UNIVERSIDADE DO SUL DE SANTA CATARINA

FERNANDO BOTTEGA HALLBERG

GESTÃO DE ARQUIVOS EM NUVEM NA ERA DA LGPD COM ENFOQUE EM UM ESCRITÓRIO DE ADVOCACIA

Palhoça

2021

FERNANDO BOTTEGA HALLBERG

GESTÃO DE ARQUIVOS EM NUVEM NA ERA DA LGPD COM ENFOQUE EM UM ESCRITÓRIO DE ADVOCACIA

Relatório de pesquisa na modalidade de Estudo de Caso apresentado ao Curso de **Tecnólogo em Gestão da Tecnologia da Informação** da Universidade do Sul de Santa Catarina, como requisito parcial à aprovação na unidade de aprendizagem de Estudo de Caso.

Orientador: Prof. Patrícia da Silva Meneghel

Palhoça

2021

FERNANDO BOTTEGA HALLBERG

GESTÃO DE ARQUIVOS EM NUVEM NA ERA DA LGPD COM ENFOQUE EM UM ESCRITÓRIO DE ADVOCACIA

Este trabalho de pesquisa na modalidade de Estudo de Caso foi julgado adequado, em sua forma final, à aprovação na unidade de aprendizagem de Estudo de Caso, do curso de **Tecnólogo em Gestão da Tecnologia da Informação** da Universidade do Sul de Santa Catarina.

Palhoça, 18 de junho de 2021.

_____

Professor e orientador Prof. Patrícia da Silva Meneghel
Universidade do Sul de Santa Catarina

AGRADECIMENTOS

Agradeço a todos que estiveram presentes nessa jornada de quase 30 anos na área de tecnologia, amigos, colegas de trabalhos, minha orientadora e principalmente meus familiares, que sempre se fizeram presentes em minha vida, e em especial, ao escritório de advocacia que cedeu seu tempo e estrutura para este estudo de caso.

RESUMO

O presente estudo de caso tem como objetivo mostrar um breve histórico do contexto em que surgiram as legislações de proteção de dados na Europa e no Brasil, bem como demonstrar de maneira simples e prática quais serão as dificuldades enfrentadas na implantação da Lei Geral de Proteção de Dados no gerenciamento de arquivos em um escritório de advocacia.

A Lei Geral de Proteção de Dados entrou em vigor em agosto de 2020, e suas penalidades passarão a ser aplicadas a partir de agosto de 2021, e obrigará todas as empresas que lidam com dados pessoais e dados pessoais sensíveis de pessoas físicas a terem controle e rastreabilidade dessas informações, e com isso surgirão diversas demandas, não somente na área jurídica, mas principalmente na área de tecnologia que dará suporte a isso tudo.

Nesse estudo de caso o enfoque foi dado ao gerenciamento de arquivos em nuvem, que se tornará praticamente obrigatório, porém a escolha não será fácil visto que os serviços deverão suportar auditoria e controle do acesso e rastreabilidade dos arquivos.

De nada adiantará as empresas, e nesse caso, um escritório de advocacia, fazer toda a implantação documental e jurídica se a tecnologia não acompanhar e der suporte.

Fato é que o maior investimento para implantação da Lei Geral de Proteção de dados será, de longe, na área de tecnologia.

Palavras-chave: LGPD. Arquivos. Nuvem.

SUMÁRIO

1 INTRODUÇÃO

Com a evolução tecnológica exponencial vivida nas últimas décadas, e uma capacidade cada vez maior de processamento e armazenamento de informações, passamos a enfrentar novos problemas que antes não existiam.

A quantidade cada vez maior de dispositivos conectados a internet, com o surgimento da IoT – Internet das Coisas[1], potencializada com o surgimento do 5G, fez com que o número de informações pessoais que transitam na internet hoje, seja inimaginável, bem como o número de caso de vazamento dessas informações.

A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais−LGPD), com vigência a partir de 18.9.2020, tem o objetivo de assegurar que os dados pessoais sejam tratados de forma adequada, protegendo a liberdade, a privacidade e o livre desenvolvimento das pessoas (TSE, 2020, p. 5).

Com o objetivo de mitigar o uso indevido e abusivo de dados, a lei será responsável por aprofundar a regulamentação das questões relativas ao uso de dados pessoais no ambiente virtual, impactando não somente as empresas brasileiras, mas todas as empresas que ofertem produtos ou serviços no cenário nacional (SEBRAE, p. 2).

Na Europa, entrou em vigor em maio de 2018, o Regulamento Geral de Proteção de Dados da União Europeia (GDPR) e se tornou um verdadeiro marco para o tratamento de dados online, e serve de modelo para a implementação desse modelo nos demais países.

1.1 PROBLEMA

O problema a ser enfrentado é: Qual ferramenta ou quais ferramentas podem ser utilizadas pelas empresas para o gerenciamento de arquivos em nuvem que atendam os requisitos da LGPD?

1.2 JUSTIFICATIVA

Uma das situações a ser enfrentada com o advento da LGPD no Brasil, é como ter controle e rastreabilidade dos dados e informações dentro da empresa. Hoje, boa parte das

[1] Internet das coisas é um conceito que se refere à interconexão digital de objetos cotidianos com a internet, conexão dos objetos mais do que das pessoas. Em outras palavras, a internet das coisas nada mais é que uma rede de objetos físicos capaz de reunir e de transmitir dados – WIKIPEDIA (PT)

empresas ainda não organiza os seus arquivos de maneira a ter auditoria e controle sobre o acesso a cada arquivo, a cada pasta e a cada compartilhamento.

Normalmente, em boa parte das empresas, existe um compartilhamento público único, e todos que tem acesso a rede da empresa, tem acesso de leitura e escrita em todos os arquivos, sem controle nenhum e sem deixar rastros.

Além disso, não há classificação das informações sensíveis e críticas, e informações essas que caso cheguem a ser vazadas resultará e multas milionárias para as empresas.

Hoje também é comum as empresas sofrerem ataques cibernéticos em que os dados são criptografados e é exigido o resgate. Com o advento da LGPD, a tendência é que a partir do momento em que as multas comecem a ser aplicadas, os ataques sejam para capturar os dados e cobrar um "resgate" para que essas informações não sejam vazadas.

Se tornará necessário que todas as empresas que tenham informações sensíveis de seus clientes, ou mesmos arquivos com informações internas, passem a ter controle absoluto dessas informações, e tenham uma maneira de auditar cada acesso a cada informação, para evitar problemas maiores que podem ter com a entrada em vigor da Lei Geral de Proteção de Dados – LGPD.

1.3 OBJETIVOS

1.3.1 Objetivo Geral

Investigar quais ferramentas podem ser utilizadas de maneira eficaz pelas empresas para armazenamento de seus arquivos em nuvem, tendo controle de acesso e auditoria, a fim de estarem adequadas a Lei 13.709/18, Lei Geral de Proteção de Dados.

1.3.2 Objetivos Específicos

a) Mapear quais são os requisitos exigidos pela LGPD para controle e tratamento de informações pessoais.
b) Pesquisar quais soluções podem ser implementadas para que uma empresa esteja devidamente adequada a LGPD.

2 REVISÃO DA LITERATURA

O tratamento de dados pessoais não é uma novidade dos dias de hoje, pelo contrário, ela sempre esteve presente no nosso dia a dia, mesmo antes do surgimento dos computadores (década de 40).

Era comum as pessoas deixarem suas informações pessoais registradas, seja em uma farmácia ou em um mercado e até mesmo no banco. Porém naquela época, não tínhamos todos os dados interligados e a informação não era sistematizada, de maneira que não se tornara um problema para a privacidade da maioria das pessoas.

Começou a ser um problema com a popularização do telefone da década de 80 e com o surgimento do telemarketing, porém somente a partir da década de 90, com o surgimento da internet, a popularização dos computadores pessoais e o surgimento dos negócios digitais, é que se tornou necessária a regulamentação da proteção desses dados.

Segundo Pinheiro (2020, p.17):

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados, especialmente os relacionados às pessoas, viabilizados pelos avanços tecnológicos e pela globalização.

Com o surgimento da internet as pessoas passaram a comprar pela rede mundial de computadores. Segundo o relatório da Unctad, o B2C[2] no Brasil teve faturamento de US$ 20 bilhões em 2019, ainda bem atrás do México, com US$ 31 bilhões. Cerca de 29% da população brasileira (ou 39% dos usuários da web no país) faz compras na internet. (VALOR ECONÔMICO)

De acordo com Mendonça (2014, p.5):

> Desde o seu surgimento, a Internet vem experimentando um número cada vez maior de usuários e de informações disponíveis na rede, da maneira cada vez mais eficiente e veloz, democratizando o acesso a ela. Não se pode olvidar também que nas últimas décadas, a função da "rede das redes" também mudou muito: de uma rede voltada para objetivos militares estratégicos, ela é hoje parte da vida de milhões de pessoas em todo o mundo, que a utilizam quase que diariamente para os mais diversos fins.

Além da possibilidade de comprar pela internet, as redes sociais nos conectaram com nossos amigos. Os brasileiros somam mais de 130 milhões de usuários no Facebook,

[2] B2C é abreviação de business to consumer, traduzindo para o português, empresa para consumidor

segundo dados da rede social disponibilizados em janeiro deste ano e compilados pelo site Statista. (R7)

Ferramentas como WhatsApp, estão instaladas em 99% dos telefones móveis no Brasil, sendo que 93% dessas pessoas utilizam o aplicativo diariamente. (TECNOBLOG)

Com todo esse uso da tecnologia, de maneira constante por cada brasileiro – e esse é o mesmo comportamento no mundo inteiro – essas empresas passaram a capturar as informações, sejam as digitadas em uma conversa privada, sejam as páginas e os posts que você curte no Facebook ou no Instagram, e através de algoritmos de inteligência passaram a identificar potenciais compradores para determinados produtos e serviços, e então, usar isso para ganhar dinheiro.

Mas não só isso, quando vamos em um laboratório fazer um exame, ou quando entramos em um hotel e preenchemos a ficha, estamos deixando nossos dados pessoais, e da mesma maneira as empresas utilizam esses dados muitas vezes sem autorização para que possam traçar perfis de consumo, e então serem mais assertivas quando vão oferecer produtos e serviços.

Segundo Mendonça (2014, p. 2):

> A sociedade de hoje é resultado de uma revolução gerada pela informação, razão pela qual ela é comumente chamada ‘sociedade da informação’. O grande fluxo informacional que circula rapidamente de um lado a outro do planeta por meio das novas ferramentas de tecnologia e de comunicação mostra que a informação é orientadora e permeadora das relações, fortalecendo-as (por um lado) e permitindo o surgimento de novas a partir da derrubada das barreiras físicas. Nos dias de hoje, é possível acompanhar fatos que acontecem em um país muito distante em tempo real através da televisão, manter conversas simultâneas com várias pessoas de vários lugares, trocando vídeos e fotos, através das redes sociais e descobrir qual a melhor rota para ir de um lugar a outro sem pegar trânsito por aplicativos de celular em apenas alguns segundos – e enquanto dirige, no breve tempo do sinal vermelho do semáforo.

Nesse cenário ainda, se tornou comum o roubo ou o vazamento de informações. Recentemente foram vazados os dados de 220 milhões de brasileiros com informações extremamente sensíveis como o CPF, salário, escore de débito etc. (TILT UOL)

Segundo Pinheiro (2020, p.17):

> Desse modo, houve a necessidade de resgatar e repactuar o compromisso das instituições com os indivíduos, cidadãos desta atual sociedade digital, no tocante à proteção e à garantia dos direitos humanos fundamentais, como o da privacidade, já celebrados desde a Declaração Universal dos Direitos Humanos (DUDH) de 1948.

Por isso se tornou tão importante que houvesse uma lei que responsabilizasse a empresa ou o responsável pela guarda das informações sensíveis, caso exista vazamento de dados.

A União Europeia foi pioneira no assunto, e aprovou em 2016 a General Data Protection Regulation (GDPR), para proteger os dados dos cidadãos europeus.

Segundo Pohlmann (2019, pg. 23):

> A GDPR é a lei de proteção de dados para países que fazem parte da União Europeia. Ela foi aprovada no ano 2016, ficando com uma *vacatio legis*[3] de dois anos, sendo vigente, portanto, a partir de 25 de maio de 2018, quando começaram a ser realizadas as fiscalizações e aplicadas as multas.

Após a aprovação da GDPR, passou a acontecer um "efeito dominó", PINHEIRO (2020, pg. 18), pois passou a se exigir dos demais países e empresas que buscam relações comerciais com a UE, que deveriam ter uma legislação no mesmo nível da GDPR.

Segundo o TSE (2020, pg. 5):

> A Lei nº 13.709, de 14 de agosto de 2018 (Lei Geral de Proteção de Dados Pessoais−LGPD), com vigência a partir de 18.9.2020, tem o objetivo de assegurar que os dados pessoais sejam tratados de forma adequada, protegendo a liberdade, a privacidade e o livre desenvolvimento das pessoas.

No Brasil, a Lei 13.709, Lei Geral de Proteção de Dados Pessoais (LGPD) foi sancionada em 14 de agosto de 2018, e alterada pela Lei 13.853/2019, porém só entrará em vigor em agosto de 2021.

Segundo Pinheiro (2020, pg. 17):

> A base desse pacto é a liberdade, mas o fiel da balança é a transparência. Sendo assim, as leis sobre proteção de dados pessoais têm uma característica muito peculiar de redação principiológica e de amarração com indicadores mais assertivos, de ordem técnica, que permitam auferir de forma auditável se o compromisso está sendo cumprido, por meio da análise de trilhas de auditoria e da implementação de uma série de itens de controle para uma melhor governança dos dados pessoais.

Portanto, a GDPR e a LGPD passam a cobrar que toda informação pessoal seja resguardada, e mais do isso, tenham formas de controle que permitam verificar se realmente estão resguardadas. Isso significa que toda a informação deverá ser auditada e passar por

---

[3] Vacatio legis é uma expressão latina que significa "vacância da lei", ou o prazo legal que uma lei demora pra entrar em vigor, de sua publicação até o início de sua vigência. No caso de uma lei que aplique multas, por exemplo, as mesmas somente poderão ser aplicadas após o período de vacatio legis.

sistemas de controle, sendo inclusive que a falta de controle sobre a informação poderá acarretar multa para a empresa.

Com a LGPD as empresas serão obrigadas a se organizar, e inclusive disponibilizar para os clientes uma forma de seus dados serem excluídos de sua base, caso o cliente assim deseje.

Diante disso, se tornará necessário que todas as empresas do país se adequem a LGPD, tanto na questão jurídica, quanto na questão tecnológica.

Juridicamente as empresas terão que se resguardar, definindo todos os procedimentos que são feitos com os dados dos clientes, desde o backup dessa informação, até mesmo quando ela é reciclada, e isso tudo deverá ser documentado.

Mas além disso, as empresas deverão ter controle sobre toda a informação sensível, cada acesso a cada arquivo deverá ser auditado e deverá sofrer um controle de quem tem acesso a cada informação, pois se houver um vazamento, a empresa deverá ter condições de saber quem vazou a informação ou ao menos, quais de seus funcionários tiveram acesso a informação, de maneira a se resguardar e não sofrer ou amenizar a multa – que não é baixa.

Neste cenário é que teremos que viabilizar soluções tecnológicas para respaldar a implantação da estratégia de proteção de dados de cada empresa, e o que pretendemos entender neste estudo de caso, é com relação aos arquivos compartilhados em um ambiente de múltiplos usuários, com armazenamento em nuvem: que soluções que poderão ser utilizadas para resguardar de maneira confiável as informações sensíveis da empresa?

O ponto chave é a rastreabilidade e a auditoria da informação: Quem acessou? Quando acessou? Quem modificou? Quem copiou? Quem deletou?

Fizemos um comparativo entre as ferramentas mais utilizadas para armazenamento em nuvem, no que tange a recursos disponíveis para atender os requisitos da LGPD.

Quadro 1: Comparativo entre ferramentas de armazenamento em nuvem

	Google Drive[4]	Dropbox[5]	OneDrive[6]	NextCloud[7]
Multiusuário	✓	✓	✓	✓
Versionamento de Arquivo	✓	✓	✓	✓
Log de alterações de arquivos	✓	✓	✓	✓
Registro de auditoria	✓ Somente nas versões business e enterprise	✓ Somente na versão business advanced	✓ Somente nas versões business e enterprise do Office 365 ou Microsoft 365	✓
Criptografia ponta a ponta	✓	✓	✓	✓
Token / 2-way-auth	✓	✓	✓	✓
Permissões detalhadas de compartilhamento	✓	✓	✓	✓

Como podemos perceber, a maior parte das ferramentas já prevê alguma espécie de auditoria e rastreabilidade dos arquivos e suas alterações, porém, dentre todos, a única ferramenta que oficialmente é adequada a GDPR é o NextCloud[8]. Além disso apenas o NextCloud permite que os arquivos fiquem armazenados em servidor próprio do cliente.

Podemos deferir desse comparativo que as ferramentas mais utilizadas ainda não estão de fato homologadas para atender a legislação de proteção de dados, e os recursos que se enquadrariam para o atendimento a legislação só estão disponíveis nas versões mais caras, portanto a LGPD abre um campo completamente novo de trabalho para profissionais da área de tecnologia.

[4] https://www.google.com/intl/pt-BR/drive/
[5] https://www.dropbox.com/pt_BR/features
[6] https://www.microsoft.com/pt-br/microsoft-365/onedrive/compare-onedrive-plans
[7] https://nextcloud.com/hub/
[8] https://nextcloud.com/gdpr/

3 PROCEDIMENTOS METODOLÓGICOS

3.1 CARACTERIZAÇÂO DO ESTUDO

Trata-se de uma pesquisa exploratória, onde vamos observar o contexto de um escritório de advocacia com relação a gestão de arquivos, para que seja possível indicar uma solução de adequação tecnológica a LGPD – Lei Geral de Proteção de Dados.

3.2 CAMPO DE ESTUDO

O estudo de caso será aplicado em um escritório de advocacia na cidade de Cascavel, PR, cujo nome será resguardado por questões éticas.

3.3 INSTRUMENTOS PARA COLETA DE DADOS

Os instrumentos de pesquisa que utilizados para estudo de caso, serão:

Entrevista: Serão entrevistados um ou mais advogados do escritório, e outras pessoas que tiverem relação com a gestão de documentos do referido escritório.

Questionário: Serão elaborados questionários para funcionários do escritório responderem, relativos ao acesso e utilização de arquivos do escritório.

4 APRESENTAÇÃO E ANÁLISE DOS RESULTADOS

Sempre foi difícil mudar uma cultura empresarial, ainda mais quando isso implica em investimento financeiro pela empresa, e muitas vezes as empresas acabam não se protegendo e assumindo o risco pelo resultado negativo.

No caso da LGPD, isso será mais complicado, pois a multa a ser aplicada é bastante agressiva.

Sobre a privacidade dos dados LIMA (2020, pg. 21):

> [...] não é de hoje que o ordenamento jurídico brasileiro protege a privacidade dos cidadãos. A Lei Geral de Proteção de Dados não é a primeira, nem a única legislação a promover a proteção de dados pessoais às pessoas naturais. Então, por que tanto fala-se acerca do impacto que a legislação causará? Ora, o impacto principal será percebido na maneira como as empresas terão que se reorganizar.

Sobre a ética empresarial, LIMA (2020, pg. 21), cita que:

> Bom seria se as empresas já aderissem à conformidade (observância às leis, às melhores práticas, à integridade e à ética) desde a fase da ideia do negócio, passando pelo desenvolvimento do projeto até a criação da empresa de fato. Contudo, não há uma cultura de integridade; a prioridade não é compliance, conformidade, adequação.

Ou seja, se por si só as empresas adotassem condutas éticas no tratamento de informações pessoais, a LGPD não seria necessária. Porém essa não é a realidade das condutas praticadas, sendo necessário a adoção de uma lei que garanta a conformidade e o respeito a privacidade das informações pessoais.

De acordo com a Lei 13.709/18, Lei Geral de Proteção de Dados: (PLANALTO)

> Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do meio, do país de sua sede ou do país onde estejam localizados os dados, desde que:
> I - a operação de tratamento seja realizada no território nacional;
> II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou
> III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.”
> § 1º Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.
> § 2º Excetua-se do disposto no inciso I deste artigo o tratamento de dados previsto no inciso IV do caput do art. 4º desta Lei.

Ou seja, toda e qualquer informação pessoal que for tratada por pessoa física ou jurídica, de direito público e privado, em território nacional, ou coletada em território nacional está sujeita a LGPD.

No caso em questão, em que o estudo de caso é em um escritório de advocacia, temos que levar em consideração que muitos dos dados tratados poderão ser dados pessoais sensíveis. Segundo a LGPD, em seu Art. 5º.: (PLANALTO)

> I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável;
> II - dado pessoal sensível: 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;

Para garantir que o escritório em questão esteja em conformidade com a LGPD, se faz necessário analisar todos os processos que envolvam o recebimento e tratamento de dados pessoais, e que o armazenamento desses dados, bem como o acesso a essas informações seja controlado e passe com um controle de auditoria.

Segundo LIMA (2020, pg. 37),

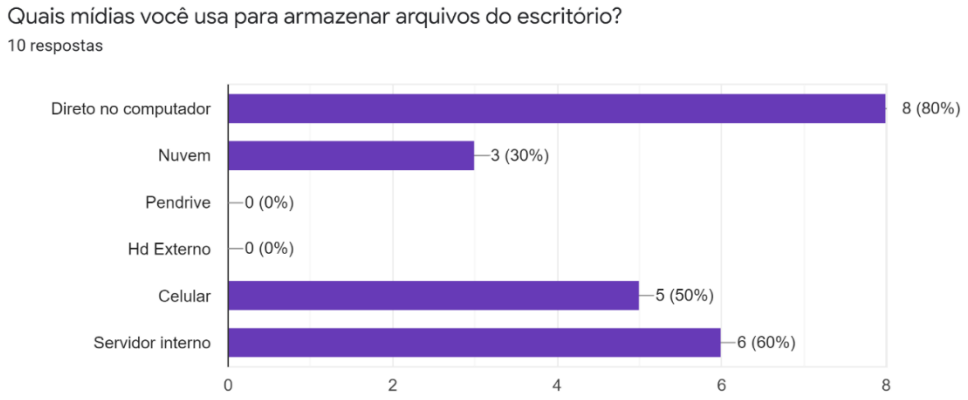
> O mapeamento do risco é indispensável na adequação, bem como monitoramento e auditoria, educação, comunicação e treinamento, e códigos de ética, políticas e procedimentos, entre outros documentos que devem ser criados ou atualizados, e as medidas cabíveis de correção em caso de não observância ao programa.

Nesse sentido, devem ser mapeados todos os processos internos que envolvam tratamento de dados pessoais, inclusive com a classificação entre dados pessoais e dados pessoais sensíveis, para que então sejam sugeridas as mudanças nos processos da empresa para que esteja em conformidade com a LGPD.

Para esse estudo de caso, vamos nos ater somente a parte tecnológica, que deve dar suporte para a implantação do LGPD no escritório de advocacia.

Foi realizado questionário e entrevista com os funcionários do escritório, para conseguir entender todo o ciclo da informação digital na empresa, cujo resultado apresento nos gráficos a seguir:

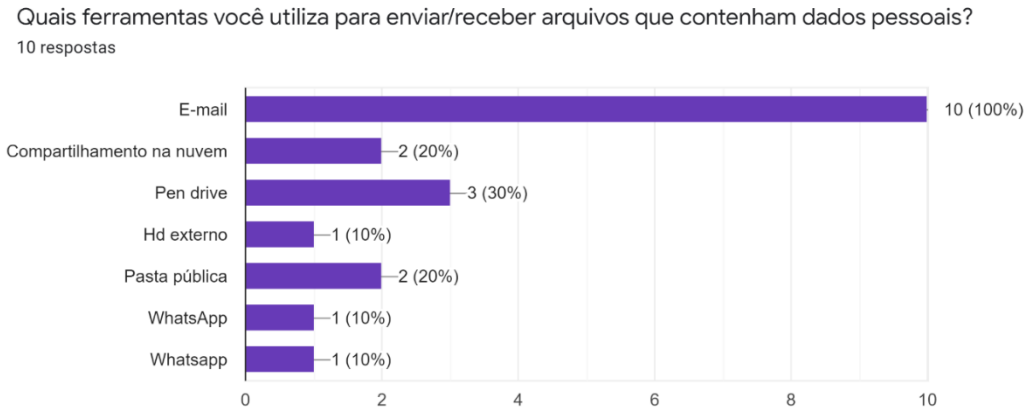
Gráfico 1 – Quais as mídias usadas para armazenamento de dados



Fonte: Autor (2021)

De acordo com o Gráfico 1, é possível perceber que a informação está distribuída de maneira desorganizada, sem uma diretriz definida, dificultando sua rastreabilidade e controle dos arquivos, bem como o backup, pois a maior parte das pessoas (80%) armazena arquivos diretamente no computador.

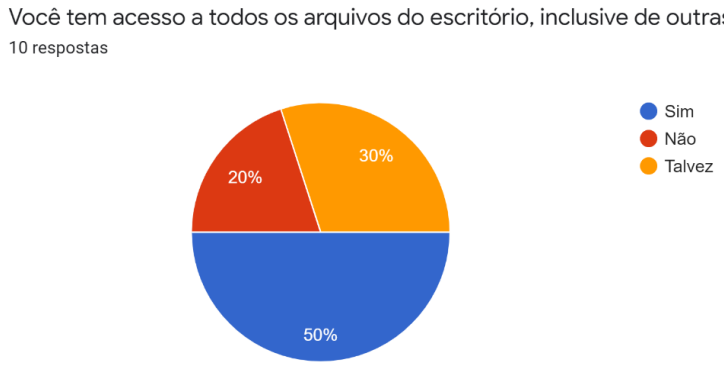
Gráfico 2 – Ferramentas utilizadas para enviar/receber arquivos com dados pessoais



Fonte: Autor (2021)

Será imprescindível a definição de processos para tratamento dos arquivos, bem como a eliminação de acesso a rede e ao computador por fontes não monitoradas como hd externo, pen drive e e-mail pessoal, inclusive podendo chegar ao ponto de monitorar as portas USB de todos os computadores, e só permitir acesso a rede de computadores autorizados.

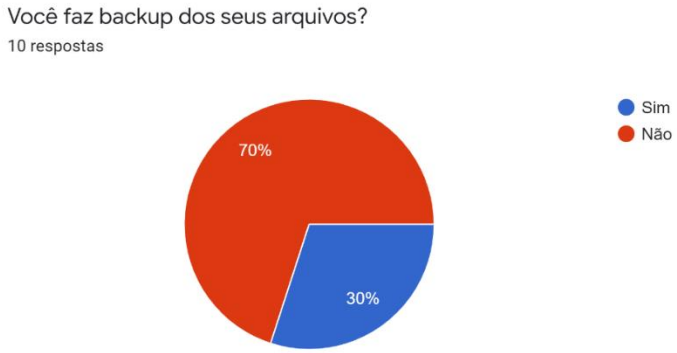
Gráfico 3 – Quem tem acesso a todos os arquivos sem nenhuma restrição



Fonte: Autor (2021)

Vejam que 50% dos funcionários têm acesso a todos os arquivos do escritório, sem nenhum tipo de controle, inclusive de outros advogados e funcionários. Se torna praticamente impossível rastrear alterações, cópias e exclusões de arquivos.

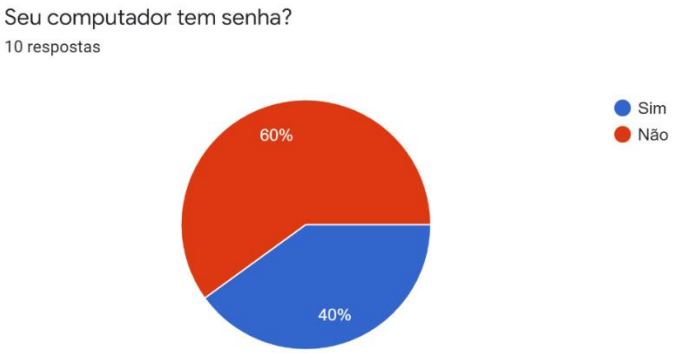
Gráfico 4 – Backup dos arquivos



Fonte: Autor (2021)

A grande maioria dos funcionários não faz backup dos arquivos, colocando muitas vezes em risco o trabalho realizado.

Gráfico 5 – Uso de senha no computador



Fonte: Autor (2021)

Mais da metade 60% não resguarda o próprio computador com senha, deixando o mesmo acessível para qualquer pessoa com acesso físico ao computador.

Gráfico 6 – Compartilhamento sem controle

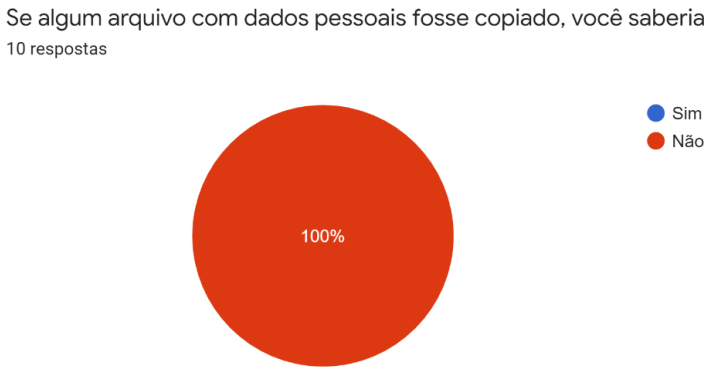
Fonte: Autor (2021)

Metade dos funcionários compartilham os arquivos de maneira pública, para quem tem acesso a rede interna.

Gráfico 7 – Rastreabilidade de arquivos apagados

Fonte: Autor (2021)

Gráfico 8 – Rastreabilidade de arquivos copiados



Fonte: Autor (2021)

Gráfico 9 – Rastreabilidade de alterações nos arquivos

Fonte: Autor (2021)

Os últimos 3 gráficos (7,8 e 9) relatam a falta de log e auditoria de modificações e cópias dos arquivos. Porém, essa é a regra geral da maior parte das empresas do Brasil, que não utilizam uma solução específica para isso, ou ainda não se preocuparam com isso.

5 CONSIDERAÇÕES FINAIS

Os resultados apresentados nos gráficos, com as informações extraídas do questionário e entrevista realizada com os funcionários do escritório de advocacia, relatam na verdade a realidade da maior parte das empresas no Brasil.

Em que pese nesse escritório exista uma relação de confiança muito grande entre as pessoas que trabalham nele e que estão juntas há bastante tempo, a Lei Geral de Proteção de Dados obrigará a empresa a documentar todo o tratamento de dados pessoais, e com isso, o tratamento de arquivos que contenham dados pessoais.

Com isso, todos os procedimentos terão que ser readequados, tendo como norte a documentação jurídica, e tendo como suporte a tecnologia.

De nada adiantará o LGPD ser implantado no papel, se disso não resultar na proteção de dados real, e mais, se na ocorrência de um vazamento de dados, não houver uma maneira de descobrir como e quando ocorreu esse vazamento, e isso só será possível com a adoção de ferramentas e políticas que suportem o controle, a rastreabilidade a auditoria da informação na empresa.

Na breve análise que fizemos de algumas ferramentas, é possível identificar que o investimento em tecnologia nos próximos anos deverá aumentar significativamente, seja pela própria vontade da empresa em adotar boas práticas de proteção de dados por conta própria, seja pela força da Lei Nacional de Proteção de Dados – LGPD.

Talvez esse seja inclusive o momento de uma valorização maior do profissional de tecnologia, muito lembrado para resolver problemas depois que eles acontecem, e raramente solicitado para implantar soluções preventivas nas empresas.

REFERÊNCIAS

TSE. **Lei geral de proteção de dados (2018)**. Brasil, 2020. Disponível em: https://www.tse.jus.br/hotsites/catalogo-publicacoes/pdf/livro-lgpd.pdf. Acesso em 9 de abril de 2021.

SEBRAE. **E-book – LGPD – Lei Geral de Proteção de Dados**. Disponível em: https://www.sebrae.com.br/Sebrae/Portal%20Sebrae/UFs/PE/Anexos/LGPD-Connect-Sebrae.pdf. Acesso em 9 de abril de 2021.

PINHEIRO, Patricia Peck. **Proteção de dados pessoais: comentários à Lei n. 3.709/2018 (LGPD)**. 2. ed. São Paulo: Saraiva Educação, 2020. 152 p.

VALOR ECONÔMICO. **Brasil sobe 10 posições em índice de e-commerce da Unctad**. Disponível em: https://valor.globo.com/brasil/noticia/2021/02/17/brasil-sobe-10-posies-em-ndice-de-e-commerce-da-unctad.ghtml. Acesso em 17 de junho de 2021.

MENDONÇA, Fernanda Graebin. **O direito à autodeterminação informativa: a (des)necessidade de criação de um novo direito fundamental para a proteção de dados pessoais no Brasil.** Disponível em: https://online.unisc.br/acadnet/anais/index.php/sidspp/article/view/11702. Acesso em 16 de maio de 2021.

R7. **Brasil é o 3º país com o maior número de usuários do Facebook**. Disponível em https://noticias.r7.com/tecnologia-e-ciencia/brasil-e-o-3-pais-com-o-maior-numero-de-usuarios-do-facebook-02032019. Acesso em 9 de abril de 2021.

TECNOBLOG. **WhatsApp chega a 99% dos celulares no Brasil; Telegram cresce**. Disponível em https://tecnoblog.net/326932/whatsapp-chega-a-99-por-cento-celulares-brasil-telegram-cresce/. Acesso em 9 de abril de 2021.

TILT UOL. **Vazamento de dados de 220 milhões de pessoas: o que sabemos e quão grave é**. Disponível em https://www.uol.com.br/tilt/noticias/redacao/2021/01/28/vazamento-expoe-dados-de-220-mi-de-brasileiros-origem-pode-ser-cruzada.htm. Acesso em 9 de abril de 2021.

POHLMANN, Sérgio Antônio. **LGPD Ninja. Entendendo e implementando a Lei Geral de Proteção de Dados nas empresas**. Editora Fross, 2019. 308 p.

LIMA, Ana Paula Morais Canto de. **LGPD – Lei Geral de Proteção de Dados. Sua empresa está pronta?** São Paulo, SP: Literare Books International, 2020.

PLANALTO, Palácio do. **Lei 13.709/2018. Lei Geral de Proteção de Dados**. Disponível em http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm. Acesso em 16 de maio de 2021.