CENTRO UNIVERSITÁRIO BRASILEIRO - UNIBRA
CURSO DE GRADUAÇÃO TECNÓLOGO EM
REDES DE COMPUTADORES

ELLOYSE VICTÓRIA GONÇALVES SILVA

LUCAS MATIAS MANÇO

PEDRO AUGUSTO RODRIGUES LINS

A APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS EM UMA CONCESSIONÁRIA DE VEÍCULOS DO RECIFE: ANÁLISE DA IMPORTÂNCIA DO TI

RECIFE/2022

ELLOYSE VICTÓRIA GONÇALVES SILVA

LUCAS MATIAS MANÇO

PEDRO AUGUSTO RODRIGUES LINS

A APLICABILIDADE DA LEI GERAL DE PROTEÇÃO DE DADOS EM UMA CONCESSIONÁRIA DE VEÍCULOS DO RECIFE: ANÁLISE DA IMPORTÂNCIA DO TI

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro – UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professor(a) Orientador(a): Msc Ameliara Freire Santos de Miranda

RECIFE/2022

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 1745.

S586a Silva, Elloyse Victória Gonçalves

A aplicabilidade da lei geral de proteção de dados em uma concessionária de veículos do Recife: análise da importância do TI. / Elloyse Victória Gonçalves Silva, Lucas Matias Manço, Pedro Augusto Rodrigues Lins. - Recife: O Autor, 2022.

38 p.

Orientador(a): Ma. Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2022.

Inclui Referências.

1. Segurança de dados. 2. Implementação da LGPD. 3. Proteção empresarial. I. Manço, Lucas Matias. II. Lins, Pedro Augusto Rodrigues. III. Centro Universitário Brasileiro - UNIBRA. IV. Título.

CDU: 004

Dedicamos este trabalho aos nossos familiares.

AGRADECIMENTOS

Agradecemos primeiramente a Deus por nos dar força de vontade e saúde para escrevermos este trabalho.

Aos nossos pais por todo o carinho, positividade e alento que nos deram.

Aos professores que nos auxiliaram em toda nossa trilha da graduação.

Aos nossos amigos que entenderam nosso momento de reta final no curso e a todos que nos ajudaram de alguma forma para estarmos aqui findando mais um ciclo da vida estudantil.

“A melhor maneira de prever o futuro é inventá-lo.”

(Alan Kay)

A LGPD EM UMA CONCESSIONÁRIA DE VEÍCULOS DO RECIFE: ANÁLISE DA IMPORTÂNCIA DO TI

Elloyse Victória Gonçalves Silva

Lucas Matias Manço

Pedro Augusto Rodrigues Lins

Orientadora Msc. Ameliara Freire Santos de Miranda

RESUMO

O presente trabalho atentou-se em trazer noções de problemas sobre vazamento de dados, a implementação da LGPD e o papel do agente de TI dentro da empresa para a segurança destes a coleta dos dados cadastrais particularmente os cadastros de pessoas físicas CPF, endereço, financeiro e entre outros, tanto no sentido de dados do cliente ou da própria empresa. Não tivemos autorização para divulgar o nome da empresa, foi analisado o sistema de prospecção de dados dos clientes e para onde eles vão, enfrentamento a pandemia do covid-19, se a empresa conta com profissional de DPO, e como se tornar um, além de explanar qual era o trabalho feito em conjunto para que a LGPD fosse respeitada na empresa, contando com os profissionais de TI, o grupo jurídico, sistema FANDI e DPO.

Palavras-chave: Segurança de dados; implementação da LGPD; Proteção empresarial.

LISTA DE ILUSTRAÇÕES

LISTA DE ABREVIAÇÕES

DPO	Data Protection Officer
F&I	Financial & Insoure
LGPD	Lei Geral Proteção de Dados
TI	Tecnologia da Informação

SUMÁRIO

1. INTRODUÇÃO

E notório que empresas se modernizaram, e é reflexo do que ocorreu nas décadas passadas na própria humanidade. Antes os dados pessoais ficavam arquivados e amontoados em pastas e salas, que eram usadas apenas para guardar estes dados. Com o aumento de dados junto ao avanço da tecnologia e com o baratear do seu custo, as empresas passaram a arquivar dados nos computadores, o que facilitaria inclusive para o compartilhamento dentro da empresa (com outros setores) ou com seus associados.

Segundo Sagan (1987, p.37) a sociedade como um todo "dependem profundamente da ciência e da tecnologia"

Com o desenvolvimento da informática, as informações foram difundidas,afinal, com o desenvolvimento da Internet e da própria informática, adentramos na sociedade da informação[1]; do fácil acesso à mesma. A dependência da informática para o processamento dos dados, atualmente, nos faz lembrar que vivemos em uma sociedade de redes e que este tear é de suma importância para a sociedade, afinal estamos interligados fortemente no que chamam de ciberespaço. Segundo MONTEIRO (2007) “Uma representação gráfica de dados abstraídos dos bancos de dados de todos os computadores do sistema humano”. E o que antes era processado e arquivado em caixas de papelão em escritório, estão armazenados em nuvens, programas ou computadores de uso empresarial.

As mudanças são bem-vindas quando a sociedade consegue economizar tempo, espaço e até mesmo contribuir com a ideia verde/sustentável. Como deixou-se de armazenar dados em papéis e passou-se a utilizar um computador[2] para fazê-lo, surgiu uma nova falcatrua sobre o uso de dados através da invasão de redes e de computadores com a finalidade de se beneficiarem com os dados pessoais de outros, surgindo assim os crimes virtuais de roubo de dados.

Com tantos crimes virtuais em nossa sociedade, com o alto valor que os dados possuem no mercado ilegal[3] e por ser um tema recorrente na mídia brasileira,

---

[1] Termo utilizado por Castells (2000)

[2] Revolução do computador disponivel em: https://brasilescola.uol.com.br/informatica/revolucao-do-computador.htm

se fez necessário pensar acerca da proteção destes dados em todas as esferas que compartilham dados pessoais.

Neste ano, o Banco Central comunicou mais de 130 mil dados pix vazados (MALAR, 2022), e segundo Wellton Máximo (2022) estes dados são de apenas uma empresa, a Abasteci Aí, que aclarou sobre o fato [que] “a exposição de dados não significa necessariamente que todas as informações tenham vazado, mas que ficaram visíveis para terceiros durante algum tempo e podem ter sido capturadas” (MÁXIMO, 2022).

Entretanto, há vazamentos de dados que comprometem os cidadãos, e é o caso das chaves-pix que são utilizadas o CPF destes usuários. Outro exemplo de vazamento de dados amplamente divulgado foi o trazido por Fernandes (2022), para a Isto é Dinheiro, no Ministério da Economia, contando com vazamento de 20 mil selfies e dados, além do RG destes usuários.

Um assunto de relevância nos últimos anos, segundo a VC S/A, em 2021 houve um aumento de 493 milhões no Brasil[4] de vazamento de dados, e empresas que deixam brechas correm o risco de pagarem altas multas, além de perder credibilidade em seu serviço, afinal a mídia mostra a sensibilidade na guarda de dados dos clientes. Neste trabalho alavancar-se-á a importância de um profissional de TI em uma empresa, precisamente iremos analisar a implementação realizadaem 2018 em determinada empresa de Venda de veículos, em Recife, Pernambuco. Tendo em vista o que houve em 2021 do vazamento dos dados de 100 milhões de veículos no Brasil[5], a referida empresa se adiantou em seguir a Lei de Proteção de Dados e se safou do prejuízo e de perder seu prestígio entre seus atuais e futuros clientes.

1.1 JUSTIFICATIVA

---

[3] Também chamado de submundo da internet ou ainda mercado clandestino, em que são vendidos ilegalmente diversos dados, objetos, drogas, órgãos, dentre outros, que por se tratar de um espaço mais profundo (deep web) é mais difícil se conseguir saber de onde está saindo aquela mercadoria ou qual o IP do usuário.

[4] Matéria disponível em: https://vocesa.abril.com.br/sociedade/vazamentos-de-dados-aumentaram-493-no-brasil-segundo-pesquisa-do-mit/ Acesso em 17 out. 2022

[5] Segundo Felipe Ventura, em matéria para o TecnoBlog, disponível em: https://tecnoblog.net/noticias/2021/01/25/exclusivo-os-detalhes-do-vazamento-sobre-100-milhoes-de-veiculos-no-brasil/ Acesso em 17 out. 2022

A Lei Geral de Proteção de Dados, que entrou em vigor em 2018, sob o nº 13.709, as empresas buscaram se adequar a esta nova realidade deproteção. O profissional de TI é essencial para que a LGPD ocorra, uma vez quepara ser implantada nas empresas, é necessário o apoio do *D*PO, profissional que é encarregado, fazendo uma ponte entre as informações fornecidas pelo cliente e da empresa, fornecendo segurança contra o uso inadequado dos dados e mitigando possíveis ciberataques.

O profissional de TI que faz com que a LGPD seja aplicada dentro da empresa, gente principal da ação de proteção. Dada a importância da segurança do armazenamento de dados, tanto por vias legais como por vias trabalhistas, este é um tema relevante no mundo cibernético, motivo pelo qual escolhemos abordar a temática.

Além do mais, os profissionais desta área, são fundamentais para oferecer os serviços às empresas tendo um bom conhecimento tanto das leis como dos programas e ações que se pode gerir, a fim de fidelizar estes clientes que necessitam estar em conformidade com a Lei.

1.2 OBJETIVOS GERAIS E ESPECÍFICOS

O objetivo geral é conhecer o funcionamento da LGPD em empresa de veículos e a importância das ações que o profissional de TI deve promover para que haja o funcionamento correto do uso dos dados dos clientes, evitando o vazamento destes. Visando a problematização destes vazamentos em uma empresa com alto fluxo de dados cadastrais, como a de venda de carros.

Tendo em vista que o profissional de TI, o DPO, precisa saber as Leis Gerais de Proteção de Dados, iremos:

- Descrever melhor os objetivos da LGPD;
- Conhecer a doutrina que é utilizada para a LGPD;

- Entender as ações necessárias do profissional de TI;
- Identificar como funciona a captação de dados na empresa de veículos em questão.

1.3 METODOLOGIA DE PESQUISA

Esta pesquisa possui o desenvolvimento como estudo de caso, o critério principal foi trazer uma coleta de dados entrevistando o funcionamento da LDPG dentro da concessionária de veículos, incrementamos trabalhos dos últimos dois anos, que estivessem publicados em Revistas Acadêmicas diversas e encontrados em portais como Scielo, Google Acadêmico e portais de artigos. Incluímos na nossa pesquisa casos de outras áreas, principalmente da área de direito, por estar em associação com a temática e, inclusive, para descrever a Lei Geral de Proteção de Dados e outro critério foi o trabalho estar em português e serem da área de TI ou de Rede de Computadores, com a temática dos problemas que podem surgir com o vazamento de dados, tanto para as empresas que não forem cautelosas quanto para os clientes destas, através de pesquisas aproximativas e explanativas ao tema em questão.

É descritiva, afinal descrever-se-á a Lei que já está em vigor e qual é o papel do profissional de TI para a boa prática do compartilhamento de dados e sua devida segurança.

Haverá abordagem de reportagens que tratam da temática de vazamento de dados e de como devemos nos precaver destes roubos cibernéticos de dados em empresas.

2. REFERENCIAL TEÓRICO

Em 14 de agosto de 2018 foi sancionada no Brasil a lei nº 13.709, através do vice-presidente Michel Temer, mais conhecida como Lei Geral de Proteção deDados (LGPD), essa sendo uma lei inspirada em um regulamento europeu: Regulamento Geral sobre a Proteção de Dados (GPDR), que garante o direito à privacidade e proteção de dados de cidadãos europeus. (MACIEL, 2019)

No Art. 1º da LGPD, informa-se que objetivo da lei é proteger os dados pessoais, garantindo a liberdade e a privacidade do titular destes dados, que ora foram recolhidos por empresas ou por outros. Diferente de quando se fala doCódigo do Consumidor e do Marco Comum da Internet, que é frouxo com relação aos dados pessoais em nosso país. A LGPD regulamenta esta proteção e possui diretrizes tanto para o uso como para a transferência destes dados pessoais, além de fazer com que as empresas sejam suscetíveis a pagar pelos erros dessesvazamentos de dados.

> Art. 1°. a lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica dedireito público ou privado, com o objetivo de proteger os direitosfundamentais de liberdade e de privacidade e livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018)

Quando sinaliza-se sobre informações pessoais, fala-se de dois tipos dedados, de acordo com o Art 5º, incisos I e II, da lei de nº 13.709/2018. O primeiro inciso trata dos dados pessoais e afirma ser uma informação utilizada para identificaruma pessoa natural, ou seja, são dados simples. No inciso II, trata sobre os dados sensíveis, e o cunho é sobre a "[...] origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosóficoou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico" (BRASIL, 2018).

O titular dos dados precisa dar autorização para que o tratamento dos dados seja realizado (SOARES, 2019, p.11) e estas dependem das diretrizes:

1- Ser consentido pelo titular;
2- a regulamentação e o cumprimento de obrigação legal se dão pelo controlador destes dados;

3- a administração pública deve executar políticas públicas previstas em leis e regulamentos para o tratamento e uso compartilhado de dados necessários;
4- quanto às pesquisas ou realizações de estudos que a envolvam, os órgãos envolvidos devem manter os dados coletados anônimos;
5- se necessário (os dados) para executar um contrato ou algo relacionado, deve ser pedido pelo titular dos dados, não por terceiros;
6- pode-se utilizar os dados de outros somente em caso de processo judicial, administrativo ou arbitral (em acordo com a Lei nº 9.307/1996);
7- em casos de proteção à vida ou da incolumidade física do titular ou de terceiros;
8- com relação à serviços de saúde ou de autoridade sanitária;
9- quando for necessário atender aos interesses do controlador ou da empresa contratada;
10- para a proteção do crédito.

Vale ressaltar que a lei exige que as atividades de processamento de dados pessoais sigam os princípios de: objetivo, suficiência, necessidade, acesso livre, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilidade e contribuição, Art.6 da Lei n°. 13.709 de 14 de agosto de 2018 (BRASIL, 2018).

Sendo esclarecido o objetivo do querer os dados, se é suficiente os enviados/compartilhados, a necessidade de ser compartilhado todos aqueles dados (junto com a relevância do pedido), o poder acessar seus próprios dados armazenados, a transparência da empresa em pedir e compartilhar com outros bancos de dados, o ressaltar a segurança empenhada no armazenamento deste, as prevenções utilizadas para evitar um provável roubo de dados, o não discriminar por dados ora antes informado (por raça, religião ou qualquer outro dado), confirmar a sua responsabilidade como empresa guardiã de dados e a sua contribuição perante outros bancos de dados são os principais princípios para o processamento destes dados.

Partindo do que foi dito até aqui, fica claro que por conta da LGPD todas as organizações brasileiras empresariais ou não, sendo grande empresa ou pequena,

devem investir em segurança tecnológica para impedir violações de dados pessoais (ROCHA, 2019).

2.1 O VALOR DOS DADOS NO MERCADO DA DARK WEB

Criminosos lucram mais de 80 milhões com dados na *dark web*, segundo Júlio César Gonsalves (2022) em matéria para o Tech Tudo, e ainda afirma que “em levantamento recente feito pela NordVPN[6], empresa que fornece soluções em redes virtuais privadas há quatro categorias de informações à venda(...)”, sendo quase 50% sendo de documentos, quase 40% dados financeiros, mais de 10% sendo de contas e com 6% e-mails e senhas.

Resultado da globalização, além de estarmos informados e conectados, é o valor dado para a informação, transformando-a em um material de alto valor no mercado e com relevância alta, seja para órgãos públicos ou privados, sendo assim, “quem tem acesso aos dados, tem acesso ao poder” (PINHEIRO, 2018, p. 50).

E este poder está em ser onisciente e com base nos dados de determinada pessoa ‘oferecer’ produtos que ela tenha interesse, seja em propagandas dentro de sites visitados, em jogos online, aplicativos ou até mesmo em redes sociais.

Além de programar alertas de promoções para produtos que possivelmente entram no nicho daquela pessoa analisada, de acordo com o que foi consumido antes e até mesmo visto em outras plataformas. Nesse sentido Silva e Silva afirmamque:

> O crescente uso das tecnologias da informação e da comunicação, em especial da Internet, imprimiu maior dinamicidade às relações econômicas, à participação política e às interações sociais, redesenhando as formas de ser e estar no mundo. Em nenhum outro momento histórico foi tão fácil e rápido acessar informações, produzir e compartilhar conteúdos, comunicar e interagir em sites de redes sociais, blogs e microblogs, tudo de maneira instantânea. O intenso desenvolvimento capitaneado pelo segmento de Tecnologias da Informação (TI) acelera ainda mais esse processo, pois a cada dia são lançados no mercado novos equipamentos, aplicativos, plataformas e ferramentas que maximizam a experiência de

[6]Matéria sobre os testes realizado pelo techtudo na plataforma NordVPN disponibilizadas em: https://www.techtudo.com.br/tudo-sobre/nordvpn

> navegação na web, o que faz com que um número crescente de pessoas almeje a inclusão digital (SILVA e SILVA, 2013, p. 2).

Entretanto, infere-se que nem tudo é tão positivo, com o aumento de pessoas navegando na internet e a cada uso (seja de serviços oferecidos na hora ou respondendo à uma pesquisa) no ciberespaço permite-se cookies, e uma situação no supermercado, por exemplo, em que o cliente/usuário não tem conexão 4G, e precisa checar algo na internet, fará um 'pequeno cadastro, inofensivo' em que deixará nome, CPF, e-mail, idade e ao menos uma informação acerca do queconsumiu ou de sua preferência. Não se educou a sociedade para os meios virtuaise está entrega seus dados facilmente, pois não tem muita ideia em que resultará isso. A infinidade de formas de recolhimento de informações no dia a dia demonstraa 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, pois em simples atos, já os libera. (SILVA; SILVA, 2013, p. 2).

Não se pode apenas culpar os usuários inexperientes, a causa não é tão simplista, não se deve encher de culpas quem não teve conhecimento acerca de seus direitos, nem tão pouco a quem confiou que os dados estariam a salvo como caráter informativo para aquela empresa. É importante um trabalho em conjunto da empresa com o cliente (transparência) e a educação da sociedade como um todo, para que as pessoas entendam sobre os direitos que possuem se tratando de seus próprios dados, necessita-se de uma disseminação de informação acerca da LGPD para que se possa dispersar esse tipo de crime, tanto por conhecimento dos usuários bem como a segurança trazida pelas empresas com profissionais de TI voltados para essa temática.

2.2 FANDI

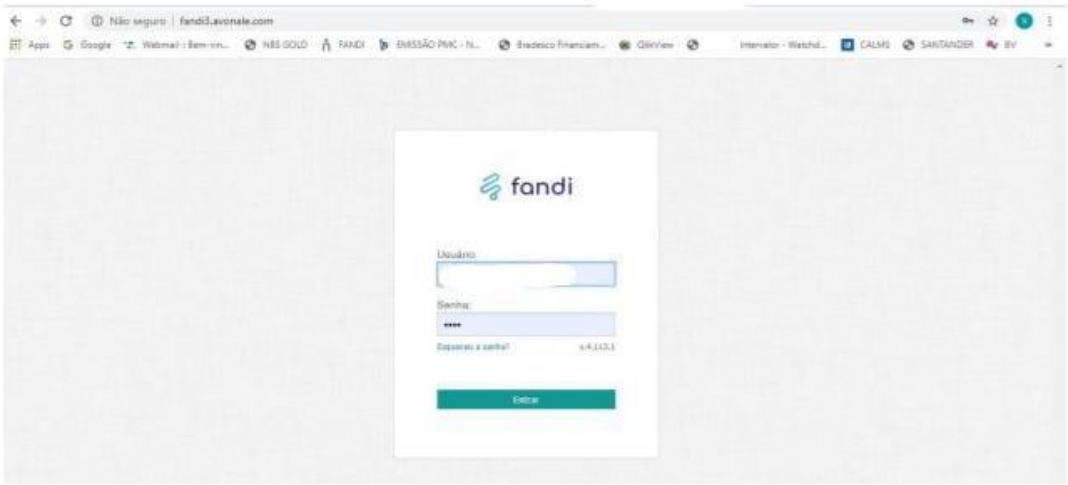
O sistema que armazena os dados pessoais desta empresa, se chama FANDI[7], e é, segundo o site da empresa uma fintech de consultoria e software como

serviço (SaaS) que possui mais de 800 funcionalidades e conecta clientes da revenda de veículos às principais Instituições Financeiras do Brasil. Existe desde 2004, e oferece ferramentas para agilizar o processo das vendas de veículos, tendo em seu sistema interligações com diversos bancos que fazem financiamento de veículos, como o Banco GM (da própria marca de carros ao qual a empresa trabalha), Santander, Banco do Brasil, Itaú, Bradesco e tantos outros. Para evitar qualquer problemática acerca de vazamento de dados, há uma parceria com uma grande empresa que armazena esses dados pessoais e que compartilha, apóssinalização do cliente, os dados com outros bancos, para aprovarem o crédito deste cliente. Salienta-se que antes da adesão da empresa ao sistema FANDI, início de 2018, não se tinha responsabilidade acerca dos dados dos clientes, só passou a ter depois que a LGPD entrou em vigor no Brasil.

O grupo do qual trata-se neste trabalho, possui outras filiais em Recife e todas elas contam com dois profissionais de TI, apoiando remotamente qualquer dificuldade encontrada pelos operadores que tomam conta do setor de aprovação decrédito, e estes se concentram em uma mesma rede de computadores, em uma mesma sala física, utilizando o mesmo sistema: o FANDI, que em seus termos de privacidade, se tratando das responsabilidades dos usuários do sistema afirma que não se responsabiliza pela instalação no equipamento do usuário ou de terceiros, devírus, trojans, malware, worm, bot, backdoor, spyware, rootkit, ou de quaisquer outros dispositivos que venham a ser criados, em decorrência da navegação na Internet pelo usuário, isso significa que é uma parceria entre o TI da empresa, do cuidar com possíveis ataques e eles, cuidando do armazenamento de dados no próprio sistema deles. A constância deste item se dá pelo fato de que o acesso ao FANDI é através de login e senha, como observa-se na Figura 1, e pode ser rompidopor algum usuário mal-intencionado que encaminhe um destes vírus ou algum tipode malware.

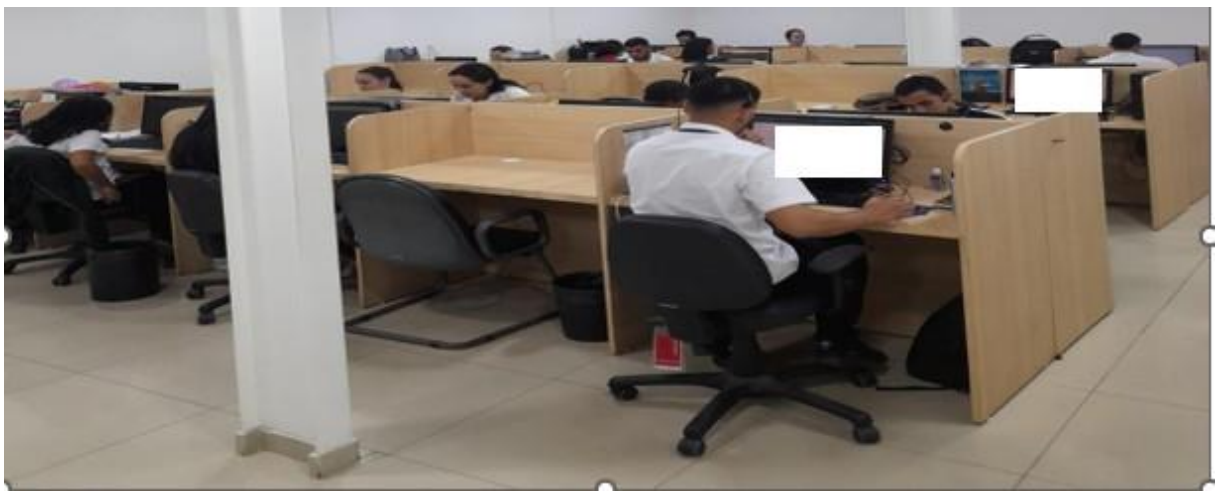
[7]Conheça a plataforma em: https://fandi.com.br

Figura 1- Acesso ao FANDI, através de um domínio próprio



Fonte: FANDI (2022)

Figura 2- Espaço físico desta rede de computadores em que os funcionários utilizam o FANDI.



Fonte: Autores

Este espaço foi implantado na sede oficial da loja de veículos assim que foi proposta uma quarentena por conta do COVID-19 aqui no Recife, enquanto puderam trabalhar, para que o sistema não fosse invadido, afinal foi na quarentena que o aumento de vazamento de dados se deu, justo por essa migração do home- office sem os devidos cuidados. A empresa em questão investiu pesado para que o sistema não fosse invadido nesta época, criando uma central, a qual vemos na Figura 2 e que continua atualmente e também, quando houve home-office destes funcionários os responsáveis pelo TI, ficaram encarregados de entrar remotamente

nos computadores pessoais dos colaboradores e fizeram alterações para que cada computador ficasse menos suscetível aos ataques, mesmo estando em um ambiente doméstico.

2.3 ACLARAÇÕES SOBRE A LEI GERAL DE PROTEÇÃO DE DADOS E QUAL A IMPORTÂNCIA DA SUA PRÁTICA NO SISTEMA FANDI EM CONCESSIONÁRIAS DE VENDAS DE VEÍCULOS

Para esclarecer o uso do sistema FANDI e a importância de aplicabilidade da LGPD, detalhar-se-á na Tabela 01 quais são os dados utilizados pelo FANDI e o funcionamento de atendimento e nos subcapítulos como são nomeados estes dados pela LGPD e qual a importância de pôr na prática a Lei.

Tabela 01- Dados recolhidos pelo FANDI

DADO COLETADO	**ETAPA**
CPF	1ª
Nome completo	1ª
Data de nascimento	1ª
Filiação	1ª
Número do RG	1ª
Endereço	2ª
Número do Telefone	2ª
Referências Pessoais	2ª
Número da CNH se possuir	2ª
Data de Validade da CNH	2ª
Banco Onde é Correntista	3ª
Agência Bancária	3ª
Número da Conta Corrente	3ª

Contato do Gerente	3ª
Vínculo Empregatício	4ª
Autônomo ou Assalariado	4ª
Nome da Empresa ou Órgão Público Onde Trabalha	4ª
Endereço da Empresa	4ª
Valor da Renda Mensal	4ª
Renda Extra se Possuir	4ª
Contato do RH em caso de CLT	4ª
Cargo/Função exercido	4ª
Patrimônio Comprovado	4ª
Marca/modelo do veículo à venda	5ª
Ano de fabricação do veículo	5ª
Valor de nota fiscal	5ª
Valor da entrada dada pelo cliente	5ª
Modo de pagamento da entrada	5ª
Número de Parcelas do financiamento	5ª
Placa do veículo – Seminovos	5ª
CPF do vendedor	6ª
Nome do vendedor	6ª
Telefone do vendedor	6ª
Nome do gerente de vendas responsável	6ª

Fonte: Os autores (2022)

Vale ressaltar que toda a coleta de dados do cliente é feita pelos vendedores, ou seja, tão logo o cliente e vendedor negociam a compra/venda em *showroom*, após demonstração do veículo, cotação de preços e demais determinantes comerciais inerentes a toda e qualquer transação comercial (lembrando que um automóvel é um bem de valor exponencial, sonho de consumo de milhões defamílias) tem-se um trabalho demorado nessa etapa da venda, por tal motivo, a área comercial da empresa costuma cobrar agilidade dos analistas de crédito após a coleta de dados, para que os mesmos deem uma devolutiva rápida e eficaz da liberação de crédito do cliente, arrematando a venda e finalizando a negociação.

O vendedor entrevista o cliente, armazena os dados dele no sistema FANDI e aguarda pela liberação e respostas de sua solicitação. Neste momento os analistas responsáveis recebem uma notificação de “análise em espera” e tratam de verificar a veracidade dos dados em fontes como Receita Federal, Serasa, além de ligarem para o cliente a fim de mitigar quaisquer dúvidas restantes.

2.4 O QUE A LGPD AFIRMA SOBRE ESTES DADOS E SEUS DESBRAVAMENTOS QUANTO À PRIVACIDADE

A LGPD em 4 tipos de dados, conforme a figura 3:

Figura 3- Tipos de Dados

Fonte: Informe CAPESESP (2021)

Os dados pessoais são os que em todo esse processo no FANDI é pedido, porém, por mais que não se trate de dados sensíveis, qualquer dado pode se tornar sensível. A LGPD entende estes dados, no seu Artº 5, inciso II: “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”.

Partindo-se do preceito que se pode traçar um perfil deste cliente com estas informações como, por exemplo, sua estrutura familiar e sua renda ou mesmo o vazamento de dados de onde trabalha e endereço empresarial, em mãos erradas, de criminosos, todos os dados são sensíveis, afinal, como afirma SÁ, 2019, apud LIMA, 2020, p.11:

> “A Lei Geral de Proteção dos dados Pessoais (LGPD) é um novo paradigma, pois envolve a alteração da maneira como as empresas lidam com dados pessoais de pessoas físicas nos meios online e offline e tem a função de proteger os direitos fundamentais de liberdade e privacidade em qualquer relacionamento que envolva dados pessoais”

A questão da liberdade e privacidade faz com que qualquer dado seja sensível, afinal, o direito à privacidade deve ser tratado segundo afirmações de RODOTÀ, 2008, p. 15 apud PEIXOTO; JÚNIOR, 2018, p.42, como “o direito de manter o controle sobre suas próprias informações e de determinar a maneira de construir a sua própria esfera particular”.

Pondo em xeque que o consumidor precisa saber onde está circulando os seus dados, a LGPD em um dos seus artigos, é afirmativa para a solicitação dotitular destes dados solicitarem à empresa, uma cópia com todas as suas informações e saber para quais finalidades foram usadas, um verdadeiro relatório, para saberem se foi utilizado esses dados apenas para o destino ao qual lhecompetia. E isso está no Art.9º

Um dos artigos da LGPD que é interessante analisar, trata-se de o titular dos dados (o cliente) poderá solicitar, junto a determinada empresa, uma cópia com todas as suas informações, bem como saber para que finalidades estas estão sendo usadas, conforme artigo 9º:

> Art. 9º O titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso: 22 I - finalidade específica do tratamento; II - forma e duração do tratamento, observados os segredos comercial e industrial; III - identificação do controlador; IV - informações de contato do controlador; V - informações acerca do uso compartilhado de dados pelo controlador e a finalidade; VI - responsabilidades dos agentes que realizarão o tratamento; e VII - direitos do titular, com menção explícita aos direitos contidos no art. 18 desta Lei (BRASIL, LGPD, 2020).

Isso significa que o titular destes dados, cliente de uma empresa que utiliza o sistema FANDI, pode escolher se seus dados podem ser compartilhados com todos os aliados financeiros que estão disponíveis na plataforma ou querer que sua ficha cadastral seja encaminhada a apenas determinado banco, e assim, consegue ter seu direito de privacidade respeitado.

Em um e-book informativo sobre a LGPD, o site O Consumerista[8], que trata das relações de consumo, traz um renomado especialista em LGPD e representante do Senado Federal no conselho da Autoridade Nacional de Proteção de Dados

[8]E-book disponível em: https://www.oconsumerista.com.br/lgpd

Pessoais (ANPD), o Fabrício da Mota Alves, para falar das relações entre titulares e empresas, quanto ao direito da privacidade e os casos na justiça acerca da temática:

> “As ações judiciais que começaram a mencionar a LGPD (antes mesmo de sua entrada em vigor) revelam que a sociedade passou a reatribuir o valor da privacidade como bem jurídico de grande relevância. O assunto agora vai exigir uma nova visão de risco e compliance especificamente dedicada à privacidade e às regulações em proteção de dados pessoais, uma vez que eventuais irregularidades poderão ter consequências financeiras e reputacionais elevadas” (O CONSUMERISTA, E-BOOK, 2021, p.10)

Evidenciando-se a privacidade do usuário e que estes dados podem serusados por pessoas mal intencionadas, destaca-se o pensamento europeu sobre a proteção de dados e dentre eles, destaca-se o italiano Rodotà (2008, p.56), que mostra que todos os dados merecem o devido cuidado e atenção, pois são dados privados, e dispensa a divisão de dados, crendo que todos: “(…) podem se tornar sensíveis se contribuem para a elaboração de um perfil; seja porque a própria esferaindividual pode ser prejudicada quando se pertence a um grupo do qual tenha sido traçado um perfil com conotações negativas”. Tomando como exemplo o preconceitocom o lugar de origem do usuário e em uma das análises feitas se é lançado o endereço e o número da casa ou apartamento no Google Maps para verem alocalização, antes de aprovarem a venda do carro, o que pode levar à levantamento de suspeitas de ‘como alguém em tais condições, em tal bairro, pode pagar x de parcelamento de carro?’, que pode levar à suspeitos ou apenas levantarproblemáticas sociais e preconceito por conta do lugar de origem do cliente.

Segundo Peixoto e Júnior (2018, p.43):

> A privacidade, a partir da visão europeia, mostra um novo perfil, apresentando-se como um direito a ter controle sobre as próprias informações e a determinar a maneira de construir a própria esfera particular – o direito à autodeterminação informativa. E isso é de extrema valia para a sociedade da informação, na qual a informação é um bem em si mesmo, é parte integrante da vida humana, em que as novas tecnologias surgem para atuar sobre esta mesma informação.

O direito à privacidade foi ganhando forma e forças, e na Constituição Federal de 1988, nos garante em seu artigo 5º que “são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. E evoluindo assim, até mesmoa lei dos anos 90, de nº 8.078/90, mais conhecida como Código de Defesa do Consumidor, previu o direito de o consumidor ter acesso às: “informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele”.

Mas, foi a partir do Marco Civil da Internet que a palavra “privacidade” passou a constar juridicamente no Brasil, estabelecendo deveres a serem observados dentro do ciberespaço. O Marco, de nº 12.965 informa que se inspiraram nosseguintes princípios na internet, em nosso país:

> “(...) liberdade, privacidade e direitos humanos; governança democrática e colaborativa; universalidade; diversidade; inovação; neutralidade da rede; inimputabilidade da rede; funcionalidade, segurança e estabilidade; padronização e in teroperabilidade e ambiente legal e regulatório”

E justamente por conta desse pensamento de ‘privacidade’ como um direito humano, não adianta apenas pensar em dados sensíveis e sim nos dados como um todo, para garantir que a lei seja implementada nos sistemas de armazenamento de dados, é necessário saber a importância do TI e o seu papel dentro desse malabarismo e as medidas de precaução para que não haja vazamento de dados.

2.5 IMPORTÂNCIA DE UM SISTEMA DE REDES FORTE CONTRA OS VAZAMENTOS DE DADOS

Nas políticas do Sistema FANDI, já se afirma que cada empresa é responsável sob a segurança da invasão do sistema pelas redes de computadores de dada empresa, como foi ressaltado anteriormente, tendo em vista essa observação, analisaremos o papel do TI para manter o funcionamento

antivazamento de dados, as medidas de precaução e a importância de se ter esse profissional fazendo a aplicabilidade da Lei Geral de Proteção de Dados acontecer.

3. O PAPEL DO TI E A IMPORTÂNCIA DESTE PROFISSIONAL NAS CONCESSIONÁRIAS DE VEÍCULOS

O papel do TI em concessionárias de veículos é justamente atuar na vigilância contra o ciberataque, e no caso desta empresa que foi o nosso estudo de caso, além dos profissionais de TI que trabalham dentro da empresa, ainda possuem um profissional encarregado, o Data Protection Officer (DPO), que orientaa equipe de TI, fazendo uma ponte entre os dados coletados pela instituição e seus compartilhamentos. Este profissional faz parte do contrato com o FANDI, com o consentimento do cliente e da empresa, há o compartilhamento de dados entre instituições bancárias e dentro do próprio sistema eles já sinalizam esse compartilhamento que gera uma lista de informações, e os dados circulam apenas entre consignatárias brasileiras, justamente para estar em conformidade com aLGPD, que regulamenta a proteção de dados dentro do sítio nacional.

Como os dados são computados de diversos computadores interligados, e compartilhado por diversos outras instituições bancárias, o processo de segurança não é algo tão simplista, é necessário que o pessoal de TI da empresa em Recife, por exemplo, tenha conhecimento da LGPD, algo que ocorreu antes da implementação do sistema FANDI, os dois profissionais de TI que existe nestaconcessionária receberam oficinas sobre a Lei e investimento de demais conhecimento que tenham a ver com ciberataques e vazamento de dados.

É um trabalho em equipe, em que o profissional DPO (também chamado de encarregado de tratamento de dados) é responsável pelo cumprimento das regras tratadas pela LGPD e é o profissional que está ali para responder e cumprir pelos direitos dos titulares dos dados (SOMBRA, 2019). O DPO desta concessionária é um profissional de TI, também, (e neste cargo-conselho, também há advogados especializados na temática de armazenamento de dados) que possui cursos que o destacam de outros profissionais, segundo matéria do Jornal Contábil (2020), citado por Esther Vasconcelos, como sendo estes:” o Information Security Foundation

(ISFS), Privacy&Data Protection Foundation (PDPF) e Privacy&Data Protection Practitioner (PDPP) do Instituto Internacional EXIN”.

E a parceria é evidenciada no trabalho de análise e de blindagem da rede, com testes que são feitos sazonalmente, com a finalidade de testar qualquer problemática. Além disso, esses profissionais devem alertar aos funcionários do F&I sobre o cuidado sobre segurança da informação. (ALERTA SECURITY, 2019)
Isto para estarem em conformidade à LGPD, que recomenda que:

> Artº. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais (BRASIL, 2018).

E as medidas são evitar o compartilhamento dos documentos dos clientes sem antes o check-up sazonal que os profissionais de TI fazem, além de não utilizarem o computador da empresa para pesquisas de cunho pessoal, não baixar nenhum tipo de documento sem antes passar no crivo do antivírus.

Em conversa com os profissionais do TI, informaram que há um programa, também sazonal[9], que promovem para educar os funcionários para a importância da privacidade e segurança dos dados, com algumas palestras sobre engenharia social, por exemplo, informações sobre ataques novos que surgiram, alguns testes de vulnerabilidade e simulação de tentativa de ataque e o que deve ser feito.

Para a Global Data Solutions (2022), em matéria em seu Blog, a importância deste profissional assegurar a segurança dos dados:

> “está ligado à confiança que sua marca, serviços e empresa transmitem aos clientes e aos clientes em potencial. Não é difícil entender que uma empresa que tem vazamentos corriqueiros dedados não transmite segurança. Desta forma, você pode perder seus

[9] Geralmente quando é contratado um número maior que quatro pessoas para áreas que necessitem a utilização do computador.

> parceiros de negócios atuais e ainda, não ter chances de crescimento no mercado."

Quando se investe em segurança, se investe em confiabilidade e em boa reputação.

Segundo a empresa de Segurança da Informação Diferencial:

> "A violação de dados gera cerca de R$ 4,7 milhões de prejuízos para os empresários brasileiros. Isso pode afetar negociações e levar à tona informações sigilosas. É necessário evitar o acesso às informações em banco de dados, criar políticas de segurança para os colaboradores e prevenir-se contra violações externas"

Torna-se uma obrigação das empresas possuir um TI capacitado para realizar as ações devidas a fim de que não haja vazamento de dados e nem invasões em seus computadores.

3.1 ADEQUAÇÃO DO DEPARTAMENTO DE SEGURANÇA DE INFORMAÇÃO À LGPD

O Departamento de Informação, constituído dos profissionais de TI e do DPO tem responsabilidades sob a gestão de segurança, mas que muitas vezes é confundido com a própria lei, sendo esta apenas um detalhe dentro do que se realiza neste setor. E quando citamos a privacidade de dados para o departamento de gerência de segurança da informação, trata-se de resguardar os dados no sistema, tendo responsabilidade de armazenar segundo a norma técnica ISO/IEC 27002.

Fontes (2020, pg.6), afirma sobre a relação do DPO, do TI responsável e da LGPD que:

> "sem um Programa Organizacional de Segurança da Informação efetivo, a organização não tem sustentabilidade para a conformidade com a Lei Geral de Proteção de Dados Pessoais – LGPD. Evidentemente esta lei tem outros controles legais que não diz respeito diretamente com a segurança da informação."

Em que se responsabiliza os profissionais, no caso da concessionária, que estão fora da empresa – os que trabalham na segurança dos dados inseridos no

sistema FANDI - e os dois funcionários do TI que estão na linha de frente na empresa. Sendo papel do DPO esclarecer dúvidas e elaborar as permissões e as diretrizes sancionadas pela lei em questão e junto com o TI responsável trabalhar para que seja mitigada qualquer ação que venha causar riscos de vazamento de dados e devem andar em conjunto para obterem agilmente as respostas para um possível ataque. Os que estão na ponta, os dois funcionários de TI, cuidam do que está ao alcance: computadores e rede do meio (dentro da própria empresa) e não seresponsabilizam sobre o que ocorre dentro do FANDI ou problemáticas acerca da proteção de dados nesta plataforma, sendo este papel do DPO, que deve se preocupar com os dados pessoais e não com as máquinas ou rede da empresa.Este profissional estará sempre focado na organização dos dados, nos titularesdeles e de seus direitos, de como irá processar e coletar estes dados pessoais, por isso este profissional deve conhecer as leis.

Em um primeiro momento parece que o DPO está acima do TI, entretanto ele faz parte do TI da empresa, é um trabalho em conjunto, ter apenas um DPO da plataforma FANDI não trará proteção total para os dados da empresa e dos seus clientes e nem tampouco ter um profissional de Redes vai dar conta, pois há a plataforma. Sendo necessário um inventário e um mapeamento desses dados que devem ser atualizados com regularidade, que segundo Calixto (2020), pode ser da seguinte forma:

> “O mapeamento destas ações é efetuado com base na probabilidade e impacto de cada risco e atribuir pesos para cada risco, (Probabilidade e Impacto do Risco) que serão inseridos na fórmula: RI (Risco Inerente) = NP (Nível de Probabilidade) X NI (Nível de Impacto)” (CALIXTO, 2020).

É através destes pesos que levar-se-á em conta a probabilidade do risco. Isso deve ser feito em empresas com número acelerado de dados, com certa fluidez no dia a dia, que é o caso desta concessionária e, por isto, confiaram o tratamento dos dados à uma plataforma, por ser oferecido controle total, com mapeamento e inventário destes dados e sobre essa escolha por uma plataforma, Silva *et al*. (2020, p.94) afirma:

> “Nesse aspecto, as plataformas de gestão de privacidade têm apresentado soluções para mapeamento de dados com as seguintes funcionalidades: Interface fácil de usar para incluir e atualizar dados. Possibilidade de inclusão em massa de dados sobre ativos e atividades de processamento de dados pessoais, bem comoatribuição de riscos. Portal com questionários prontos ou customizáveis para envio automatizado para obtenção de informação sobre ativos e atividades de processamento. Gestão do fluxo de trabalho e automação de processos de mapeamento de dados. Painel visual da localização dos ativos de TI e do fluxo de dados paraoutros países. Painel de controle com os indicadores mais relevantes.” (SILVA *et al*., 2020, p.94)

A escolha de uma plataforma viabiliza para a empresa um dos pontos que a norma ISSO 27005 define para a resposta aos riscos, transferindo-o para a plataforma de gestão, o FANDI. Chama-se de transferência de risco, de acordo com a norma, e o risco é responsabilidade do FANDI e registrada essa cláusula no contrato, como versa a norma. (PEREIRA; BERGAMASCHI, 2018, p.14). Dentro desta norma, há ainda outros pontos que se deve estar atento: mitigar o risco, que jáfoi citado neste documento, eliminar as ameaças na raiz do problema e aceitar os pequenos riscos. (PEREIRA; BERGAMASCHI, 2018, p.14).

3.2 MEDIDAS DE PRECAUÇÃO CONTRA O VAZAMENTO DE DADOS

Só ocorre vazamento de dados se ocorrer um ataque, e ataque, para Coelho (2014, p.3): é qualquer ação que comprometa a segurança de uma organização. O profissional de TI vai agir para que os dados da empresa estejam a salvo 24h por dia, afinal, quando se trata dos “dados pessoais chegam a fazer às vezes da própria pessoa, em uma série de circunstâncias, nas quais a sua presença física seria outrora indispensável”. (DONEDA, 2011)

Controlar os dados é uma forma de gerenciar os riscos, e que se aplicam políticas de privacidade, procedimentos, diretrizes, práticas ou estruturas organizacionais (Norma ISO/IEC 27002: 2013)

Ainda segundo a norma ABNT ISSO/IEC 27002:2013, o controle se dá na proteção de todos os ativos da empresa, seja de informação (base de dados, contratos, acordos, documentações diversas etc.), de software (sistema FANDI, as ferramentas e os utilitários em geral), de hardware (as mídias, equipamentos em

geral, a própria rede), as pessoas (garantindo que sejam esclarecidas sobre prováveis ataques) e a reputação da instituição para o qual trabalha.

Os profissionais de TI devem atentar a todos os cuidados, afinal, no Art. 42º, afirma que: “O controlador ou o operador que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, em violação à legislação de proteção de dados pessoais, é obrigado a repará-lo”. O que significa que qualquer dano sofrido pelo titular dos dados, seja ele de qualquer cunho, quem responderá judicialmente é o profissional que cuidava dos dados, significando que houve uma falha em seu trabalho e, por falta de suporte e segurança, ele pode se complicar. Obviamente, como a rede de concessionária de veículos possui apoio de um DPO, dos dois TI e de uma equipe jurídica, o funcionário estaria precavido, mesmo assim, ficaria malvisto e possivelmente ser intitulado como incompetente.

Segundo uma empresa de Segurança da Informação, chamada Eval, há seis passos que se podem seguir para evitar os riscos de vazamento de dados, são estes:

1- Conscientização

Que deve ser feita com todos os funcionários que tenham acesso ao uso da internet dentro do estabelecimento, promover, como já foi dito anteriormente, testes contínuos de vulnerabilidade e de penetração, uso de senhas fortes, hardware de armazenamento seguro de chaves e aplicação consistente dos patches de software em todos os sistemas. (EVAL,2022)

2- Desenvolver plano de resposta a vazamentos de dados

Segundo a empresa Eval (2022): “consiste em um conjunto de ações destinado a reduzir o impacto do acesso não autorizado a dados e a mitigar osdanos causados se uma violação ocorrer”. Deve-se criar estratégias para a recuperação dos dados em caso de desastres, definir ações que serão seguidaspara proteger essa base, analisar a legislação, ou seja, ter de cor e salteado na cabeça a LGPD e saber aplicá-la, dentre outros.

3- Ter uma política de segurança da informação que contemple a proteção dos dados

Reunindo-se sempre com os outros profissionais, tanto o DPO, grupo jurídico da empresa e ao sistema FANDI, para garantir a eficácia da aplicação da LGPD pelo DPO e dos agentes de TI. Devendo ser feita a descrição de “como a companhia realiza a proteção dos seus ativos e dados”. E neste documento, deve ser “apresentada ainda uma definição de como procedimentos de segurança serãoexecutados e os métodos para avaliar a eficácia da política e como as correções necessárias serão feitas”. (EVAL, 2022)

4- Certificar se a equipe está bem treinada contra o vazamento de dados

De acordo com a empresa de Segurança da Informação, EVAL, em seu portal, os funcionários devem ser capacitados, em diversas dimensões dessa capacitação e lista:

a. ensinar aos funcionários situações que possibilitam este vazamento;
b. garantir que todos os dados sejam criptografados em qualquer ação executada, em conformidade com o documento que foi produzido no ponto anterior;
c. certificar que os processos sejam dinâmicos e automáticos;
d. conscientizar os funcionários sempre, a fim de reduzir os riscos de ataques.

5- Adote ferramentas eficazes na proteção dos dados

A Eval sugere uma arquitetura de nuvem para proteger esses dados, além de recursos como ferramentas de monitoração e controle do acesso à informação, proteger os dados em movimento (canal SSL/TLS), proteger o dado em repouso, em memória e ter uma ferramenta de prevenção à perda de dados (DLP).

6- Testar seu plano e as políticas, abordando todas as áreas consideradas de risco

Por fim, fazer acontecer a proteção como um todo. É uma rotina trabalhosa, de testes, de análise, de conversa com os outros funcionários, mas é de segurança e de credibilidade tanto para os agentes de TI como para os outros setores que lidam com a adequação à Lei Geral de Proteção de Dados.

4. CONCLUSÃO

A urgência em seguir a Lei de nº 13.709/2018, é conseguir ter credibilidade depois de uma nuvem ameaçadora de vazamento de dados em tantas empresas e os clientes sempre perguntam para onde irão os seus dados, qual a razão de pedir tantos dados para a compra de um automóvel. Como foi afirmado outrora, em 2021 ocorreu um vazamento de dados de veículos alarmante, que chegou ao número de 100 milhões de dados apenas no Brasil, o perigo é tanto para as concessionárias quanto para os clientes ou clientes em potencial levando ao descrédito o trabalho sério e aplicado dos profissionais de TI e de DPO.

Com a aprovação da LGPD e com sua implementação em todos os setores da empresa, a promoção de palestras, a promoção da sua importância e do cuidado ao utilizar a rede de Internet para assuntos pessoais, levam a um total controle de segurança para a empresa em questão. E observa-se que nem todas as empresas estão preparadas para responderem acerca de sua proteção de dados, afinal os funcionários e a reportar sobre o tema em outras empresas do ramo não chegam a uma conclusão ou nem sequer a uma exatidão à transparência do uso dos dados dos seus clientes.

Traçou-se as verdadeiras atribuições do TI e do DPO, deixando claro que trabalham em conjunto, sendo codependentes e não um cargo acima do TI dentro da empresa, sendo apenas parte da norma ISO/IEC 27002, não diminuindo em nenhum momento a importância dos profissionais, que poderiam ter sido mal interpretadas quando se fala em gerenciamento de dados.

Evidenciou-se, no decorrer deste trabalho, que as empresas, sejam elas de qualquer ramo, necessitam de um profissional atento aos dados e principalmente

com a precaução de ações criminosas. Além do mais, não se trata de apenas defender os dados dos clientes, mas os da própria empresa, por questões financeiras, afinal o sequestro de dados das empresas também vale uma grande soma em dinheiro para os criminosos do ciberespaço.

Destacamos que não é um papel teórico e sim de grande relevância para a aplicação da LGPD na rede de computadores da empresa de vendas de veículos novos e seminovos. Trabalhar-se-á os pontos importantes em subtítulos para alcançarmos maior compreensão do papel do profissional de TI no próximo capítulo.

REFERÊNCIAS

ABNT- Associação Brasileira de Normas Técnicas. NBR ISO/IEC 27002 –Tecnologia da informação – Técnicas de segurança – Código de prática para a gestão da segurança da informação. Rio de Janeiro, ABNT, 2005.

ALERTA SECURITY. **Afinal, o que é plano de conscientização em segurança da informação?** 2019. Disponível em: https://www.alertasecurity.com.br/afinal-o-que-e-plano-de-conscientizacaoem-seguranca-da-informacao/. Acesso em: 23 out. 2022

BRASIL. **Lei 13.709 de 14 de agosto de 2018**. Dispõe sobre a proteção de dados pessoais e altera a Lei nº12.965, de 23 de abril de 2014 (Marco Civil da Internet). Diário Oficial da República Federativa do Brasil, 15 agosto de 2018. http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 17 out. 2022

CALIXTO, Melissa da Silva. **ANÁLISE DA IMPLANTAÇÃO DA GESTÃO DE RISCOS NA TECNOLOGIA DA INFORMAÇÃO: UM ESTUDO DE CASO.** 2020. Trabalho de Conclusão de Curso (Tecnólogo em Gestão da Tecnologia da Informação) - Instituto Federal de Educação, Ciência e Tecnologia de Santa Catarina, FLORIANÓPOLIS, 2020.Disponível em: https://repositorio.ifsc.edu.br/bitstream/handle/123456789/1668/Analise%20da%20implanta%C3%A7%C3%A3o%20da%20gest%C3%A3o%20de%20riscos%20na%20tecnologia%20d a%20informa%C3%A7%C3%A3o%20-%20um%20estudo%20de%20caso.pdf?sequence=1&isAllowed=y. Acesso em 03. out. 2022

CAPESESPE. **Tipos de Dados na LGPD**. 2022. Disponível em: https://servicos.capesesp.com.br/campanhas/informecapesesp/edicao_22/pagina-02.html Acesso em 19 out. 2022

CASTELLS, Manuel. **A sociedade em rede** (A era da informação: economia, sociedade e cultura). v.1. 3. ed., São Paulo: Paz e Terra, 2000.

COELHO, Flavia Estélia Silva. Gestão da Segurança da Informação - NBR 27001 e NBR 27002, 2014

CUEVA, Ricardo Villas Boas, Segurança de Informações e proteção de dados pessoais. **A Lei Geral de Proteção de Dados Pessoais LGPD: aspectos práticos e teóricos relevantes no setor público e privado**. / Denise de Souza Luiz Francoski, Fernando Antônio Tasso - coordenação. -- 1. ed. -- São Paulo: Thomson Reuters Brasil, 2021.

DIFERENCIALL**. A importância da segurança da informação para a sua empresa**. [s.d]. Disponível em: https://diferenciall.com.br/a-importancia-da- seguranca-da-informacao-para-a-sua-empresa/ Acesso em: 24 out.2022

EVAL. **6 Passos simples para evitar o vazamento de dados**. 2022 Disponível em: https://www.evaltec.com.br/6-passos-simples-para-evitar-vazamento-de-dados/ Acesso em: 25 out. 2022

FERNANDES, Aryel. Vazamento de dados: falhas no Ministério da Economia expõe RGs e Selfies. 2022. **ISTOÉ DINHEIRO**. Disponível em: https://www.istoedinheiro.com.br/vazamento-de-dados-falha-na-economia-expoe-rgs-e-selfies-de-identificacao/ Acesso em 18 out. 2022

FOLHA DE PERNAMBUCO. **Sócios do Sport recebem ameaças de golpistas após vazamento de dados.** Disponível em: https://www.folhape.com.br/esportes/socios-do-sport-recebem-ameacas-de-golpistas-apos-vazamento-de-dados/241416/ Acesso em 16 out. 2022

GLOBAL DATA SOLUTIONS. 2022. **TI e a segurança de dados: entenda.** Disponível em: https://globaldata.com.br/ti-e-a-seguranca-de-dados-entenda-a- importancia/ Acesso em: 24 out. 2022

GONSALVES, Júlio César. Criminosos lucram 88 mi vendendo dados pessoais na dark-web. **TECHTUDO.** 2022. Disponível em: https://www.techtudo.com.br/listas/2022/06/criminosos-lucram-r-88-mi-vendendo-dados-pessoais-na-dark-web-proteja-se.ghtml Acesso em 20 out. 2022

JORNAL CONTÁBIL. **Profissional DPO: Entenda o que faz e saiba como se tornar um!** 2020. Disponível em: https://www.jornalcontabil.com.br/profissional-dpo-entenda-o-que-faz-e-saiba-como-se-tornar-um/ Acesso em 24 out. 2022

LIMA, Victtor Henrique Pereira. **LGPD análise dos impactos da implementação em ambientes corporativos: Estudo de Caso.** 2020. (TCC) Bacharelado em Ciências da Computação. Escola de Ciências Exatas e da Computação. Pontifícia Universidade Católica de Goiás. Disponível em: https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/108/1/LGPD%20-%20ANALISE%20DOS%20IMPACTOS%20DA%20IMPLEMENTAC%CC%A7A%CC%83O%20-%2003-12%20-%20final.pdf Acesso em 22 out. 2022

MACIEL, Rafael Fernandes. **Manual Prático sobre a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/18).** 1. ed. Goiânia: RM Digital Education, 2019.

MALAR, Pedro João. Banco Central anuncia vazamento de dados ligados a mais de 130 mil chaves pix. Disponível em: https://www.cnnbrasil.com.br/business/banco-central-anuncia-vazamento-de-dados-ligados-a-mais-de-130-mil-chaves-pix/ Acesso em 30 nov. 2022

MÁXIMO, Wellton. Banco Central comunica vazamento de dados de 137,3 mil chaves pix. **AGÊNCIA BRASIL.** Disponível em: https://agenciabrasil.ebc.com.br/economia/noticia/2022-09/banco-central-comunica-vazamento-de-dados-de-1373-mil-chaves-pix Acesso em 16 out. 2022

MONTEIRO, Silvana Drumond. O ciberespaço: o termo, a definição e o conceito. DataGramaZero - **Revista de Ciência da Informação**, v. 8, n. 3, p. 1-21, 2007. Disponível em: >http://hdl.handle.net/20.500.11959/brapci/6089< Acesso em: 20 out. 2022.

PEREIRA, Helena Acácio Santini; BERGAMASCHI, Alessandro Bunn. Manual de gestão de riscos do INPI. Rio de Janeiro: Instituto Nacional da Propriedade Industrial, 2018

ROCHA, Camila P D *et al.* Segurança da Informação: A ISO 27.001 como Ferramenta de Controle para LGPD. **Revista de Tecnologia da Informação eComunicação da Faculdade Estácio do Pará**, v. 2, n. 3, p. 78-97, 2019.

RODOTÀ, Stefano. **A vida na sociedade de vigilância: privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SAGAN, Carl. **O mundo assombrado pelos demônios**. São Paulo: Cia das Letras, 1997.Disponível em: <https://biblioteca.ibge.gov.br/visualizacao/livros/liv101631_informativo.pdf> Acesso em 18 out. 2022

SILVA, Laercio. *et al.* Proteção de dados: desafios e soluções na adequação à lei. – Rio de Janeiro: Forense, 2020. Edição do Kindle

SOMBRA, Thiago Luís Santos. **Fundamentos da Regulação da Privacidade e Proteção de Dados.** 1. ed. São Paulo: Revista dos Tribunais, 2019, p.47.

PINHEIRO, Patrícia Peck. **Proteção de dados pessoais. Comentários à lei 13.709/2018 (LGPD).** São Paulo: Saraiva Jur, 2018.

SOARES, Ramos Rafael. **Lei Geral de Proteção de Dados: Direito à privacidade no mundo globalizado.** 2019. [TCC]. Graduação em Direito. 31f. Prontifica Universidade Católica de Goiás. 2020. Disponível em: >https://www.google.com/url?sa=t&source=web&rct=j&url=https://repositorio.pucgoias.edu.br/jspui/bitstream/123456789/1201/1/RAFAEL%2520RAMOS%2520SOARES%2520-%2520Artigo.pdf&ved=2ahUKEwiK7O2w-9P8AhXKq5UCHejLBpsQFnoECBAQAQ&usg=AOvVaw1gW8wYK3VwoOOs5TKhKZ4F<Acesso em: 25 out. 2022.

PEIXOTO, Erick Lucena Campos. JÚNIOR, Marcos Ehrhardt. **Breves notas sobre a resignificação da privacidade.** Rev. Bras. de Dir. Civ., V.16, abril-junho, 2018. Disponível em: >https://rbdcivil.ibdcivil.org.br/rbdc/article/view/230<