UNIVERSIDADE CESUMAR – UNICESUMAR
ENGENHARIA DE SOFTWARE

GLEDSON EDGAR FABRIS

SEGURANÇA DE DADOS:
Lei Geral de Proteção de Dados (LGPD)

Curitiba
Agosto/2020

RESUMO

Lei Geral de Proteção de Dados (LGPD), certamente é um dos assuntos mais discutidos devido a sua regulamentação em território brasileiro. Através de pesquisas realizadas pode-se adiantar que, conforme a regulamentação imposta aos dados, o titular dos dados terá maior segurança dos dados coletados. A lei ainda não aplicada em território brasileiro, mas que entrará em vigência proporcionando garantia de maior sigilo e proteção aos seus dados coletados e de forma consentida, um cenário que antes de vigorar a Lei Geral de Proteção de Dados (LGPD), um cenário que poderíamos saber da existência mais faltava fiscalização e informação sobre o assunto, ao entrar em vigor a Lei Geral de Proteção de Dados (LGPD) passará e ser obrigatório no Brasil, sendo reportado ao cidadão com maior clareza quais dados foram coletados e sobre o tratamento realizado nos dados, acompanhado de acesso livre as informações, caso tenha alguma correção a ser realizada ou até a exclusão de um dados que o cidadão não esteja de acordo com a divulgação . A Lei Geral de Proteção de Dados (LGPD) além de possuir um conjunto de condições impostas de como será coletado até e exclusão dos dados coletados, também terá como responsabilidade de reportar de maneira clara e detalhada e para qual finalidade eles foram ou serão utilizados. Sem uma lei em vigor para proteção de dados, pode-se obter manipulações de forma a beneficiar terceiros como também gerar impactos negativos a sociedade devido ao seu valor.

Palavra-Chave: regulamentação; condições; coletados;

1 INTRODUÇÃO

Segurança de dados vem sendo um assunto discutido de forma mais intensa nos últimos anos, nos afirmando ser um assunto de muita relevância e que deve ser discutido exaustivamente para que os dados sejam mantidos de forma integra e segura.

A falta de segurança tem intensificado o interesse pela posse desses dados, sendo ele de forma lícita ou ilícita, dados estes que estando sobre posse do poder de entidades influenciadoras podendo ser um grande desastre para sociedade tornando

possível uma manipulação de resultados e tomando vantagem num jogo de interesse seja ela de pequeno ou grande porte.

Visando a segurança dos dados, e sendo constituindo a criação da lei de proteção de dados (LGPD), teremos maior segurança em nossas informações fornecidas digitalmente ou por meios não digitais, iremos deter de informações dos nossos dados como de que forma ela está sendo tratada e para que finalidade e também quem está realizando o tratamento de suas informações.

> “As adequações para a nova lei trazem a necessidade de acompanhamento e busca de novas tecnologias que apoiem as empresas tanto na gestão dos dados, quanto no atendimento aos usuários, privace by design, segurança da informação, portabilidade, anonimização, qualidade e governança de dados, entre outras adequações.” (ARRUDA, 2019, p. 2).

Teremos novidades e grandes desafios nos próximos anos, com a internet das coisas (IOT), inteligência artificial (IA) como também big data, tecnologias que vem em um crescimento exponencial, temos a informatização sendo cada vez mais incluída em inúmeras vertentes e em diversos processos nos meios como economia, medicina no agronegócio dentre outros variados setores. Toda essa informatização, resulta na geração de um gigantesco volume de dados onde será realizado o tratamento desses dados tudo com consentimento e dentro dos critérios estabelecidos por lei, garantindo a privacidade e integridade dos dados.

1.1 Objetivos

O objetivo geral deste TCC será, através de pesquisa explicativa afim de, desmistificar e de certa forma provocar o conhecimento da Lei Geral de Proteção de Dados (LGPD), e o impacto gerado sobre a segurança e a privacidade desses dados, o conhecimento das leis de proteção de dados seja no meio digital ou não digital, sendo de pessoas físicas como também de pessoas jurídicas e qual é a situação das empresas com relação a se adequar com a Lei Geral de Proteção de Dados (LGPD).

Portanto, os seguintes objetivos específicos se fizeram necessários: O assunto de proteção de dados deve ser reconhecido, como conhecimento adquirido, gerado após apresentar o que será abrangido, com o vigor da Lei de Proteção de Dados (LGPD), após o esclarecimento da Lei Geral de Proteção de Dados (LGPD) de forma objetiva,

simples e clara, conforme sancionado e impresso no diário oficial da união onde entrará em vigor em agosto de 2020, tendo como alvo, evidenciar se com a existência e aplicação destas leis como também a fiscalização que rege sobre ela, frisando a real garantia de transparência e integridade como também da segurança dos dados coletados com consentimento do cidadão.

1.2 Justificativa

Devido ao assunto não é tratado de uma forma simplificada e tem pouca repercussão quando entra no contexto da lei, deixando curiosos sobre o assunto de segurança de dados com ainda mais perguntas sobre o assunto, além de ressaltar uma sensação em que isso será uma barreira ainda maior com relação a saber que tipo de tratamento é realizado com os dados pessoais. O principal foco será deixar de forma mais clara, alguns pontos principais sobre o assunto segurança de dados.

> “Se você não está pagando por um produto, é sinal de que o produto é você.” (Andrew Lewis - jornalista americano)

Tendo como exemplo o escândalo Cambridge Analytica, caso ocorrido no ano de 2016, que utilizou um aplicativo para realizar a coleta de informações de 87 milhões de usuários sem o consentimento deles. A ação de realizar a coleta e a obtenção da posse desses dados resultou no favorecimento de privilégios e vantagens para a elaboração de roteiros para campanha política do candidato à presidência Donald Trump, visto que se utilizando da psicométrica, poderiam vir a traçar um perfil muito próximo de cada indivíduo ou do público alvo, tendo informações relevantes como traços de personalidade, estilo de comportamento, habilidades ou até o nível de concordância com determinado assunto.

Em plena corrida da política norte americana entre os partidos Republicanos e Democratas, inicialmente surgiram alguns boatos, com possível uso dos dados vazados da plataforma de redes sociais Facebook para influenciar eleitores. Essa falha na segurança na proteção dos dados dos usuários, ocorreu no vazamento de dados do Facebook, expondo informações dos usuários e de seus amigos que realizaram o quis de personalidade, que acabou em corroborar, ocasionando na vitória

na política norte americana do então eleito Presidente Donald Trump do partido Republicano.

A empresa Cambridge Analytica foi alvo de inúmeras investigações e também sendo bombardeada por todos os lados com pedidos de explicações de suas ações, pôr fim a empresa Cambridge Analytica assumiu a culpa do fato ocorrido, reconhecendo que os dados foram utilizados para influenciar eleitores através do uso dos dados coletados no Facebook ao descumprir regra regulamentadoras de sigilo e segurança de dados, resultando na entrada do pedido de falência encerrando então suas atividades.

> A empresa se declarou culpada de descumprir a ordem do regulador britânico de meios de revelar a informação que tinha sobre um professor americano, David Carroll, que pediu para saber quais dados sobre ele a companhia tinha e como os havia obtido. (EXAME, 2019).

Outro caso também de grande repercussão que se tornou muito conhecido, foi o “caso Snowden”, por se tratar de um cenário de espionagem a nível global, Fato ocorrido em 2013, devido ao vazamento de dados sigilosos do governo norte americano, o caso Snowden, em que um ex-técnico da CIA, Edward Snowden, veio a tornar público os dados e documentos sobre programas de vigilância comandados pela Agencia de Segurança Nacional (NSA) que os Estados Unidos (EUA) programas com o “XKeyscore ou “XKS”, que até era de conhecimento era exclusivamente para realizar o monitoramento de cidadãos norte americanos, como esse vazamento de dados tornou-se público que o sistema de monitoramentos não é somente utilizado para monitorar os cidadãos americanos, mais também é possível realizar todos os registro e rastros das atividades online dos usuários da rede de internet como também pesquisas em banco de dados que possuem o compartilhamento ativo de e-mail e até fazer o monitoramento em tempo real de conversas de presidentes e líderes de outros países. Embora a Agencia de Segurança Nacional (NSA) tenha se pronunciado referente ao caso, que o recurso utilizado esta dentro da lei dos Estados Unidos (EUA) respeitando rigorosamente os critérios de restrição de uso, podendo ser solicitado pelos líderes do pais para fins específicos de para obter informações mais precisas como alvos de inteligência estrangeiros legítimos e caso precisem de informações necessárias para proteger o país e seus devidos interesses.

De fato que casos como esses advindo da pratica de coleta de dados para obter favorecimento de vantagens e realizar espionagens tem se disparado um alerta da forma como se é obtido toda essa base de conhecimento, e se é possível intervermos em determinados aspectos inserindo limitações no fornecimento de dados pessoais.

2 REFERENCIAL TEÓRICO

O decreto da lei vem de encontro com a falta de segurança e de informação e de como é realizado o tratamento dos dados seja ele de pessoa física ou pessoa jurídica, dados sendo eles sensíveis ou não. Com a vigência ocorrendo no prazo estipulado agosto de 2020, se tem o respaldo da vigência da lei sobre o tratamento desses dados e de que forma isso está sendo feito, dissimulando qualquer tipo de irregularidade com essas informações.

De acordo com Art.6ª da lei Nº 13709, de 14 de agosto de 2018, traz uma abordagem sobre as atividades de tratamento de dados pessoais e que elas deverão ter a boa-fé, salientando sobre a transparência de como será realizado.

> Agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018, p. 17)

Conforme publicado no portal EBC, o governo brasileiro publicou no Diário Oficial da União a Medida Provisória 869/18 que criou a Autoridade Nacional de Proteção de Dados (ANPD). A medida prevista na Lei Geral de Proteção de Dados (LGPD), Lei 13.709/2018 que realiza o detalhamento das regras para realização da coleta e tratamento de dados de indivíduos por empresas e por instituições públicas. A Autoridade Nacional de Proteção de Dados (ANPD), será composta por um conselho formado de cinco diretores indicados pelo Presidente da República. Foi assegurado que os primeiros mandados terão uma duração diferenciada com o período de 2(dois) até 6(seis) anos posteriormente entrara em vigência o período no cargo por 4(quatro) anos previstos, salvo os casos de renúncia, condenação judicial ou pena de demissão decorrente de processo administrativo disciplinar que iram perder os cargos.

A Autoridade Nacional de Proteção de Dados (ANPD) poderá contará ainda com um Conselho Nacional de Proteção de Dados Pessoais e Privacidade composto por 23 membros, do Poder Executivo, do Senado, da Câmara dos Deputados, do Conselho Nacional de Justiça, um do Conselho Nacional do Ministério Público, do Comitê Gestor da Internet no Brasil, instituições científicas, tecnológicas e de inovação, de entidades da sociedade civil com atuação comprovada em proteção de dados pessoais e de entidades representativas do setor empresarial relacionado à área de tratamento de dados pessoais.

A norma aprovada em julho de 2018, pelo Senado e sancionada em agosto pelo presidente Michel Temer que, na ocasião, foi vetado o trecho do texto que previa o órgão regulador para a proteção dos dados. Ao vetar a criação da Autoridade Nacional de Proteção de Dados, o Planalto alegou o risco de que o órgão fosse contestado por vício de origem, uma vez que o Legislativo não poderia dispor sobre a organização do Estado, uma prerrogativa do Executivo.

Diferentemente do que propunha inicialmente o texto aprovado pelo Congresso, que previa a criação de uma entidade autônoma ligada ao Ministério da Justiça, a nova autoridade será um órgão da Presidência da República, que teria apenas "autonomia técnica". Os integrantes da Autoridade Nacional de Proteção de Dados virão de cargos remanejados de outros órgãos da administração.

2.1 Mudanças na Lei de proteção de dados

O texto do Ministério Público foi assinado pelo presidente Michel Temer e, além da criação da Autoridade Nacional de Proteção de Dados (ANPD), juntamente trouxe algumas modificações em partes da Lei de Proteção de Dados. Entre os pontos que foram alterados está o prazo de aplicação da lei que passou de 18 para 24 meses da data da sanção da Lei 13.709. Com isso, a lei está prevista para ser aplicada a partir de 14 de agosto de 2020.

Michel Temer também revogou o trecho que impedia que entidades privadas tratassem dados referentes a segurança pública, defesa, segurança ou atividades de investigação e repressão de infrações penais. O texto também altera o trecho em que trata do uso de dados sensíveis do setor de saúde autorizando a troca de informações dos pacientes também entre as prestadoras de plano de saúde. Antes a lei vedava a

comunicação ou o uso compartilhado entre controladores de dados pessoais sensíveis referentes à saúde com objetivo de obter vantagem econômica. A autorização recaía apenas para fins de portabilidade de dados quando consentido pelo titular.

A sanção da Lei Geral de Proteção de Dados (LGPD), completa 2(dois) anos em agosto de 2020, e o Senado realizou uma votação no dia 26 de agosto, onde foi estabelecido a medida provisória 959/20, sugerindo o adiamento da Lei Geral de Proteção de Dados (LGPD). Conforme a Medida Provisória 959/20, foi realizado a votação no Senado, mas foi excluído um dos textos do artigo, esse texto retirado se tratava do adiamento da vigência da Lei Geral de Proteção de Dados (LGPD). Sendo assim continua sendo válido a vigência da Lei Geral de Proteção de Dados (LGPD), Lei nº 13.709, conforme previsto de entrada em vigor em agosto de 2020.

Mesmo ocorrendo ou não o adiamento de vigorar a Lei Geral de Proteção de Dados (LGPD), as empresas terão que adotar medidas impostas de manter os dados em segurança.

No período em que passamos pela pandemia do novo corona vírus (COVID-19), muitas das empresas se adequaram a nova realidade, onde para alguns é um momento de dificuldade, para outros se torna uma oportunidade de negócios e momento de inovar como empresas que aderiram ao trabalho home office e acabaram obtendo maiores resultados de seus colaboradores e os benefícios acabaram indo mais além com redução de gastos com infraestrutura do ambiente de trabalho.

Mudanças ocorrendo no ambiente de trabalho e também na governança e políticas de privacidade e segurança dos dados, com adoção de um programa de conformidade de acordo com a área de negócios, também conhecido como “Compliance”, as empresas devem adotar algumas fases sendo ajustadas conforme a necessidade, sendo considerado como principais a conscientização da importância da Lei Geral de Proteção de Dados (LGPD), podendo ser realizado de diversas formas como através de treinamentos apresentando os pontos de inovações de impacto ao negócio. Outra fase importante é tornar claro qual será o fluxo dos dados coletados como, forma que foi coletado, aonde foi armazenado, de que forma foi armazenado, passou por determinado tratamento, para que finalidade os dados foram tratados, quais os resultados obtidos, se ocorreu a portabilidade desses dados e assim por diante,

tornando um mapeamento completo desse fluxo. O próximo passo sendo de análise dos pontos críticos e problemas a serem corrigidos, após todo o mapeamento é realizado a estratégia do plano de ações tendo como prioridade criticidade a situações que impõe maiores riscos. Seguindo o passo seguinte será o de implementação de estratégias para se iniciar o tratamento dos pontos críticos e de riscos mapeados na análise, seguindo de uma fase que nunca acaba, que é a fase de monitorar todas as etapas anteriores, e realizando atualizações quando ocorrer a identificação de mais pontos críticos ou sempre que houver a necessidade.

Conforme pesquisa realizado pela Serasa Experian, diante da pandemia do novo corona vírus (COVID-19), e com o distanciamento social adotado como medida de prevenção, é fato que o número de transações online teve um aumento de usuários de serviços digitais, juntamente a isso ocorreu um aumento e a preocupação com possíveis fraudes e segurança de dados.

Os consumidores que vem a compartilhar as informações pessoais, quando ocorrido por meio de uma solicitação explícita nos sites que visitam, subiu de 28,4% para 33,4% no período de 1(um) ano, e o número de internautas que sempre compartilharam seus dados pessoais, ainda que não se sintam seguros, caiu de 35,7% para 30,9% no mesmo período, conforme pesquisa realizada a nível nacional pela Serasa Experian. Em meio a fraudes e exposições de dados pessoais ocorreu o aumento em 2020 ficando em 17,4% se comparado com 2019 que havia 12,7%.

Quando há a necessidade de realizar o compartilhamento dos dados com empresas online, o principal aspecto avaliado para 59,1% dos consumidores é a confiabilidade da marca de mercado lhe proporciona, vindo na sequência de 50,1% dos usuários querem saber se a política de segurança e privacidade do site é apresentada de maneira clara.

Os dados que também foram coletados, é que 75% dos consumidores desconhecem ou conhecem pouco sobre a Lei de Proteção de Dados, e 6(seis) em cada 10(dez) brasileiros tomam como base para realizar o fornecimento seus dados pessoais a confiabilidade construída com uma previa interação com empresas e marcas com experiencias positivas.

No ano de 2018 no Reino Unido 6(seis) em cada 10(dez) pessoas afirmaram estar totalmente ou parcialmente cientes sobre o Regulamento Geral de Proteção de Dados

(GDPR), lei que se assemelha com a adotada pela União Europeia desde maio de 2018.

Em caráter emergencial no dia 26 de agosto de 2020, foi realizado em sessão remota, a medida provisória 959, que tem como objetivo realizar o adiamento da Lei Geral de Proteção de Dados (LGPD), onde a lei com inicio previsto de vigorar em agosto de 2020, com interferência do atual presidente Jair Messias Bolsonaro, foi realizado edição no texto da medida preventiva postergando o prazo de vigência para maio de 2020, devido ao cenário de pandemia do novo corona vírus (COVID-19), as empresas não conseguiram se programar e preparar para as mudanças.

3 O QUE SÃO CONSIDERADOS DADOS?

Informações de meio digitais ou não digitais, sendo elas fornecidas de forma consentida, sendo de pessoa física ou jurídica de direito público ou privado. As informações estabelecem insumos para que os dados que ainda não apresentam relevância, devido a não ter passado por algum tipo de tratamento, permanecendo de forma bruta e sem significado algum.

Os dados passam a ter relevância a partir do momento que é realizado o fluxo de tratamento dos dados, parar que venham ter sentido para algum determinado fim e que seja agregado valor sobre esses dados, podendo tornar um dado um objeto de tomada de decisão, poder de influência, gatilhos para o consumo, obtenção de conhecimento e tendências legitimas para alguma ocasião.

Temos dois tipos de dados onde são classificados como sendo dados pessoais e dados sensíveis.

3.1 Dados pessoais

Trata-se de informações que permitam realizar a identificação de forma direta ou indireta de um indivíduo ou entidade, pode-se possuir status ativo ou inativo em casos de falência, são considerados dados pessoais: nome, RG, CPF, gênero, data e local de nascimento, telefone, endereço residencial e comercial, geolocalização, fotos, prontuário de saúde, histórico de pagamentos, hábitos de consumo, endereço de IP e histórico de navegação dentre outros.

- Nome e Sobrenome – Informação contida no documento de Certidão de Nascimento, onde é transcrito e realizado registro em cartório civil;
- Número de documentos – Sequência numérica de identificação de um documento como a Carteira Nacional de Habilitação (CNH), Passaporte e o número do Registro Geral (RG) podendo ser também alfanumérica dependendo do estado em que foi realizado o Registro Geral (RG);
- Telefone para contato – Número de lista, divulgado para contato;
- Endereço residencial - São os dados necessários para que seja possível realizar a localização do indivíduo (nome da rua, Avenida, Travessa, número de casa ou apartamento, bloco, andar, terreno, lote);
- Geolocalização – Define a posição do cidadão ou de algo, através de um sistema de coordenadas;
- IP – É o endereço de Protocolo da Internet, vem do inglês Internet Protocol address (**IP** address), trata-se de um rótulo numérico designado a um dispositivo como computadores, impressoras dentre outros dispositivos que esteja conectado a uma rede;
- E-mail – Endereço de correio eletrônico;
- Perfil Comportamental – Baseado nos históricos de navegação, hábitos de consumo, fotos, postagens dentre outros;

3.2 Dados sensíveis

Os dados considerados sensíveis são dados que estão sujeitos a condições de tratamento mais específicas, onde venham a revelar dados pessoais como opiniões públicas e políticas, filiação sindical, questões genéticas, biométricas e sobre a saúde, etnia, origem racial, crença religiosas ou filosófica, dados relacionados à vida sexual e a orientação sexual do cidadão.

Na totalidade do conjunto de dados pessoais considerados sensíveis, existem dados que requerem mais de atenção, quando envolvem crianças e adolescentes. Quando o foco estiver sobre menores de idade, é imprescindível obter o consentimento inequívoco de um dos pais ou responsáveis e se ater a pedir apenas o conteúdo estritamente necessário para a atividade econômica ou governamental em questão, e

não repassar nada a terceiros. Sem o consentimento, só pode coletar dados se for para urgências relacionadas a entrar em contato com pais ou responsáveis e/ou para proteção da criança e do adolescente. De acordo com Art.1ª da Lei Nº 8.069, de 13 de Julho de 1990, a lei dispões de proteção integral à criança e também ao adolescente, e temos no Art. 2ª da Lei Nº 8.069, de 13 de Julho de 1990, que reconhece para efeitos da lei que cidadão com idade de até doze (12) anos incompletos é considerado criança, e cidadão que possuem idade entre 12(doze) anos completos e 18 (dezoito) anos incompletos são considerados adolescentes.

Ainda sobre os dados sensíveis, firmou-se que empresas privadas sendo especializadas no assunto e possuam autorização ativa do seu registro para a atividade de tratamento de dados e o governo também podem realizar o tratamento dos dados se tiverem o consentimento explícito do cidadão e para uma finalidade declarada de forma transparente e definida. Porém, a Lei Geral de Proteção de Dados Pessoais permite também que os dados poderão passar pelo tratamento sem consentimento e assegurado por lei, caso seja definido por analise que isso é possível quando for indispensável em situações ligadas a alguma obrigação legal a políticas públicas, a estudos via órgão de pesquisa, direito concedido em contrato ou processo, à preservação da vida como também da integridade física de uma pessoa, à tutela de procedimentos realizados por profissionais de áreas da saúde ou sanitária e prevenção contra possíveis fraudes contra o titular dos dados.

3.2.1 Os dados considerados sensíveis

- Religião - A religião é um dos aspectos de maior influência na vida de um indivíduo, trata-se de crença e o poder de influência perante a sociedade;
- Origem racial - Características como a cor da pele e origem social passam a ter valor significativo e significados distintos de acordo com as culturas, diferenças mais comuns se referem cor de pele, tipo de cabelo, traços faciais e cranial, descendência dos antepassados e, também a genética;
- Classificação - Uma forma de estabelecer critérios para ordenar os dados sendo estabelecido algum critério;
- Orientação sexual - Aponta por qual ou quais sexos ou gêneros tem atração, seja sexual ou romântica.

- Saúde – Ritmo de vida envolvendo o estado físico e psíquico e bem estar;
- Filosófico ou político - Busca encontrar um significado mais profundo de acontecimentos em busca de conhecimento, se possui o poder de influência as pessoas;
- Opinião política - Por meios de comunicação, expressa um posicionamento de apoio ou de pressão a determinado tema;
- Filiação sindical - Consiste em uma organização e o agrupamento de algumas pessoas de uma determinada profissão que por meio de uma organização interna fazem a representação da respectiva profissão, a fim de gerar melhorarias as condições de vida e trabalho;
- Genética - Hereditariedade onde cada indivíduo traz consigo a estrutura e das funções dos genes;
- Biométrica - Se trata de uma forma de identificar unicamente cada indivíduo por meio de características físicas ou comportamentais únicas;

3.3 Dados anonimizados ou pseudonimizado

Utiliza-se de uma técnica durante o tratamento dos dados onde tem como característica realizar a dissociação de informações que seja possível realizar a identificação de um indivíduo. Os dados anonimizados são dados que não podem estar associados a um indivíduo específico, seja de maneira direta ou indireta se utilizando de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento em questão.

4 QUEM SÃO OS STAKEHOLDERS ENVOLVIDOS NO TRATAMENTO DE DADOS?

Os stakeholders envolvidos no processo de tratamento de dados, tem como responsabilidade reportar a autoridade nacional de proteção de dados (ANPD), qualquer sinistro que ocorra com os dados tratados desde uma manipulação erroneamente ocorrida ou até mesmo um cenário de vazamento de informação desses dados que estavam sobre sua responsabilidade. Essa prestação de contas ao órgão regulador é realizada de forma indireta, visto que temos um intermediário entre

controlador/operador e a autoridade nacional de proteção de dados (ANPD), sendo nomeada como encarregado.

> Controlador e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem, especialmente quando baseado no legítimo interesse. (BRASIL, 2018, p. 15)

5 AGENTES DE TRATAMENTO DE DADOS

O controlador e operador podem também ser chamados de agentes de tratamento, devem manter os registros das operações de tratamentos de dados, apontando a finalidade, tempo de processamento dos dados, estipular prazo para ação de tratamento de dados, segurança dos dados, sigilo e a privacidade dos dados, consentimento dado, ou não.

Conforme Art. 37, Lei Nº 13.709, DE 14 DE AGOSTO DE 2018, estipula-se que esse registro será especialmente importante, quando o processamento se der pelo legítimo interesse do Controlador.

Os controladores e operadores, dentro de suas competências, pelo tratamento de dados sendo ele individual ou por meio de associações, poderá formular regras respeitando as boas práticas da governança que estabelecem os critérios e condições de organização, o regime de funcionamento, os procedimentos, reclamações e petições dos titulares, as normas de segurança, os padrões técnicos tratamento, as obrigações específicas para os stakeholders envolvidos no tratamento, as ações socioeducativas, os mecanismos internos de supervisão e de análise de riscos dentre outros aspectos relacionados ao tratamento de dados pessoais.

5.1 Controlador

O controlador pode-se utilizar de argumentação e justificar que determinado tratamento se faz necessário para tal finalidades e que seja realizado a sua atividade. Assim, o tratamento dos dados pode ser justificado como uma forma de aprimoramento do processo de vendas de algum determinado produto e, que poderá gerar um considerável aumento da receita da empresa que irá realizar o tratamento destes dados.

Ainda que a empresa venha a realizar a justificativa em que o tratamento de dados pessoais, é realizado com base em legítimo interesse, existem limites legais ao se referir ao tratamento dos dados. Não será possível realizar o tratamento dos dados, caso prevaleça o direito e a liberdade fundamental do titular e que seja imposto a proteção dos dados pessoais.

5.2 Operador

O operador deve realizar o tratamento conforme instruções fornecidas pelo controlador que deverá supervisionar se as instruções realmente foram seguidas e se o operador cumpriu o as normas conforme estabelecidas e que a responsabilidade pelo cumprimento da Lei Geral de Proteção de Dados (LGPD) e a Lei de Acesso à Informação ou Lei do Habeas Data.

Art. 39. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo controlador, que verificará a observância das próprias instruções e das normas sobre a matéria. o operador responde solidariamente pelos danos causados pelo tratamento quando descumprir as obrigações da legislação de proteção de dados ou quando não tiver seguido as instruções lícitas do controlador, hipótese em que o operador se equipara ao controlador.

5.3 Encarregado

O encarregado também reconhecido como Data Protection Officer (DPO), é a pessoa indicado pelo controlador e operador, conforme Lei Geral de Proteção de Dados (LGPD) é obrigatoriedade a presença de um encarregado ou DPO para todas empresas e profissionais liberais, garantindo que o texto seja seguido à risca. O encarregado (DPO) que vai assumir o papel de realizar o canal de comunicação entre controlador e os titulares e a autoridade nacional. Sendo um canal como orientador para a entidade e os contratados para adotarem as boas práticas no processo de tratamentos dados de forma bruta até ao final do tratamento dos dados.

Caberá ao encarregado (DPO), aceitar reclamações e comunicados emitidos pelos titulares para esclarecimento e prestação de contas, recebera também comunicados da Agência Nacional de Proteção de Dados (ANPD).

De acordo com Art. 41 da Lei Geral de Proteção de Dados (LGPD), será obrigatório para as empresas realizar a nomeação da figura do encarregado (DPO) de proteção de dados pessoais, essa indicação poderá ser pessoa física como um profissional responsável que esteja inserido dentro da empresa, ou também poderá realizar a indicação do encarregado (DPO) sendo uma pessoa jurídica que possui qualificação e amplo conhecimento técnico e sobre o regimento das leis, políticas e atividades da organização.

Serão estabelecidas pela Autoridade Nacional de Proteção de Dados (ANPD), exceções caso não faça sentido ao ramo e tamanho da instituição, sendo assim, os casos se fazem necessários por análise de viabilidade, com a decisão se o negócio estará salvo da indicação de um encarregado (DPO).

> "Essa figura aparece pela primeira vez em 1977, na Lei de Proteção de Dados da Alemanha...Cabe a ele tornar realidade dentro das organizações o que estabelece a lei." (Nuria López, DPO do Opice Blum Advogados Associados).

De forma clara, o encarregado (DPO) faz o papel de sentinela ou guardião dos dados e que possui como missão, realizar a propagação da cultura da Lei Geral de Proteção de Dados (LGPD) dentro das organizações, realizando adequações para que a empresa esteja alinhada de acordo com a lei e orientações de como garantir o melhor tratamento possível e para finalidade especifica dos dados pessoais e com segurança aplica e em níveis adequados.

As empresas que buscam adequar-se à Lei Geral de Proteção de Dados (LGPD), tem-se adotado de estratégia de contratação de serviços de terceiros para resolver seus problemas de adequações com a lei em curto espaço de tempo, utilizando-se da indicação do DPO as a Service, onde trata-se de profissionais que possuem certificação e tem como proposta flexibilidade de atuação com contrato por horas de consultoria podendo chegar a 200 horas/ano e redução de custos para as empresas que devem se adequar à Lei Geral de Proteção de Dados (LGPD).

5.4 Autoridade nacional de proteção de dados (ANPD)

A autoridade nacional de proteção de dados (ANPD) órgão de administração pública responsável por zelar, implementar e realizar a fiscalização do cumprimento da lei,

poderá determinar ao controlador que seja elaborado relatórios de impacto a proteção de dados pessoais, sobre suas operações de tratamento conforme os termos regulatórios.

Caberá a autoridade nacional de proteção de dados (ANPD) articular sua atuação com o Sistema Nacional de Defesa do Consumidor do Ministério da Justiça e com outros órgãos e entidades com competências sancionatórias e normativas afetas ao tema de proteção de dados pessoais, e será o órgão central de interpretação desta Lei e do estabelecimento de normas e diretrizes para a sua implementação.

O Conselho Nacional do Ministério Público (CNMP) decidiu indicar os Advogados Luiz Fernando Bandeira de Mello Filho e Silvio Roberto Oliveira de Amorim Junior, para representarem o Conselho Nacional do Ministério Público (CNMP) como titular e suplente, respectivamente, na composição do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, integrante da estrutura da Autoridade nacional de proteção de dados (ANPD).

Conforme o padrão internacional da Lei de Proteção de Dados, deve-se haver uma autoridade autônoma e independente onde não pode haver vínculo a outros órgãos, Para maneira em que a Autoridade nacional de proteção de dados (ANPD) arquitetou-se, ela não se enquadra nas leis internacionais de proteção de dados, pois existe um vínculo com órgãos do governo e hierarquias integrando a Presidência da República. Sendo assim, caso torne-se necessário uma avalição ou algum tipo de investigação e seja preciso acionar a Autoridade nacional de proteção de dados (ANPD), e tenha o envolvimento a algum órgão publico os conflitos de interesse tornam-se ainda mais relevantes.

5.5 Conselho Nacional de Proteção de Dados Pessoais e da Privacidade

O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade que trata-se de um conselho multisetorial tendo como membros empresas, governo e ongs, tendo como uma de suas atribuições realizar a elaboração de normas e condutas para a Política Nacional de Proteção de Dados Pessoais e da Privacidade o quadro do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por 21(Vinte e um) membros. Os membros que compõe o Conselho Nacional de Proteção de Dados Pessoais e da Privacidade têm o prazo de atuação com período

de 2(dois) anos, porem podem vir a ser substituídos pela Presidente da República caso se faça necessário. Os indicação dos membros multisetoriais abrangem áreas como:

- Poder Executivo;
- Sociedade Civil;
- Instituições Cientificas;
- Setor produtivo;
- Senado;
- Câmara dos Deputados;
- Conselho Nacional de Justiça;
- Comitê Gestor da Internet;
- Empresários;

6 TRATAMENTO DE DADOS

O tratamento de dados pode ser interpretado como qualquer ato que esteja relacionado a utilização de dados sejam eles:

- Coleta - Realizado a coleta dos dados de forma consentida, para finalidade específica;
- Armazenamento - Contempla em manter a coleção dos dados em repositório de forma segura;
- Acesso - Tomar conhecimento ou realizar a consulta de informações com possibilidade da utilização das informações obtidas de um cidadão, órgão ou entidade, podendo se observar restrições aplicadas;
- Processamento - Onde realiza-se o processamento dos dados para obtenção de determinado resultado;
- Reprodução - Realizar cópia de um dado existente obtido por meio de qualquer processo;
- Arquivamento - Manter registros dos dados no banco de dados mesmo que os tenham o período de vigência esgotado ou perdido a validade;

- Classificação - Realizar de forma ordenada, conforme critério previamente estabelecido;
- Comunicação - Emissão de informações adequadas as políticas de ação sobre os dados;
- Utilização - Onde e para qual finalidade será realizado o aproveitamento dos dados após tratamento;
- Compartilhamento -
- Controle da informação – Regulamentar, determinar ou realizar o monitoramento quais quer ações sobre o dado;
- Eliminação - Exclusão ou destruição total dos dados armazenados no repositório;
- Divulgação - Realizar a divulgação, propagação, difusão ou multiplicação dos dados;
- Disposição - Disponibilização dos dados de acordo com algum critério estabelecido ou de força maior;
- Extração - Realizar a cópia ou retirada de dados do repositório;
- Modificação - Efetuar a alteração do dado, afins de correção ou restrição;
- Produção - Criação de bens e de serviços através do tratamento dos dados;
- Transferência - Realizar a transferência de dados de uma área de um repositório para outro, podendo também ser transferido a terceiro;
- Transmissão - Realizar a movimentação dos dados, ponto a ponta por meio de dispositivos elétricos, telefônicos, radioelétrico, eletrônicos, telegráficos, pneumáticos dentre outros;

A autoridade nacional de proteção de dados (ANPD) salienta sobre o tratamento de dados que deve se observar boa fé e princípios.

6.1 Tratamento de dados sensíveis

Ocorrera quando titular ou responsável legal consentir de forma específica para finalidades especificas. Os dados sensíveis poderão ser utilizados sem consentimento nos casos de cumprimento das obrigações legais.

> Cumprimento de obrigação legal ou regulatória pelo controlador;
> tratamento compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;
> realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;
> exercício regular de direitos, inclusive em contrato e em processo judicial, administrativo e arbitral, este último nos termos da Lei nº 9.307, de 23 de setembro de 1996 (Lei de Arbitragem);
> proteção da vida ou da incolumidade física do titular ou de terceiro; (BRASIL, 2018, p. 7)

6.2 Término do tratamento de dados

Após o tratamento de dados e os mesmos sendo utilizados para os determinados fins e proposito legitimo, específico e seguido de informar ao titular sem a possibilidade de alteração de forma incompatível a essas finalidades, temos o processo de verificação, onde será averiguado se foi alcançado o objetivo alvo, caso os dados sejam desnecessários ou de baixo valor para atingimento da finalidade do objetivo específico alvo, teremos por fim o período de tratamento dos dados. Conforme Art. 16, os dados pessoais serão eliminados após o término de seu tratamento, no âmbito e nos limites técnicos das atividades, autorizada a conservação para as seguintes finalidades.

> cumprimento de obrigação legal ou regulatória pelo controlador;
> estudo por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;
> transferência a terceiro, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei; ou
> uso exclusivo do controlador, vedado seu acesso por terceiro, e desde que anonimizados os dados. (BRASIL, 2018, p. 9)

6.3 Direitos do titular

Acesso facilitado as informações e sobre o tratamento e para qual finalidade está sendo utilizado pelo controlado e operador os seus dados coletados e tratados. Nesse ponto a transparência irá fazer a diferencia, respeitando os direitos de liberdade e privacidade. O titular terá também acesso as informações como identificação e contato do controlador.

> O tratamento de dados pessoais será irregular quando deixar de observar a legislação ou quando não fornecer a segurança que o titular dele pode esperar (BRASIL, 2018, p. 17)

6.3.1 Punições por descumprimento da lei

Com os direitos de privacidade dos dados garantido por lei, seja de pessoa física ou jurídica, possui punições caso venha ocorrer o descumprimento da lei prevista como: Multa simples de 2% (dois por cento) do faturamento da empresa no seu último exercício limitando a R$ 50.000.000.,00 (Cinquenta milhões de reais) por dia e por infração cometida. Art. 52, da lei No 13.709, de 14 de agosto de 2018 (Brasil, 2018).

> 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. (BRASIL, 2018, p. 16)

6.3.2 Seguro de proteção de dados

O seguro de proteção de dados também chamadas de segurança cibernética, tem aquecido o mercado das seguradoras, as empresas estão aderindo seguro cibernético para cobrir possíveis prejuízos causados por ataques de hackers. Mundialmente, grande parte das empresas que são vítimas de ataques cibernéticos são empresas de pequeno e médio porte, por obter ter um baixo investimento em segurança cibernética deixando vulnerabilidades a serem exploradas por hackers mal intencionados que podem realizar ataques de inúmeras formas como de negação de serviço, captura de dados pessoais sigilosos podendo chegar até mesmo extorsão solicitando algum valor de resgate onde na maioria das vezes sendo cobrado por meio de criptomoedas que possui transferências de valores que se assemelham a transações bancarias convencionais, porem as transferências utilizando as criptomoedas possuem características destaque o anonimato e dificuldade em realizar a rastreabilidade, a mais conhecida é o ”Bitcoin”.

As empresas de grande porte já possuem um investimento em segurança e políticas de segurança robustas no quesito segurança digital, além de um time de especialistas em segurança que acompanham todos os passos com o intuito de realizar testes de invasão detectando fragilidades e possíveis vulnerabilidades, tudo com o principal objetivo de gerar o menor impactos possível em serviços e plataformas digitais diminuindo da melhor forma possível o impacto de um ação maliciosa, mesmo assim, com todo esse aparato ainda acontece frequentes ataques em grandes empresas.

O Brasil está na lista dos principais alvos de ataques cibernéticos que estão crescendo diariamente, estando presente entre os principais alvos dos hackers. Para cobrir prejuízos e os danos causado por um ataque cibernético malicioso, seja um ataque de uma interrupção nas operações, captura de dados sigilosos como cartão de crédito ou documentos pessoais, as empresas que tem optado em aderir a uma seguradora de serviços digitais terão um custo desse seguro, que será por conta da empresa, podendo haver variação de valor de acordo com o tamanha da empresa, mesmo assim ainda terá que passar por uma vistoria detalhada de especialistas de segurança cibernética verificando desde a parte física como infraestrutura, instalações e alocação de equipamentos como também passara por analise os algoritmos de tratamento para possível aprovação. Com a posse das informações coletadas, tratadas e a gestão de informações corporativas tem se tornado um diferencial a obtenção de seguros cibernéticos que devem seguir uma serie de normativas estabelecidas onde devem conter camadas de proteções conforme prevista na Lei Geral de Proteção de Dados (LGPD).

O seguro cibernético fica a critério da empresa que realiza a gestão das informações de armazenar ou tratar os dados, ou seja, aderindo ou não a contratação de seguradoras não resultara na diminuição das responsabilidades legais nem a isenção de normas previstas na Lei Geral de Proteção de Dados (LGPD), muito menos quanto ao peso das punições previstas na lei.

6.3.3 Startups

Onde houver ocorrência da punição por meio de multa aplicada envolvendo startups, o valor da punição será abaixo do limite previsto na Lei Geral de Proteção de Dados (LGPD), devido as circunstâncias em virtude do regime diferenciado das empresas considerado de pequeno porte.

7 LEI DO HABEAS DATA

O Habeas data surgiu na constituição brasileira desde 1988, um requerimento onde não é gerado custas judiciais sendo gratuito por lei, essa lei foi inspirada em países como Portugal, Espanha e Estados Unidos, que adotam os direitos desde os anos de

1970, onde passaram a incluir o direito de cidadãos acessarem dados pessoais em bancos de entidades governamentais. Países como Espanha e Estados Unidos passaram a incluir o habeas data na Constituição por motivação exclusivamente político onde o Sistema Nacional de Informações (SNI), sendo mantido um banco de dados para o regime militar no período de 1964 a 1985, reunindo diversas informações sobre os cidadãos brasileiros, onde foi concedido a proteção e o direito de obter o conhecimento das informações e dos registros relacionados à própria pessoa ou até mesmo realizar a correção dos dados, desde que seja esgotada as vias administrativas para que se obtenha as informações desejadas ou solicitadas. Com isso cabe a garantir que o cidadão possua acesso aos dados e as informações pessoais que estejam sobre o poder do governo brasileiro, podendo também estar de posse de entidades privadas que obtenham informações pessoais que sejam de caráter público. Caso não haja uma convincente justificativa para legitimar a posse dos dados, eles serão um agravante ao direito e à intimidade conforme informa o Art. 5. da Constituição Federal, se não há possibilidade de acesso ao registro público e dos dados relativos à intimidade da pessoa e que é um direito à informação e a protocolo do processo que é regulamentado pela LEI Nº 9.507, DE 12 DE NOVEMBRO DE 1997. Pode-se haver uma exceção para essa regra onde ocorre o caso do cônjuge pedir a liberação de dados do parceiro falecido.

8 TRABALHOS RELACIONADOS

Com base nas pesquisas de conteúdo, que obtinham relação com a Lei Geral de Proteção de Dados (LGPD), foi encontrado como alguns dos principais temas, o qual trata-se os trabalhos relacionados, para gerar um complemento de conteúdo relacionados ao tema que foi realizado o estudo.

8.1 Proteção de dados e sua importância política e econômica no Brasil

É inevitável que deixamos rastros todos os dias, em diversas atividades cotidianas, mais ainda tratando-se do rastro digital que ocorre quando damos um “like” ou realizamos o compartilhamento de algo de nosso interesse nas redes sociais, uma ação como essa é coletada como sua preferência sobre alguns temas. Ao realizar um

cadastro para obter acesso a um site ou serviço na internet, fornecemos dados importantes, como as informações dos dados do seu documento de identificação (RG) ou carteira de motorista (CNH) e até mesmo o seu endereço. Ao informar o seu número de Cadastro de Pessoa Física (CPF) na compra ou ganhar desconto de um produto qualquer, estamos fornecendo ao vendedor nossos dados e informações sobre o que temos interesse e o valor que gastamos. A utilização de acesso digital para entrar em um prédio, deixamos o registro biométrico sob a responsabilidade das empresas e órgãos, em que, muitas vezes são desconhecidos.

Existem casos em que a simples proximidade de dispositivos como câmeras e microfones pode significar a gravação de imagens com registro de gestos e conversas. Os rastros de nossas atividades, assim como informações sobre nós como RG, CPF, data de nascimento, sexo, etnia, endereço residencial e comercial, nome de pai e da mãe, ou seja, uma verdadeira infinidade de dados informados que ao serem coletados e tratados, transformam-se em dados pessoais de um determinado cidadão. Com a expansão cada vez maior das tecnologias digitais, uma grande variedade de informações são transformadas em bits sendo 0 e 1, que estarão reunindo e fazendo um cruzamento dessas informações que analisadas em bancos de dados de capacidade continuamente crescente e com sistemas cada vez mais complexos de diversos algoritmos de coleta e tratamento de dados, inclusive com alta capacidade de processamento e inclusão de sistemas de inteligência artificial (IA).

8.2 Riscos

Com a disseminação da coleta massiva de informações das pessoas, os riscos de abusos e violação ao direito à privacidade garantido no Brasil pela Constituição Federal vêm crescendo, provocando o debate sobre a necessidade de legislações específicas. No Brasil, há duas propostas tramitam no Congresso. Outros países já contam com suas normas. As violações e os abusos envolvem desde empresas privadas ao Poder Público, de equipamentos e grandes bancos de dado.

Em 2013, o Tribunal Superior Eleitoral (TSE) firmou acordo para repassar os dados de mais de 100 milhões de eleitores à empresa de crédito Serasa, essa medida que acabou suspensa após a infinidade de críticas. Em 2015, a Samsung admitiu que aparelhos chamados por ela de “TVs inteligentes” gravavam as conversas próximas.

Em 2014, o ex-agente da Agência Nacional de Segurança dos Estados Unidos Edward Snowden denunciou que o governo daquele país espionava autoridades e pessoas em diversos países, com auxílio de grandes empresas de tecnologia.

8.3 Manipulação eleitoral

Nos últimos tempos, a discussão que gira em torno dos riscos aos sistemas democráticos do setor eleitoral é encarrada como ponto de maior criticidade devido aos fatos ocorridos no meio eleitoral de alguns países e que o Brasil estaria nessa lista de países, como um fruto de desejo pois o Brasil possui um certo peso na influência internacional. Em março, reportagens de jornais no Reino Unido e nos Estados Unidos revelaram um vazamento de dados de 87 milhões de pessoas coletados no Facebook por meio de um aplicativo de perguntas, que foram posteriormente repassados a uma empresa britânica de marketing digital, Cambridge Analytica. Munida dessas informações, ela teve papel decisivo na eleição de Donald Trump e na saída do Reino Unido da União Europeia, conhecida como “Brexit”. A firma também operou em eleições de outros países, como Quênia, Austrália, México, além de estabelecer escritório no Brasil.

Ao reunir informações sobre o perfil das pessoas, suas preferências, seus medos e suas visões de mundo, marqueteiros e responsáveis por campanhas conseguiam produzir e disseminar conteúdos quase personalizados. Em reportagem da TV britânica Channel 4, um dos dirigentes da Cambridge Analytica relatou que a empresa explorava sentimentos dos eleitores, como o medo, para vincular os receios dos públicos-alvo a candidatos adversários, buscando manipular as emoções em favor de seus clientes. Coincidência ou não, Donald Trump recebeu esse apoio e acabou sendo eleito presidente do país mais poderoso do mundo depois de sair de uma posição desacreditada.

O escândalo alertou autoridades e usuários para os riscos da falta de proteção de dados pessoais. Governos dos Estados Unidos, do Reino Unido e, inclusive, do Brasil, abriram investigações sobre o caso. O presidente do Facebook, Mark Zuckerberg, e outros dirigentes da plataforma foram sabatinados nos parlamentos dos EUA e do Reino Unido. Na ocasião, Mark Zuckerberg admitiu que a empresa falha no cuidado com a privacidade de seus usuários e anunciou algumas medidas.

8.4 Mercadoria valiosa

Outro risco está no aumento da demanda pela coleta de dados na economia. Essas informações vêm sendo consideradas um insumo fundamental para diversos setores, recebendo o apelidados de “novo petróleo” por empresas, organizações internacionais e analistas. Os dados são a base de processos da “indústria 4.0” ou “transformação digital”. Segundo o Fórum Econômico Mundial, a transformação digital pode gerar até US$ 10 trilhões anuais na próxima década (R$ 35,4 trilhões, ou 5,3 vezes o Produto Interno Bruto brasileiro registrado em 2017). A Europa projeta um crescimento da sua economia de dados de € 285 bilhões para € 739 bilhões entre 2015 e 2020.

Com isso, a coleta de dados tornou-se um negócio não apenas de empresas de tecnologia da informação, mas de uma gama variada de setores, provocando preocupações quanto a usos indevidos. Em 2011, a Disney foi multada em R$ 10 milhões por coletar e compartilhar informação de crianças, violando a Lei de Proteção Online da Infância dos Estados Unidos da América.

No Brasil, disparou o número de farmácias passaram a oferecer descontos em troca de descontos. O Ministério Público do Distrito Federal e Territórios (MPDFT) abriu investigação neste ano para apurar se as informações estavam sendo repassadas a planos de saúde. Redes de supermercado também passaram a oferecer descontos em troca de cadastros em programas de fidelização por meio de aplicativos. No ano passado, o Instituto de Defesa do Consumidor (Idec) questionou o Grupo Pão de Açúcar sobre o tratamento das informações com vistas a averiguar se não haveria desrespeito ao Marco Civil da Internet.

8.5 Discriminação

Os dados das pessoas são usados também para definir perfis de consumidores. São práticas como essa que se vem aumentando os questionamentos sobre a discriminação de pessoas por classe, cor e endereço à contratação de serviços. A organização ProPublica, dos Estados Unidos, denunciou em 2016 que o mercado imobiliário aproveitava a segmentação do Facebook para excluir negros de anúncios de imóveis.

Em 2018, o Ministério Público do Rio de Janeiro abriu investigação contra o site de venda de passagens e pacotes Decolar.com ao constatar discriminação nos preços ofertados de acordo com a localização do usuário. O Instituto de Defesa do Consumidor (Idec) lançou campanha criticando a “nota de crédito”, um índice formulado a partir das informações de cada pessoa para definir, entre outras coisas, limite de cartão de crédito e condições de financiamento. A entidade cobra transparência para que os cidadãos saibam os critérios utilizados e como estão sendo classificados.

8.6 Segurança

A falta de segurança na guarda das informações, uma das dimensões da proteção de dados, também ganhou visibilidade. Em 2017, a agência de crédito Equifax teve dados de 143 milhões de clientes vazados. A firma está sendo acionada judicialmente em processo avaliado em US$ 70 bilhões. Em 2016, um vazamento envolveu informações de 57 milhões de usuários da plataforma de mobilidade Uber, sendo 196 mil brasileiros.

9 LEI DA UNIÃO EUROPEIA ATINGE TODO O MUNDO

A lei afeta o Facebook, Google e até mesmo empresas no Brasil, com regra em que se exige de quando venha ocorrer os cenários em que se tenha conformações e fatos do vazamento de informações de pessoais que seja avisado em até 72 horas impondo multas duras para o não cumprimento do acordado.
A lei de proteção de dados pessoais da União Europeia, que está vigente desde maio de 2018, tem o poder de afetar a vida de todas as empresas e os usuários que tiverem relações com o bloco econômico e político europeu que é formado atualmente por 28 países.
Segue alguns pontos considerados principais do GDPR:

- Os usuários podem, em algumas situações pontuais, verificar, corrigir ou até mesmo deletar as informações que empresas guardam sobre ele;

- As empresas devem coletar somente os dados necessários para que seus serviços funcionem de forma adequada;
- O ato de coleta e o uso de dados pessoais só podem ser realizados com consentimento explícito do titular dos dados;
- As informações de crianças e jovens terão proteção especial;
- O prazo para que seja reportado aos clientes é de 72 horas, onde ocorrerem casos com indícios que tiverem dados hackeados;
- As empresas devem informar o termo de política de forma clara com linguagem compreensível de sua política de proteção de dados;
- Casos de infrações terão punição com multa pesada, de € 20 milhões ou 4% do volume global de negócios da empresa envolvida;
- Os dados de europeus podem ser transferidos somente para os países que possuem uma lei em vigência de proteção de dados no mínimo equivalente a europeia;
- As empresas que tratem os dados de cidadãos europeus têm que seguir a lei europeia;
- As grandes entidades processadoras de informação têm de guardar os históricos, de todas as vezes em que os dados foram manipulados;

9.1 Efeitos da GDPR no Brasil

Mesmo que a lei de proteção de dados pessoais da União Europeia, seja direcionada aos europeus como também a pessoas de outras nacionalidades mais que moram na Europa, a lei pode gerar um potencial impacto aos internautas e as empresas de tecnologia de todo mundo. Considerando que toda e qualquer companhia que manipule dados pode ser impactada, caso guarde ou receba informações de europeus, que advém desde instituições financeiras como até pousadas e ou restaurantes em pontos de turísticos.

As empresas brasileiras terão como responsabilidade se adequar e colocar em pratica as regras da Lei Geral de Proteção de Dados (LGPD), caso isso não ocorra as empresas estarão sujeitas a penalidades sendo às sanções previstas na lei, ainda que, especialistas informam que a falta de uma lei de proteção de dados no Brasil

poderia gerar complicações para as empresas visto que é realizado um excessivo no processamento de cidadãos europeus. Os países que possuem a lei de proteção de dados, não terão certeza que irá receber os dados de cidadãos europeus para passarem por tratamento, casos onde apresentem alterações na lei de proteção de dados ou algum tipo de impeditivo como o nível de segurança atual, o pais e suas leis passaram por análise onde será verificado o nível de segurança adotado durante o fluxo de tratamento.

Ainda sobre segurança, o nível adotado de proteção pela União Europeia, está presente em quinze (15) países, que estão de acordo com a lei europeia anterior, sendo assim, vigorando a GDPR ocorre uma nova fase para países vizinhos, realizando a adequação para ver se essas leis estão alinhadas e sendo seguidas.

Um fato ocorrido o caso Snowden o foi levado aos tribunais de justiça europeus as práticas de segurança adotada a respeito dos dados pessoais no Reino Unido e de organizações como a Agência de Segurança Nacional (NSA).

O analista de sistemas e ex-agente da Agencia de Inteligência Civil (CIA) Edward Snowden, veio a tornou público o fato que a agência de espionagem norte-americana obtinha ordens judiciais secretas para obter acesso aos serviços conectados de cidadãos, tendo como objetivo, realizar a coleta e abastecimento de um sistema de monitoramento em massa, outros meios juntamente utilizados para realização da coleta eram por aplicativos de jogos, quis e redes sociais.

O tribunal europeu julgou e logicamente considerou as práticas de utilizadas ilegais por descumprimento da dei de proteção de dados, como medida imediata ao ocorrido a União Europeia veio a estabelecer um novo acordo de tratamento e transferência de dados com os Estados Unidos(EUA), esse novo acordo realizado chamado de safety shield ou escudo de proteção, entrou em vigor em 2016 mas, conforme apontam observadores e especialistas europeus, não está em conformidade com o GDPR e poderá passar por atualizações.

9.2 Direito ao Esquecimento

O Tribunal de Justiça da União Europeia decidiu em 2014, que as principais ferramentas de busca da internet, deveriam excluir os resultados e os links onde foram

contestados por cidadãos europeus desde que as páginas exibidas possuíssem informações pessoais desatualizadas ou equivocadas.

O chamado direito ao esquecimento deixa de ser uma decisão da Justiça e passa a ser lei onde se torna obrigado a deletar registros de informações pessoais e de todos os serviços que manipulam os dados das pessoas, incluindo as redes sociais como o Facebook, Twitter como também meios de pagamento e de serviços como de turismo. Com o GDPR, a exclusão das informações é uma obrigatoriedade, porém com a ressalva de que as empresas poderão manter as informações realmente necessárias o para propósitos históricos, estatísticos, científicos, saúde pública e até mesmo para exercer o direito de liberdade de expressão.

9.3 Proteção para crianças

O direito ao esquecimento foi criado um capítulo especial para proteção as crianças, com intuito de evitar a exposição excessiva na internet e redes sociais que teriam interesse em contar com crianças entre seus membros terão de pedir consentimento aos pais. Cada país decidirá a faixa etária se aplica essas restrições, que poderá variar dos treze (13) aos dezesseis (16) anos. Para utilização da plataforma como WhatsApp foi estabelecido a faixa etária de 16 anos a idade mínima para usar o app no bloco comum europeu.

9.4 Portabilidade de dados

O titular dos dados pessoais passou a ter o direito de realizar a portabilidade de suas informações de um serviço conectado para outro, sem sofrer qualquer tipo de restrição por parte da empresa atual. A portabilidade assemelha se a uma portabilidade de um número de celular, onde troca-se de operadora mais se mantem o número do celular. As empresas devem criar meios para clientes baixarem um pacote com todas os dados armazenados por ela, assim como o Facebook e Google já possuem.

9.5 Alerta a clientes hackeados

As empresas passam a ser obrigadas a avisar clientes, todas as vezes que tiverem seus servidores comprometidos por hackers e que resulte na exposição de informações pessoais. O período que as empresas têm é de 72 horas desde quando tomaram ciência do vazamento dos dados, inclusive se os sistemas hackeados forem os de empresas terceirizadas.

9.6 Transferência de dados

As informações de europeus só podem ser transferidas para empresas que estiverem em países que possuem as leis de proteção de dados tendo como requisito mínimo que seja equivalente às leis da União Europeia. Caso a empresa não possui os requisitos mínimos, outra saída para essas empresas é de adotar um conjunto de práticas para que atendam o que é acordado com o GDPR. As empresas europeias, por sua vez, serão cobradas para apenas contratar fornecedores que cumpram a lei.

10 ESTRATÉGIA PARA OBTENÇÃO DE DADOS

Nos dias que ocorrem, as empresas ganham valor com a excelência na prestação de serviços como também na oferta valores justos e objetos de interesse para seus clientes, um desses objetos de interesse podendo ser chamado de dados, para obtenção dos dados as empresas se utilizam de estratégias variadas uma delas utilizada pela empresa Cambridge Analytica para obter posse de dados foi a arquitetura de realizar a criação do quiz “This is Your Digital Life” no Facebook, a empresa de consultoria e marketing digital Cambridge Analytica utilizou de uma estratégia que pode-se dizer infalível para obter posse de um verdadeiro ouro, melhor dizendo o novo ouro, o novo ouro é uma referenciação aos dados de usuários. Dados que inclusos em plataformas robustas e amplamente utilizadas como Facebook e Google, visto que essas plataformas possuem um gigantesco volume de dados e se fez dos dados um grande alvo de interesse e o qual foi destaque em noticiários em todo o planeta, noticiando o vazamento de dados de 87 milhões de usuários da plataforma Facebook e foram usados pela empresa de consultoria Cambridge Analytica.

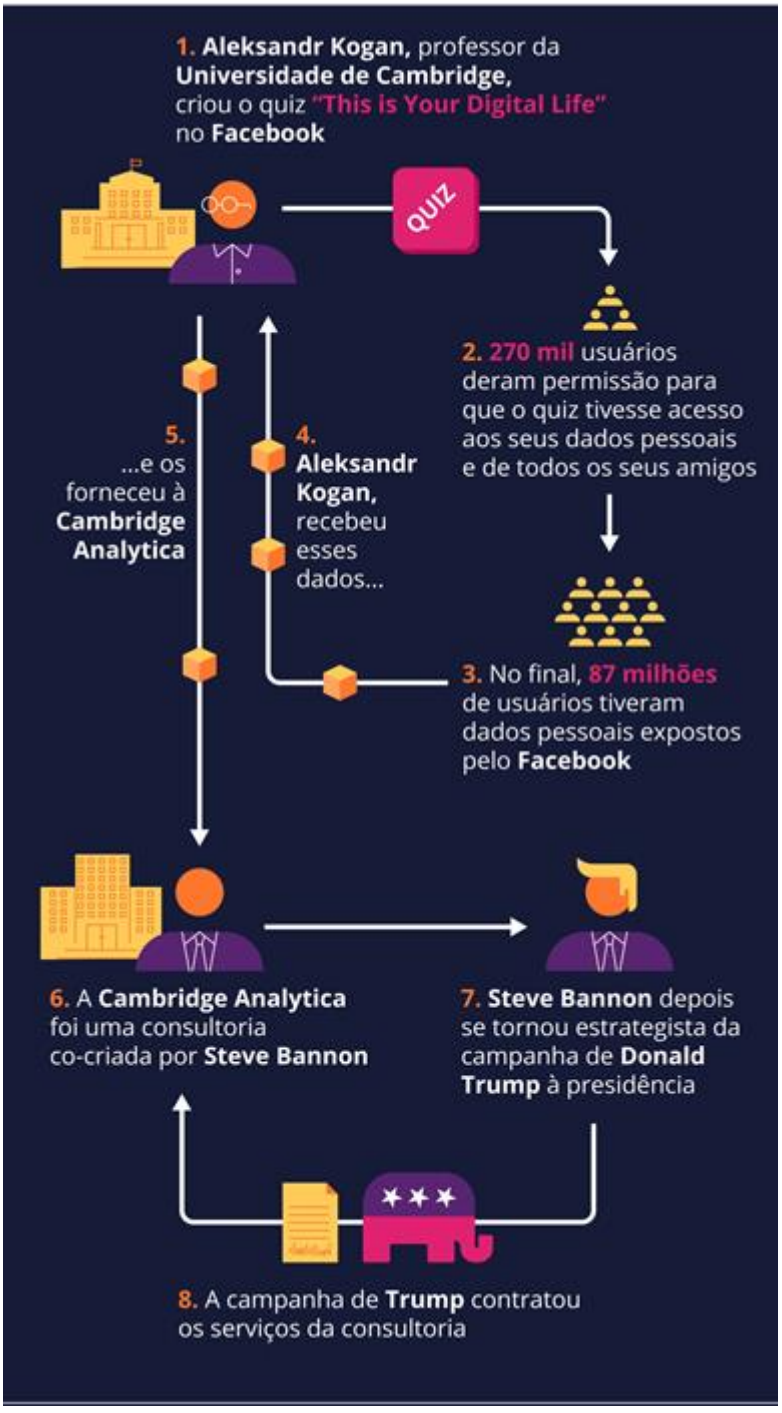
Mesmo que empresas se utilizem de meios estratégicos para obtenção de dados elas devem respeitar políticas de privacidade estipulados por órgãos reguladores como o órgão regulador britânico, ICO “Information Commissioner's Office”.

A empresa de consultoria e marketing digital Cambridge Analytica reconheceu ter desrespeitado a ordem do órgão regulador britânico (ICO), órgão que é o encarregado de da proteção de dados.

> “A titular do órgão, Elizabeth Dunham, criticou a plataforma pelos erros nos casos. “O Facebook falhou em proteger de maneira suficiente a privacidade de seus usuários antes, durante e depois o processamento ilegal de seus dados. Uma companhia deste tamanho e expertise deveria ter sabido melhor como atuar e deveria ter feito melhor”, afirmou, em comunicado oficial da autoridade.” (PORTAL EBC, 2018).

A divulgação da arquitetura utilizada pela empresa Cambridge Analytica (Figura 1), divulga como foi todo o fluxo de obtenção de dados.

Figura 1 - Arquitetura



Autor: G1.com, Infográfico elaborado em: 20/12/2018

11 COMO APRIMORAR A SEGURANÇA DAS INFORMAÇÕES NA ERA DO TRABALHO REMOTO?

Com programas como Mobility que vem se difundindo com grande celeridade na cultura de empresas atuantes em território nacional, reforça ainda mais a atenção no

quesito segurança digital. Em empresas adeptas de programas Home Office é flexibilizando o ambiente de trabalho principalmente em casa e às vezes no escritório isso, é um desafio e tanto, ainda mais porque a demanda por trabalho remoto é inevitável. De acordo com um levantamento da Confederação Nacional das Indústrias (CNI), mais de 80% dos trabalhadores brasileiros admitem que gostariam de ter algum tipo de atividade remota. Outra análise, dessa vez da consultoria Robert Half, aponta o Brasil como o terceiro país do mundo no ranking com o maior aumento das iniciativas de flexibilização e digitalização dos espaços de trabalho.

Saindo da questão se Home Office ou trabalho remoto se é vantagem ou desvantagem para empresa e se melhora ou não as entregas dos resultados de seus colaboradores, com o avanço da tecnologia e da Internet, ganhamos uma série de novas ferramentas que estão revolucionando a disponibilidade das informações. Por outro lado, o acesso móvel das plataformas de negócios também provoca suas questões. A maior delas, sem dúvida, é que os dados sigilosos de sua operação podem estar em risco, diante de ameaças cada vez mais sofisticadas. Ao realizar conexão as redes não seguras e devido a praticidade, efetuar a vinculação de contas particulares junto a conta corporativa estaria abrir uma porta de vulnerabilidade para realizar coleta de dados, podendo ser ela de forma lícita ou ilícita com aplicações maliciosas.

Líderes e executivos estão sendo chamados a entender como implementar essas ações com segurança, extraindo o máximo valor e qualidade da distribuição móvel das forças de trabalho. Segundo pesquisas do Gartner, até 2021, aproximadamente 75% de todas as iniciativas para alavancar novas formas de trabalho digital ao redor do mundo falharão. Entre os motivos, estão a falta de liderança, dificuldades relacionadas a infraestrutura e, ainda, a falta de atenção às brechas de segurança geradas a partir da maior mobilidade dos colaboradores.

A missão dos líderes é de tornar a experiência móvel dos colaboradores muito mais proveitosa e produtiva para a organização, sem descuidar das questões práticas da política de segurança.

Neste cenário, é importante que as companhias entendam o que está em jogo com o deslocamento dos espaços de trabalho. Por exemplo: para que a mobilidade corporativa funcione efetivamente, é preciso garantir a alta disponibilidade dos

sistemas e a conectividade à disposição dos profissionais. Esse passo é essencial para garantir uma experiência adequada aos colaboradores.

No entanto, o trabalho remoto deve ser trabalhado de forma adequada, sem descuidar da segurança. Por isso, é sempre importante que as companhias desenvolvam planos voltados à identificação e mitigação das ameaças externas, criando ambientes realmente preparados para combater as possíveis vulnerabilidades ou riscos e, ao mesmo tempo, maximizar a oferta de tecnologia aos profissionais. Após essa análise, as empresas poderão adotar soluções práticas e totalmente direcionadas as suas necessidades operacionais.

Uma das ações fundamentais para garantir a disponibilidade de dados de forma segura é a implementação de um firewall na rede. Essa é uma ação de segurança primordial e bastante eficiente, pois é esse o recurso que ajudará a filtrar as solicitações, protegendo os sistemas corporativos. O firewall é uma importante ferramenta de controle, capaz de avaliar e identificar os comportamentos suspeitos dos usuários.

Outra dica é construir políticas de Controle de Acesso mais ajustadas, estabelecendo os níveis de identificação, autenticação e disponibilidade das informações a partir do perfil, cargo e área do colaborador. Reforçar a necessidade de proteger os dados mais sigilosos é importante, principalmente, com o avanço dos programas de BYOD em inglês Bring Your Own Device (Traga seu próprio Dispositivo), em que cada funcionário pode usar seus próprios equipamentos. Desta forma, ao estabelecer diferentes níveis de privilégio no acesso, evita que um colaborador tenha acesso a dados que não são de sua competência.

Vale destacar, ainda, que os líderes de tecnologia também devem reforçar as regras e modalidades dos processos de identificação e autenticação do acesso aos sistemas corporativos. Criar regras específicas para a definição de senhas e combinar diferentes fatores de autenticação para login e visualização de conteúdo são duas etapas muito indicadas. O objetivo dessas ações é simples: quanto mais camadas de proteção no acesso aos seus sistemas, maior o nível de proteção de seus sistemas.

Além disso, é essencial que as companhias consigam monitorar e controlar a performance de suas redes. Nesse contexto, uma opção é investir em ações de Shadow IT com a contratação de serviços direcionados à avaliação contínua da rede.

Essa prática possibilita um ciclo de inovação mais rápido e orientado aos resultados, sem a necessidade de alteração física do ambiente. Dessa forma, é possível reduzir o tempo e a burocracia das aprovações internas e consolidar mecanismos de controle muito mais rápidos. Em tempos de transformação diária da área de TI, agilizar a análise é fundamental para avaliar o uso de aplicações desconhecidas ou não autorizadas e para prevenir vazamentos de dados e outros incidentes, não há mais dúvidas de que o trabalho remoto é o futuro das operações. Com esse caminho, as companhias terão mais agilidade e oportunidades para integrar novos talentos, tornar a tomada de decisão mais rápida e satisfazer os consumidores de forma completa. A boa notícia é que até mesmo os desafios para a gestão das informações, hoje, estão mais simples e fáceis de se vencer. O mercado está preparado para apoiar as organizações que querem trilhar com sucesso essa jornada. Sem dúvida, os executivos que optarem por liderar suas empresas com segurança vão garantir o sucesso e a perpetuidade dos negócios na nova era digital.

12 METODOLOGIA

O método de pesquisa utilizado foi a básica estratégica, pela qual foi realizado o uso da coleta dos dados através de pesquisa em literaturas digitais. Tendo como base a Lei Geral de Proteção de Dados (LGPD), Nº 13.709, de 14 de agosto de 2018, que entrara em vigência em agosto de 2020. A pesquisa foi realizada para fins de esclarecer pontos específicos e de certa forma provocar o interesse sobre a lei que entrara em vigor trazendo e, realizando uma abordagem de forma clara e simplificada pontuando alguns pontos estrategicamente escolhidos e especificamente para salientar o quanto é importante que os dados estejam protegidos e com segurança.
Considerando que os dados são um produto de grande valor, ainda quando passado por um tratamento adequado de dados, pode-se traçar um perfil de um indivíduo podendo gerar causas drásticas ao regime político que rege sobre o país,
O impacto pode chegar de pequenas a grandes proporções impactando as decisões de empresas, como a escolha da data de lançamento do novo produto ou a tomada de decisão de uma estratégia de negócio e a até mesmo escolha de um novo presidente.

13 CONSIDERAÇÕES FINAIS

Diante do fim do trabalho podemos considerar que a explanação sobre a Lei Geral de Proteção de Dados (LGPD) tornou-se mais clara em pontuais aspectos de tratamento de dados, desmistificando informações tornando o conhecimento sobre o assunto menos enigmático lhe deixando mais detalhado nos pontos onde foi abordado em detalhes os processos de tratamento de dados e citando por meio de exemplos o real poder que um tratamento de dados, podendo interferir em decisões de uma nação.

Obter o conhecimento sobre para qual a finalidade da coleta de nossos dados e porque passam pelo tratamento e pôr fim a destruição desses dados, será de grande importância e estaremos amparados por lei caso ocorra alguma falha de um tratamento inadequado pelo operador e controlador de dados ou até um vazamento de informações pessoais e sensíveis.

Como um supervisor de todos os passos realizados durante o processo de tratamento teremos a Autoridade Nacional de Proteção de Dados (ANPD) que terá a missão de fiscalizar os processos e técnicas adotadas para que esse tratamento ocorra com segurança preservando a integridade dos dados do cidadão.

14 REFERÊNCIAS

ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS. **ABNT NBR 6023**:Informação e documentação: referências: elaboração. Rio de Janeiro, 2018.

BRASIL, **Diário Oficial da União**, dispõe sobre a proteção de dados pessoais, Publicado em: 15/08/2018 | Edição: 157 | Seção: 1 | Página: 59 Órgão: Atos do Poder Legislativo Disponível em: <http://www.justicaeleitoral.jus.br/arquivos/tre-go-lei-13-709-2018>. Acesso em: 04 out. 2019.

BRASIL, **Diário Oficial da União**: Imprensa Nacional, Publicado em: 15/08/2018, Edição: 157, Seção: 1, Página: 59 Órgão: Atos do Poder Legislativo LEI NO 13.709, DE 14 DE AGOSTO DE 2018. Disponível em: <https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-norma-pl.html>. Acesso em: 11 nov. 2019.

BRASIL, **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Legislação Informatizada - LEI Nº 13.709, DE 14 DE AGOSTO DE 2018 - Publicação Original. Brasília - DF, p. 30, ago. 2018. Disponível em:<https://www2.camara.leg.br/legin/fed/lei/2018/lei-13709-14-agosto-2018-787077-publicacaooriginal-156212-pl.html>. Acesso em: 04 out. 2019.

BRASIL. LEI NO 13.709, DE 14 DE AGOSTO DE 2018. Imprensa Nacional, 2018. Disponível em: <http://www.in.gov.br/materia/-/asset_publisher/Kujrw0TZC2Mb/content/id/36849373/do1-2018-08-15-lei-no-13-709-de-14-de-ag>. Acesso em: 30 nov. 2019.

CIO, **Como aprimorar a segurança das informações na era do trabalho remoto?,** Disponível em: <https://cio.com.br/como-aprimorar-a-seguranca-das-informacoes-na-era-do-trabalho-remoto/>. Acesso em: 10 dez. 2019.

Diário dos Campos, **Geral**, Governo britânico multa Facebook por violação de privacidade. Publicado em 25/10/2018 - 14:29, Disponível: em:<https://www.diariodoscampos.com.br/noticia/governo-britanico-multa-facebook-por-violacao-de-privacidade>. Acesso 05 dez. 2019.

Editora Abril, **Exame**, P. AFP, Cambridge Analytica se declara culpada por uso de dados do Facebook, Disponível em:<https://exame.abril.com.br/tecnologia/cambridge-analytica-se-declara-culpada-por-uso-de-dados-do-facebook/>. Acesso em:26 nov. 2019.

PORTAL EBC, **Agência Brasil**, Governo britânico multa Facebook por violação de privacidade, Disponível em: <http://agenciabrasil.ebc.com.br/internacional/noticia/2018-10/governo-britanico-multa-facebook-por-violacao-de-privacidade>. Acesso em: 05 dez. 2019.

PORTAL EBC, **Agência Brasil**, Governo publica MP que cria órgão para proteção de dados, Disponível em: < http://agenciabrasil.ebc.com.br/geral/noticia/2018-12/governo-publica-mp-que-cria-orgao-para-protecao-de-dados>. Acesso em: 10 dez. 2019.

PORTAL EBC, **Agência Brasil**, Proteção de dados ganha importância na política e economia no Brasil, Disponível em: <https://agenciabrasil.ebc.com.br/economia/noticia/2018-05/protecao-de-dados-ganha-importancia-na-politica-e-economia-no-brasil>. Acesso em: 28 jul. 2020.

Serasa Experian, **Whitepaper**, A sua empresa já está preparada para a Lei Geral de Proteção de Dados Pessoais, Disponível em: <https://www.serasaexperian.com.br/blog/sua-empresa-esta-preparada-para-a-lgpd?> Publicada em 10/04/2019. Acesso em: 11 nov. 2019.

PORTAL GOV.BR, **Presidência da República**, Subchefia para Assuntos Jurídicos, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm#:~:text=e%20ao%20adolescente.-,Art.,e%20um%20anos%20de%20idade>. Acesso em: 16 ago. 2020.

PORTAL GOV.BR, **Presidência da República**, Regulamento do direito de acesso a informações e disciplina o rito processual do habeas data, Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l9507.htm#:~:text=Regula%20o%20direito%20de%20acesso,rito%20processual%20do%20habeas%20data.&text=Par%C3%A1grafo%20%C3%BAnico.&text=2%C2%B0%20O%20requerimento%20ser%C3%A1,de%20quarenta%20e%20oito%20horas>. Acesso em: 22 ago. 2020.

Postal UOL, **Segurança**, para se precaver da LGPD, empresas correm atrás de seguro cibernético, Disponível em: <https://www.uol.com.br/tilt/noticias/redacao/2020/08/23/cresce-procura-por-seguro-para-riscos-ciberneticos.htm>. Acesso em: 29 ago. 2020.

PORTAL EBC, **Agência Brasil**, Vigência da Lei de Proteção de Dados depende de sanção da MP 959, Disponível em: <https://agenciabrasil.ebc.com.br/politica/noticia/2020-08/vigencia-da-lei-de-protecao-de-dados-depende-de-sancao-da-mp-959>. Acesso em 05 set. 2020.

Canaltech, **Espionagem**, XKeyscore: programa da NSA é capaz de vigiar os internautas em tempo real, Disponível em: <https://canaltech.com.br/espionagem/XKeyscore-um-programa-da-NSA-capaz-de-vigiar-os-internautas-em-tempo-real/ >. Acesso em 12 set. 2020.

THE Social Dilemma, Direção de Jeff Orlowski, Produção de Exposure Labs Argent Pictures The Space Program. Estados Unidos: Netflix, 2020. (94min.).

THE Hack, Direção de Karim Amer e Jehane Noujain, Produção de Noujain Films. Estados Unidos: Netflix, 2019. (104min.).

CONNECTED: The Hidden Science of Everything, (Temporada 1). Direção: Christopher Collins, Produtora Zero Point Zero Production, Estados Unidos: Netflix, 2020.