LGPD MODEL CANVAS: PROPOSTA DE UM FRAMEWORK PARA DIAGNOSTICAR AS EMPRESAS PARA A LGPD

LGPD MODEL CANVAS: PROPOSAL FOR A FRAMEWORK TO DIAGNOSE COMPANIES FOR THE LGPD

Marcelo Tsuguio Okano [1]
Lamara Ferreira [2]
Henry de Castro Lobo dos Santos [3]
Edson Luiz Ursini [4]

Resumo: *Esse artigo tem como objetivo mapear, através do LGPD Model Canvas, os processos que tratam os dados pessoais e diagnosticar quais não estão de acordo com a nova Lei Geral de Proteção de Dados Pessoais. Foi apresentado um estudo de caso único da aplicação do framework LGPD Model Canvas no processo de admissão de funcionário realizado pelo RH de uma empresa de Monitoramento e Segurança. Analisou-se o processo visual, colaborativo e multidisciplinar, para levantamento dos processos que tratam dados pessoais, no presente estudo de caso, representado pelo processo de admissão, permitiu identificarmos 13 vulnerabilidades que precisam ser corrigidas e direcionadas no plano de ação. Após o diagnóstico de conformidade do processo de admissão da empresa de segurança perante a à LGPD, ficou claro que o LGPD Model Canvas pode ser utilizado como uma ferramenta para mapeamento das informações dos processos que tratam dados pessoais e levantamento de vulnerabilidades*

Palavras-chave*: LGPD. Canvas. LGPD Model Canvas. Framework.*

Abstract: *This article aims to map, through the LGPD Model Canvas, the processes that handle personal data and diagnose which ones are not in accordance with the new General Law for the Protection of Personal Data. A single case study of the application of the LGPD Model Canvas framework in the employee admission process carried out by the HR of a Monitoring and Security company was presented. The visual, collaborative and multidisciplinary process was analyzed to survey the processes that deal with personal data, in this case study, represented by the admission process, it allowed us to identify 13 vulnerabilities that need to be corrected and addressed in the action plan. After the compliance diagnosis of the security company's admission process to the LGPD, it became clear that the LGPD Model Canvas can be used as a tool for mapping the information of the processes that handle personal data and survey vulnerabilities.*

Keywords: *LGPD. Canvas. LGPD Model Canvas. Framework.*

1 Doutor em Engenharia de Produção (UNIP). Doutor em Administração (pela FGV-EAESP). Matemático. Mestre em Administração (pela USCS). Professor no Programa de Pós-graduação em Engenharia de Produção (PPGEP) da UNIP. Professor no Centro Paula Souza (CPS) e Pesquisador colaborador na FT UNICAMP. Lattes: http://lattes.cnpq.br/2884802638051403 . ORCID: https://orcid.org/0000-0003-1680-782 .
E-mail: marcelo.okano@fatec.sp.gov.br.

2 Graduação em Gestão da Tecnologia da Informação. Mestranda em Gestão e Tecnologia em Sistemas Produtivos pela UPEP-CPS. Owner da LFerreira consultoria. Lattes: http://lattes.cnpq.br/5232949283498734. ORCID: https://orcid.org/ 0000-0002-9790-9485. E-mail: lamara.ferreira@cpspos.sp.gov.br .

3 Doutorando e Mestre em Tecnologia pela Faculdade de Tecnologia da Universidade Estadual de Campinas e Pós-graduado pelo Centro Paula Souza. Arquiteto de Segurança da Informação em Cloud na Gerdau Brasil. Lattes: http://lattes.cnpq.br/3884137732632652. ORCID: https://orcid.org/ 0000-0003-1400-3811. E-mail: h190839@dac.unicamp.br .

4 Graduação em Engenharia Industrial Elétrica Opção Produção pelo Centro Universitário da FEI. Graduação em Administração de Empresas pela Universidade de São Paulo. Mestrado em Engenharia Elétrica pela Universidade de São Paulo. Doutorado em Engenharia Elétrica pela Universidade Estadual de Campinas (1994). Habilitado como professor Livre Docente da Faculdade de Tecnologia, FT, da Universidade Estadual de Campinas. É orientador de mestrado e doutorado da pós-graduação na FT-UNICAMP. Cadastrado como professor participante da pós-graduação (doutorado) na FEEC-UNICAMP. Lattes: http://lattes.cnpq.br/8766578585291045. ORCID: https://orcid.org/0000-0003-1867-3804. E-mail: ursini@ft.unicamp.br .

Introdução

As preocupações com a segurança das informações e dados pessoais estão cada dia mais presentes na vida cotidiana das empresas, pois com a rápida evolução das tecnologias para armazenamentos destes dados, também aumentam as necessidades de segurança e proteção destas informações por parte das organizações.

O Governo Brasileiro sancionou a lei Nº 13.709, de 14 de agosto de 2018, também conhecida como a Lei Geral de Proteção de Dados Pessoais (LGPD) e esta dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2021).

A LGPD (Lei Geral de Proteção de Dados Pessoais) atribui a titularidade dos dados à pessoa física a ela referente, e institui regras para o uso dos dados, visando à proteção dessas pessoas físicas (cidadãos) e de seus direitos fundamentais como a liberdade, privacidade e livre desenvolvimento, entre outros (MAGACHO ; TRENTO, 2021).

As empresas terão que se adaptar a esta nova lei e a partir de agosto de 2021 sofrerão penalidades legais se não cumprirem as exigências. Com intuito de facilitar essa adaptação, esse artigo tem como objetivo mapear, através do LGPD Model Canvas, os processos que tratam os dados pessoais e diagnosticar quais não estão de acordo com a nova Lei Geral de Proteção de Dados Pessoais.

Será apresentado um estudo de caso único da aplicação do framework LGPD Model Canvas demonstrando como ele contribuiu no mapeamento dos processos de requisição de dados pessoais e se estão ou não em conformidade com a LGPD.

O framework LGPD Model Canvas, criado por Lamara Ferreira, foi inspirada nos métodos ágeis, nos pilares do modelo *Privacy by Design*, nos benefícios do Design Thinking e no modelo *Business Model Canvas* e pode ser aplicado nas empresas que buscam se adequar a LGPD.

Fundamentação Teórica

A busca pela governança e proteção dos dados pessoais, têm se consolidado cada vez mais nas organizações, impulsionada pela Lei Geral de Proteção de Dados, conhecida como LGPD. É o que afirma Vasconcelos (2020) “a adequação demonstra o respeito aos dados pessoais daqueles que deram preferência a esse empreendimento, na hora de buscar produtos e serviços”. Nesse cenário, as organizações que buscam estar em conformidade com os regulamentos e criar uma cultura de privacidade, para que novos produtos e serviços já nasçam adequados. Por se tratar de uma legislação que engloba conceitos de segurança da informação e boas práticas de governança, para descomplicar e facilitar o processo da jornada de adequação, nasceu o framework *LGPD Model Canvas*, criado por Lamara Ferreira.

LGPD

Em 2018, foi criada a Lei Federal 13.709/2018, doravante denominada LGPD, influenciada e inspirada pelo Regulamento Geral de Proteção de Dados da União Européia (GPDR), para regulamentar o tratamento de dados pessoais (GROSSI, 2020; GUNTHER, COMAR E RODRIGUES, 2020; MARTINI e BERGSTEIN, 2019).

Segundo Grossi (2020), dado pessoal é aquele que se encontra atrelado à projeção, à extensão ou à dimensão de uma determinada pessoa, tanto na sua esfera individual, quanto em sua esfera relacional. Para Martini e Bergstein (2019), toda a informação relacionada à pessoa natural, identificada ou identificável, é denominada na nova legislação de dado pessoal. No trabalho de Gunther, Comar e Rodrigues (2020), dado pessoal é informação relacionada a pessoa natural identificada ou identificável, e dado sensível é todo dado pessoal sobre origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso,

filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural.

Segundo o artigo dos autores Martini e Bergstein (2019), quando se reúne um "conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico", forma-se um banco de dados pessoais. Considera-se tratamento de dados "toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração (art. 5, X, LGPD)

A LGPD (Lei Geral de Proteção de Dados pessoais), foi promulgada em 14 de agosto de 2018, diante uma pressão decorrente da entrada em vigor do Regulamento Geral de Proteção de Dados da União (GPDR), na União Europeia, buscando harmonizar e atualizar conceitos de modo a mitigar riscos e a estabelecer regras claras sobre a proteção de dados pessoais no Brasil (GROSSI, 2020). O texto entrou em Vigor em 18 de setembro de 2020 e dará um prazo até 1 de agosto de 2021 para as organizações se adaptarem a Lei, e após isso, as empresas que não estiverem de acordo com a norma poderá ter punições que podem chegar até 2% do faturamento, até o limite de 50 milhões de reais.

A Lei Federal 13.709/2018 (LGPD) estabelece que toda a gestão de dados pessoais deverá ser realizada de maneira precisa e segura, pautada no consentimento prévio, na manifestação livre, informada e inequívoca do titular dos dados coletados e tratados pela qual concorda com o tratamento de seus dados pessoais para uma finalidade determinada (MARTINI e BERGSTEIN, 2019). Em resumo, o objetivo da legislação relativas ao tratamento de dados pessoais é justamente assegurar o respeito dos direitos e liberdades fundamentais, nomeadamente do direito à vida privada, que precisa ser preservado mesmo dentro de um ambiente de riscos e incertezas. O ponto central da nova lei é que nenhuma instituição pode utilizar os dados de nenhum cidadão sem o seu consentimento explícito. O texto também traz garantias para o usuário, que pode solicitar que seus dados sejam deletados, revogar um consentimento, transferir os dados para outro fornecedor de serviços, entre outras ações. E o tratamento dos dados deve ser feito levando em conta alguns quesitos, como finalidade e necessidade, que devem ser previamente acertados e informados ao cidadão (SERPRO, 2020).

LGPD Model Canvas

Origem do LGPD Model Canvas - O LGPD Model Canvas foi inspirado nos métodos ágeis, nos pilares do modelo Privacy by Design, nos benefícios do Design Thinking e no modelo Business Model Canvas. A metodologia Privacy by Design, foi desenvolvida pela Comissária de Informação e Privacidade de Ontário, Canadá, Dra. Ann Cavoukian, que é amplamente conhecida no mundo todo e inserida na GPDR (Regulamento Geral sobre a Proteção de Dados) e na LGPD. Cavoukian (2009) defende que a privacidade deve ser pensada logo no início do projeto e incorporada no centro de todo o desenvolvimento. Segundo Cavoukian (2009), para criar a cultura de privacidade, as organizações precisam inserir este conceito no centro de todos os processos, como parte dos valores da empresa e na cultura organizacional.

O projeto e a implementação de requisitos de privacidade em sistemas é um problema difícil e requer a tradução de complexas questões sociais, legais e éticas em requisitos de sistema. O conceito de Privacy by Design foi proposto para servir como uma diretriz sobre como abordar essas questões. Privacy by Design consiste em uma série de princípios que podem ser aplicados desde o início do desenvolvimento de sistemas para mitigar preocupações de privacidade e alcançar conformidade de proteção de dados (GÜRSES *et al*, 2011).

Cavoukian (2009) apresenta os seguintes princípios orientadores:

1. Proativo e não reativo; preventivo e não corretivo;
2. Privacidade como padrão;
3. Privacidade incorporada ao design;
4. Funcionalidade completa: soma positiva e não soma zero;
5. Segurança ponta a ponta: proteção durante todo o ciclo de vida;

Revista Humanidades e Inovação - ISSN 2358-8322 - Palmas - TO - v.9, n.20

6. Visibilidade e transparência;
7. Respeito pela privacidade do usuário.

Nesse cenário, é uma abordagem que esteja inserida às inovações, que seja eficaz e amplamente acessível. De acordo com Brown (2010), o Design Thinking oferece uma abordagem desse tipo, que possa ser integrada a todos os aspectos dos negócios e da sociedade e que os indivíduos e equipes possam utilizar para gerar ideias inovadoras que sejam implementadas e que, portanto, façam a diferença.

O design thinking é um processo comumente usados por designers para encontrar a solução para problemas complexos, navegar por ambientes novos ou incertos e criar um produto para o mundo. O design thinking usa os principais elementos e habilidades de jogo, empatia, reflexão, criação e experimentação para colaborar, criar e desenvolver as descobertas. No design thinking, o fracasso não é uma ameaça, mas um caminho para o aprendizado posterior. Por meio da observação, síntese, alternativas, pensamento crítico, feedback, representação visual, criatividade, resolução de problemas e criação de valor, os empreendedores podem usar o design thinking para identificar oportunidades únicas de empreendimento (BLACK et al., 2019).

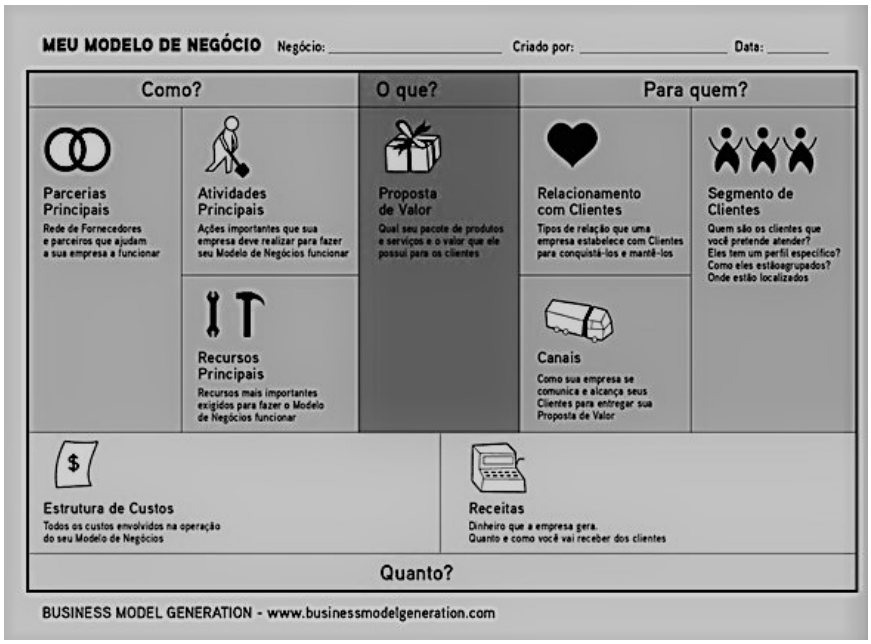
Corroborando com este conceito, surgiu a necessidade de criar um método visual para trazer luz às principais preocupações relacionadas à privacidade e proteção e busca pela conformidade das organizações às necessidades e requisitos trazidos pela LGPD. Dessa forma, foi escolhido o modelo Canvas para criar uma ferramenta de trabalho visual, englobando nove necessidades principais para discussão, preenchimento e análise.

A inspiração para este modelo foi o Business Model Canvas, que de acordo com Clark (2013) o quadro de modelo de negócios confere um atalho visual para simplificar organizações complexas. Na mesma perspectiva, Clark (2013) reforça que as imagens ajudam a transformar suposições não verbalizadas em informações explícitas. E que informações explícitas nos ajudam a pensar e comunicar mais efetivamente.

O Business Model Canvas (BMC), Figura 1, foi desenvolvido por Alex Osterwalder e Yves Pigneur, e cocriado com uma série de 470 praticantes de todo o mundo. Oferece uma tela simples, visual e de uma página sobre a qual se pode projetar, inovar e dialogar sobre os modelos de negócios (Burkett, 2013).

Osterwalder (2004) introduziu esse modelo de negócios para fornecer um meio eficiente de capturar completamente os aspectos-chave de como uma empresa pode aproximar-se de uma proposta de negócio particular e é composto de nove "blocos de construção" englobando um conjunto relativamente completo e abrangente de medidas de planejamento de negócios. As dimensões do Canvas podem ser interpretadas através dos blocos de construção: como – parcerias principais, atividades principais e recursos principais; o que – proposta de valor; para quem – relacionamento com clientes, canais e segmentos de clientes; quanto – estrutura de custos e receitas.

Figura 1. Business Model Canvas (BMC)



Fonte: Business model Generation (2015).

O Framework LGPD Model Canvas

Partindo da abordagem metodológica descritiva, optou-se pela divisão do framework LGPD Model Canvas em nove blocos (Figura 2). A proposição do uso do Canvas para modelagem de negócios criado por Alexander Osterwalder e apresentado no seu livro – Business Model Generation. Osterwalder (2011) aponta sobre como projetar e implementar sistematicamente estes modelos. Sobre a importância de questionar, desafiar e transformar modelos ultrapassados.

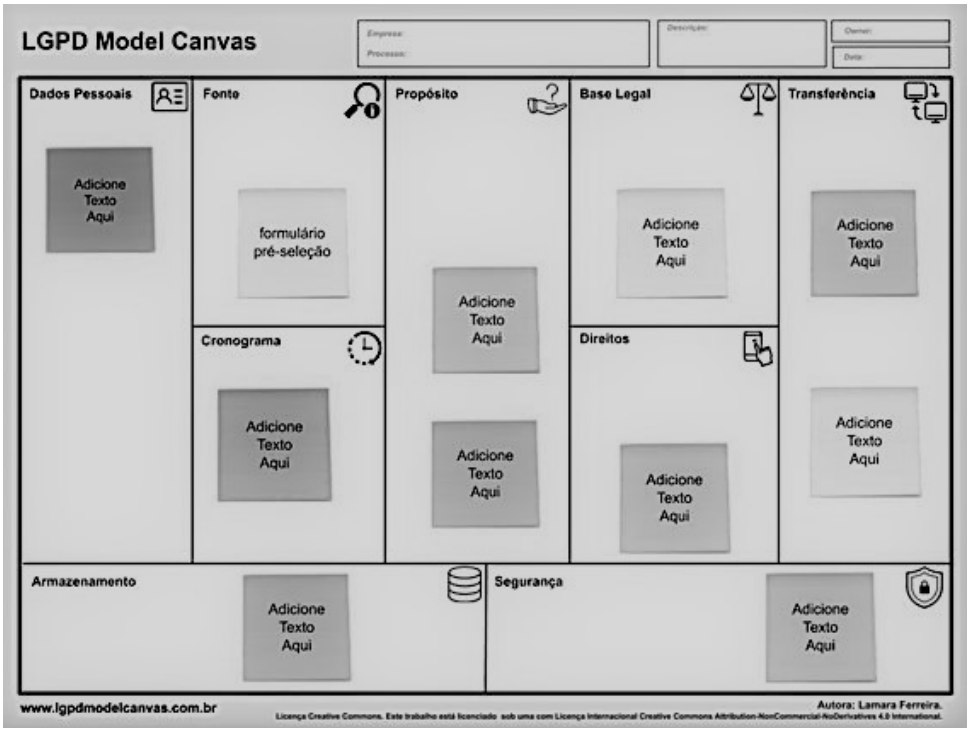
Nesse ínterim, o framework LGPD Model Canvas busca através do poder da colaboração e facilitação, alcançar benefícios além dos formulários, seguindo as etapas de preenchimento:

a) Deverá ser preenchido um LGPD Model Canvas para cada processo (relação 1 para 1). É fundamental entender quais os principais produtos/serviços que a empresa oferece, seus papéis como controlador/operador, volumetria e áreas envolvidas nos processos que tratam os dados pessoais.

b) Quem deve ser envolvido: Grupo multidisciplinar que de forma direta ou indireta lida com o tratamento de dados pessoais.

É iniciado o preenchimento seguindo a ordem da direita para a esquerda e de cima para baixo, iniciando em "Dados Pessoais" e finalizando em "Segurança".

Figura 2. Framework LGPD Model Canvas



Os blocos do LGPD estão descritos no Quadro 01.

Quadro 1. Blocos do LGPD Model Canvas

BLOCO	DESCRIÇÃO
Dados pessoais	Analisar o ciclo de vida dos dados pessoais, desde a coleta até o descarte. Levantar todas as categorias de dados pessoais e destacar aqueles que são considerados sensíveis perante a LGPD, para posteriormente analisar as bases legais que podem ou não, legitimar a coleta.
Fonte	Analisar de quais fontes os dados podem ser obtidos do titular, incluindo são só os canais oficiais de comunicação, como também os informais que podem fazer parte do dia a dia, como por exemplo: envio dos dados do cliente via WhatsApp. Todos os meios possíveis para receber os dados pessoais, devem ser considerados.
Propósito	Analisar qual a finalidade para a realização do tratamento dos dados, porque existe esta necessidade de tratamento. Importante refletir se todos os dados que são coletados (coluna 1) são imprescindíveis para a finalidade pretendida. Se houver algum dado que não tem um propósito claro, uma necessidade específica para tratamento, deve ser analisada a possibilidade de excluí-lo da coleta.
Base Legal	Analisar de acordo com a LGPD (Art. 9º) quais as bases legais que autorizam a coleta dos dados pessoais. Importante também verificar se está descrito de forma clara e transparente a finalidade para que os dados do titular estão sendo coletados e tratados.

Cronograma	Analisar o ciclo de vida dos dados pessoais e as bases legais que autorizam o tratamento dos dados pessoais, para verificar por quanto tempo podem permanecer armazenados e após o alcance da finalidade pretendida ou cancelamento de contrato, por mais quanto tempo devem permanecer até o descarte. Desta forma, deverá ser preenchido o cronograma referente ao armazenamento e descarte dos dados pessoais.
Direitos	Analisar de que forma a empresa está demonstrando os direitos dos titulares, donos dos dados e de que forma está estruturada para atender estas solicitações. Levar em consideração o capítulo 3 da LGPD, exclusivo sobre os direitos dos titulares e procedimentos internos para a empresa analisar e resolver tais solicitações, tanto de clientes, prospects, colaboradores, ex-colaboradores e demais casos.
Transferência e compartilhamento	É comum que os dados pessoais de uma empresa sejam compartilhados com órgãos, outras empresas, para o alcance de determinadas finalidades. No entanto, as empresas precisam analisar como está a segurança e o cumprimento da LGPD especialmente por outras empresas que tratam dados pessoais em seu nome, como terceiros, parceiros e fornecedores. Além disso, é necessário analisar se estes processos de compartilhamento estão de acordo com as bases legais levantadas ou regulamentadas por contratos que incluem cláusulas relacionadas ao cumprimento da LGPD e acordos de confidencialidade. Importante ressaltar também que os dados podem ser transferidos para outros países, especialmente nos casos em que há o uso de *Cloud Computing* e neste caso, deverá estar em conformidade com o capítulo V da LGPD. Nos casos em que a empresa não tem base legal para o compartilhamento com terceiros, exemplo em casos de promoção e marketing, deve solicitar o consentimento do titular de forma clara e objetiva.
Armazenamento	Analisar de que maneira os dados pessoais estão armazenados, seja de maneira estruturada ou não estruturada, como por exemplo: planilhas, banco de dados, sistemas, arquivos texto, no aparelho celular do colaborador, redes sociais, na pasta de rede da empresa, em repositórios cloud ou no armazenamento local, na máquina do colaborador. Importante lembrar também dos dados pessoais salvos em pen-drive e hd-externo. Importante analisar também o nível de controle de acesso e permissões vinculadas, de acordo com perfis.
Segurança	A segurança da informação é considerada uma premissa para a proteção de dados, desta forma, precisamos analisar se os dados estão protegidos contra acessos indevidos, que podem ocasionar violações. Da mesma forma, é fundamental analisar se a empresa possui política de segurança da informação implementada, divulgada internamente e reforçada em workshops e treinamentos. A criptografia deverá ser prevista para os dados pessoais tanto em repouso quanto em trânsito, pois em caso de violação os mesmos pelo menos devem estar em um formato ininteligível. Importante reforçar que a segurança da informação deve ser uma premissa desde a concepção de novos projetos e deve fazer parte do direcionamento estratégico das empresas, pois demandará investimentos em profissionais especializados e ferramentas.

Durante a aplicação do framework nota-se que as visões, experiências e vivências sobre os processos que tratam dados pessoais são complementadas por perfis multidisciplinares e compartilhadas.

O processo de mapeamento de processos que tratam dados pessoais, por meio da aplicação do framework, faz com que os colaboradores que participem da dinâmica se tornem verdadeiros facilitadores e os grandes responsáveis pela privacidade e proteção de dados em suas respectivas áreas, ao colocar a "mão na massa" e propor as devidas ações, soluções e melhorias.

A privacidade deve ser considerada desde o início/concepção do projeto e incorporada durante todo o processo, assim, o método LGPD Model Canvas será aplicado em dois momentos:

1- AS IS: partindo de uma "foto do momento atual da empresa" onde todos os processos existentes, que realizam o tratamento de dados pessoais serão levantados. No entanto, para que a adequação seja efetiva de fato, a equipe de colaboradores da empresa precisa "colocar a mão na massa" e visualizar como a privacidade e proteção de dados influencia e reflete no seu dia a dia nos serviços empresariais. Essa ideia vai de encontro com as considerações de Vidal (2006), que diz que o ponto mais vulnerável em um sistema computacional também é o componente humano. Dessa forma, somente documentos, ferramentas, tecnologias e treinamentos de conceitos não podem resolver todas as questões de privacidade e conformidade nas organizações.

Nesse cenário, visando criar uma dinâmica participativa, colaborativa, ágil e eficaz, o LGPD Model Canvas pode ser aplicado e incorporado às práticas e rotinas da empresa, assim como ocorre com os métodos ágeis, a exemplo do SCRUM. Dessa forma, a empresa cresce em aprendizagem organizacional, torna a privacidade parte da sua cultura e forma pessoas que serão os facilitadores internos, para tratar no dia a dia das questões de privacidade ao longo dos projetos de forma proativa e sem silos (departamentos). A empresa ganha independência, autonomia, agilidade, e assim não precisa ficar dependente de terceiros para tratar todas as questões de privacidade e proteção de dados.

2- TO BE: "O projeto LGPD não tem fim." O tema privacidade e proteção de dados não pode ser tratado apenas como um único projeto que tem data de início e fim e depois esquecido. Deve ser visto e respeitado como um programa que garante sua continuidade dentro da organização e permeia por todos os projetos que diretamente ou indiretamente lidam com dados pessoais. Dessa forma, a organização poderá aplicar o método LGPD Model Canvas sempre que surgir uma nova demanda: seja um novo projeto, produto, serviço, evento, aplicativo ou campanha de vendas. Recomenda-se que o ideal é aplicar logo nos estágios iniciais, como por exemplo, após o pontapé inicial do projeto. Analisar os processos e as soluções tecnológicas que podem acarretar algum risco para a privacidade e liberdade dos usuários, logo nos estágios iniciais, permite que a organização possa ajustar no início, quando é mais barato e fácil de corrigir.

Estágios para Aplicação do Método

Ao aplicar o framework LGPD Model Canvas, seja para o mapeamento AS IS ou TO BE, a organização deverá levar em conta os seguintes estágios até a aplicação do método:

- Processo de brainstorming para concepção da cultura de privacidade:

De acordo com Brown (2010) o brainstorming demonstra o seu valor quando a meta é abrir uma ampla variedade de ideias. Reforça que outras abordagens são importantes para fazer escolhas, mas que não há nada melhor do que uma boa sessão de brainstorming para criá-las.

Durante o brainstorming com os colaboradores da empresa serão levantados a vivenciar a cultura organizacional, para que possam incluir a privacidade no centro dos processos, como um valor fundamental para toda a organização, corroborando com as ideias da metodologia *Privacy by Design*. Durante esta etapa é questionada a missão, a visão e os valores da organização. Logo em seguida, a privacidade é relacionada neste contexto: O que significa a privacidade de dados pessoais para a organização e como ela se relaciona com a sua missão, visão e valores.

- Alinhamento sobre os conceitos e fundamentos da LGPD:

Para que todos possam "estar na mesma página" se faz necessário compreender sobre a Lei Geral de Proteção de Dados e seus principais, conceitos e fundamentos, um workshop ou

treinamento é recomendável para a contextualização de todos os colaboradores que participarão da aplicação do LGPD Model Canvas.

Metodologia

Para responder à questão de pesquisa e atender ao objetivo da pesquisa, os seguintes métodos de pesquisas foram utilizados:

A primeira etapa foi a pesquisa bibliográfica em livros, artigos científicos, teses e dissertações sobre os temas privacidade, LGPD, Modelo de negócios Canvas e LGPD model Canvas para elaborar o arcabouço teórico.

A segunda etapa foi a elaboração do instrumento de pesquisa que consistiu em um roteiro de entrevistas semiestruturadas com perguntas abertas e fechadas, o processo selecionado foi admissão de funcionário realizado pelo RH. Após a realização do processo de recrutamento/seleção e aprovação do candidato em todas as etapas, os documentos são enviados para realização da admissão do colaborador na empresa. O roteiro com as perguntas está no apêndice A.

A terceira etapa consistiu nas entrevistas com os gestores das empresas que utilizaram o LGPD model Canvas conforme as descrições no Quadro 2. Foram entrevistados o principal responsável de cada departamento da empresa, que possui o tratamento de dados pessoais. Os questionamentos foram feitos de forma coletiva e colaborativa, seguindo os pilares do Design Thinking, optamos por colocar as áreas em conjunto: "várias cabeças juntas, vão pensar melhor do que uma sozinha".

Quadro 2. Características dos entrevistados

EMPRESA	ÁREA	CARGO OU FUNÇÃO
Monitoramento e Segurança	RH	Gestor de RH
	TI	Analista de TI Sênior
	Administrativo	Assistente administrativos
	Operações	Gestor de Operações
	Comercial/Marketing	Analista de Marketing
	Alta Direção	Diretoria
	Atendimento ao Cliente	Analista de atendimento e atenção ao cliente

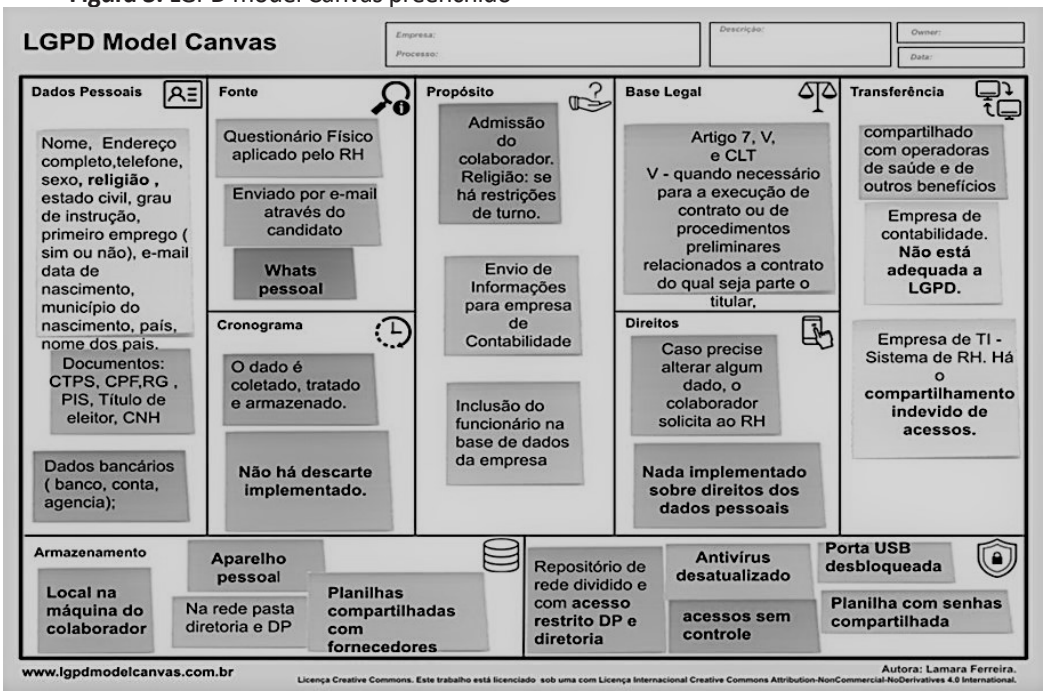
Fonte: Autores

As entrevistas, juntamente com outras fontes de evidências como observação direta e fontes secundárias de informações, serviram para a base dos estudos de casos. Para Yin (2001), um estudo de caso é: "uma investigação empírica que investiga um fenômeno contemporâneo dentro de seu contexto da vida real, e, quando os limites entre o fenômeno e o contexto não estão claramente definidos". E com relação à questão de pesquisa, o estudo de caso procura responder "como" e "por que" um fenômeno acontece; não exige controle sobre os eventos comportamentais; e ainda possui enfoque nos acontecimentos contemporâneos (Yin, 2001). Os resultados e análises das entrevistas estão no próximo tópico.

Resultados e discussão

A Figura 3 apresenta o LGPD model Canvas preenchido com de acordo com as entrevistas realizadas.

Figura 3. LGPD model Canvas preenchido



Fonte: Autores

Ao realizar o preenchimento de cada coluna analisando as questões pertinentes, surgiram 13 pontos de atenção, que podem levar a falta de cumprimento dos princípios e capítulos da Lei Geral de Proteção de Dados, no processo de admissão, relacionados aos seguintes pontos que foram destacados nos post-its no formato em negrito:

- Dados pessoais: O campo religião é um dado sensível perante a LGPD e a empresa não possui uma base legal para coletá-lo. A finalidade dele, coluna propósito é analisar se o colaborador possui alguma restrição de horário, visto que será necessário em alguns casos trabalhar à noite e final de semana. Como sugestão para o plano de ação é revisar este processo e alterar o questionamento da religião por: "Há alguma restrição de horário e para trabalhar aos finais de semana?";
- Fonte: Foi verificado que o colaborador do RH em alguns casos, recebe as informações da ficha de admissão via WhatsApp pessoal, o que aumenta as chances de um vazamento, pois não há qualquer controle implementado neste caso. Como sugestão para o plano de ação é revisar a utilização do WhatsApp pessoal.
- Transferência: A empresa compartilha dados pessoais para a empresa de contabilidade que não está adequada a LGPD. Da mesma forma, compartilha os dados com o fornecedor de TI que cuida do sistema de RH da empresa e solicita as credenciais dos colaboradores, havendo uma violação clara de segurança da informação, que pode levar ao comprometimento dos dados pessoais.
- Cronograma: Os dados nunca são descartados, desta forma, a empresa possui todos os dados desde o primeiro colaborador. Como sugestão para o plano de ação a empresa deve analisar os períodos que necessitam armazenar os dados após a demissão, de acordo com a legislação trabalhista e implementar na rotina.
- Direitos: A empresa não apresenta os direitos dos colaboradores como titulares dos dados pessoais e não está preparada para atender as solicitações. Como sugestão no plano de ação, recomendamos que a empresa crie a política de privacidade englobando os direitos dos titulares e disponibilize uma central de privacidade na Intranet, para receber e tratar tais solicitações, de acordo com procedimentos.
- Armazenamento: Foi verificado que apesar de haver uma pasta na rede compartilhada com o setor de RH, o colaborador também armazena os dados localmente em sua máquina, violando a política de segurança da informação. Da mesma forma, estes dados também permanecem no seu

celular pessoal, quando são enviados via *WhatsApp*. Além disso, verificamos que os fornecedores também acessam planilhas com os dados pessoais dos colaboradores, o que poderia ser consultado no sistema, sem haver a necessidade de estruturar e armazenar em planilhas.

- Segurança da informação: Foi verificado que os acessos estão sem qualquer tipo de controle, desta forma, qualquer colaborador pode ter acesso aos dados pessoais, independente de setor, função ou cargo, o que claramente representa um alto risco para violação dos pessoais, tendo em vista que estas informações, podem cair na mão de quem não poderia ter acesso. Também foi identificado que as estações de trabalho e servidores estão com os antivírus desatualizados, o que representa um problema crítico de segurança. Além disso, foi identificado que as portas USB estão desbloqueadas, o que pode facilitar a cópia e uso indevido dos dados pessoais, sobretudo mais um risco de segurança da informação ao injetar dispositivos que podem estar infectados.

Analisamos que o processo visual, colaborativo e multidisciplinar, para levantamento dos processos que tratam dados pessoais, no presente estudo de caso, representado pelo processo de admissão, permitiu identificarmos 13 vulnerabilidades que precisam ser corrigidas e direcionadas no plano de ação. Estes ajustes podem estar relacionados tanto a medidas organizacionais como melhoria de processos, quanto técnicas que podem demandar ajustes nos sistemas e implementação de ferramentas.

Foi percebido também que o realizar o mapeamento preenchendo no LGPD Model Canvas, gerou um grande engajamento pelas diversas áreas da empresa e foi possível perceber a clara compreensão do que precisa ser considerado em nossas atividades quando realizamos o tratamento dos dados pessoais.

Conclusão

Após o diagnóstico de conformidade do processo de admissão da empresa de segurança perante a à LGPD, ficou claro que o LGPD Model Canvas pode ser utilizado como uma ferramenta para mapeamento das informações dos processos que tratam dados pessoais e levantamento de vulnerabilidades.

Durante a aplicação do framework nota-se que as visões, experiências e vivências sobre os processos que tratam dados pessoais são complementadas por perfis multidisciplinares e compartilhadas.

O processo de mapeamento de processos que tratam dados pessoais, por meio da aplicação do framework, faz com que os colaboradores que participem da dinâmica se tornem verdadeiros facilitadores e os grandes responsáveis pela privacidade e proteção de dados em suas respectivas áreas, ao colocar a "mão na massa" e propor as devidas ações, soluções e melhorias.

Como pesquisas futuras propõe-se o uso do LGPD model Canvas em outras áreas e empresas para as pesquisas.

Referências

BLACK, Stewart et al. Design thinking. **Organizational Behavior**, 2019.

BRASIL. Lei Geral de Proteção de Dados Pessoais (LGPD**). Lei nº 13.709,** de 14 de agosto de 2018. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm . Acesso em: 20 mar. 2021.

BROWN, **Tim. Design Thinking:** uma metodologia poderosa para decretar o fim das velhas ideias. Rio de Janeiro: Campus, 2010.

BURKETT, Ingrid. **Using the business model canvas for social enterprise design**. Recuperado de http://knode.com.au/wp-content/uploads/Knode_BusModCanv4SocEntDesign_E1LR_30p.pdf , 2013.

BUSINESS MODEL GENERATION. Recuperado de http://www.businessmodelgeneration.com, 2015.

CAVOUKIAN, Ann . «Cavoukian, Ann. "7 Foundational Principles"» (PDF). "Privacy by Design The 7 Foundational Principles". **"Information and Privacy Commissioner of Ontario"**. agosto de 2009

CLARK, T.; OSTERWALDER, A.; PIGNEUR Y. **Business Model You:** o modelo de negócios pessoal. Alta Books, Rio de Janeiro, RJ, Brasil. 2013.

GROSSI, Bernardo Menicucci (Org.). **Lei Geral de Proteção de Dados:** Uma análise preliminar da Lei 13.709/2018 e da experiência de sua implantação no contexto empresarial, Porto Alegre, RS: Editora Fi, 2020.

GUNTHER, L. E., COMAR, R. T., & RODRIGUES, L. E. A Proteção e o Tratamento Dos Dados Pessoais Sensíveis Na Era Digital e o Direito À Privacidade: Os Limites Da Intervenção Do Estado. **Relações Internacionais no Mundo Atual**, 2(27), 25-41. 2020

GÜRSES, Seda; TRONCOSO, Carmela; DIAZ, Claudia. Engineering privacy by design. **Computers, Privacy & Data Protection**, v. 14, n. 3, p. 25, 2011.

MAGACHO, Bruna Toledo Piza; TRENTO, Melissa. LGPD e compliance na Administração Pública: O Brasil está preparado para um cenário em transformação contínua dando segurança aos dados da população? É possível mensurar os impactos das adequações necessárias no setor público. **Revista Brasileira de Pesquisas Jurídicas**, v. 2, n. 2, 2021.

MARTINI, S. R., & BERGSTEIN, L. G. Aproximações entre o direito ao esquecimento e a lei geral de proteção de dados pessoais (LGPD). **Revista Científica Disruptiva**, 1(1), 160-176. 2019

OSTERWALDER, ALEXANDER. **The Business Model Ontology:** A Proposition In A Design Science Approach. 169 F. Tese (Doutorado) - University Of Lausanne, Lausanne 2004.

OSTERWALDER, Alexander; Pigneur Y. **Business Model Generation:** Inovação Em Modelos De Negócios. Alta Books, Rio de Janeiro, RJ, Brasil. 2011

SERPRO. **LGPD entra em vigor, 18 set. 2020**. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/lgpd-entra-em-vigor . Acesso em: 22 mar. 2020.

VASCONCELOS, Kleber. **Os benefícios da implementação da LGPD.** SERPRO, 26 out. 2020. Disponível em: https://www.serpro.gov.br/lgpd/noticias/2020/beneficios-riscos-lgpd-empresas . Acesso em: 10 nov. 2020.

VIDAL, M. T. V. L. **Segurança em redes**. Niterói: UFF, 2006.

YIN, R.K. **Estudo De Caso: Planejamento E Métodos**. Porto Alegre: Bookman, 2001

Recebido em 21 de agosto de 2022.
Aceito em 20 de setembro de 2022.