados pessoais (SILVA; SILVA, 2013, p. 2).

Uma lei que trata a questão de proteção de dados objetiva justamente equilibrar essa dicotomia de poder sobre as informações pessoais, ocorrida entre o titular dos dados pessoais e todo aquele que faça uso deles. O estabelecimento de padrões mínimos a serem seguidos, visa assegurar os direitos fundamentais de liberdade e de privacidade de cada indivíduo.

2.2 Desafios da TI para Atendimento à LGPD

Segundo o Guia de Boas Práticas – Lei Geral de Proteção de Dados (ANPD, 2020), a privacidade deve ser um padrão dos sistemas de TI, sem sombra de dúvida a LGPD é uma lei que vai afetar muitos processos dentro das empresas e a equipe de TI necessita saber como e quando agir nas situações em que for acionada.

Cabe salientar que para o projeto de adequação à lei ter êxito, os departamentos de TI e jurídico devem trabalhar concomitantemente. Além disso, pelo fato da TI ser responsável pelas tecnologias utilizadas nas empresas, é preciso também uma aproximação mais apurada com as outras áreas para um maior embasamento no monitoramento de utilização das tecnologias disponibilizadas.

Pode-se afirmar que o primeiro desafio da TI é entender a LGPD, é extremamente necessário compreender os princípios, bases legais, como a lei funciona na prática e seus principais pontos relevantes, pois de outra forma, como a equipe será capaz de realizar todos os ajustes necessários para que as ferramentas e tecnologias estejam em conformidade com a lei?

O caminho para a capacitação é bastante extenso, envolve desde o nível de conscientização e de treinamento sobre os assuntos de privacidade e proteção de dados até o entendimento de quanto uma organização está apta a atender os requisitos regulatórios.

Assim sendo, uma avaliação de riscos minuciosa pode ser uma boa prática para o êxito nessa jornada, como é possível observar na figura 1.

Figura 1 - Guia de Avaliação de Riscos de Segurança e Privacidade

Fonte: ANPD, 2020

Na sequência de desafios, a compreensão do fluxo dos dados certamente está entre os principais que a LGPD traz para os profissionais de TI, é essencial o suporte da TI para que todos os departamentos de uma empresa entendam como os dados são coletados, armazenados, processados, desde a concepção até o descarte. A responsabilidade pelo mapeamento de dados precisa ser dividida entre as diferentes áreas.

Mais um impasse são os mecanismos de proteção, porque a referida lei, no artigo 6°, incisos VII e VIII, cita textualmente que deverão ser feitos investimentos em soluções de cibersegurança: "VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;" (LGPD, 2018).

Por isso, a equipe de TI precisa estar atenta a soluções que atendam ao mesmo tempo a lei e as demandas da empresa, focando em minimizar riscos e incidentes, prevenção de vazamento de dados e ataques cibernéticos.

Outra questão que entra para o ranking dos desafios é o investimento em armazenamento de dados, já que a lei exige garantias de segurança e privacidade das informações, por isso, é preciso ter em mente a obrigação em dispor de um ambiente de armazenamento e backup seguro, que ao mesmo tempo seja flexível para se adequar ao crescimento da empresa.

Ainda no quesito armazenamento, as tecnologias em nuvem tornaram-se praticamente indispensáveis, pela rapidez, facilidade de gerenciamento e diminuição de custos. Em contrapartida, é preciso um cuidado redobrado com a segurança e disponibilidade dos dados, por isso, é de suma importância que o provedor de serviços seja escolhido de forma muito criteriosa.

No rol dos desafios não poderia deixar de ser citado o Plano de Recuperação de Desastres - PDR[5], que se trata de um plano de ação para restabelecer processos, dados e sistemas todas as vezes que ocorra um desastre, podendo ser voluntário ("*crackers*"[6], incendiários etc.),

involuntário (acidentes, falta de energia etc.) ou natural (terremotos, enchentes, incêndios naturais etc.). O objetivo é restaurar no menor tempo possível os serviços de TI que sustentam os processos críticos do negócio.

A norma NIST SP 800-37 (2018), descreve o PRD como um plano de informação do sistema com foco projetado para restaurar a funcionalidade de um sistema, aplicação ou infraestrutura de instalação de computadores em um site alternativo após uma emergência, e complementa informando que se aplica a grandes rupturas, geralmente físicas, para os serviços que negam o acesso a infraestrutura de instalação principal para um período prolongado.

Portanto, para a obtenção de sucesso em um PRD contempla o desenvolvimento de uma documentação que englobe ações muito bem planejadas a serem adotadas antes, durante e após um desastre.

2.3 Ferramentas e Soluções para Adequação à LGPD

Uma vez enumerados os desafios que a LGPD traz aos profissionais da área de TI, independentemente do porte da empresa, existem ferramentas que realmente farão a diferença em uma adequação aos requisitos da lei.

2.3.1 Plano de Segurança da Informação

É possível afirmar que nos dias de hoje a informação é um ativo de grande valor, pode-se dizer até que está entre os principais patrimônios de qualquer empresa, gerando uma necessidade de controles de segurança da informação para a sua proteção.

A informação possui um grande valor e é considerada um dos principais patrimônios para as empresas, por este motivo, é de suma importância que seja estabelecido controles de Segurança da Informação para protegê-la de possíveis ameaças.

Nesse contexto, é preciso que haja parâmetros de proteção que estejam de acordo com a importância que a informação tem para a empresa, uma classificação. A realidade da maioria das empresas, principalmente as de pequeno e médio porte, é a dificuldade na definição do "dono" da informação, ou seja, o responsável por sua classificação, o que dificulta a implementação de programas relacionados à segurança da informação.

Uma grande parte das organizações utiliza a seguinte classificação:

- Confidencial: mais alto nível de proteção;
- Interna: ativos que podem ser compartilhados em áreas internas da empresa;
- Pública: acesso liberado a qualquer pessoa.

E o que ocorre quando uma informação não é classificada? Existe a possibilidade de ser considerada pública e não retratar o seu grau real de criticidade.

A família de normas ISO/IEC 27000 se apresenta como excelente suporte para elaboração de um planejamento de segurança de informação, com destaque para a norma ISO/IEC 27001 que é a principal norma utilizada como base para organizações obterem a certificação em gestão de segurança de informação, por definir os requisitos do Sistema de Gestão de Segurança da Informação (SGSI). É uma boa prática associá-la a outras duas normas: ISO/IEC 27002 (código de práticas com um conjunto completo de controles) e ISO/IEC 27005 (gestão de riscos de segurança da informação). A partir do entendimento dessas normas, é possível estabelecer regras com clareza e objetividade, definição de ações e responsabilidades

na tratativa de dados e informações. Como consequência, virão as regras de proteção em todos os processos e tecnologias que façam parte da rotina da organização, de maneira que se tornem um padrão a ser seguido e respeitado por todas as partes interessadas[7].

A norma ISO/IEC 27001 (ABNT, 2013) possui diversos requisitos referentes à proteção de dados pessoais, que podem ser usados para fundamentar a conformidade com a LGPD, com destaque para: a pseudonimização e criptografia de dados pessoais, o controle de acesso com nível de privilégio preestabelecido, e ainda, a exigência de prevenir a exploração de vulnerabilidades técnicas.

2.3.2 Política de Senhas Complexas e Autenticação em Múltiplos Fatores (MFA)

A rotina de um usuário corporativo é cercada de várias contas e acessos a dados, o caminho mais fácil costuma ser colocar algo fácil de lembrar, o que fragiliza a segurança e coloca em risco toda a rede da organização.

A identificação é o processo pelo qual um requerente afirma possuir uma determinada identidade perante uma entidade. A autenticação de entidades se refere ao processo pelo qual o requerente prova sua identidade através de uma verificação feita pela entidade (OPPLIGER, 2012).

Uma das invasões mais comuns é o chamado "ataque por força bruta", o método utilizado pelos "*crackers"* é o de tentativa e erro, que pode ser feito manual ou automaticamente. As senhas simples podem ser "quebradas" em questão de poucos minutos.

É extremamente importante que as empresas adotem uma política de "senhas fortes", para impedir esse tipo de ataque e limitar outras tentativas de invasão, além disso, para um acréscimo de segurança, é recomendável a autenticação em múltiplos fatores.

A autenticação em múltiplos fatores é programada para exigir informações de verificação adicionais, visando elevar o nível de proteção dos sistemas, é uma maneira de confirmar a identidade de quem está tentando entrar. A metodologia é baseada em três tipos de informações adicionais:

• Algo que você sabe: conhecimento de uma senha ou um PIN memorizado;

• Algo que você tem: coisas que o usuário possui, como um crachá, chave USB segura ou smartphone;

• Algo que você é: aspectos que provam quem é o usuário, como biometria (impressão digital, reconhecimento facial, digitalização de voz, retina, íris, entre outros).

Cada vez mais as empresas precisarão dar uma maior atenção à gestão de cadastros e senhas, conscientizando os usuários e demonstrando a sua importância no combate aos ataques cibernéticos.

2.3.3 Proteção dos "*Endpoints"* [8]

A proteção de "*endpoints"* é caracterizada por atividades que visam assegurar que os dispositivos estejam protegidos contra ciberataques, contempla medidas de atualização constante dos serviços de segurança e sistemas operacionais, de maneira que sejam detectados malwares, infiltrações e outros programas maliciosos.

Conforme descreve Nakamura & Geus (2014), na proteção de um sistema inicialmente é preciso relacionar todos os recursos que podem estar suscetíveis a algum risco: o que é

necessário proteger, os recursos mais importantes e de que forma as informações estão armazenadas. Seguindo esse princípio, os "*endpoints"* necessitam de uma atenção especial.

As ferramentas que são especializadas em segurança dos "*endpoints"* proporcionam a prevenção de invasões em computadores, servidores e outros dispositivos conectados à rede de uma organização.

Quando utilizadas junto ao firewall, possibilitam o monitoramento de atividades em tempo real e mantêm os gestores informados sobre qualquer evento suspeito que possa se tornar uma vulnerabilidade.

2.3.4 Segurança Física dos Data Centers e Segurança na Nuvem

A segurança física também é muito importante e a proteção do Data Center contra invasões necessita de investimentos como controle de acesso somente para pessoas autorizadas, sistema de vigilância com câmeras, proteção contra incêndios, curtos-circuitos, inundações, entre outros.

Um relatório desenvolvido recentemente pelo "*Uptime Institute Intelligence"* (ASCIERTO, R., & TRAVER, T., 2021) destacou aspectos considerados fundamentais para blindar um Data Center: identificar os pontos fracos, as abordagens específicas de proteção, atualizar processos e protocolos de segurança e testá-los continuamente. Para os especialistas do instituto, tais práticas são capazes de reduzir as ameaças físicas, humanas e digitais que podem ocorrer nesses ambientes.

A segurança em nuvem auxilia muito nas aplicações voltadas para operações em larga escala, possibilitando o crescimento de serviços e protegendo os dados de negócios em Data Centers, o trabalho remoto, por exemplo, é um grande impulsionador para reforçar a preservação dos ambientes virtuais.

Por isso, a escolha do provedor deve ser muito criteriosa e configura mais um desafio para a área de TI, garantir o crescimento da atividade sem colocar os dados em risco e conseguir que o provedor proporcione a visibilidade que a regulamentação exige.

2.3.5 Classificação e Armazenamento dos Dados

A LGPD é bem taxativa em relação ao armazenamento de dados, é preciso acima de tudo ter consentimento do titular e as informações devem ser revisadas regularmente, pois a empresa deve armazenar os dados somente enquanto estiverem sendo usados, e para o propósito para o qual foram coletados, e ainda, o titular dos dados pode revogar o consentimento a qualquer momento.

Em um compromisso compartilhado com outras áreas igualmente importantes na organização, o setor de TI é responsável por diagnosticar, executar o plano de adequação à lei, e por acompanhar a eficiência das ações em todas as plataformas de entrada e saída de dados sensíveis de funcionários, parceiros, fornecedores e clientes no dia a dia.

Logo, as empresas que operam com dados (em qualquer volume) em sistemas ERP[9], CRM[10], contabilidade etc., precisam repensar bastante as suas estruturas de tecnologia para assegurar que os dados não sejam vazados, e nem que eles sejam armazenados sem consentimento de titulares.

E isso requer uma mudança de visão da própria TI sobre seus equipamentos, processos e sobre a forma como lidam com dados, abrindo espaço para novos modos de usar a tecnologia e os dados.

Não somente na adequação à LGPD, mas como melhoria contínua do armazenamento de dados, é uma boa prática prever e antecipar eventos que possam comprometer a privacidade, buscar soluções de backups que sejam ágeis e ao mesmo tempo confiáveis, que possibilitem o monitoramento, a integridade das informações e a recuperação de dados.

2.3.6 *"Application Programming Interface"* [11] (API)

Em um primeiro momento pode ser bastante tentador implementar a LGPD com aplicações e automatizações, principalmente nas questões relacionadas ao consentimento do usuário. Atualmente, grande parte das empresas utilizam essa tecnologia para troca de informações tanto em sistemas internos quanto externos para comunicação com clientes e parceiros.

Pode-se exemplificar citando algumas APIs mais conhecidas: públicas (YouTube, Facebook, Whatsapp), privadas ("*Internet Banking"*, Assistentes Virtuais), parcerias (ERP, CRM). As APIs já são parte do dia a dia dos usuários da Internet, de acordo com o relatório "*State of the Internet*", da Akamai, as chamadas de API representam 83% de todo o tráfego na web.

Para Sheth (1999), a interoperabilidade de dados pelos sistemas de informação é importante, principalmente: a) pelo progresso que a Internet proporcionou na distribuição de dados e na interconexão de sistemas de informação distribuídos – ou seja – sistemas de informação desenvolvidos e gerenciados por diferentes instituições; b) pela própria especialização destes sistemas de informação, que tem objetivos voltados para atividades específicas, como o caso de redes sociais, e; pelo reúso e análise de dados para a criação de novas informações e o posterior reúso e compartilhamento destas novas informações ou dos dados originais em outros sistemas de informação.

Certamente uma API agrega valor ao negócio por trazer melhores serviços e agilidade, entretanto, fornecem um canal direto a terceiros para os dados armazenados, tanto corporativos quanto pessoais, estando altamente sujeita a ataques. A principal questão é como assegurar que o compartilhamento de dados esteja alinhado com as políticas de segurança e privacidade?

E mais, foram observados princípios da LGPD? A tarefa não é tão fácil assim, é preciso estudar a fundo a "*compliance"*[12] com a LGPD para não gerar inconsistências futuras nos sistemas envolvidos.

É recomendado para mitigação desses riscos realizar uma análise de segurança específica para API: deve ser multidisciplinar, envolvendo as equipes de segurança, desenvolvimento e infraestrutura, pelo fato de aspectos de governança, ciclo de desenvolvimento, código e operação serem fundamentais nesse processo.

Testes de segurança nas APIs e realização de treinamentos específicos contemplando todos os envolvidos, também contribuem para a minimização dos riscos. Existem vários tipos de testes à disposição: funcional, confiabilidade, carga, segurança, IU (integridade-usabilidade), negativo e validação.

2.3.7 Treinamento

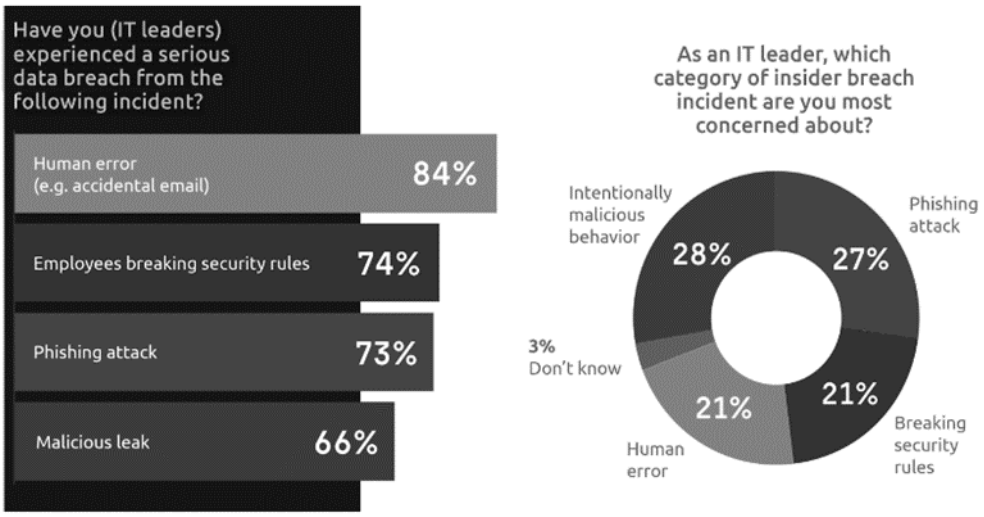
Além de todo o investimento tecnológico, que certamente contribui para que as empresas se adequem à LGPD, uma mudança cultural é primordial na busca da conformidade, sendo extremamente necessário atentar para o elemento humano. O estudo 2021 "*Data Breach*

Investigations Report" (DBIR) da Verizon mostrou que a maioria das violações de dados, como "*ransomware"* e "*phishing",* envolveu um fator humano, e mais, 85% das violações de dados ocorridas em 2020 envolveram uma interação humana.

A vulnerabilidade interna oriunda de fator humano costuma ser a mais difícil de solucionar, a maioria das empresas está despreparada para evitar violação de dados ocasionadas por colaboradores. E por que isso ocorre?

O comportamento humano é bastante complexo e quase impossível de se prever, a figura 2 mostra o resultado do relatório "*Insider Data Breach Survey*" 2021, em que perguntas feitas para líderes de TI sobre violação de dados internos em 2020, apresentam o fator humano como a causa mais recorrente.

Figura 2 - Relatório de violação de dados internos



Fonte: Insider Data Breach Survey, 2021

As respostas para a pergunta "Você já passou por uma violação de dados causadas por alguns desses incidentes?": falha humana acidental (84%), colaboradores quebrando regras de segurança (74%), ataque de "*phishing"* (73%) e vazamentos maliciosos (66%). Já para a outra pergunta "Para você como um líder de TI, qual categoria de violação de dados internos causa maior preocupação?", as respostas foram: comportamento malicioso intencional (28%), "*phishing"* (27%), quebra de regras de segurança (21%), falha humana (21%) e não sabe (3%).

A mesma pesquisa revela um dado preocupante, 23% dos colaboradores acreditam ter direito a levar os dados em caso de uma mudança de emprego. Por isso, o aumento da terceirização de serviços, o regime híbrido de trabalho e a rotatividade de funcionários aumentam ainda mais o risco de roubo de informações.

Uma das formas de mitigar esses riscos é a arquitetura "*Zero Trust"* [13], em que os acessos aos recursos são concedidos ou negados baseados nas permissões atribuídas ao usuário, de acordo com sua função na organização. Ainda assim, está sujeito a ameaças internas, como um colaborador insatisfeito, espionagem industrial, entre outros.

Os treinamentos devem reforçar a importância de seguir os regulamentos e protocolos de segurança digital, é essencial programas de treinamento e reciclagem tecnológica bem estruturados, e ainda, serem extensivos para todos os níveis hierárquicos.

Um grande erro em muitas organizações é partir do princípio de que aqueles com cargos de alto escalão detêm conhecimento em tecnologia e segurança, focando assim nos níveis operacionais. No entanto, as gerências e diretorias são aqueles que mais têm acesso às informações privilegiadas, e muitas vezes ficam sem treinamento.

O ideal é todo esse processo passar por uma democratização do conhecimento, difundindo o conceito de segurança da informação de forma estruturada e horizontal, demonstrando clareza sobre as estratégias de segurança da organização, propiciando treinamentos, palestras e informativos sobre o tema.

A conscientização da equipe sobre o seu papel na tratativa dos dados pessoais e sensíveis é uma forte ferramenta para contra-atacar a ocorrência de violação de dados internos.

3. Metodologia

A realização deste trabalho configura uma pesquisa exploratória, utilizando métodos de pesquisas bibliográficas em livros, artigos científicos, dissertações e publicações. A sua elaboração baseou-se no método hipotético-dedutivo.

No desenvolvimento do trabalho primeiramente é apresentada a questão da privacidade e proteção de dados, na sequência os desafios da TI para atendimento à LGPD e finalmente, as ferramentas e soluções para adequação à LGPD. Com o intuito de validar o estudo de forma eficaz foi feita uma pesquisa de campo com questões pertinentes à adequação das empresas e profissionais de TI, sua divulgação abrangeu tanto meios acadêmicos quanto empresariais. Uma breve análise dos resultados encontra-se na seção 4.

O tipo de pesquisa de campo adotado para fundamentação do objeto de estudo foi o quantitativo-descritivo, elaborando 06 questões pertinentes ao “Impacto da LGPD na Tecnologia da Informação e os Desafios para os Profissionais da Área”, utilizando a ferramenta Google Forms.

É importante ter uma política para controlar questionários incompletos, por essa razão, o processo de criação da pesquisa contemplou a questão de consistência e integridade das respostas. Nesse sentido, todas as questões foram marcadas como de preenchimento obrigatório.

4. Resultados e Discussões

O formulário foi difundido tanto no meio acadêmico quanto empresarial na região Metropolitana de Campinas, no período de 23/09/2022 a 22/10/2022, o levantamento e análise dos dados baseou-se em informações obtidas com o retorno de 71 questionários, contendo dados nominais[14] e ordinais[15].

4.1 Pesquisa de Campo

A compilação dos dados permite afirmar que 72,5% das respostas correspondem a profissionais da área de TI; no quesito adequação à LGPD, quase 60% das empresas estão em conformidade com a lei, e 24,6% encontram-se ainda em processo de transição. O que possibilita

registrar a preocupação das organizações em alcançarem a "*compliance"* com a referida lei.

No que se refere ao nível de conhecimento sobre LGPD, apresentou-se as opções para autoavaliação: Excelente (6 respostas), Muito bom (10 respostas), Satisfatório (21 respostas), Moderado (24 respostas) e Fraco, revelou-se nesta amostragem que apenas 10 respostas (14,1%) se autoavaliaram como nível fraco no entendimento da lei.

As duas perguntas seguintes são referentes a treinamentos e ferramentas disponibilizadas e consolidam o fato da grande maioria (85,9%) afirmar ter conhecimento considerável sobre a referida lei.

A pergunta "Qual é a sua percepção sobre os treinamentos de conscientização?", apresenta escala ordenada variando de "concordo plenamente" a" não tive treinamento", e continha os seguintes questionamentos:

- ✓ A linguagem é acessível a todos os colaboradores (as respostas "concordo plenamente" e "concordo "correspondem a 64%, contraposto a "não tive treinamento" e "discordo totalmente" que totalizaram 36%).
- ✓ Existe uma preocupação em criar uma cultura de tratativa de dados pessoais e sensíveis. (as respostas "concordo plenamente" e "concordo "correspondem a 72%, contraposto a "não tive treinamento" e "discordo totalmente" que totalizaram 28%).
- ✓ Os instrutores demonstram conhecimento sobre o assunto. (as respostas "concordo plenamente" e "concordo "correspondem a 75%, contraposto a "não tive treinamento" e "discordo totalmente" que totalizaram 25%).
- ✓ Contribuiu para o nível de conhecimento que tenho do assunto (as respostas "concordo plenamente" e "concordo "correspondem a 80%, contraposto a "não tive treinamento" e "discordo totalmente" que totalizaram 20%).

A pergunta "Ferramentas disponibilizadas para tratativa de dados pessoais e sensíveis na empresa em que você trabalha:", apresenta escala ordenada variando de "concordo plenamente" a" não foi disponibilizado", e continha os seguintes questionamentos:

- ✓ O Plano de Segurança de Informação estabelece regras claras e objetivas (as respostas "concordo plenamente" e "concordo "correspondem a 65%, contraposto a "não foi disponibilizado" e "discordo totalmente" que totalizaram 35%).
- ✓ A política de senhas complexas é efetiva e devidamente monitorada (as respostas "concordo plenamente" e "concordo "correspondem a 64%, contraposto a "não foi disponibilizado" e "discordo totalmente" que totalizaram 36%).
- ✓ As medidas de atualização dos serviços de segurança e operacionais são constantes (as respostas "concordo plenamente" e "concordo "correspondem a 68%, contraposto a "não foi disponibilizado" e "discordo totalmente" que totalizaram 32%).
- ✓ Houve um investimento para melhorar a segurança física dos Data Centers (as respostas "concordo plenamente" e "concordo "correspondem a 67%, contraposto a "não foi disponibilizado" e "discordo totalmente" que totalizaram 33%).

Finalizando a pesquisa com a pergunta: "Qual aspecto da adequação à LGPD você considera mais desafiador para o profissional de TI?" A tabela 1 compila as opções apresentadas:

Tabela 1 - Aspectos da adequação à LGPD considerados desafiadores para os profissionais de TI

Opções apresentadas na pesquisa	Número de respostas	Porcentagem do total
Compreender os princípios e bases legais	27	38,02%
Mapeamento dos dados pessoais e sensíveis	13	18,31%
Investimento em soluções de cibersegurança	28	39,44%
Investimento em armazenamento de dados	01	1,41%
Outros (*)	02	2,82%
TOTAIS	**71**	**100,00%**

Fonte: Autoria própria, 2022

(*) As duas respostas deste item deixado em aberto citam a alta direção:
- Convencer a alta diretoria do investimento que deve ser feito na Segurança da Informação.
- Apoio da alta direção.

A análise da amostra revela um aspecto positivo que é a preocupação das empresas em se adequar à LGPD, apenas 15,4% ainda não iniciaram a adequação à lei, o mesmo acontecendo com os profissionais da área de TI, que estão buscando um maior entendimento de como obter "*compliance"* com a lei, já que a grande maioria, 85,9% autoavaliaram positivamente o nível de conhecimento no assunto.

No que se trata de aspectos desafiadores, em primeiro lugar no ranking vem investimento em soluções de cibersegurança, demonstrando que apesar das organizações saberem a importância da adequação à LGPD, ainda não estão dispostas a investir adequadamente. Ao mesmo tempo, o segundo colocado dos aspectos desafiadores é compreender os princípios e bases legais, corroborando a tese de que os profissionais da área de TI sentem a necessidade de aprofundamento nos requisitos da lei.

É importante ressaltar que o estudo não é conclusivo, trata-se de uma amostragem, podendo não retratar a realidade de outras localidades e outros grupos de entrevistados.

5. Considerações Finais

O avanço da tecnologia e o mundo ficando cada vez mais digital fizeram com que a informação se tornasse uma importante moeda de troca para o acesso das pessoas a serviços e produtos. É uma tendência mundial a necessidade de criar normas e regulamentos para o processamento transparente dessas informações.

Essa nova realidade ocasiona vários questionamentos: Como introduzir políticas relacionadas à proteção e privacidade dos dados? Qual o melhor caminho para mudar velhos hábitos e métodos operacionais, fazendo com que todos estejam dispostos a deixarem um lugar

comum? A atitude de sair de uma zona de conforto, estar aberto a diferentes alternativas que possam beneficiar o negócio, poderá alavancar tanto o crescimento individual quanto o coletivo.

Conscientização é a palavra-chave para que essas ações possam provocar efeitos positivos a curto, médio e longo prazo, partindo de um diagnóstico abrangente, que levante pontos de aprimoramento, determine com clareza as responsabilidades de cada componente do time e aponte, de forma realista, como e onde a organização pode estar genuinamente pronta para o atendimento à LGPD.

Existe uma crença de que o fator humano é o elo mais fraco da corrente na questão de proteção de dados. Por outro lado, com ferramentas e treinamentos adequados, um profissional bem capacitado e conscientizado pode se tornar, a médio e longo prazo, uma "barreira" de primeira linha de defesa.

À vista de tudo o que foi apurado nesse breve estudo, conclui-se que o papel dos profissionais de TI é fundamental para o sucesso na jornada de adequação à LGPD, entretanto, precisarão estar altamente capacitados para implementar as mudanças necessárias, e serem os agentes que compartilharão as informações com as demais áreas. Ou seja, é parte do seu escopo de trabalho o desenvolvimento de soluções que otimizem as coletas e tratamentos de dados, em conformidade com a legislação.

Em contrapartida, as organizações precisarão alavancar os investimentos em soluções de cibersegurança e armazenamento de dados, abandonando de vez o pensamento de considerá-los como um gasto secundário, é crucial começar a compreender a sua relevância para o sucesso de um negócio.

Notas Finais

[1]Especialista em Administração Industrial pela USP, Tecnóloga em Processos de Produção pela FATEC São Paulo, aluna do curso de Tecnologia de Segurança da Informação na FATEC Americana, trabalha atualmente como DPO – Encarregada de Dados na ZL Brasil.

[2] Especialista em Gestão de Segurança da Informação pela FIAP, professor de graduação na FATEC Americana e Analista de projetos de segurança no CERT.br.

[3]Lei Geral de Proteção de Dados, Lei N° 13.709, de 14 de agosto de 2018.

[4]Tecnologia da Informação.

[5] Sigla em inglês, DRP – "*Disaster Recovery Plan"*.

[6] Palavra do inglês para definir indivíduos que possuem um conhecimento elevado na área de tecnologia da informação, mas que utilizam suas habilidades em benefício próprio ou para prejudicar outras empresas e pessoas.

[7] Tradução do inglês *"stakeholders"*, todos os grupos de pessoas ou organizações que podem ter algum tipo de interesse pelas ações de uma determinada empresa.

[8] Tradução literal para o português é "ponto de extremidade" , pode ser definido como os dispositivos finais que estão conectados a um terminal de rede – computadores, tablets, smartphones ou qualquer dispositivo conectado em uma rede interna ou externa.

[9] Sigla para "*Enterprise Resource Planning*" – traduzindo do inglês, "Planejamento dos Recursos da Empresa".

[10] Sigla usada para "*Customer Relationship Management*", traduzindo para o português, "Gestão de Relacionamento com o Cliente".

[11] Tradução para o português: Interfaces de Programação de Aplicações.

[12] Refere-se a estar em conformidade com, ao ato ou prática de obedecer leis, regras, ordens ou pedidos.

[13] Tradução para o português: política de confiança zero.

[14] Determina-se a proporção de respostas das categorias sem ordenação.

[15] Possuem uma escala ordenada em relação a um assunto específico, como por exemplo: "concordo", "concordo parcialmente", "não concordo".

Referências

AKAMAI. The State of the Internet report, 2022. Disponível em: <https://www.akamai.com/our-thinking/the-state-of-the-internet/global-state-of-the-internet-security-ddos-attack-reports>. Acesso em 28 out. 2022. Citado na página 9.

ASCIERTO, R., & TRAVER, T. Data center security: Reassessing physical, human ando digital disks. Uptime Institut e Intelligence, 2021. Disponível em: <https://uptimeinstitute.com/uptime_assets/fff48756c66a70ad900b0f7fb65d7cae20e8204b64fafa17b7b2f7bff0287ab-data-center-security.pdf?mkt_tok=NzExLVJJQS0xNDUAAAGGwaAwvqOnwwZt_-z2pHJ-YE8RXSweulJFP1hrSJUJf4FRbmfENYIbB22BYtGSHTmmUjxFnWygpFRs9QVw4RSGVnfziqjY_JppeHvxmxRZ>. Acesso em 07 set. 2022. Citado na página 8.

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. ABNT NBR ISO/IEC 27001 – Tecnologia da informação – Técnicas de segurança – Sistemas de gestão de segurança da informação – Requisitos. ABNT, 2013. Citado na página 7.

BRASIL. ANPD, Autoridade Nacional de Proteção de Dados pessoais. Disponível em: <https://www.gov.br/anpd/pt-br>. Acesso em 26 abr. 2022. Citado na página 4.

BRASIL. Proteção de dados pessoais (lei 13.709/2018). Brasília: Senado Federal, 2018. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709compilado.htm>. Acesso em 24 jun. 2022. Citado na página 5.

CARVALHO, G. P., & PEDRINI, T. F. (2019). Direito à privacidade na lei geral de proteção de dados pessoais. Revista Da ESMESC, 26(32), 363–382. Disponível em: <https://revista.esmesc.org.br/re/article/view/217>. Acesso em 24 jun. 2022. Citado na página 3.

EGRESS SOFTWARE TECHNOLOGIES. Insider Data Breach Survey Report, 2021. Disponível em: < https://www.egress.com/blog/what-is-human-layer-security/2021-insider-breach-survey>. Acesso em 02 out. 2022. Citado na página 10.

GARCEL, Adriane; MORO, Sergio Fernando; SOUZA NETTO, José Laurindo de; HIPPERTT, Karen Paiva. Lei geral de proteção de dados: diretrizes e implicações para uma sociedade pandêmica. Coletâneas de artigos jurídicos: em homenagem ao Professor José Laurindo de Souza Netto. Viviane C. de S. K., Adriane G., José L. de S. N. 1.ed., Curitiba: Clássica Editora, 2020. ISBN 978-65-87965-03-1. p. 319-344. Citado na página 3.

NAKAMURA, Emilio; GEUS, Paulo Lício. Segurança de Redes: em ambientes cooperativos. São Paulo: Novatec, 2014. Citado na página 7.

NATIONAL INSTITUTE OF STANDARDS AND TECHNOLOGY. NIST SP 800-37 Rev.2 – Risk Management Framework for Information Systems and Organizations: A System Life Cycle Approach for Security and Privacy, 2018. Disponível em: <https://csrc.nist.gov/publications/detail/sp/800-37/rev-2/final>. Acesso em 13 set. 2022. Citado na página 6.

OPPLIGER, R. Contemporary Cryptography. Norwood, MA: Artech House. Second Edition. 2012. 503 p. (Computer Security Series). Citado na página 7.

PRIVACIDADE e proteção de dados: entenda qual é a diferença. Privacy Tech, 2022. Disponível em: https://privacytech.com.br/protecao-de-dados/privacidade-e-protecao-de-dados-entenda-qual-e-a-diferenca,414166.jhtml#%3E. Acesso em: 31 ago. 2022. Citado na página 3.

SHETH, A. P. Changing Focus on Interoperability in Information Systems:From System, Syntax, Structure to Semantics. In: Goodchild, M. et al. (Eds.). Interoperating Geographic Information Systems. Boston, MA: Springer US, 1999. p. 5–29. Citado na página 9.

SILVA, Rosane Leal; SILVA, Letícia Brum. A proteção jurídica de dados pessoais na internet: análise comparada do tratamento jurídico do tema na União Europeia e no Brasil. Direito e novas tecnologias. Florianópolis: FUNJAB, 2013. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=e4d8163c7a068b65>. Acesso em 5 jul. 2022. Citado na página 4.

VERIZON. Data Breach Investigations Report (DBIR), 2021. Disponível em: <https://www.verizon.com/business/resources/reports/dbir/>. Acesso em 02 out. 2022. Citado na página 9.

ZANINI, L.E. DE ASSIS. A proteção da imagem e da vida privada na França. Revista de Derecho Privado, 2018. p. 157–175. Disponível em: <https://doi.org/10.18601/01234366.n34.06>. Acesso em 29 ago. 2022. Citado na página 2.