**CURSO DE DIREITO**

Lucas Rösner Ferreira

# A LEI 13.709/18 E OS NOVOS DESAFIOS DIANTE DE UM CONTEXTO TECNOLÓGICO

Capão da Canoa
2021

Lucas Rösner Ferreira

# A LEI 13.709/18 E OS NOVOS DESAFIOS DIANTE DE UM CONTEXTO TECNOLÓGICO

Projeto de Trabalho de Curso, modalidade monografia, apresentado ao Curso de Direito da Universidade de Santa Cruz do Sul, UNISC, como condição para aprovação na disciplina de Trabalho de Curso.

Orientadora: Profa. Ms. Ana Helena Karmas Hoefel Pamplona

Capão da Canoa

2021

## AGRADECIMENTOS

Agradecer a Deus e a todas as pessoas que de alguma forma contribuíram para a realização e conclusão deste trabalho, é sem dúvidas uma tarefa difícil, mas no fim, gratificante, sendo assim, gostaria de deixar expresso os seguintes agradecimentos:

Em primeiro lugar agradeço a meus pais, Janete Rösner e Amarildo da Silva Ferreira, por serem inspiração de vida, dedicação no que estão dispostos e por todo apoio de divergentes maneiras que me concederam, sempre positivos e pacientes, da qual se tornaram meu porto seguro na construção deste trabalho, nunca medindo esforços para qualquer ajuda que precisei, em qualquer âmbito. Obrigado por tanto pai e mãe.

Agradeço a minhas irmãs, por todo apoio e em especial a minha namorada Karen Bresolin, que chegou a minha vida justamente nesse período, onde foi muito corrido, mas ela estava sempre ao meu lado, sendo paciente, não medindo esforços para me apoiar.

As professoras Ana Helena Karnas Hoefel Pamplona e Elis Cristina Uhry Lauxen por todo aprendizado e dedicação que me forneceram ao longo destes anos na graduação, muitos especificamente na construção deste trabalho. Agradeço ainda a todos os demais funcionários da UNISC que de alguma maneira me relacionei, em especial a Coordenação do Direito.

Por fim a Deus novamente, por ter me dado a felicidade de ter em minha vida estas pessoas especiais que agregaram na construção deste trabalho, concebendo-me ensinamentos, paciência e calma para não desistir.

*“É no conhecimento que existe uma chance de libertação.”*
**Leandro Karnal**

## RESUMO

O direito à privacidade é uma garantia constitucional no ordenamento jurídico interno. Assim, quando da perspectiva da proteção dos dados dos usuários, as empresas devem ter uma responsabilidade ainda maior, principalmente, se a divulgação de quaisquer informações puder gerar dano à pessoa. Trata-se de não apenas um dever decorrente do exercício da atividade empresarial, mas da própria proteção à dignidade dos sujeitos. Nesse sentido, essa pesquisa assumirá como problemática: quais as aplicações da Lei Geral de Proteção de Dados Pessoais (LGPD para as empresas quando da proteção dos dados dos usuários? Assim, parte do pressuposto que diante dos avanços dos recursos tecnológicos, é fundamental que as normas acompanhem as novas necessidades sociais. Para desenvolver essa pesquisa, elege-se como objetivo geral **c**ompreender como a Lei Geral de Proteção de Dados Pessoais (LGPD) modifica o comportamento das organizações quanto ao dever da proteção dos dados do usuário. Essa pesquisa foi desenvolvida a partir de uma revisão bibliográfica exploratória. O objeto apresenta uma mutação o que requer exames sobre o seu movimento e, por consequência, seus possíveis impactos.



**Palavras-Chave**: Privacidade. Usuários da rede. Responsabilidade empresarial. Proteção.

## ABSTRACT

The right to privacy is a constitutional guarantee in the internal legal system. Thus, from the perspective of protecting user data, companies should have an even greater responsibility, especially if the disclosure of any possible information causes harm to the person. It is not only a duty arising from the business exercise, but also the protection of the subjects' dignity. In this sense, this research will assume as problematic: what are the applications of the General Law for the Protection of Personal Data (LGPD for companies when protecting the data of users? So, part of the assumption that in view of the advances in technological resources, it is essential that the norms accompany the new social needs.To develop this research, the general objective is to understand how the General Law for the Protection of Personal Data (LGPD) modifies the behavior of associations regarding the duty to protect user data. from an exploratory bibliographic review. The object presents a mutation which requires exams about its movement and, consequently, its possible impacts.



**Keywords:** Privacy. Network users. Corporate responsibility. Protection.

**SUMÁRIO**


**1 INTRODUÇÃO ..... 4**

**2 PROTEÇÃO DE DADOS: LEI 13.709/18: CARACTERÍSTICAS GERAIS, DIREITO COMPARADO E A JUDICIALIZAÇÃO ..... 6**

**2.1 Sanções e responsabilidade ..... 10**

**2.2 Direito digital como forma de prevenção ao crime cibernético..... 16**

**2.2.1 Panorama sobre temas diversos que envolvem o direito digital ..... 21**

**3 A EFICÁCIA NO COMBATE A ESSAS INFRAÇÕES, PARA EMPRESAS E PESSOAS FÍSICAS ..... 24**

**3.1 Identificação do autor ..... 24**

**3.2 A eficácia da legislação no combate ..... 28**

**3.3 Onde está o maior impacto no vazamento de dados ..... 31**

**3.4 Casos midiáticos no Brasil ..... 40**

**3.5 Das sanções aplicada em outros países ..... 43**

**4 OS RECURSOS TECNOLÓGICOS DE SEGURANÇA EXISTENTES NA ATUALIDADE, NA PROTEÇÃO DE DADOS ..... 46**

**4.1 O sistema de proteção de dados mais avançado na atualidade ..... 46**

**4.1.1 A forma como esses sistemas são desenvolvidos ..... 49**

**4.2 Investimento de empresas em sistemas de proteção ..... 51**

**4.3 Sistemas de proteção do Poder Judiciário ..... 56**

**5 CONCLUSÃO..... 62**

## 1 INTRODUÇÃO

O direito à privacidade é classificado como uma garantia fundamental de primeira dimensão. Ainda assim, é fundamental que o Estado desenvolva um conjunto de políticas públicas que possibilitem o indivíduo exercer essa garantia. No âmbito do ordenamento jurídico interno, a Constituição Federal da República Brasileira de 1988 (CFRB/88), dentre outros dispositivos, reconhece no art. 5º, rol dos direitos individuais.

Com a integração dos recursos tecnológicos nas práticas cotidianas, cada vez mais, há uma preocupação com a proteção dos dados pessoais na rede. Essa preocupação estende-se quando da manipulação das informações por pessoas jurídicas das informações e, principalmente, quanto a um possível dever de sigilo nas informações dos dados.

Ainda que o Código Civil de 2002 (CC/02) não tenha trazido de forma expressa a responsabilidade civil das organizações na tutela dos dados dos pessoais dos usuários, essa matéria suscitou intenso debate na sociedade fazendo com que o legislativo editasse algumas normas que buscassem tutelar esse bem jurídico. Assim, o Marco Civil, Lei nº 12.965, de 23 de abril de 2014, e, posteriormente, aLei Geral de Proteção de Dados Pessoais (LGPD) buscam criar uma tutela específica para essas relações sociais.

Ainda assim, quando a perspectiva da proteção dos dados dos usuários, as empresas devem ter uma responsabilidade ainda maior, principalmente, se a divulgação de quaisquer informações puder gerar dano a pessoa. Trata-se de não apenas um dever decorrente do exercício da atividade empresarial, mas da própria proteção à dignidade dos sujeitos.

Nesse sentido, essa pesquisa assumirá como problemática: quais as aplicações da Lei Geral de Proteção de Dados Pessoais (LGPD) para as empresas quando da proteção dos dados dos usuários? Assim, parte do pressuposto que diante dos avanços dos recursos tecnológicos, é fundamental que as normas acompanhem as novas necessidades sociais. Logo, seria a LGPD é um mecanismo eficiente para tutelar a privacidade dos dados dos usuários ainda que no ambiente virtual.

Ademais, o direito à privacidade, ainda que um direito fundamental de primeira de primeira dimensão, demanda do Estado ações positivas para a sua concretização. Todavia, para além de estabelecer normas de conduta, é preciso de que o poder público verifique se as organizações estão de fato cumprindo e observando as disposições normativas.

Para desenvolver essa pesquisa, elege-se como objetivo geral compreender como a Lei Geral de Proteção de Dados Pessoais (LGPD) modifica o comportamento das organizações quanto ao dever da proteção dos dados do usuário. De forma específica, compreender à proteção de dados enquanto um direito disruptivo, verificar o direito à privacidade de dados no ordenamento jurídico interno; e por fim analisar o disposto na Lei Geral de Proteção de Dados Pessoais (LGPD) quanto ao comportamento organizacional de tutela aos dados dos usuários.

Essa pesquisa foi desenvolvida a partir de uma revisão bibliográfica exploratória que examinou de forma qualitativa os textos inclusos após a seleção com o uso de descritores. Quanto ao método, para analisar a categoria normativa, optou-se pelo dedutivo

A sociedade está, cada vez mais, interconectada por meios de recursos tecnológicos. Todavia, além e benefícios, também é fundamental que os estudos verifiquem eventuais impactos sociais da introdução desses recursos. Dentre esses, a divulgação de dados pessoas quando ligada ao exercício de uma atividade empresarial precisa de um exame específico diante do dano que pode causar àquele que teve os dados expostos e a importância social que uma organização desempenha na sociedade.

Por fim, quando da relevância científica, esse estudo se coloca como justificável, posto que, seu objeto ainda carece de maior exame diante da escassez do exame da ciência jurídica sobre a matéria. Ademais, o objeto apresenta uma mutação o que requer exames sobre o seu movimento e, por consequência, seus possíveis impactos.

## 2 Proteção de dados Lei 13.709/18: características gerais, direito comparado e a judicialização

O direito é produto da atividade humana e do conhecimento da realidade. Portanto, é uma categoria que surge da inovação e para não correr o risco de caducar precisa estar em constante movimento para acompanhar as novas necessidades sociais. Nesse sentido, ao passo que a sociedade inova em suas criações essas possuem grande relevância para sociedade, é vital que esse passe por um processo de adaptação.

A priore, o sistema jurídico deve ser compreendido enquanto um conjunto de normas, em sentindo amplo: postas por uma autoridade competente e direcionadas a determinados sujeitos (NADER, 2012). Trata-se, em seu fim, de um instrumento e proteção ao cidadão contra ingerências daqueles que estão exercendo o poder estatal.

Um ato para ser relevante ao Direito deve estar institucionalizado em seu ordenamento. Logo, o mesmo passa de ato para fato jurídico. Esse fato subjacente desencadeia certo valor (esse valor está ligado a ideias de justiça, moral e ética) que confere significação a ação ou omissão. Haveria uma norma que representa a relação ou medica que integra um elemento ao outro.

Para Miguel Reale (2012) a conceituação de Direito, tal como sua finalidade e objetivo, está nitidamente vinculada ao que ele chama de Teoria Tridimensional. Um fato de relevância jurídica, desencadearia um valor e por conseguinte uma norma de aplicação ao desajuste ou premiação.

É de grande importância para o meio político entender os efeitos das políticas inovadoras nas atividades de inovação em organizações, especialmente empresas - pois políticas de inovação têm a intenção de influenciar a amplitude e natureza da inovação na economia. Logo, é fundamental implementar políticas e práticas de inovação pode ser complexo e influenciado pelo seu uso prático em diferentes níveis organizacionais e jurisdicionais, e não apenas por sua intenção em habilitar a legislação.

O caráter disruptivo do direito está ligado a um lapso temporal. Em um determinado momento o ordenamento jurídico teve que adaptar-se a determinada demanda social. Se em 1948 a Declaração Universal dos Direitos Humanos aprecia um documento vanguardista, atualmente essa é posta como

um documento histórico de fundamental importância para tutela da dignidade. Ou seja, ao longo do tempo essa careceu de seu caráter inovador para entrar no processo de consolidação.

Refletindo sobre o processo de disrupção e a criação normativa, Lima (2018) leciona que:

> Distupção sustentáveis (podemos substituir com segurança “inovação” para os propósitos presentes) fornecem entrega ou desempenho aprimorado de um produto ou serviço estabelecido, “ao longo das dimensões de desempenho que os principais clientes nos principais mercados têm valorizado historicamente”. (LIMA, 2018, p. 18).

O principal impacto da inovação é a satisfação das necessidades humanas, individuais ou coletivas, atuais ou futuras. Na prática, é difícil saber se as inovações vão se transformar em resultados sociais ou privados, o que não impede que a inovação continue sendo uma prioridade máxima. Além disso, a inovação não é necessariamente satisfatória para todos aqueles envolvidos (OSLO, 2018).

Nesse contexto inovador, a revolução digital pode ser entendida enquanto fenômeno que de certa forma facilite e/ou melhore a qualidade de vida. Sua essência é a da mutação. Ou seja, a alteração de formas fundamentais, a disponibilidade de informação no tempo e no espaço, e também o custo desta informação. O potencial existe agora para fazer a informação disponível a qualquer momento que o consumidor deseje (ao invés de quando é conveniente para o produtor distribuí-la).

Nesse sentido, a Era Digital é, para o campo jurídico, como uma alegoria e até fantamasgoria ao passo que é equiparada ao espectro. Ao passo do seu crescimento, ainda, poderia ser considerada um vírus de extremo contagio, uma vez que a comunicação sem conteúdo além de ser vazia, a longo prazo prejudica a capacidade racional doindivíduo.

Desta forma, ao passo que há disseminação em massa de conteúdo vazio, o indivíduo atrela-se as informações de pouca carga conteudistica e paulatinamente vai perdendo sua capacidade de análise crítica que, conforme Hans (2013) possui exercício intrinsecamente vinculado as atividades de ler e pensar.

Muitos são os exemplos das consequências do consumo de informação de massa e seus efeitos catastróficos na sociedade. No setor da economia, tem-se o conhecido *Flash Crash*, em 2011, que colocou a economia mundial em cheque após a divulgação de informações errôneas e manipuladas. Já na política, tem-se a mesma discussão junto com a eleição do presidentedos

Estados Unidos, Donald Trump, e as possíveis inverdades veiculadas durante a campanha política. Tamanha é a preocupação com as consequências da comunicação em massa e sem conteúdo, que o termo que define o ano de 2017, eleito pelo famoso e conceituado dicionário Oxford, é a "pós-verdade". Sinalagma que parece encaixar muito aos estudos deHans (2013).

Atualmente, muitos são os exemplos de normas buscam a tutela das questões ligadas a correlação entre direito e inovações da informática. Com o avanço das novas tecnologias e das virtualizações sociais, a chamada Lei do Maro Civil, *Lei nº 12.965, de 23 de abril de 2014,*visa regulamentar a vida no espaço virtual.

Todavia, com o aprimoramento dos recursos, houve a necessidade do avanço normativo a fim de proteger os dados do usuário. A LGPD, cria mecanismo que garantam a privacidade no chamado cyberespaço.

Assim, não apenas ordenamento tem que adaptar-se ao processo de inovação. É fundamental que os sujeitos que lidam com a norma jurídica estejam atendados, não apenadas aos novos comandos normativos, mas a novas e específicas necessidades que demandaram a construção de novas.

No entanto, as mudanças estão chegando inegavelmente. Avanços tecnológicos iminentes podem trazer benefícios aos clientes na forma de preços mais baixos e maior facilidade de uso dos serviços jurídicos, bem como maior acesso à justiça. Mas também podem representar tempos igualmente difíceis para as bancas de advocacia. Sobre a adaptação dos advogados ao direito disruptivo, CHRISTENSEN (2020) faz a seguinte reflexão:

> Um escritório de advocacia que integrasse esse tipo de programa disruptivo em suas operações, e contribuísse para a expansão contínua de suas capacidades, logo se veria eliminando muitos de seus associados, porque eles não seriam mais necessários: o computador estaria executando as tarefas

> que eles empreendido anteriormente (CHRISTENSEN, 2020, on-line),

Diante disso, como qualquer mudança social, o direito disruptivo traz modificações que devem ser verificadas com cautela. Todavia, diante do constante processo de transformação, a incorporação das técnicas de inovação ao setor jurídico parece ser uma variável inevitável. Logo, cabe aos operadores não temer a incorporação de novos recursos aos seus ambientes laborais, mas compreender que com esse processo haverá uma readaptação do espaço, como também a abertura para novos campos e demandas de atuação.

Assim, é fundamental a busca de comportamentos que busquem conciliar estas duas realidades (proteção de dados pessoais *versus* desenvolvimento tecnológico) é relevante tendo em vista que limitar excessivamente a divulgação de dados pessoais e permitir que o avanço tecnológico continue sem impor a ele nenhum limite e regulamentação parecem não ser razoáveis.

Castells (1999) já projetava algumas das consequências dessa invasão aos dados virtuais:

> Como resultado, cada um de nós viverá cada vez mais em nosso próprio universo de informações único: a 'bolha do filtro'. Receberemos principalmente notícias que são agradáveis, familiares e que confirmam nossas crenças - e como esses filtros são invisíveis, não saberemos o que está sendo escondido de nós. Nossos interesses passados determinarão a que estaremos expostos no futuro, deixando menos espaço para os encontros inesperados que estimulam a criatividade, a inovação e a troca democrática de ideias (*CASTELLS, 1999, XX).*

O avanço tecnológico, além de trazer vários benefícios para a sociedade, também trouxe preocupações no que se refere à inserção de dados pessoais na internet quando advir no futuro o desejo de indisponibilizá-los, além das novas formas como estas informações são empregadas, acenderam o debate sobre o direito de proteger a privacidade dos usuários, além dos seus dados pessoais.

## 2.1 Sanções e responsabilidade

O Direito surgiu para possibilitar uma convivência pacífica, por isso faz jus, a urgência de atualização ou edição de uma regulamentação específica no que tange às punibilidades, que devem ser mais severas, a fim de evitar ou desmotivar conflitos referentes às relações raciais e intolerantes, pois o que se está em jogo é a proteção do bem jurídico na dimensão individual ou coletiva.

Diante disto, a CFRB/88, em seu art. 5º estabelece que:

> Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade [...] (BRASIL, 1988).

Conforme Branco e Mendes (2012) direito à privacidade é classificado como uma garantia fundamental de primeira dimensão. Ainda assim, é fundamental que o Estado desenvolva um conjunto de políticas públicas que possibilitem o indivíduo exercer essa garantia. Ademais, Bulos (2020) leciona que a privacidade sustenta a dignidade humana e outros valores importantes, como liberdade de associação e liberdade de expressão. Tornou-se uma das questões de direitos humanos mais importantes da era moderna.

Todavia, para além de estabelecer normas de conduta, é preciso de que o poder público verifique se as organizações estão de fato cumprindo e observando as disposições normativas.

Há algum tempo que as pessoas em todo o mundo se preocupam com a privacidade dos dados e têm boas razões para isso. Violações de dados, ameaças à segurança e crimes cibernéticos podem levar a consequências negativas e até mesmo prejudiciais, por isso é muito importante cumprir os regulamentos de privacidade de dados.

A LGPD, que entrou em maio de 2018, tem sido uma etapa essencial para fortalecer os direitos fundamentais dos cidadãos na atual Revolução Digital, monitorar as empresas e evitar que essas empresas usem dados indevidamente para seus ganhos de capital, o que coloca o usuário em risco.

Junto com a segurança de dados, a privacidade de dados cria uma área de proteção de dados com dados utilizáveis protegidos como saída. No entanto, a privacidade de dados não se trata apenas do tratamento adequado

dos dados, mas também da expectativa pública de privacidade, centrada no indivíduo como uma figura-chave.

No que se refere a privacidade, o art. 5º, XX, tutela o direito à vida privada, intimidade e honra no rol dos direitos individuais. Já no âmbito normativo infraconstitucional, esse valor recebe guarita, dentre outros documentos, no CC/02, em seu art. 21 que estabelece que a vida privada da pessoa natural é inviolável. Ademais, a chamada LGPD, traz novas delimitações normativas para a proteção dos dados.

Embora a LGPD não tenha sido a primeira lei de privacidade, foi a lei de proteção de dados mais abrangente e inovadora que refletiu a nova era digital na maneira como os dados são criados e gerenciados nos processos de negócios cotidianos modernos. Leciona Guerra (2014) que:

> Privacidade significa respeitar os indivíduos. Se uma pessoa deseja manter algo privado, é desrespeitoso ignorar os desejos dessa pessoa sem uma razão convincente para fazê-lo. Obviamente, o desejo de privacidade pode entrar em conflito com valores importantes, portanto, a privacidade nem sempre pode vencer na balança. Às vezes, os desejos das pessoas por privacidade são simplesmente deixados de lado por causa da visão de que o dano em fazer isso é trivial (GUERRA, 2014, p. 14).

De fato, esse conceito de privacidade, a vida privada toma novos contornos com as modificações das relações sociais. Nesse sentido, Arendt (2017) leciona que privacidade moderna, diferentemente da que existia na antiguidade, não é apenas oposto à esfera política, mas se contrapõem à esfera social, possuindo como primordial função a de abrigar o que é íntimo. Buscando tutelar esse novo valor, o art. 2º da LGPD estabelece como diretrizes:

> A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Assim, a supracitada norma recepciona preceitos estabelecidos no Máximo Texto e reconhece que a privacidade deve ser tutelada por todos os sujeitos que compõe a sociedade. Inclusive, o art. 3º versa que a norma se aplica a pessoa natural ou por pessoa jurídica de direito público ou privado. Tal ampliação é considerado um grande avanço normativo e faz da LGPD e um marco na tutela desse bem jurídico.

De fato, pode se verificar também quando correlacionado a doutrina da Guerra (2014) que compreende que do direito à privacidade decorre à proteção da reputação depende da proteção não apenas contra falsidades, mas também contra certas verdades. Para esse autor, saber detalhes particulares sobre a vida das pessoas não leva necessariamente a um julgamento mais preciso sobre as pessoas.

Ainda para Guerra (2014), a privacidade de dados se concentra nos direitos dos indivíduos, no objetivo da coleta e processamento de dados, nas preferências de privacidade e na forma como as organizações governam os dados pessoais dos titulares dos dados. Nessa perspectiva, a LGPD se se concentra em como coletar, processar, compartilhar, arquivar e excluir os dados.

Ainda quando dos direitos individuais, um reflexo do direito à privacidade é a inviolabilidade ao domicílio. Nesse sentido, o já citado art. 5º, XI, versa que

> A casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial (BRASIL, 1988).

Lembra Castells (1999) que as pessoas estabelecem limites com os outros na sociedade. Esses limites são físicos e informativos. Precisam de lugares de solidão para onde se possam se retirar, lugares onde estejam livres do olhar dos outros. O autor destaca que espaços são fundamentais para que os sujeitos possam de relaxar e sentir-se à vontade.

Castells e Cardoso (2006) acreditam que romper esses limites pode criar situações sociais embaraçosas e prejudicar nossos relacionamentos. A privacidade também é útil para reduzir o atrito social que se encontram na vida e fundamental para que o indivíduo desenvolva sua personalidade.

Cumpre ressaltar que, o ordenamento jurídico interno está em consonância com as normas de direito internacional, visto que, a DUDH/48, em seu art. 12, versa que ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. De fato, a partir da técnica de interpretação sistêmica do ordenamento jurídico interno e internacional, no direito à privacidade está implícito no direito à vida e à liberdade garantidos aos cidadãos.

No âmbito conceitual, Branco e Mendes (2012) lecionam que o domicílio delimita um espaço físico em que o indivíduo desfruta da privacidade, em suas variadas expressões. Para esses, nesse espaço o indivíduo não deve sofrer intromissão por terceiros, e deverá gozar da tranquilidade da vida íntima. Ou seja, é um local em que deve ter repouso e tranquilidade.

Ademais, os supracitados autores ainda afirmam que assim o conceito de domicílio abrange 'todo lugar privativo, ocupado por alguém, com direito próprio e de maneira exclusiva, mesmo sem caráter definitivo ou habitual'. Para esses, o conceito constitucional de domicílio é, assim, mais amplo que aquele do direito civil. De fato, o ordenamento jurídico interno vem ampliando a interpretação desse instituto.

Por sua vez o Pacto de San José da Costa Rica, em seu art. 11, 2, quando da tutela da proteção da honra e da dignidade, versa que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.

Buscando delimitar o conceito de domicílio, o CC/2002, em seu art. 70 versa que esse é o lugar onde em que a pessoa natural estabelece a sua residência com ânimo definitivo. Todavia, diante das complexidades das relações da vida, esse reconhece que as pessoas podem possuir mais de um domicilio. Logo, art. 71 dispõe que se a tiver diversas residências, onde, alternadamente, viva, considerar-se-á domicílio seu qualquer dessas.

Buscando tutelar a prática profissional, em seu art. 72 há uma extensão desse instituto. Assim, o dispositivo versa que é também domicílio da pessoa natural, quanto às relações concernentes à profissão, o lugar onde está é exercida. De fato, essa garantia vem sendo observada quando do julgamento

de lides contendo a matéria em e, partir, da técnica de interpretação extensiva, até por vezes tendo seu sentido ampliado.

Na medida em que a relação com os meios de comunicação se intensifica e a produção em massa torna-se evidente, surge a preocupação geral de garantir uma mídia livre, independente, plural e diversificada, preocupação esta que passa a se fixar como o ideal a ser alcançado para que o direito à liberdade de buscar, difundir e receber informações possa ser realizado em sua plenitude (SILVEIRA, 2016).

Sendo o Brasil um país signatário da Declaração Universal dos Direitos Humanos de 1948 (DUHD) e do Pacto de San Jose da Costa Rica de 1969, esse possui o deve de garantir esse direito fundamental. Nesse sentido o documento americano dispõe que:

> 4. O acesso à informação em poder do Estado é um direito fundamental de cada indivíduo. Os Estados têm a obrigação de garantir o pleno exercício deste direito. Este princípio permite apenas limitações excepcionais que devem ser previamente estabelecidas por lei no caso de um perigo real e iminente que ameace a segurança nacional em sociedades democráticas (CADH, 1969).

Ademais, lembra Reimão (2011) que o acesso do público à informação e proteger as liberdades fundamentais, de acordo com a legislação nacional e acordos internacionais. Para Reimão (211) é esse instrumento deve ser compreendido como parte de um aparelho de coerção e repressão que, muito mais do que afetar a circulação de alguns bens culturais, restringia a produção e circulação da cultura. Ademais, ainda é uma forma de exercício de controle estatal.

Ao passo em que a mídia constitui um importante meio de transmissão de informações com o intuito de educar e democratizar surge questionamentos direcionados ao potencial que as mídias sociais têm em criar condições manipulativas e gerar tendências nas preferências e opiniões da população sobre determinado tema. (SILVEIRA, 2016).

Esses fatos demonstram a influência das desses recursos nas relações modernas, a dimensão imprevisível que tais ferramentas podem assumir e a vulnerabilidade à qual todos, irrestritamente, estão sujeitos. Ainda assim, Reimão (2011) justifica que nada pode suspender garantias individuais e criam

condições para à divulgação da informação, à manifestação de opiniões e às produções culturais e artísticas.

De fato, se outrora uma informação sensacionalista praticada na presença de um grupo de pessoas gerava um inegável prejuízo para o ofendido, hodiernamente, a mesma ofensa, se veiculada em uma rede social, pode atingir nefastas proporções (OLIVEIRA, 2003). É notória, assim, a carga negativa que se atribui ao estilo sensacionalista. As características desse tipo de produção informativa baseada no exagero podem justificar a situação.

Por outro, contrasta-se com o desvio da finalidade dessas redes, porque os usuários passaram a escrever informações que com certa frequência violam direitos e garantias fundamentais, praticados por usuários que por muitas vezes se escondem por trás de apelidos, pseudônimos e perfis falsos, cometendo crimes ocultados pelo anonimato (LEITE, 2016).

Ainda assim, lembra Fiss (2005) que:

> [...] uma sociedade democrática está continuamente em processo de mudança, terá restrições de direitos e liberdades e seus procedimentos serão frequentemente questionados. Isso é garantido pelo direito à liberdade de expressão, que, portanto, é vista como um pré-requisito da democracia. Consequentemente, a democracia pode ser vista como um sistema político "trágico" (FISS, 2005, recurso digital, grifo nosso).

Entretanto, lembra Leitão (2011) que isso não garante que a liberdade de expressão é ou poderá ser absoluta e deve ser respeitada em todos os espaços um código de conduta específico. Ainda assim, essa esclarece que a censura – mais que um ato de poder oficial – se sofisticou e se consolidou como um instrumento institucional, sustentado por rígidos mecanismos de controle e administração da informação

Ainda para Leitão (2011), o público em geral está se tornando mais ciente de todos os seus direitos crescentes de dizer àqueles que coletam seus dados pessoais que esperam ter seus dados pessoais protegidos e têm direito de acessar e controlar seus dados pessoais. Assim, leciona Castells e Cardoso (2006) que privacidade de dados está relacionada a como uma informação - ou dados - deve ser tratada com base em sua importância relativa.

Já para Rodatà (2018), para uma empresa, a privacidade de dados vai além das proteções de informação de seus funcionários e clientes. Também inclui as informações que ajudam a empresa a operar, sejam dados proprietários de pesquisa e desenvolvimento ou informações financeiras que mostram como ela está gastando e investindo seu dinheiro. Ademais, lembra o autor que:

> Quando os dados que deveriam ser mantidos em sigilo chegam às mãos erradas, coisas ruins podem acontecer. Uma violação de dados em uma agência governamental pode, por exemplo, colocar informações ultrassecretas nas mãos de um estado inimigo. Uma violação em uma empresa pode colocar dados proprietários nas mãos de um concorrente (RODATÀ, 2018, recurso digital).

Importante ainda, diante de um mercado globalizado e de venda informações, é a questão levantada por Fradera (2006). Esse lembra que os dados estão se tornando cada vez mais valiosos. Além disso, as habilidades e oportunidades para recuperar diferentes tipos de dados pessoais estão evoluindo extremamente rápido. Logo, o processamento não autorizado, descuidado ou imprudente de dados pessoais pode causar grandes danos a pessoas e empresas.

## 2.2 Direito digital como forma de prevenção ao crime cibernético

O Direito Digital é a vertente jurídica da chamada Sociedade da Informação, idealizada por Alvin Tofler nos anos 1970, em sua inesquecível obra A Terceira Onda (ARAÚJO, 2017). Teoricamente, o "Direito Digital" se baseia no "Direito da Internet", formado na literatura científica de língua inglesa, que vários pesquisadores consideram um ramo distinto do Direito.

A defasagem do Direito convencional em relação ao mundo digital se traduz no fenômeno em que a norma estará sempre correndo atrás do fato, num contínuo movimento de “gato e rato” (ARAÚJO, 2017). O Direito Digital, que se desenvolveu nas últimas duas décadas, é uma nova disciplina jurídica que consiste na incidência de normas jurídicas aplicáveis ao chamado ciberespaço, num reconhecimento de que a legislação e a doutrina jurídica tradicionais são insuficientes para regular as relações no mundo virtual, os

quais desafiam novas perguntas e novas respostas, num ambiente desprovido das conhecidas fronteiras espaço-tempo (ARAÚJO, 2017).

Atualmente, é comum traçarmos paralelismos entre grandes conquistas da humanidade de outrora e a Revolução Digital (ARAÚJO, 2020). A revolução digital pode ser entendida enquanto fenômeno que de certa forma facilite e/ou melhore a qualidade de vida. Sua essência é a da mutação. Ou seja, a alteração de formas fundamentais, a disponibilidade de informação no tempo e no espaço, e também o custo desta informação. O potencial existe agora para fazer a informação disponível a qualquer momento que o consumidor deseje (ao invés de quando é conveniente para o produtor distribuí-la).

O uso da internet era bastante limitado no século XX, vindo a se tornar mais acessível a grande massa da população em meados dos anos 2000. Com esse acesso, viu-se a necessidade e comodidade de criar-se uma forma onde pessoas pudessem interagir sem ter que sair de casa, dando início assim as redes sociais.

Assim, foi responsável por promover uma modificação significativa na percepção, na sensação, no pensamento e na própria vida social dos indivíduos, sem que ainda seja possível avaliar todas as consequências dessa transformação. Conquanto favoreça o estabelecimento de contatos com estranhos e elimine a distância entre as pessoas, a hipercumunicação digital acaba por anular a relação, a proximidade e a amizade. Afinal, nessa raivosa e ruidosa ágora contemporânea que são as redes sociais, tudo está excessivamente próximo, de maneira que não há mais distinção entre emissão e recepção.

Tendo em vista as vantagens trazidas e que poderiam ser úteis para a sociedade, acontece a expansão para a sociedade em geral, que começa a desfrutar desse veículo virtual, para socializar mediante a rede, caindo no gosto da população e sendo sucesso imediato entre todos que usufruíam.

A revolução digital pode ser entendida enquanto fenômeno que de certa forma facilite e/ou melhore a qualidade de vida. Sua essência é a da mutação. Ou seja, a alteração de formas fundamentais, a disponibilidade de informação no tempo e no espaço, e também o custo desta informação. O potencial existe agora para fazer a informação disponível a qualquer momento que o

consumidor deseje (ao invés de quando é conveniente para o produtor distribuí-la).

Buscando estabelecer um linearidade histórica, tem sido frequentemente referida como a terceira revolução industrial e implica a mudança da tecnologia mecânica e eletrônica analógica para a tecnologia digital, ocorrendo desde a década de 1980 até os dias atuais. A revolução digital é tanto uma manifestação quanto resultado do surgimento das tecnologias de informação e comunicação e, assim, inaugura a Era da Informação. Esta revolução implica a produção em massa e uso generalizado de digitais circuitos lógicos e suas tecnologias que derivados seja, o computador, celular e smartphone. As importantes consequências tecnológicas, sociais, econômicas e políticas ocasionadas explicam sua natureza revolucionária. A sociedade da informação representa o ambiente natural desse fenômeno.

Todavia, o impacto da difusão descontrolada das tecnologias digitais é transformação da comunicação e das relações sociais. A informação, o jornalismo, os veículos de comunicação e o comportamento do consumidor de informações. Estudos e previsões apontam para mudanças radicais do uso de plataformas de transmissão da informação e esta situação gera inúmeros desafios tanto para os a revolução digital e os desafios da comunicação profissionais da comunicação como para os usuários dos veículos, indicando inclusive a necessidade de uma mudança na formação de inúmeras categorias profissionais.

> Novamente a relação computação, comunicação e conteúdo determina o monopólio do poder e a soberania dos Estados dentro da era digital e, diante de um mundo cada vez mais globalizado, os donos destas ‘pontes’ podem vir a ditar as regras, cada vez mais. (ARAÚJO, 2017, p. 33).

A revolução digital foi responsável por promover uma modificação significativa na percepção, na sensação, no pensamento e na própria vida social dos indivíduos, sem que ainda seja possível avaliar todas as consequências dessa transformação. Conquanto favoreça o estabelecimento de contatos com estranhos e elimine a distância entre as pessoas, a hipercumunicação digital acaba por anular a relação, a proximidade e a amizade. Afinal, nessa raivosa e ruidosa ágora contemporânea que são as

redes sociais, tudo está excessivamente próximo, de maneira que não há mais distinção entre emissão e recepção.

Tendo em vista as vantagens trazidas e que poderiam ser úteis para a sociedade, acontece a expansão para a sociedade em geral, que começa a desfrutar desse veículo virtual, para socializar mediante a rede, caindo no gosto da população e sendo sucesso imediato entre todos que usufruíam.

Diante dos avanços e impactos da revolução digital, o Estado verifica a necessidade de disciplinar as normas específicas para o chamado espaço digital.  o Direito é a realização ordenada e garantida do bem comum numa estrutura tridimensional bilateral atributiva, ou, de uma forma analítica: direito é a ordenação heterônima, coercível e bilateral atributiva das relações de convivência, segundo uma integração normativa de fatos segundos valores.

Com o rápido desenvolvimento da economia digital, é necessário criar salvaguardas jurídicas coerentes, globais e abrangentes, incluindo garantias confiáveis de proteção legal que regulem o uso de tecnologias digitais, a fim de minimizar os riscos de digitalização e legitimar novos ativos, ambos tangíveis e intangível. Organizações internacionais e estados estão desenvolvendo ativamente estratégias para adaptar as leis sobre o uso de tecnologias digitais modernas. Os principais problemas, no entanto, são que, por um lado, as estratégias propostas são setoriais e abordam apenas alguns aspectos da digitalização e, por outro lado, as soluções muitas vezes visam a prossecução de uma agenda política em detrimento de um avanço coerente. olhando para uma estratégia legal global.

Fundamentalmente, duas abordagens principais para o futuro do direito no contexto da digitalização podem ser identificadas. A primeira é a abordagem utilitária, que se concentra na resolução de tarefas funcionais estritamente definidas (inteligência financeira, aprovação de regulamentos técnicos, etc.) atendendo aos interesses e de estados e organizações internacionais específicas. A segunda é a abordagem metodológica, que possibilitaria soluções globais e abrangentes.

A lei digital pode ser definida como os direitos e restrições legais que regem o uso da tecnologia. Apesar de atualmente, muitas pessoas ainda são serem cidadãos digitais responsáveis. Assim, se refere a requisitos legais, decisões legais e ética que se relacionam com ambientes digitais e, portanto,

pode afetar diretamente os alunos em salas de aula, funcionários e organizações como um todo. Alguns dos desenvolvimentos legais na legislação canadense têm se mostrado evolucionários.

> Exigem dos operadores jurídicos novas interpretações quanto à liberdade de expressão e seus limites, exame de autenticidade da prova eletrônica, hermenêutica aplicável ao Direito do Consumidor, proteção de dados pessoais, proteção da propriedade intelectual, tipifi cação de crimes eletrônicos, intimação das partes em processo judicial por meio virtual, tributação de operações comerciais e miríade de exemplos que desafiam o Poder Judiciário. São lacunas que, muitas vezes, não podem ser atendidas apenas pelos esforços da boa hermenêutica criada pelos pretórios, mas também pela contínua atualização das leis. (ARAÚJO, 2017, p. 33).

A Lei 12.965, 23 de abril de 2014, denominado de Marco Civil da Internet, também tem como escopo disciplinar uso da Internet no âmbito cível e possui reflexos efeitos diretos na esfera penal, cível e, especialmente, na investigação criminal. Em uma primeira análise, chama a concretização da ponderação dos princípios para aplicação e formulação da lei. Posto que, mostra-se um avanço, tal como traz em seu escopo temerária possibilidade de invasão da privacidade dos usuários da rede mundial de computadores.

Trata-se de uma lei que, por vocação, produz efeitos nas mais variadas esferas do direito (processual, consumerista, constitucional, empresarial, penal, etc) e possui natureza legal substantiva, ou seja, definem relações jurídicas, criam direitos e impõe obrigações. Nesse sentido, a norma causou grande efeito na disciplina das relações jurídicas em meio cibernético, impactando significativamente no garantismo jurídico, na judicialização, nos direitos do usuário e nas obrigações do estado e dos fornecedores.

Ao longo do texto normativo, a referida lei destaca um rol de garantias aos usuários, entre esses destacam-se a extraterritorialidade; o dever de lei e foro brasileiro; a garantia da liberdade de expressão e não remoção de conteúdo; a proteção da privacidade; a garantia da neutralidade; a garantia da qualidade da conexão; a garantia do direito de acesso a internet e inclusão digital; a garantia de uso de software livre (padrões abertos); o dever de guarda de provas eletrônicas; o dever de proteção de crianças e adolescentes na web; o dever de educação; e por fim as penalidades por descumprimento.

O bem jurídico tutelado é a inviolabilidade das informações sendo esta decorrência natural do direito à privacidade, de caráter constitucional e essencial para a convivência em sociedade. A inviolabilidade de dados e informações armazenados em sistemas computadorizados surge como um novo bem jurídico a ser tutelado pelo Direito Penal, de forma a garantir a privacidade e a integridade desses bens.

Dessa maneira, os responsáveis pelos provedores de acesso não poderão privilegiar alguns serviços de Internet em detrimento de outro. Por fim, cabe salientar que o acesso a dados de terceiros fica condicionado a decisão/ordem judicial. Todavia, o que se questiona é se tais informações, na pratica, não podem ser comercializadas ou ter outros usos indevidos.

O Marco Civil é uma tentativa legal do Estado brasileiro de proteger o direito de expressão das pessoas e ao mesmo tempo de tentar regrar os usuários da internet, para que se guarde a intimidade e a honra das pessoas usuárias desse meio. Os principais efeitos desse documento são regrar o acesso à internet, dar mais qualidade aos acessos à internet e educar a população quanto ao uso consciente da internet e de seus limites, como também as consequências do uso indevido da internet.

### 2.2.1 Panorama sobre temas diversos que envolvem o direito digital

Tendo em vista as vantagens trazidas e que poderiam ser úteis para a sociedade, acontece a expansão para a sociedade em geral, que começa a desfrutar desse veículo virtual, para socializar mediante a rede, caindo no gosto da população e sendo sucesso imediato entre todos que usufruíam.

No que tange ao estudo em questão, que foca na influência do uso desta no meio trabalhista, só vai aparecer com mais intensidade em meados dos anos 2000, quando o número de usuários praticamente dobrou, tendo a grande massa da população mais acesso à internet. Em 2002, com a criação do “fotolog” tem-se uma maior divulgação de fotos pessoais, determinado momento em que as pessoas começaram a expor suas intimidades com mais frequência.

Com a internet como meio de comunicação, a troca de informações se dá de forma mais célere. No começo do século com o envio de um e-mail, era

encaminhado automaticamente e a parte para qual foi encaminhada a mensagem poderia no instante em que tivesse acesso à rede, responder de forma imediata, chegando assim uma resposta quase que imediata.

O problema de violação de direitos autorais sempre foi uma das questões mais difíceis de resolver em nossa sociedade. A lei de direitos autorais tem evoluído ao longo dos anos e se adaptou com sucesso às novas tecnologias que surgiram.

Mas com a Internet a batalha parece perdida, pois permite o acesso a uma enorme quantidade de informação a qualquer hora, em qualquer lugar, sem constrangimentos. A Internet costuma ser espaço que possibilita de uma grande copiadora que pode fazer e distribuir um número ilimitado de cópias de conteúdo em todo o mundo.

A característica anônima da Internet não contribui para a aplicação da lei, e muitos prevêem que os criadores de propriedade intelectual relutarão em criar trabalhos para o ambiente da Internet, uma vez que os criadores serão incapazes de proteger seus interesses de copyright. Mas a idéia de acesso aberto a esses materiais não diminuiu o fluxo de novas informações que fluem para a Internet.

Novos problemas de direitos autorais levantados pela Internet podem forçar uma revisão das atuais leis de direitos autorais, mas a maioria dos internautas acha que a Internet deve ser deixada em paz. Esta não é a opinião dos proprietários de direitos autorais, que desejam que os governos tomem medidas e apliquem as leis de direitos autorais existentes na Internet.

O principal problema vem do caráter internacional da Internet, o que gera dúvidas sobre quais leis devem ser aplicadas. Embora os países tenham assinado tratados de proteção de direitos autorais, algumas pessoas pensam que o ciberespaço deve ser considerado uma entidade separada e que diferentes leis devem ser criadas.

> O Direito Digital ainda está em busca da melhor regulação para o direito dos autores. De um lado, há que se reconhecer que o Direito Digital é um direito comunitário, multicultural, com dinamismo próprio, aberto e colaborativo, onde a transmissão contínua de dados, em escala mundial, é uma de suas características. Mas, por outro lado, tais singularidades têm que ser balanceadas com a proteção jurídica da criação

> humana, que urge igualmente ser valorizada, não apenas pelo interesse individual, mas também público, preservando-se, sobretudo, a autenticidade da obra, que é um direito moral do autor, independente da tecnologia utilizada para a sua divulgação. (ARAÚJO, 2017, p. 28).

A Internet e os serviços on-line fornecem um vasto leque de informações, de acesso imediato, disponíveis em quase todo o lado e a baixo custo. Essas informações estão em constante mudança e expansão. Todavia, a maioria dos itens que se encontrará na Internet são elegíveis para proteção de direitos autorais, incluindo o texto de páginas da web, documentos de texto ASCII, conteúdo de e-mail e mensagens da Usenet, arquivos de som, arquivos gráficos, programas de computador executáveis e listagens de programas de computador. Páginas da Web, mensagens de e-mail e até mensagens públicas são protegidas por direitos autorais assim que são criadas. Assim, facilidade com que trabalhos protegidos por direitos autorais podem ser copiados e distribuídos pela Internet, e o fato de que o ciberespaço não existe em qualquer época ou lugar não ajuda muito.

Os grupos dedicados à pirataria de software na Internet usam computadores host para configurar secretamente lojas de software roubado. Os piratas então passam mensagens ao redor do mundo para que outros piratas possam fazer o download do software. Os administradores dos hosts normalmente não estão cientes desse uso criminoso de seus hosts. E como toda a operação pode levar não mais do que 24 horas, é virtualmente impossível para os encarregados da aplicação da lei tomarem medidas para fechá-la. Mesmo quando eles são capazes de fazer isso, é virtualmente impossível saber onde o próximo local surgirá. (ARAÚJO, 2017).

Logo, a Internet começou a ser usada por desenvolvedores, revendedores e licenciadores de software como meio de publicidade e canal de distribuição de seus softwares. No entanto, colocar ou permitir que outros coloquem software na Internet aumenta drasticamente o risco de violação. É ainda mais problemático para os fornecedores que optam por não distribuir produtos de software pela Internet.

# 3 A EFICÁCIA NO COMBATE A ESSAS INFRAÇÕES PARA EMPRESAS E PESSOAS FÍSICAS

## 3.1 Identificação do autor

A segurança e a privacidade dos dados são parte da tecnologia da informação que lida com a capacidade de uma organização ou indivíduo de determinar os dados em um sistema que pode ser compartilhado com terceiros (STALLINGS, 2015). Além disso, ajuda as organizações a proteger os dados no escritório e nas mãos dos funcionários, reduz as vulnerabilidades que os hackers podem explorar as informações.

Stalling e Brown (2014) afirma que, embora a segurança de dados e a privacidade de dados pareçam semelhantes, são bastante diferentes uma da outra. Para esses, a segurança de dados trata da proteção de dados contra criminosos cibernéticos, enquanto a privacidade de dados trata de como organizações de dados ou indivíduos coletam, armazenam e usam legalmente os dados.

Ainda para Stalling (2015), a segurança de dados inclui um conjunto de padrões e diferentes salvaguardas e medidas que uma organização está tomando para evitar que terceiros acessem não autorizados a dados digitais, ou qualquer alteração, exclusão ou divulgação intencional ou não intencional de dados. E concentra na proteção de dados contra ataques maliciosos e evita a exploração de dados roubados (violação de dados ou ciberataque). Inclui controle de acesso, criptografia, segurança de rede, entre tantos outros.

Leciona Rodatà (2018) que o objetivo da proteção de dados pessoais não é apenas proteger os dados pessoais, mas proteger os direitos e liberdades fundamentais das pessoas que estão relacionados com esses dados. Ao proteger os dados pessoais, é possível garantir que tais núcleos essenciais não sejam violados.

As proteções de privacidade envolvem a garantia de segurança para dados pessoais e todas as atividades associadas envolvidas na coleta, armazenamento, processamento, acesso, transmissão, compartilhamento e descarte de dados. Historicamente, as organizações não tinham controles de

segurança de dados fortes e abrangentes implementados em toda a empresa, em todos os dispositivos finais.

Esclarece Guerra (2014) que, na era digital, normalmente aplicamos o conceito de privacidade de dados a informações pessoais críticas, também conhecidas como informações de identificação pessoal e informações pessoais de saúde. Isso pode incluir números do seguro social, registros médicos e de saúde, dados financeiros, incluindo contas bancárias e números de cartão de crédito, e até mesmo informações básicas, mas ainda confidenciais, como nomes completos, endereços e datas de nascimento.

Lima (2016) lembra que as empresas devem proteger a privacidade de seus consumidores é uma meta principal, se preocupam com a privacidade de seus consumidores e apoiam o cumprimento dessa meta com práticas de privacidade transparentes e consistentemente seguidas que demonstram esse cuidado, construirão conexões emocionais com sua marca, que vai melhorar o valor da marca.

As organizações que implementam tais controles irão, como resultado, reduzir o número de incidentes de segurança que resultam em violações de privacidade. Menos violações significam que a empresa não perde a confiança e, consequentemente, perde clientes ou outros tipos de negócios. Isso também significa que a empresa não precisa lidar com multas, penalidades plurianuais ou processos civis após o efeito das violações.

Ainda para Lima (2016), os regulamentos de proteção de dados são necessários para garantir um comércio e uma prestação de serviços justos e amigos do consumidor. Logo, os dispositivos de proteção de dados pessoais causam uma situação em que, por exemplo, os dados pessoais não podem ser vendidos livremente, o que significa que as pessoas têm um maior controle sobre quem os faz e que tipo de ofertas fazem.

Para garantir a segurança dos dados pessoais, é importante saber quais dados estão sendo processados, por que estão sendo processados e com que base. Além disso, é importante identificar quais medidas de proteção e segurança estão em uso (RODATÀ, 2018). Tudo isso é possível por meio de uma auditoria minuciosa de proteção de dados, que identifica o fluxo de dados e se os regulamentos de proteção de dados estão sendo seguidos(RODATÀ, 2018).

A responsabilidade civil, encontra-se cada vez mais presente no cotidiano e apresenta-se, baseada no princípio legislativo de que aquele que causar dano a outrem, seja essa moral ou material deve reestabelecer o bem ao estado em que se encontrava antes do seu ato danoso e, caso o reestabelecimento não seja possível, deverá compensar o dano causado.

Lembra Diniz (2020) que:

> A responsabilidade civil é a aplicação de medidas que obriguem uma pessoa a reparar dano moral ou patrimonial causado a terceiros, em razão de ato por ela mesma praticado, por pessoa por quem ela responde, por alguma coisa a ela pertencente ou de simples imposição lega (DINIZ, 2020, recurso digital).

No âmbito normativo, o Código Civil de 2002 (CC/02), em seu art. 186, versa que, aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito. Por sua vez, o art. 187, estabelece que também comete ato ilícito o titular de um direito que, ao exercê-lo, excede manifestamente os limites impostos pelo seu fim econômico ou social, pela boa-fé ou pelos bons costumes (BRASIL, 2002).

Neste contexto, a responsabilidade civil das empresas tem se tornado cada dia mais presente na sociedade, despertando o interesse jurídico não só dos pacientes, mas de toda a classe médica que busca respaldo e apoio junto ao ordenamento jurídico. Ademais, no contexto do atendimento virtual, é fundamental pensar na proteção desse bem jurídico no espaço virtual.

Nesse sentido, cumpre lembrar que o CC/02 estabelece o dever de reparação. Assim, o art. 927 versa que:

> Art. 927. Aquele que, por ato ilícito (arts. 186 e 187), causar dano a outrem, fica obrigado a repará-lo. Parágrafo único. Haverá obrigação de reparar o dano, independentemente de culpa, nos casos especificados em lei, ou quando a atividade normalmente desenvolvida pelo autor do dano implicar, por sua natureza, risco para os direitos de outrem (BRASIL, 2002).

É importante destacar que todas as empresas possuem dados, como arquivos pessoais, dados de clientes, informações de produtos e transações financeiras. As decisões que a administração toma com base nesses dados

são os processos de trabalho seguidos pelos funcionários para entregar produtos e serviços de qualidade. Lembra Borba (2010) que, na verdade, os dados são um dos ativos mais importantes de uma organização.

Por esse motivo, a LGPD acrescentou outra camada de importância à segurança de dados, tornando-a não apenas um requisito comercial, mas também um requisito legal. Assim, o legislador optou por uma interpretação ampliativa do sentido de dados pessoais e, dentre outras coisas, o art. 5º, versa que:

> Para os fins desta Lei, considera-se: 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; [...] (BRASIL, 2018).

De fato, a Lei de Proteção de Dados contém um conjunto de princípios que as organizações, o governo e as empresas devem seguir para manter os dados de alguém precisos, protegidos, protegidos e legais. Entretanto, essa traz uma clausula de exclusão as entidades governamentais. Assim, dispõe que:

> O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei. § 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso[...] (BRASIL, 2018).

Outra evolução normativa, é que essa exige que as organizações implementem medidas técnicas e organizacionais adequadas para garantir e ser capaz de demonstrar que o processamento é realizado em conformidade com o regulamento. Assim, o supracitado artigo ainda versa que:

> segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção:

> adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

A partir do exame normativo, é possível verificar que uma parte importante dessas medidas é o treinamento de conscientização sobre segurança: os funcionários precisam estar cientes da importância de seguir os procedimentos e processos de segurança de dados.

## 3.2 Eficácia da legislação no combate

Cumpre lembrar que os princípios estabelecidos na Lei de Proteção de Dados ajudam as empresas a garantir que os detalhes de seus funcionários, clientes e usuários sejam devidamente protegidos. Leciona Borba (2010) que como empregador e gerente de negócios, tem-se o dever de garantir que todas as informações estejam corretas.

Ademais, Rodatà (2018) destaca que seguir os procedimentos adequados de proteção de dados também é crucial para ajudar a prevenir crimes cibernéticos, garantindo que os detalhes, especificamente bancários, endereços e informações de contato sejam protegidos para evitar fraudes. Na prática, uma violação em sua proteção de dados pode custar caro. E os clientes e funcionários afetados, em alguns casos, podem buscar compensação contra a empresa.

Para Rodatà (2018), quando os clientes fornecem suas informações pessoais a empresas, esses confiam dados pessoais que podem ser usados contra si se caírem em mãos erradas. É por isso que a privacidade de dados existe para proteger esses clientes, mas também as empresas e seus funcionários, de violações de segurança.

No que se refere ao consentimento, estabelece a norma, em seu art. 8º, que:

> O consentimento previsto no inciso I do art. 7º desta Lei deverá ser fornecido por escrito ou por outro meio que demonstre a manifestação de vontade do titular. § 1º Caso o consentimento seja fornecido por escrito, esse deverá constar de cláusula destacada das demais cláusulas contratuais. § 2º Cabe ao controlador o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei. § 3º É vedado o tratamento de dados pessoais mediante vício de consentimento. § 4º O consentimento deverá referir-se a finalidades determinadas, e as autorizações genéricas para o tratamento de dados pessoais serão nulas. § 5º O consentimento pode ser revogado a qualquer momento mediante manifestação expressa do titular, por procedimento gratuito e facilitado, ratificados os tratamentos realizados sob amparo do consentimento anteriormente manifestado enquanto não houver requerimento de eliminação, nos termos do inciso VI do caput do art. 18 desta Lei (BRASIL, 2018).

Diante da análise do dispositivo, verifica-se que cumprir os regulamentos de privacidade de dados é importante não apenas porque informações confidenciais podem ser mal utilizadas no caso de ocorrer uma violação de dados, mas também porque existem leis que impõem essa conformidade.

Entretanto, um dos principais motivos pelos quais as empresas cumprem os regulamentos de privacidade de dados é evitar multas. Dentre os dispositivos que estabelecem esse tipo de sanção, destaca-se o art. 52 que versa da seguinte forma:

> Os agentes de tratamento de dados, em razão das infrações cometidas às normas previstas nesta Lei, ficam sujeitos às seguintes sanções administrativas aplicáveis pela autoridade nacional: I - advertência, com indicação de prazo para adoção de medidas corretivas; II - multa simples, de até 2% (dois por cento) do faturamento da pessoa jurídica de direito privado, grupo ou conglomerado no Brasil no seu último exercício, excluídos os tributos, limitada, no total, a R$ 50.000.000,00 (cinquenta milhões de reais) por infração; III - multa diária, observado o limite total a que se refere o inciso II (BRASIL, 2018).

Para cumprir os regulamentos de privacidade de dados, se precisa atender a certos requisitos legais. Um desses requisitos é a implementação de fortes proteções de segurança para garantir a proteção da privacidade dos dados. Com essas medidas, o número de ameaças à segurança diminuirá significativamente e sua empresa não sofrerá perda de receita

Como mencionado antes, uma violação de dados pode levar ao roubo de informações valiosas do cliente, o que pode impactar negativamente os proprietários dos dados. Leciona Borba (2010) que a maioria das organizações possui um código de ética em vigor. Mesmo aqueles que não o possuem seguem pelo menos certas práticas éticas. Sem isso, eles não seriam capazes de permanecer no mercado. Uma dessas políticas afirma que as informações confidenciais devem ser tratadas com responsabilidade e usadas apenas para fins comerciais.

Buscando criar uma gestão organizacional dos dados, Stallings (2015) leciona que Sempre que dados pessoais são coletados, esses precisam ser devidamente identificados e inventariados. Logo, a empresa também precisa fornecer um método de rastreamento para todos os dados que tornará mais fácil localizar e proteger. Tudo isso precisa estar de acordo com os padrões legais e recomendados.

Desta forma, as organizações que cumprem os regulamentos de privacidade de dados devem garantir integridade, confidencialidade e disponibilidade de dados com salvaguardas físicas, técnicas e administrativas. Essas proteções precisam ser eficazes na detecção e interrupção do acesso não autorizado aos dados.

Nesse sentido e buscando outras proteções, o art. 10 da LGPD, versa que:

> O legítimo interesse do controlador somente poderá fundamentar tratamento de dados pessoais para finalidades legítimas, consideradas a partir de situações concretas, que incluem, mas não se limitam a: I - apoio e promoção de atividades do controlador; eII - proteção, em relação ao titular, do exercício regular de seus direitos ou prestação de serviços que o beneficiem, respeitadas as legítimas expectativas dele e os direitos e liberdades fundamentais, nos termos desta Lei (BRASIL, 2018).

Para Stallings (2015) também é vital monitorar, avaliar e atualizar constantemente a segurança das informações para garantir que novas ameaças possam ser enfrentadas e tratadas de maneira adequada e eficiente. O autor esclarece que ainda que todas as políticas de conformidade, o sistema não pode ser totalmente protegido contra violações de dados e ataques cibernéticos. É por isso que toda organização precisa ter um plano de resposta

eficaz para violações de dados, bem como funcionários treinados nesses planos de resposta a violações.

Como já disposto, todos os processos e planos de conformidade precisam ter a documentação adequada. É importante manter essa documentação disponível com um bom sistema de gerenciamento de conteúdo. Stallings (2015) defende que em grandes corporações também deve ter um funcionário responsável pelo gerenciamento desses documentos.

Buscando compreender as estratégias de segurança de proteção de dados de uma organização, Stallings (2015) afirma que essa também precisa ter um processo definido para relatar não conformidade e um plano de escalonamento. Além disso, se precisa provar que é continuamente aderente por meio de auditoria, monitoramento e uso de controles.

### 3.3 Onde está o maior impacto no vazamento de dados

Junto com a segurança de dados, a privacidade de dados cria uma área de proteção de dados com dados utilizáveis protegidos como saída. No entanto, a privacidade de dados não se trata apenas do tratamento adequado dos dados, mas também da expectativa pública de privacidade, centrada no indivíduo como uma figura-chave.

Embora a LGPD não tenha sido a primeira lei de privacidade, foi a lei de proteção de dados mais abrangente e inovadora que refletiu a nova era digital na maneira como os dados são criados e gerenciados nos processos de negócios cotidianos modernos. Leciona Guerra (2014) que:

> Privacidade significa respeitar os indivíduos. Se uma pessoa deseja manter algo privado, é desrespeitoso ignorar os desejos dessa pessoa sem uma razão convincente para fazê-lo. Obviamente, o desejo de privacidade pode entrar em conflito com valores importantes, portanto, a privacidade nem sempre pode vencer na balança. Às vezes, os desejos das pessoas por privacidade são simplesmente deixados de lado por causa da visão de que o dano em fazer isso é trivial (GUERRA, 2014, p. 14).

De fato, esse conceito de privacidade, a vida privada toma novos contornos com as modificações das relações sociais. Nesse sentido, Arendt

(2017) leciona que privacidade moderna, diferentemente da que existia na antiguidade, não é apenas oposto à esfera política, mas se contrapõem à esfera social, possuindo como primordial função a de abrigar o que é íntimo. Buscando tutelar esse novo valor, o art. 2º da LGPD estabelece como diretrizes:

> A disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; eVII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais (BRASIL, 2018).

Assim, a supracitada norma recepciona preceitos estabelecidos no Máximo Texto e reconhece que a privacidade deve ser tutelada por todos os sujeitos que compõe a sociedade. Inclusive, o art. 3º versa que a norma se aplica a pessoa natural ou por pessoa jurídica de direito público ou privado. Tal ampliação é considerado um grande avanço normativo e faz da LGPD e um marco na tutela desse bem jurídico.

De fato, pode se verificar também quando correlacionado a doutrina da Guerra (2014) que compreende que do direito à privacidade decorre à proteção da reputação depende da proteção não apenas contra falsidades, mas também contra certas verdades. Para esse autor, saber detalhes particulares sobre a vida das pessoas não leva necessariamente a um julgamento mais preciso sobre as pessoas.

Ainda para Guerra (2014), a privacidade de dados se concentra nos direitos dos indivíduos**,** no objetivo da coleta e processamento de dados, nas preferências de privacidade e na forma como as organizações governam os dados pessoais dos titulares dos dados. Nessa perspectiva, a LGPD se se concentra em como coletar, processar, compartilhar, arquivar e excluir os dados.

Castells e Cardoso (2006) acreditam que romper esses limites pode criar situações sociais embaraçosas e prejudicar nossos relacionamentos. A

privacidade também é útil para reduzir o atrito social que se encontram na vida e fundamental para que o indivíduo desenvolva sua personalidade.

Cumpre ressaltar que, o ordenamento jurídico interno está em consonância com as normas de direito internacional, visto que, a DUDH/48, em seu art. 12, versa que ninguém será sujeito a interferências na sua vida privada, na sua família, no seu lar ou na sua correspondência, nem a ataques à sua honra e reputação. De fato, a partir da técnica de interpretação sistêmica do ordenamento jurídico interno e internacional, no direito à privacidade está implícito no direito à vida e à liberdade garantidos aos cidadãos.

No âmbito conceitual, Branco e Mendes (2012) lecionam que o domicílio delimita um espaço físico em que o indivíduo desfruta da privacidade, em suas variadas expressões. Para esses, nesse espaço o indivíduo não deve sofrer intromissão por terceiros, e deverá gozar da tranquilidade da vida íntima. Ou seja, é um local em que deve ter repouso e tranquilidade.

Ademais, os supracitados autores ainda afirmam que assim o conceito de domicílio abrange ‘todo lugar privativo, ocupado por alguém, com direito próprio e de maneira exclusiva, mesmo sem caráter definitivo ou habitual’. Para esses, o conceito constitucional de domicílio é, assim, mais amplo que aquele do direito civil. De fato, o ordenamento jurídico interno vem ampliando a interpretação desse instituto.

Por sua vez o Pacto de San José da Costa Rica, em seu art. 11, 2, quando da tutela da proteção da honra e da dignidade, versa que ninguém pode ser objeto de ingerências arbitrárias ou abusivas em sua vida privada, na de sua família, em seu domicílio ou em sua correspondência, nem de ofensas ilegais à sua honra ou reputação.

Buscando delimitar o conceito de domicílio, o CC/2002, em seu art. 70 versa que esse é o lugar onde em que a pessoa natural estabelece a sua residência com ânimo definitivo. Todavia, diante das complexidades das relações da vida, esse reconhece que as pessoas podem possuir mais de um domicilio. Logo, art. 71 dispõe que se a tiver diversas residências, onde, alternadamente, viva, considerar-se-á domicílio seu qualquer dessas.

Buscando tutelar a prática profissional, em seu art. 72 há uma extensão desse instituto. Assim, o dispositivo versa que é também domicílio da pessoa

natural, quanto às relações concernentes à profissão, o lugar onde está é exercida. De fato, essa garantia vem sendo observada quando do julgamento de lides contendo a matéria em e, partir, da técnica de interpretação extensiva, até por vezes tendo seu sentido ampliado.

Na medida em que a relação com os meios de comunicação se intensifica e a produção em massa torna-se evidente, surge a preocupação geral de garantir uma mídia livre, independente, plural e diversificada, preocupação esta que passa a se fixar como o ideal a ser alcançado para que o direito à liberdade de buscar, difundir e receber informações possa ser realizado em sua plenitude (SILVEIRA, 2016).

Sendo o Brasil um país signatário da Declaração Universal dos Direitos Humanos de 1948 (DUHD) e do Pacto de San Jose da Costa Rica de 1969, esse possui o deve de garantir esse direito fundamental. Nesse sentido o documento americano dispõe que:

> 4. O acesso à informação em poder do Estado é um direito fundamental de cada indivíduo. Os Estados têm a obrigação de garantir o pleno exercício deste direito. Este princípio permite apenas limitações excepcionais que devem ser previamente estabelecidas por lei no caso de um perigo real e iminente que ameace a segurança nacional em sociedades democráticas (CADH, 1969).

Ademais, lembra Reimão (2011) que o acesso do público à informação e proteger as liberdades fundamentais, de acordo com a legislação nacional e acordos internacionais. Para Reimão (211) é esse instrumento deve ser compreendido como parte de um aparelho de coerção e repressão que, muito mais do que afetar a circulação de alguns bens culturais, restringia a produção e circulação da cultura. Ademais, ainda é uma forma de exercício de controle estatal.

Ao passo em que a mídia constitui um importante meio de transmissão de informações com o intuito de educar e democratizar surge questionamentos direcionados ao potencial que as mídias sociais têm em criar condições manipulativas e gerar tendências nas preferências e opiniões da população sobre determinado tema. (SILVEIRA, 2016).

Esses fatos demonstram a influência das desses recursos nas relações modernas, a dimensão imprevisível que tais ferramentas podem assumir e a

vulnerabilidade à qual todos, irrestritamente, estão sujeitos. Ainda assim, Reimão (2011) justifica que nada pode suspender garantias individuais e criam condições para à divulgação da informação, à manifestação de opiniões e às produções culturais e artísticas.

De fato, se outrora uma informação sensacionalista praticada na presença de um grupo de pessoas gerava um inegável prejuízo para o ofendido, hodiernamente, a mesma ofensa, se veiculada em uma rede social, pode atingir nefastas proporções (OLIVEIRA, 2003). É notória, assim, a carga negativa que se atribui ao estilo sensacionalista. As características desse tipo de produção informativa baseada no exagero podem justificar a situação.

Por outro, contrasta-se com o desvio da finalidade dessas redes, porque os usuários passaram a escrever informações que com certa frequência violam direitos e garantias fundamentais, praticados por usuários que por muitas vezes se escondem por trás de apelidos, pseudônimos e perfis falsos, cometendo crimes ocultados pelo anonimato (LEITE, 2016).

Ainda assim, lembra Fiss (2005) que:

> [...] uma sociedade democrática está continuamente em processo de mudança, terá restrições de direitos e liberdades e seus procedimentos serão frequentemente questionados. Isso é garantido pelo direito à liberdade de expressão, que, portanto, é vista como um pré-requisito da democracia. Consequentemente, a democracia pode ser vista como um sistema político "trágico" (FISS, 2005, recurso digital, grifo nosso).

Entretanto, lembra Leitão (2011) que isso não garante que a liberdade de expressão é ou poderá ser absoluta e deve ser respeitada em todos os espaços um código de conduta específico. Ainda assim, essa esclarece que a censura – mais que um ato de poder oficial – se sofisticou e se consolidou como um instrumento institucional, sustentado por rígidos mecanismos de controle e administração da informação

Ainda para Leitão (2011), o público em geral está se tornando mais ciente de todos os seus direitos crescentes de dizer àqueles que coletam seus dados pessoais que esperam ter seus dados pessoais protegidos e têm direito de acessar e controlar seus dados pessoais. Assim, leciona Castells e Cardoso

(2006) que privacidade de dados está relacionada a como uma informação - ou dados - deve ser tratada com base em sua importância relativa.

Já para Rodatà (2018), para uma empresa, a privacidade de dados vai além das proteções de informação de seus funcionários e clientes. Também inclui as informações que ajudam a empresa a operar, sejam dados proprietários de pesquisa e desenvolvimento ou informações financeiras que mostram como ela está gastando e investindo seu dinheiro. Ademais, lembra o autor que:

> Quando os dados que deveriam ser mantidos em sigilo chegam às mãos erradas, coisas ruins podem acontecer. Uma violação de dados em uma agência governamental pode, por exemplo, colocar informações ultrassecretas nas mãos de um estado inimigo. Uma violação em uma empresa pode colocar dados proprietários nas mãos de um concorrente (RODATÀ, 2018, recurso digital).

Importante ainda, diante de um mercado globalizado e de venda informações, é a questão levantada por Fradera (2006). Esse lembra que os dados estão se tornando cada vez mais valiosos. Além disso, as habilidades e oportunidades para recuperar diferentes tipos de dados pessoais estão evoluindo extremamente rápido. Logo, o processamento não autorizado, descuidado ou imprudente de dados pessoais pode causar grandes danos a pessoas e empresas.

Por exemplo, especificamente, quando do contexto pandêmico, inúmeras organizações tiveram que desenvolver suas atuações através teleatendimento. Quando da reflexão da proteção dos dados dos usuários do paciente, parece que as normas devem ser ainda mais observadas, visto que, podem ocasionar um dano maior a honra dos usuários.

A responsabilidade civil das empresas médicas configura-se com um dever desse profissional de reparar o dano causado a um paciente, sendo essa indenização de forma patrimonial, diferente do que acontecia na antiguidade que era cobrado da integridade física do responsável.

Nesse sentido, a Resolução nº 2.217 de 27 de setembro de 2018 e Lei nº 13.787, de 27 de dezembro de 2018,dispõem sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente. Assim, em seu art. 2º essa versa que o processo de digitalização de prontuário de paciente será realizado de forma a

assegurar a integridade, a autenticidade e a confidencialidade do documento digital.

Ademais, os parágrafos dos referidos artigos ainda versam que:

> § 1º Os métodos de digitalização devem reproduzir todas as informações contidas nos documentos originais. § 2º No processo de digitalização será utilizado certificado digital emitido no âmbito da Infraestrutura de Chaves Públicas Brasileira (ICP-Brasil) ou outro padrão legalmente aceito. § 3º O processo de digitalização deve obedecer a requisitos dispostos em regulamento (BRASIL, 2018).

Lembra Rodatà (2018) que o não cumprimento dos regulamentos de proteção de dados pessoais pode levar a situações ainda mais duras, em que é possível extrair todo o dinheiro da conta bancária de uma pessoa ou mesmo causar uma situação de risco de vida, manipulando informações de saúde.

Dessa forma comenta Fradera (2006):

> A consideração da natureza da responsabilidade médica como contratual não tem como efeito tornar presumível a culpa. É ao paciente, ou, se for o caso, a seus familiares que incumbe demonstrar a inexecução da obrigação, por parte do profissional. Provada a culpa do profissional com relação aos cuidados dispensados ao doente, será aquele constrangido à reparação do dano causado. (FRADERA, 2006, p. 123).

Não tem como negar que nos dias atuais existe a formação de um contrato quando um médico atende um paciente. Esse contrato mantém uma obrigação subjetiva, pois apesar de tudo, o médico não pode prometer a cura ao paciente, e sim usar todo o seu conhecimento para fazer o tratamento mais adequado para que o paciente fique bem.

Assim dispões Gonçalves (2014):

> Comprometem-se os médicos a tratar o cliente com zelo, utilizando-se dos recursos adequados, não se obrigando, contudo, a curar o doente. Serão, pois, civilmente responsabilizados somente quando ficar provada qualquer modalidade de culpa: imprudência, negligência ou imperícia. (GONÇALVES, 2014, p. 15).

Como dito, para que o médico seja responsabilizado por um dano, tem que se provar a culpa, conforme consta no §4º art. 14 do Código de Defesa do Consumidor. Já que a medicina não é uma ciência exata, às vezes, mesmo

que o profissional tenha feito o tratamento usando todas as técnicas e medicamentos corretos, não atingiu a cura. Ou seja, ele fez tudo que estava ao seu alcance, mas por uma coisa adversa, a qual talvez nem se possa identificar o paciente não apresentou melhora.

Seguindo essa premissa, no Código de Defesa do Consumidor (CDC/90), estão os art. 6º, III:

> São direitos básicos do consumidor: III – a informação adequada e clara sobre os diferentes produtos e serviços, com especificação correta de quantidade, características, composição, qualidade de preço, bem como sobre os riscos que apresentem (BRASIL, 1990)

Para Rodatà (2018), em relação aos clientes, garantir que seus dados sejam mantidos seguros é o mínimo que as pessoas esperam das empresas com as quais negociam ou nas quais investem. A governança de dados adequada gera confiança. Esse protege a reputação da uma empresa, estabelecendo como a marca se posiciona no mercado.

Ademais, o art. 31 estabelece que:

> A oferta e apresentação de produtos devem assegurar informações corretas, claras, precisas, ostensivas e em língua portuguesa sobre suas características, qualidades, quantidade, composição, preço, garantia, prazos de validade e origem, entre outros dados, bem como sobre os riscos que apresentam à saúde e segurança dos consumidores. (BRASIL, 1999).

Se estendendo esse dever de informar não só para os pacientes, como também para os seus familiares ou responsáveis, os quais devem ser orientados de todos os cuidados que devem ter com o doente. Segundo Melo (2008) o dever mais importante do médico deveria ser o de continuar aprimorando e atualizando para um melhor atendimento aos seus pacientes, procurando sempre novas técnicas, medicamentos que sejam mais eficazes para tratamentos.

Para Rodatà (2018), a privacidade reflete, portanto, duas noções subjacentes. Em primeiro lugar, a privacidade em geral e a privacidade informativa em particular são sempre questões de grau. Raramente alguém está em uma condição de completa inacessibilidade física ou informativa para outras pessoas, nem desejaria permanecer assim. Em segundo lugar, embora a privacidade das informações possa ser valiosa e merecedora de proteção,

muitos defensores da privacidade ponderados argumentam que ela não tem, por si só, significado moral ou valor inerente.

Confidencialidade e privacidade são princípios relacionados, ambos protegendo o paciente da divulgação de registros médicos. Embora a confidencialidade seja geralmente considerada uma regra ética para profissionais médicos e a privacidade como uma questão legal, muitos países também codificaram a confidencialidade médica dentro das leis nacionais ou dos princípios da lei comum, o que significa que as informações médicas não podem ser divulgadas sem o consentimento do paciente. Os prestadores de cuidados de saúde são, portanto, geralmente obrigados por lei ao dever de confidencialidade e privacidade.

Para Rodotà (2018), duas tendências um tanto distintas levaram ao aumento do acesso ao registro de saúde primária e subsequentes preocupações sobre privacidade. Um tem a ver com os registros de saúde primários, independentemente de como são criados e mantidos; a outra envolve registros de saúde armazenados eletronicamente.

Leciona Villas-Bôas (2015) que as abordagens éticas, legais e outras existentes para proteger a confidencialidade e a privacidade dos dados pessoais de saúde oferecem algumas salvaguardas, mas permanecem lacunas e limitações importantes. Para o autor, à medida que os registros continuam a suplantar os encontros face a face em nossa sociedade, não houve nenhuma tendência compensatória de dar ao indivíduo o tipo de controle sobre a coleta, uso e divulgação de informações.

Rodotà (2018) ainda lembra que quantidade e o tipo de informações sobre cuidados de saúde agora coletadas também aumentaram nos últimos anos. A participação na prestação de cuidados de saúde de muitos indivíduos e grupos de provedores diferentes exerce forte pressão para documentar cada vez mais detalhadamente. O número crescente de tecnologias disponíveis para diagnóstico e terapia significa que os detalhes que um provedor poderia em um determinado momento convocar devem agora ser registrados e, assim, estar disponíveis para inspeção por outros.

Ainda para autor supracitado, quanto mais detalhadas forem as informações sobre um indivíduo ou classe de indivíduos, mais apropriado, espera-se, será o tratamento que receberão. Além disso, a documentação do

atendimento e dos fatores de risco é essencial para promover a continuidade do atendimento ao longo do tempo e entre os provedores. É também uma primeira defesa contra acusações de imperícia.

Além disso, a crise do COVID-19 tornou as questões de privacidade de dados ainda mais salientes. Conforme as organizações coletam informações pessoais sobre a saúde dos funcionários e viagens como parte de sua resposta para conter a propagação do vírus, essas precisam tomar medidas adequadas para proteger a privacidade dos funcionários e manter a conformidade com os regulamentos de privacidade de dados aplicáveis.

### 3.4 Casos midiáticos no Brasil

Atualmente, para além da privacidade, o direito ao esquecimento é o direito que um indivíduo possui de que um fato, ainda que comprovado, ocorrido em momento indeterminado, não seja exposto ao público em geral, causando-lhe sofrimento ou transtornos. Trata-se de um direito que possui assento constitucional e legal no Brasil considerando que é uma consequência do direito à vida privada (privacidade), intimidade e honra, assegurados pela CRFB/1988 (art. 5º, X) e pelo Código Civil (SCHREIBER, 2014).

No entanto, também ocorre um movimento de grande “exposição midiática”. As pessoas vivem conectadas e diariamente um volume muito grande de informação e dados pessoais são despejados na internet viabilizando uma diversidade de violações a direitos fundamentais. Essas violações, a seu turno, têm levado ao surgimento de esforços para contê-las, a exemplo da LGPD, levando a pensar sobre até que ponto seria razoável restringir a divulgação destas informações na Web ante ao risco de gerar um colapso no avanço tecnológico (MORATO; CICCO, 2015).

Assim, é fundamental a busca pros comportamentos que busquem conciliar estas duas realidades (proteção de dados pessoais versus desenvolvimento tecnológico) érelevante tendo em vista que limitar excessivamente a divulgação de dados pessoais e permitir que o avanço tecnológico continue sem impor a ele nenhum limite e regulamentação parecem não ser razoáveis.

O avanço tecnológico, além de trazer vários benefícios para a sociedade, também trouxe preocupações no que se refere à inserção de dados pessoais na internet quando advir no futuro o desejo de indisponibilizá-los, além das novas formas como estas informações são empregadas, acenderam o debate sobre o direito de proteger a privacidade dos usuários, além dos seus dados pessoais.

Nesse contexto, pode-se compreender o direito ao esquecimento como a pretensão de recobrar o domínio sobre os fatos pessoais depois que eles foram legitimamente divulgados. Consiste, substancialmente, em uma reintegração do poder de dispor, depois de sua perda determinada pela publicação da notícia pessoal (BUCAR, 2013).

Embora a terminologia “direito ao esquecimento” possa induzir ao entendimento diverso, o direito ao esquecimento não impõe uma obrigação de esquecer. Não se trata de exigir que outros sujeitos esqueçam os fatos que nos concernem, mas apenas de impedir a divulgação de informações pessoais quando não haja mais interesse social no conhecimento de determinado fato (BUCAR, 2013).

O que se protege é o livre desenvolvimento da personalidade que seria afetado pela difusão de fatos passados e não pela recordação não exteriorizada. Não existe, portanto, dever de esquecer, mas sim dever de não divulgar fatos passados que possam ocasionar dano ao livre desenvolvimento do projeto vital dos indivíduos (BUCAR, 2013).

Com o advento da internet, este direito ao esquecimento clássico, de perfil bem definido, sofre profundas transformações, passando a abranger uma vasta gama de possibilidades.É que a informação divulgada na internet não representa mais um evento isolado, como ocorre com a apresentação televisiva ou com a publicação do exemplar de um jornal geralmente destinado ao lixo após a leitura (CONSALTER, 2016). Uma vez divulgada, a informação se pereniza na internet, podendo ser acessada rapidamente por qualquer usuário, sem que haja qualquer distinção entre informações desatualizadas e mais recentes.

Não obstante a dificuldade em se fazer valer o direito ao esquecimento em razão do desenvolvimento tecnológico e da internet, Consalter (2016)

entende que é possível fazer uso dos próprios recursos da tecnologia da informação para, de tempos em tempos, suprimir dados, imagens, enfim, arquivos diversos da rede até que estes, com o passar do tempo, desapareçam. A autora entende que, para tanto, “a solução mais eficaz está na arquitetura da rede, disseminando ferramentas tecnológicas que subordinam a acessibilidade de determinado dado a um lapso temporal” (CONSALTER, 2016, p. 348).

Embora não possa dizer que esta é uma tarefa impossível, reafirme-se que não é uma empreitada fácil. Melhor explicando, é bem provável que as informações referindo-se à intimidade de alguém disponibilizadas na internet tenham sido publicadas por ele próprio e, depois, retiradas. No entanto, é possível que alguém tenha feito uma cópia e a disponibilizado em outros locais. Um exemplo bastante simples é um amigo que pode ter sido marcado na rede social há muitos anos. Neste caso, independentemente da vontade do principal interessado, ou seja, a pessoa a que as informações veiculadas se referem, não é possível exercer controle sobre as cópias existentes sob a responsabilidade de terceiros, de maneira que referidas informações podem seguir por distintos caminhos.

Outra questão que enseja preocupação é a falta de consenso que ainda paira sobre ser ou não o direito ao esquecimento um direito da personalidade. Consalter (2016) entende que o primeiro passo a ser dado quando se trata do direito ao esquecimento é que os ordenamentos jurídicos concebam-no com um direito fundamental; que o indivíduo possa exercê-lo se tiver interesse e se estiverem presentes os pressupostos jurídicos necessários para tanto.

Já Schreiber (2013) destaca que o rol de direitos da personalidade é aberto e, portanto, não taxativo, estimula o debate sobre novas esferas de realização da pessoa humana. Este autor também tratou, no ano de 2013, sobre o avanço tecnológico e a velocidade como a informação se propaga na internet. Assim, o citado autor leciona que:

> A internet não esquece. Ao contrário dos jornais e revistas de outrora, cujas edições antigas se perdiam no tempo, sujeitas ao desgaste de seu suporte físico, as informações que circulam na rede ali permanecem indefinidamente. Pior: dados pretéritos vêm a tona com a mesma clareza dos dados mais recentes, criando um delicado conflito no campo do direito. De um lado, é certo que o público tem o direito de relembrar fatos antigos. De outro, embora ninguém tenha o direito de apagar os fatos deve-se evitar que uma pessoa seja perseguida, ao

> longo de toda sua vida, por um acontecimento pretérito (SCHREIBER, 2014, p. 172).

O supracitado autor ainda reconhece o direito ao esquecimento e a liberdade de informação como direitos de matriz constitucional e propõe que a ponderação seja aplicada. Para esse é fundamental valer-se de parâmetros que torne possíveis verificar com os princípios predomina no caso concreto. Trata-se assim da técnica de ponderação de princípios para a resolução do caso concreto.

De fato, o direito ao esquecimento tem sido aplicado no direito brasileiro há muito tempo, fazendo uso, principalmente, da analogia. Como lembra Morato (2015), a apreciação de casos com vistas a compreender o direito ao esquecimento. Muitos são os casos veiculados na mídia que são constantemente retratados que foram objetos de enfretamento nos tribunais quanto ao direito de esquecimento.

Recentemente, quando do enfretamento da matéria, o STF, o Ministro Fachin reconheceu que a Constituição Brasileira recepciona um direito ao esquecimento, mas esse deve ser examinado sempre analisando as especificidades do caso concreto. Ainda que o pedido do pleito do Recurso 1.010.606/RJ tenha sido negado, o julgado foi fundamental para a discussão da matéria no ordenamento jurídico interno, visto que, buscava discutir o limite da Rede Globo em transmitir o caso “Aída Curi”.

## 3.5 Das sanções aplicada em outros países

A preocupação com a proteção dados é uma tendência no direito comparado. Nether (2018) expõe que o Regulamento Geral de Proteção de Dados da União Europeia ('GDPR') executa fielmente as implicações da metáfora do petróleo, apesar do ajuste inadequado da metáfora. O GDPR presume que os dados pessoais são importantes, tanto que todos os aspectos da interação com os dados requerem um planejamento cuidadoso.

Especificamente, no caso do referido conjunto normativo, Nether (2018) esclarece que as práticas da indústria da informação e até mesmo a literatura acadêmica sobre técnicas de identificação de ponta. Para o autor, por essa e

outras razões, o GDPR tem um alcance extraordinariamente amplo em todas as dimensões. Duas definições de limite são 'dados pessoais' e as atividades de informação consideradas 'processamento'.

Estudando os pressupostos históricos e a política legislativa, Guerra (2014) afirma que na Europa há muito reconhece a privacidade explicitamente como um direito humano. Ainda para o autor, os compromissos europeus vão além do lar, o foco de tantas leis americanas, para incluir proteções para a vida familiar, comunicações, reputação e, com o aumento da era da informação, para a privacidade no contexto do processamento de dados.

Guerra (2014) esclarece que embora os advogados norte-americanos possam se referir amplamente a 'privacidade' ou 'privacidade de informações', a lei europeia discute a privacidade de informações como 'proteção de dados'. De fato, Nether (2018) reconhece que na Europa, a proteção de dados é cada vez mais vista como separada do direito à privacidade. A proteção de dados se concentra em se os dados são usados de forma justa e com o devido processo enquanto a privacidade preserva o ideal ateniense de vida privada.

Guerra (2014) aponta que em 1990, a Comissão Europeia temia que as leis nacionais divergentes de proteção de dados prejudicassem o mercado interno na UE. 24. Nesse ano, publicou uma proposta de diretiva relativa à proteção de dados. Após cinco anos de negociações, a Diretiva de Proteção de Dados final foi adotada em 1995. A Diretiva estabeleceu um regime omnibus baseado nos FIPs, que se aplicava à maior parte dos setores público e privado (com exceção deste último). A Diretiva exigia que os Estados-Membros aprovassem legislação de implementação.

Nether (2018) acredita que os problemas surgiram rapidamente com a diretiva. A Diretiva não harmonizou totalmente as leis nacionais de privacidade e, mesmo na Europa, os países se comportaram de forma oportunista para cortejar as grandes tecnologias com sinais de aplicação fraca e esquemas fiscais vantajosos.

Mesmo entre os países comprometidos com a privacidade, a fiscalização foi frouxa, com os franceses multando o Facebook em meros 150.000 euros em 2017. Essa lacuna de fiscalização deixou a Europa com a reputação de região com regras, mas sem policiamento real, enquanto os

Estados Unidos eram vistos como não estando vinculados às regras, mas tinham a Federal Trade Commission na ronda de fiscalização.

Ainda para, Nether (2018) , o GDPR é a tentativa da UE de abordar essas e outras deficiências. Fez isso em um processo completamente diferente dos esforços legislativos dos Estados Unidos. Os legisladores europeus iniciaram um processo que envolveu uma grande variedade de consultas a especialistas e profunda sofisticação sobre como as práticas de informação podem ser manipuladas para fugir das metas regulatórias.

# 4 OS RECURSOS TECNOLÓGICOS DE SEGURANÇA EXISTENTES NA ATUALIDADE, NA PROTEÇÃO DE DADOS

## 4.1 O sistema de proteção de dados mais avançado na atualidade

Monteiro, Vignoli e Almeida (2020) buscam compreender a construção histórica da ciência da informação, principalmente, direcionando o estudo para o impacto que os avanços da tecnológicos após a década de 1990 ocasionaram para o aprimoramento desse campo do conhecimento. De pronto, esses destacam que categorias como nanotecnologia, microbiologia, realidade virtual, inteligência artificial (ia), neurofisiologia e ciências cognitivas foram diretamente afetadas por esse processo.

Entretanto, ao passo que verificam inúmeras evoluções, os autores também percebem que o avanço da articulação entre ciência e tecnologia promoveu um processo de laicização entre alguns campos do saber. Nessa perspectiva, destacam que cisões disciplinares e a ultraespecialização fundadas em um projeto de ciência subsidiado são interpostas por narrativa moderna do conhecimento. Ou seja, ao invés de integrar, há um processo de separação entre campos do saber.

Para Monteiro, Vignoli e Almeida (2020) apresentam a definição de algumas categorias, mas utilizando o recurso dialético também promovem a reflexão entre esses objetos examinados. Assim, a cultura cibernética é apresentada como um recurso tecnológico, mas ao mesmo tempo enquanto um conjunto de expectativas sociaisque estão em constante processo de renovação social.

Monteiro, Vignoli e Almeida (2020) compreendem a cibercultura como uma categoria que existe em realidades virtuais multidimensionais em rede global, sustentadas por computador, acessadas por computador e / ou geradas por computador, mas também enquanto um fechamento do espaço e do tempo, comprimido pelos avanços tecnológicos capaz de criar uma especialização e alienação crescentes nas extensões tecnológicas de nos corpos e mundo.

Monteiro, Vignoli e Almeida (2020) partem do pressuposto que o pós-humano marca o fim da dissolução do sujeito racional autônomo do humanismo: o sujeito é descentrado não apenas em relação a si mesmo, mas

também em relação ao mundo. Por sua vez, o ciberespaço situa o sujeito como múltiplos pontos em um mapa da realidade virtual e a cibercultura captura o sujeito 'sem sujeito' dentro de uma teia de redes interativas, deslocando a autonomia. A tecnologia expandiu e aperfeiçoou as técnicas de representação 'do real' a ponto de o status ontológico do real ser questionado em grande escala.

Nesse contexto, os autores esclarecem as narrativas humanista e marxista mais ou menos sectárias não conseguiram explicar a simbiose entre seres humanos e tecnologias, inteligência e tecnologia, bem como a condição humana frente a este estágio de integração sociotécnico. Todavia, ao longo de sua pesquisa, esses verificam que houve um processo de assimilação, na medida em que se opõe à representação.

Os pesquisadores verificam a iminente necessidade de criação de um novo paradigma que seja pautada em uma mudança epistemológica na Ciência. Assim, esses apontam que, no contexto de Segunda Guerra Mundial, muito importante foram as contribuições do ponto de vista pragmático e do desenvolvimento de conceitos metodológicos como entropia, informação, termodinâmica, equilíbrio de sistemas e mensagens, homeostase, input e output e feedback.

Enquanto argumento de autoridade, Monteiro, Vignoli e Almeida (2020) expõe as contribuições de Wiener (1970) quando da postulação de significado de Cibernética enquanto uma forma de controle e comunicação no animal e na máquina. Para os autores, foi fundamental para dissociar esse de conceitos vazios, ao passo que, assume que esse instrumento mina a distância simbólica entre o metafórico e o real, abandonando este último ao apresentar uma simulação cada vez mais real de uma realidade.

Ainda destacando as contribuições de Wiener (1970), esses lembram que o autor já alertava para eventuais relações de domínio entre criação e criador. Em apud é possível verificar que: quando comando as ações de outra pessoa, comunico-lhe uma mensagem, e embora tal mensagem esteja no modo imperativo, à técnica de comunicação não difere de uma mensagem de fato (WIENER, 1970).

Fazendo um contraponto a teoria marxista, esses lembram que a doutrina humanista liberal do individualismo possessivo - a liberdade de dispor

de propriedade à vontade, incluindo a propriedade do corpo - está perdida nas redes do ciberespaço. O movimento do humano para o pós-humano articulado é, com efeito, uma transição da ordem para o caos.

De fato, as maiores contribuições de Monteiro, Vignoli e Almeida (2020) são quando da reflexão de que a interface homem/máquina se torna um lugar em que as noções tradicionais de subjetividade e incorporação são potencialmente abandonadas. Apesar das tentativas de sustentar a noção do sujeito humanista liberal, o final do século XX viu uma nova maneira de ver os seres humanos. Daí em diante, os humanos deveriam ser vistos principalmente como entidades de processamento de informações que são essencialmente semelhantes a máquinas inteligentes

Ainda quando da análise da pesquisa de Monteiro, Vignoli e Almeida (2020), esses destacam os estudos de Pearson (2014) que compreende que o transumanismo é a união de robôs, humanos e IA, até chegar ao homo whateverus (o homem tudo). Correlacionando com a vivência na cibercultura, esses lembram que nesse espaço, o self é múltiplo, fluido e constituído apenas por meio da interação com a tecnologia. os humanos deveriam ser vistos principalmente como entidades de processamento de informações essencialmente semelhantes a máquinas inteligentes

Monteiro, Vignoli e Almeida (2020) destacam que a evolução continua, tanto no mundo dos robôs quanto no mundo dos humanos, dando origem ao homo machinus. De fato, no ambiente tecnológico, o homem constrói uma identificação de indivíduo é múltiplo, fluido e constituído apenas por meio da interação com a tecnologia. os humanos deveriam ser vistos principalmente como entidades de processamento de informações essencialmente semelhantes a máquinas inteligente

Uma das contribuições dos autores é propor a reflexão de que se o corpo é sempre cibernético no ciberespaço, a identidade é simulada abertamente. Travestir por recursos digitais é um recurso padrão para assumir uma nova identidade. Entretanto, esses chamam à atenção para o ato de que novos dilemas surgem, visto que, o pós-humano não significará um estágio pós-ético, na melhor das hipóteses, estar-se-á tratando de um contexto “super-ético”, isto é, uma ética superior aplicada indistintamente aos comportamentos humanos e não humanos, responsabilizando-os com o mesmo rigor.

Outra contribuição da pesquisa é a conclusão de que o poder de descentramento do ciberespaço permitiu que o sujeito desaparecesse na "hiperrealidade" das reproduções e representações digitais que "não têm relação com nenhuma realidade: é seu próprio simulacro puro. Entretanto, os autores destacam que o pós-humano já faz parte de nossa realidade, desde próteses mecânicas, implantes médicos, procedimentos estéticos até a extensão da nossa memória, por meio das plataformas digitais e dos mecanismos de busca. Logo, é fundamental uma readaptação a nova realidade.

Por fim, Monteiro, Vignoli e Almeida (2020) destacam que devem ser observadas as etiquetas conceituais que surgem para definir este momento e outros que virão se não cotejadas, são vagas, porque o espectro da teoria do pós-humano é vasto e complexo. Tal como, na relação cibercultural entre corpo e tecnologia, não existe identidade. E essa pode gerar efeitos negativos como fake News.

### **4.1.1 A** forma como esses sistemas são desenvolvidos

Há muito tempo se discute a necessidade de proteger ativos de um local ou organização. Muitos sensores (por exemplo, radar, detectores infravermelhos, câmeras de vídeo, detectores de vibração e assim por diante) estão sendo desenvolvidos e implantados (BOLZANI, 2004). As saídas desses sensores podem gerar informações numerosas e desconexas. Consequentemente, o pessoal de segurança recebe muitos “relatórios de sensores” que podem ser significativos ou não para a construção de suas ações.

Conforme Capel (1997), em sua origem, um plano pode ser um instrumento para avaliar a segurança da instalação informática com base nas informações do sensor, informando um analista de segurança ou guarda do status de segurança da instalação e respondendo a atividades de segurança de alta probabilidade com ações apropriadas.

Todavia, um sistema pode abordar um número significativamente crescente de relatórios de sensores e uma quantidade cada vez maior de

informações e, consequentemente, uma carga de trabalho imensamente grande de pessoal de segurança, aplicando a lógica Bayesiana ou outras técnicas para fornecer uma hipótese de nível superior do que está acontecendo(BOLZANI, 2004).. Esse sistema pode reduzir o número de alarmes falsos com os quais o pessoal de segurança precisa lidar e fornecer uma maior conscientização da situação de segurança.

Os sistemas de segurança e proteção correspondem a um conjunto de vários meios ou dispositivos projetados para proteger pessoas e bens contra uma ampla gama de perigos, incluindocrime,incêndio, acidentes, espionagem, sabotagem, subversão e ataque(BOLZANI, 2004).

As origens dos sistemas de segurança são cientificamente catalogadas, mas as técnicas de proteção da casa, como o uso de fechaduras e janelas gradeadas, são muito antigas(BOLZANI, 2004). Conforme as civilizações se desenvolveram, a distinção entre segurança passiva e ativa foi reconhecida, e a responsabilidade pelas medidas de segurança ativa foi atribuída à polícia e a agências de combate a incêndio.

Ainda para Capel (1997), em meados do século XIX, as organizações privadas começaram a construir serviços de segurança eficientes em grande escala. Ainda conforme o autor, a Organização Pinkertonfoi uma das primeiras a oferecer um serviço de inteligência de contrainformação de segurança interna, investigação e a buscar a aplicação da lei para empresas privadas.

Outro marco foi o desenvolvimento, pela organização Sorensen, de um sistema direcionado para construção de um serviço de controle de perdas para a indústria(BOLZANI, 2004). Essa ação buscou centrar sua atenção para a importância de recurso humano treinado para prevenir e lidar com perdas em crimes, incêndios, acidentes e desastres naturais.Assim, foi a primeira organização que estabeleceu um padrão para serviços de segurança na Europa.

Para Capel (1997), as duas grandes Guerras trouxeram uma maior consciência sobre a necessidade de um sistema de segurança como meio de proteção contraespionagem militar, sabotagem e subversão direcionada aos ambientes estatais. Estudos centraram-se no desenvolvimento de programas que superassem as falhas apontadas durante os conflitos.

Detalha Bolzani (2004) que especificamente, depois da Segunda Guerra Mundial, grande parte desse aparato foi retido como resultado de tensões internacionais e os programas de produção de defesa e tornou-se parte de um complexo cada vez mais profissionalizado de funções de segurança.

Desde a década de 1960, os sistemas de segurança relacionados ao crime cresceram de maneira especialmente rápida na maioria dos países(BOLZANI, 2004). Entre os fatores contribuintes, estão o aumento no número de empresas sensíveis à segurança; desenvolvimento de novas funções de segurança, como proteção de informações proprietárias; aumentar a informatização de informações confidenciais sujeitas a vulnerabilidades únicas; melhor notificação de crimes e, consequentemente, maior conscientização; e a necessidade em muitos países de segurança contramanifestações violentas, bombardeios e sequestros.

## 4.2 Investimento de empresas em sistemas de proteção

Os sistemas de segurança estão se tornando cada vez mais automatizado, particularmente na detecção e comunicação de perigos e vulnerabilidades. Esses mecanismos, entre outras coisas, concentram-se na proteção contra crimes e acidentes (BOLZANI, 2004). Por exemplo, é crescente a utilização de dispositivos de detecção que indiquem a intrusão de agentes indesejados e sistemas de alarme que responda a situações que apontem focos possíveis de incêndio.

Especificamente no que se refere à proteção se estabelece no uso de tecnologia, o desenvolvimento e a difusão de sistemas e hardware de segurança em várias partes do mundo têm sido processos desiguais. Relativamentepaíses considerados em desenvolvimentoainda possuem dificuldade de acesso a equipamentos e técnicas sofisticadas por inúmeras situações, dentre essas, a falta de investimentos públicos direcionados a pesquisas científicas na área.

A segurança tem a ver com o processo ligado à atenuação de qualquer tipo integridade funcional contra forças de mudança que ver como hostis quanto à manutenção de sobrevivência (BOLZANI, 2004). Assim, a segurança é geralmente aceita como um sentimento de conforto sobre a não ocorrência

de danos, medo, ansiedade, opressão, perigo, pobreza, defesa, proteção e preservação dos valores essenciais e ameaça a esses valores.

Trata-se de um valor comumente associado ao alívio de ameaças para valorizar valores, especialmente aquelas ameaças que ameaçam a sobrevivência de um determinado objeto de referência. De acordo com o acima exposto, Buzan afirma que:

> A segurança tem a ver com a ausência de perigos ou ameaças à capacidade de uma nação de se proteger e desenvolver, promover seus valores e interesses legítimos e melhorar o bem-estar de seu povo. Assim, a segurança interna poderia ser vista como a liberdade ou a ausência dessas tendências, o que poderia prejudicar a coesão interna e a existência corporativa de um país e sua capacidade de manter suas instituições vitais para a promoção de seus valores centrais e objetivos sócio-políticos e econômicos, bem como atender às legítimas aspirações do povo (BUZAN, 1991, p. 35-36).

Portanto, pode-se inferir que a segurança, seja ela clássica, centrada no estado e tradicionalista, tem tudo a ver com a proteção de bens, incluindo recursos vivos e não-vivos contra perdas ou danos. O paradigma da segurança tradicional é uma construção realista de segurança na qual o objeto de referência é o estado (BUZAN, 1991). Equaciona segurança com paz e prevenção de conflitos através de meios militares, ou seja, políticas de dissuasão, defesa não ofensivas e afins.

Esse valor ainda pode ser entendido como um estudo da ameaça, uso econtrole da força militar, ou seja, excede as situações que tornam mais provável o uso da força, os modos como o uso da força afetam indivíduos, estados, sociedades e as políticas específicas que os estados empregam a fim de prevenir ou envolver-se em guerras (CAPEL, 1997).

Todavia, é preciso ampliar e aprofundar a definição de segurança. Atualmente, verificamos esses valores associados às questões como meio ambiente, ameaças políticas, econômicas e sociais colocam em perigo as vidas e propriedades do indivíduo, ao invés da concentração na sobrevivência do Estado (BOLZANI, 2004). Ou seja, a definição desse valor não implica em uma conceituação predominantemente militar, não aprecia o fato de que a maior ameaça à sobrevivência do Estado pode não ser militar, mas ambiental, de saúde, política, social e econômica.

A segurança nesse sentido é orientada para a emancipação humana. Significa que as pessoas/cidadãos devem ser liberadas desses desafios, dificuldades e restrições que podem impedi-los de realizar o que livremente escolheriam fazer, o que inclui epidemias, pobreza, opressão, má educação, crises e assim por diante (BOLZANI, 2004). Atualmente, a política, as questões ecológicas, econômicas e demográficas que não são militares tendem a representar sérias ameaças à segurança das pessoas.

É preciso esclarecer que um conjunto de segurança não se limita às atividades do estado, como regulamentação ou fiscalização legal, mas refere-se a um conjunto mais amplo de objetivos para gerenciar a conduta(BOLZANI, 2004). É uma eventualidade temporalmente estendida, caracterizada pela calculabilidade e previsibilidade das consequências futuras da conduta e os esforços programáticos para controlar essas consequências.

Assim, abrange formas de informação e conhecimento, representações, práticas e formas institucionais que se articulam de maneiras novas e específicas, e servem para imaginar, dirigir e agir sobre corpos, espaços e fluxos(BOLZANI, 2004). Além da segurança informática produzida pelo uso real ou potencial da força, um conjunto de segurança também pode abranger índices físicos usadospara produzir segurança por meios simbólicos.

Segurança informática refere-se à *proteção* de pessoal, hardware, software, redes, informações de dados entre outros, contra ações vandalismo, roubo, catástrofes provocadas pelo homem, desastres naturais e danos acidentais (BOLZANI, 2004). Ou seja, é um conjunto de ações que visa evitar um ataque que poderia causar sérios prejuízos a qualquer instituição.

O avanço tecnológico, além de trazer vários benefícios para a sociedade, também trouxe preocupações no que se refere à inserção de dados pessoais na internet quando advir no futuro o desejo de indisponibilizá-los, além das novas formas como estas informações são empregadas, acenderam o debate sobre o direito de proteger a privacidade dos usuários, além dos seus dados pessoais. A Lei Geral de Proteção de Dados Pessoais (LGPD) buscou criar uma tutela específica para essas relações sociais.

Leciona Moraes (2011) que cada organização precisa de proteção contra ataques cibernéticos e ameaças à segurança. O crime cibernético e o malware são ameaças constantes para qualquer pessoa com presença na

Internet, e as violações de dados são demoradas e caras. Os serviços de um provedor confiável de segurança da informação reduzirão os riscos das informações digitais e manterão os sistemas funcionando sem interrupções.

Por esse motivo, a LGPD acrescentou outra camada de importância à segurança de dados, tornando-a não apenas um requisito comercial, mas também um requisito legal. Assim, o legislador optou por uma interpretação ampliativa do sentido de dados pessoais e, dentre outras coisas, o art. 5º, versa que:

> Para os fins desta Lei, considera-se: 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; [...] (BRASIL, 2018).

De fato, a Lei de Proteção de Dados contém um conjunto de princípios que as organizações, o governo e as empresas devem seguir para manter os dados de alguém precisos, protegidos, protegidos e legais. Entretanto, essa traz uma clausula de exclusão as entidades governamentais. Assim, dispõe que:

> O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios de proteção de dados pessoais elencados no art. 6º desta Lei.§ 1º É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso[...] (BRASIL, 2018).

Outra evolução normativa, é que essa exige que as organizações implementem *medidas técnicas e organizacionais adequadas para garantir e ser capaz de demonstrar que o processamento é realizado em conformidade com o regulamento. Assim, o supracitado artigo ainda versa que:*

> […] segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão; VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; X - responsabilização e prestação de contas: demonstração, pelo agente,

> da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

A partir do exame normativo, é possível verificar que uma parte importante dessas medidas é o treinamento de conscientização sobre segurança: os funcionários precisam estar cientes da importância de seguir os procedimentos e processos de segurança de dados.

Moraes (2011) afirma que A segurança da informação desempenha quatro funções importantes para uma organização que permite a operação segura do aplicativo implementado nos sistemas de TI da organização, protege os dados que as organizações coletam e usam, protege os ativos de tecnologia em uso na organização e, por último, é proteger a capacidade de funcionamento da organização.

Já para Oliveira (2013) esse conjunto de técnica também permite a operação segura do aplicativo implementado nos sistemas de TI da organização. Isso ocorre porque, para proteger os dados, a organização aplicará ou instalará o software apropriado que protegerá os dados, como antivírus e outros aplicativos protegidos.

Silva (2011) compreende que essas ações protegerá os dados que a organização coleta e usa. Se as informações forem deixadas desprotegidas, elas podem ser acessadas por qualquer pessoa. Se a informação cair em mãos erradas, essa pode destruir vidas, encerrar negócios e também ser usada para causar danos.

Conforme Oliveira (2013) os programas de segurança da informação garantirão que as informações apropriadas sejam protegidas tanto pelos requisitos comerciais quanto legais, tomando medidas para proteger os dados da organização. Para o autor, além disso, tomar medidas para proteger as informações das organizações é uma questão de manter a privacidade e ajudará a prevenir o roubo de identidade.

Moraes (2011) compreende que, em uma organização, as informações são ativos de negócios importantes e essenciais para os negócios e, portanto, precisam ser devidamente protegidas. Isso é especialmente importante em um ambiente de negócios cada vez mais interconectado, no qual as informações agora estão expostas a um número crescente e a uma variedade maior de

ameaças e vulnerabilidades. Causar danos, como código malicioso, hacking de computador e ataques de negação de serviço, tornaram-se mais comuns, mais ambiciosos e mais sofisticados (MORAES, 2011).

Por fim, Oliveira (2013) compreende que em termos de proteção da funcionalidade de uma organização, tanto o gerenciamento geral quanto o gerenciamento de TI são responsáveis por implementar a segurança da informação que protege a capacidade de funcionamento da organização.

## 4.3 Sistemas de proteção do Poder Judiciário

Antes da entrada em vigor da LGPD, que contém disposições específicas sobre o assunto, à luz das regras de responsabilidade e dos padrões de boa-fé, os processadores de dados no Brasil são obrigados a tomar medidas técnicas, físicas e organizacionais razoáveis para proteger a segurança dos dados pessoais.

O Marco Civil da Internet também estabelece disposições relativas à segurança de dados pessoais. Exige que as medidas e procedimentos de segurança e confidencialidade no armazenamento e tratamento de dados pessoais sejam informados de forma clara pelo responsável pela prestação dos serviços.

A jurisprudência estabeleceu a obrigação dos provedores de serviços e redes de estabelecer e manter registros de acesso (como endereços IP e logins) para identificar usuários que possam cometer crimes ou atos de infração. Se esses registros não forem mantidos por um período de tempo razoável, o provedor de serviços ou a rede podem ser considerados conjuntamente responsáveis por um ato de infração. Os padrões de segurança de dados devem ser repassados ao internauta e obedecer aos padrões (ainda a serem definidos em regulamento) que serão produzidos pelo Governo Federal.

Em julho de 2016, devido a falhas de segurança, foi publicado um banco de dados do Município de São Paulo expondo dados pessoais de cerca de 650 mil pacientes e agentes públicos do sistema público de saúde (SUS). Os dados incluem endereço, número de telefone e até informações médicas. Detalhes

das fases da gravidez e casos de aborto também foram expostos. As planilhas foram rapidamente retiradas do site do município e uma investigação foi aberta para investigar quem era o responsável. De acordo com uma regulamentação do Ministério da Saúde, os pacientes do SUS têm direito ao sigilo de seus prontuários, mesmo após o óbito. Dentre as possíveis consequências, os indivíduos cujos nomes constam da lista exposta também podem sofrer práticas de diferenciação de preços em operadoras de planos de saúde ou se tornarem vítimas de roubo de identidade.

Bancos e instituições financeiras também puderam acessar informações de um banco de dados de trabalhadores que solicitaram aposentadoria. A violação foi apurada porque as empresas ofereciam crédito aos trabalhadores como aposentados, antes mesmo de serem notificados pelo Instituto Nacional do Seguro Social (INSS) sobre a homologação de seu pedido de aposentadoria. O Ministério Público Federal em São Paulo havia investigado a origem da infração e no final de setembro propôs uma ação contra o INSS e a Tifim Recuperadora de Crédito e Cobranças Ltda. O processo baseia-se nas proteções de privacidade da Constituição, Código Civil e Legislação do Consumidor.

Em 2017 foi promulgada a Lei 13.444 / 2017 . A lei estabeleceu a Identificação Civil Nacional (ICN). O ICN pretende construir um RG nacional que lucrará com o banco de dados biométrico atualmente em poder do Tribunal Superior Eleitoral (TSE) que, no Brasil, também é o órgão executivo responsável pela organização das eleições.

Votação é obrigatória para cidadãos alfabetizados maiores de 18 anos e menores de 70, e opcional para cidadãos entre 16 e 18 anos e maiores de 70 anos. Os cidadãos cujo voto é obrigatório e que não o cumpra ficam impedidos de requerer passaporte, contrair empréstimos junto de instituições financeiras e assumir cargos públicos (ou, se já exercerem funções públicas, de receber o seu vencimento).

O Código Eleitoral de 1932 torna o voto uma exigência legal. Atualmente, o registro eleitoral também é regulamentado pelo Código Eleitoral de 1965 e pela Lei nº 6.236/1975. Além disso, a votação também é eletrônica, cujos aspectos são regulamentados pela Lei nº 6.996/1982 e Lei nº 7.444/1985, além de diversas resoluções do Tribunal Superior Eleitoral. De acordo com o

TSE (2021), em setembro de 2014, havia uma estimativa de 142.822.046 eleitores registrados no Brasil.

Nos termos dos artigos 42 e 58 do Regulamento 477/07 da Anatel , os usuários devem fornecer um conjunto mínimo de dados pessoais para poder assinar um serviço de telefonia móvel. Essas informações incluem nome, número da carteira de identidade e número de contribuinte. Existe regulamentação específica para estrangeiros que desejam adquirir um cartão SIM brasileiro - é necessário apresentar o passaporte.

Legalmente estruturado pela Constituição de 1988, o Ministério Público (Ministério Público) abriga promotores públicos independentes nos níveis federal e estadual. Os Ministérios têm funções específicas no Brasil para defender a justiça e levar casos em todos os níveis do sistema judiciário brasileiro, como perante o Supremo Tribunal Federal e os tribunais estaduais de apelação. Os promotores públicos operam independentemente dos três principais poderes do governo e ajudam a proteger os direitos constitucionais, iniciando ações civis para julgar questões que envolvem direitos coletivos. Atualmente, existem 31 representações Ministérios Públicos em todo o Brasil.

Todos os procuradores dos Ministérios Públicos podem iniciar uma ação civil ou procedimento se acreditar que há fundamento na lei. Essa flexibilidade relativa apresenta amplas implicações para a proteção de dados, uma vez que um promotor público pode agir sob a LGPD fora da Autoridade Nacional de Proteção de Dados (ANPD), o que poderia levar a uma forma brasileira única de fazer cumprir e esclarecer a lei. Por um lado, a insegurança jurídica pode surgir de uma profusão de iniciativas individuais do Ministério Público. Por outro lado, o papel dos Ministérios Públicos é fundamental, pois pode servir de freio a qualquer ação do NDPA que seja contrária ao interesse público do consumidor.

Além dos Ministérios Públicos, a jurisprudência recente no Brasil também ilumina alguns desafios regulatórios únicos que enfrentam a implementação da LGPD. Esta jurisprudência ilustra como a proteção de dados era uma questão fundamental no sistema judicial antes da promulgação da recente lei, em particular na área da proteção do consumidor. Algumas das decisões mais importantes esclareceram muitas questões para a proteção de

dados, como os direitos dos titulares dos dados, o escopo da vigilância e a aplicação de princípios essenciais de processamento, como a limitação da finalidade. Como tal, compreender as implicações desta jurisprudência é fundamental para compreender como os reguladores irão implementar o LGPD.

O Supremo Tribunal Federal, que atua como a mais alta corte do Brasil, recentemente emitiu uma decisão relacionada à Covid-19. Neste caso (ADI 6387), uma disposição legal exigia o compartilhamento de dados pessoais para fins estatísticos como uma medida de emergência em resposta à pandemia. Muitas organizações em todo o Brasil contestaram esta medida provisória, argumentando que ela não atendia aos padrões de limitação de finalidade, transparência e segurança da informação, e que era excessivamente ampla. O Tribunal concordou, defendendo uma barreira mais elevada para a limitação da finalidade e muitos aspectos-chave da LGPD, bem como esclarecendo algumas questões constitucionais em torno da proteção de dados.

Embora a decisão não tenha neutralizado todos os riscos para a proteção de dados no Brasil, ela estabeleceu precedentes para tribunais de primeira instância e enviou uma mensagem clara ao reconhecer a proteção de dados como um direito fundamental autônomo. Ao decidir assim, o Tribunal reconheceu que outras proteções constitucionais de indivíduos, como privacidade e devido processo legal, se estendiam explicitamente ao mundo online e à proteção de dados pessoais. Também esclareceu que, ao contrário dos argumentos do Procurador-Geral da República e do Procurador-Geral da República, não existem dados irrelevantes nos dias de hoje, e mesmo dados pessoais que podem parecer triviais, como nomes de pessoas, números de telefone e endereços, merecem proteção constitucional contra abusos. A decisão teve, nomeadamente, influência da Carta Europeia dos Direitos Fundamentais.

Outro caso recente discutiu as implicações do consentimento para a indústria de creditscoring no Brasil. Embora a obtenção de consentimento não seja obrigatória para empresas que atuam em creditscoring, o Superior Tribunal de Justiça, a mais alta corte de apelação na jurisdição brasileira, considerou que tais empresas devem seguir os padrões de proteção de dados

no processo de creditscoring. O Tribunal discutiu cinco princípios gerais que as entidades devem seguir no futuro.

Além disso, os tribunais também esclareceram de forma independente o direito de ser esquecido. No Google Brasil Internet Ltda em 2018, um tribunal de primeira instância no Brasil determinou que os mecanismos de pesquisa deveriam defender o direito dos indivíduos de serem esquecidos na indexação dos resultados da pesquisa. Embora o Superior Tribunal de Justiça ainda possa decidir o alcance desse direito no âmbito da LGPD, este caso ilustra que a questão já recebeu atenção de pelo menos um tribunal importante do país e pode ter influência para decisões judiciais em andamento.

Por fim, dois casos adicionais também esclarecem como a jurisprudência recente influenciou a proteção de dados no Brasil. Um caso considerou ilegais os contratos que impedem os consumidores de opinar sobre o escopo da divulgação de dados (Processo “José Galvão Silva vsProcob SA”, Recurso Especial 1.758.799, Estado de Minas Gerais, decidido pelo Tribunal Superior da Justiça em novembro de 2019). Outro mandou o governo de São Paulo remover câmeras dos metrôs, constatando que essa instalação generalizada de equipamentos de vigilância.

O Sistema Nacional de Defesa do Consumidor (SNDC) também levanta complexidades para a implementação da LGPD no Brasil. Estabelecido com o Código Brasileiro de Defesa do Consumidor em 1990 e regulamentado pelo Decreto Presidencial nº 2.181 / 1997, o SNDC reúne órgãos federais, estaduais e municipais, bem como organizações da sociedade civil, para prevenir, investigar e processar violações à lei de defesa do consumidor. Como amplo arcabouço institucional de defesa do consumidor, o SNDC possui mais de 30 anos de atuação e abrange 798 unidades espalhadas por 591 cidades brasileiras.

As Procuradoria de Proteção e Defesa do Consumidor (PROCONS) atuam no Sistema Nacional para auxiliar os consumidores a protocolar queixas administrativamente, fornecer instruções e informações sobre os direitos do consumidor e verificar julgamentos. Os Procons emitiram algumas decisões relacionadas à proteção de dados ao longo dos anos que chamaram a atenção.

Por exemplo, uma decisão em 2019 do Procon de São Paulo resultou em uma grande multa para Google e Apple por impor cláusulas abusivas pelo uso do FaceApp sem disponibilizar tais cláusulas em português. Outra, em 2020, viu o Procon-SP chegar a um acordo com a distribuidora de energia Enel sobre reclamações de consumidores sobre aumento e cobrança incorreta. No acordo, o Procon estipulou que a Enel deve demonstrar a segurança e as medidas técnicas que tomará para garantir que o problema não se repita.

# 5 CONCLUSÃO

A partir do desenvolvimento do objeto dessa pesquisa, foi possível perceber que A privacidade de dados sempre foi importante. Porém, à medida que mais dados são digitalizados e compartilhamos mais informações online, a privacidade dos dados assume maior importância.

A proteção de dados deve ser uma prioridade para qualquer empresa. Isso inclui proteger a disponibilidade dos dados para os funcionários que deles precisam, a integridade dos dados (mantê-los corretos e atualizados) e a confidencialidade dos dados (a garantia de que estão disponíveis apenas para pessoas autorizadas).

Dessa forma, o uso dos dados indevidos pode ser direcionado para publicidade de produtos e serviços em que se pensou, empurrando-o lentamente e induzindo-o a uma compra. Mais perigoso é que esse perfil também pode ser usado para fins políticos. A história ensinou que o conhecimento detalhado da origem étnica e das crenças políticas ou religiosas das pessoas pode, nas mãos erradas, literalmente representar uma ameaça à vida

O vazamento de dados pessoais pode causar danos significativos à reputação das empresas e também penalidades, por isso é importante cumprir os regulamentos de proteção de dados pessoais. As organizações que não implementam proteções de privacidade e, subsequentemente, sofrem violações, perderão a confiança, o que, por sua vez, resultará em lucros menores e menos clientes.

Assim, verificou-se que aLGPD é uma lei fundamental no Brasil. O seu não cumprimento pode ter consequências graves. A violação da lei de proteção de dados pode fazer com que você e sua empresa sejam processados, resultando em punições severas. Isso pode incluir multas de ou medidas sancionatórias.

Ademais, percebeu-se que A segurança informática abrange os objetos que os funcionários e convidados realmente interagem fisicamente e as próprias pessoas. A ideia de focar na segurança do local é diminuir a probabilidade de danos a pessoas, propriedades e informações. Embora a segurança da sua rede proteja os dados de serem acessados remotamente, os

dados têm a mesma probabilidade de serem comprometidos de forma informática.

Assim, a informação é o elemento mais importante da organização para fazer negócios. Além disso, uma organização mantém dados de seus clientes, por isso é fundamental para eles protegerem as informações. Ao proteger o armazenamento de informações; pode permitir que a organização administre negócios também.

Para que a cibercultura produza esse efeito específico, ocorreu uma mutação no comportamento social que possibilitou uma alteração na subjetividade humana. Atualmente, vive-se a fase transumano, pós-humano, superinteligência, híbridos e singularidades que se tornam recorrentes em discussões que põem em pauta a relação dos seres humanos e não humanos, entre seres e tecnologias.

A segurança da informação é muito importante em uma organização para proteger os aplicativos implementados nas organizações e proteger o armazenamento de dados no computador. Além de proteger os dados, o aplicativo instalado também precisa ser protegido, pois pode contribuir para perda ou danos às informações.

## REFERÊNCIAS


ARAÚJO, M. B. **Comércio eletrônico; marco civil da internet; direito digital.** Rio de Janeiro: Confederação Nacional do Comércio de Bens, Serviços e Turismo, 2017

BRANCO, P. G. G.; MENDES, G. F. **Curso de direito constitucional**, 12º ed. São Paulo: Saraiva,2017.

BRASIL. [Constituição (1988)]. Constituição Federal da República Brasileira de 1988. *In*: **VADE**Mecum. São Paulo: Saraiva: 2021.

BRASIL. Lei nº 8.069, de 13 de julho de 1990. Dispõe sobre o estatuto da criança e do adolescente e dá outras providências. *In*: **VADE**Mecum. São Paulo Saraiva, 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.*In*: **VADE**Mecum. São Paulo: Saraiva: 2021.

BRASIL. Lei Geral de Proteção de Dados Pessoais**.**Lei **nº 13.709, de 14 de agosto de 2018.***In*: **VADE**Mecum. São Paulo: Saraiva, 2021.

BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.**Diário Oficial da União,** Brasília, 27 de dezembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm. Acesso em: 21 mai., 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.*In*: **VADE**Mecum. São Paulo: Saraiva: 2021.

BULOS, U. L. **Constituição federal anotada.** 18. ed. São Paulo: Saraiva, 2020.

CASTELLS, M. **A sociedade em rede.** São Paulo: Paz e Terra, 1999.

CASTELLS, M.; CARDOSO, G. (Org.). **A sociedade em rede:** do conhecimento a acção política. Lisboa: Imprensa Nacional: Casa da Moeda, 2006.

CERVO Amado Luiz; BERVIAN Pedro Alcino. **Metodologia científica**. 5. ed. São Paulo: Prentice Hall, 2002.

DINIZ, M. H. **Curso de direito civil brasileiro.** 20. ed. São Paulo: Saraiva, 2020.

CONVENÇÃO AMERICANA DE DIREITOS HUMANOS. **Pacto de San Jose da Costa Rica.** Assembleia de 1969. Disponível em:http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm
Acesso em: 21 mai. 2021.

CHRISTENSEN, C. **Ideias e ações** Disponível em: https://claytonchristensen.com/ideas-in-action/. Acesso em: 07 mar. 2021

GIL, Antônio C. **Métodos e técnicas de pesquisa social.** 6. ed. São Paulo: Editora Atlas, 2017.

leitlima
GUERRA, S. C. S. **O direito à privacidade na internet:** uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2014.

HANS, B. C. **No exame**: reflexões sobre a era digital. São Paulo: Antropos, 2013.

FISS, Owen M. **A Ironia da liberdade de expressão:** Estado, regulação e diversidade na esfera pública. Rio de Janeiro: Renovar, 2005.

LEITE, F. P. A. O exercício da liberdade de expressão nas redes sociais: e o marco civil da internet. **Revista de Direito Brasileira**, São Paulo, SP, n. 6, v. 13 , n. 6, p. 150 - 166 , jan./abr. 2016.

LEITÃO, B. J. M. Bi**bliotecas públicas, bibliotecários e censura na Era Vargas e regime militar:** uma reflexão. Rio de Janeiro: Intertexto; Interciência, 2011.

LIMA, G. D. **Manual de direito digital:** fundamentos, legislação e jurisprudência. Curitiba: Appris, 2016.

LIMA, **H. C. S. (Coord.). Direito, tecnologia e inovação.** São Paulo: D'Plácido, 2018.

NADER, P. **Introdução ao estudo do direito.** 34 ed. Rio de Janeiro: Forense, 2012.

OLIVIEIRA, L. **A importância histórico-social das redes.** Rio de Janeiro: Terceiro Setor, 2003.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS EM PARIS. **Declaração universal dos direitos humanos de 1948.** Disponível em:
http://www.onu.org.br/img/2014/09/DUDH.pdf. Acesso em: 21 mar. 2021

REALE, M. **Lições preliminares do Direito,** 27 ed. São Paulo, Saraiva, 2002.

REIMÃO, S. **Repressão e resistência:** censura a livros na ditadura militar. São Paulo: Fapesp, 2011.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2018. E-book.

SILVEIRA, C. M. **Regulação da mídia e liberdade de expressão:** análise da experiência alemã. Rio de Janeiro: EdPUC, 2016.

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

STALLING, W. BROWN, L. **Segurança de computadores**. 2. ed. São Paulo: Pearson Education do Brasil, 2014.

VILLAS-BÔAS, Maria Elisa. O direito-dever de sigilo na proteção ao paciente. **Revista Biomédica,**
**L** São Paulo, n 23, a. 3, p. 13-23, 2015. Disponível em: https://www.scielo.br/pdf/bioet/v23n3/1983-8034-bioet-23-3-0513.pdf. Acesso em: 21 mai. 2021.

BORBA, J. E. T. **Direito societário.** 12. ed. Rio de Janeiro: Renovar, 2010.

BRANCO, P. G. G.; MENDES, G. F. **Curso de direito constitucional**, 12º ed. São Paulo: Saraiva,2017.

BRASIL. CONSELHO NACIONAL DE JUSTIÇA. **Enunciado 531.** Disponível em: https://www.cjf.jus.br/ enunciados/ enunciado/142. Acesso em: 10 set.. 2021.

BRASIL. [Constituição (1988)]. Constituição Federal da República Brasileira de 1988. *In*: **VADE**Mecum. São Paulo: Saraiva: 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.*In*: **VADE** Mecum. São Paulo: Saraiva: 2021.

BRASIL. Lei Geral de Proteção de Dados Pessoais**.**Lei **nº 13.709, de 14 de agosto de 2018.***In*: **VADE** Mecum. São Paulo: Saraiva, 2021.

BRASIL. Lei nº 13.787, de 27 de dezembro de 2018. Dispõe sobre a digitalização e a utilização de sistemas informatizados para a guarda, o armazenamento e o manuseio de prontuário de paciente.**Diário Oficial da União,** Brasília, 27 de dezembro de 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13787.htm.
Acesso em: 09 mai., 2021.

BRASIL. Lei nº 10.406, de 10 de janeiro de 2002. Institui o Código Civil.*In*: **VADE** Mecum. São Paulo: Saraiva: 2021.

CASTELLS, M. **A sociedade em rede.** São Paulo: Paz e Terra, 1999.

CASTELLS, M.; CARDOSO, G. (Org.). **A sociedade em rede:** do conhecimento a acção política. Lisboa: Imprensa Nacional: Casa da Moeda, 2006.

CONSALTER, Zilda Mara. **Direito ao esquecimento**. Curitiba: Juruá Editora, 2016.

CONVENÇÃO AMERICANA DE DIREITOS HUMANOS. **Pacto de San Jose da Costa Rica.** Assembleia de 1969. Disponível em:http://www.pge.sp.gov.br/centrodeestudos/bibliotecavirtual/instrumentos/sanjose.htm
Acesso em: 10 set. 2021.

DINIZ, M. H. **Curso de direito civil brasileiro.** 20. ed. São Paulo: Saraiva, 2020.

GONÇALVES, Carlos Roberto. **Direito Civil brasileiro:** responsabilidade civil. 5 ed. São Paulo: Saraiva, 2010.

GUERRA, S. C. S. **O direito à privacidade na internet:** uma discussão da esfera privada no mundo globalizado. Rio de Janeiro: América Jurídica, 2014.

HANS, B. C. **No exame**: reflexões sobre a era digital. São Paulo: Antropos, 2013.

FISS, Owen M. **A Ironia da liberdade de expressão:** Estado, regulação e diversidade na esfera pública. Rio de Janeiro: Renovar, 2005.

LEITE, F. P. A. O exercício da liberdade de expressão nas redes sociais: e o marco civil da internet. **Revista de Direito Brasileira**, São Paulo, SP, n. 6, v. 13 , n. 6, p. 150 - 166 , jan./abr. 2016.

LEITÃO, B. J. M. Bi**bliotecas públicas, bibliotecários e censura na Era Vargas e regime militar:** uma reflexão. Rio de Janeiro: Intertexto; Interciência, 2011.

LIMA, G. D. **Manual de direito digital:** fundamentos, legislação e jurisprudência. Curitiba: Appris, 2016.

MÈLO, Augusto. **Proteção de dados pessoais na era da informação**. Curitiba: Juruá Editora, 2019.

MORAES, Melina Ferracini de. **Direito ao esquecimento na internet**: das decisões judiciais no Brasil. Curitiba: Juruá Editora, 2018.

MORATO. Antônio Carlos; CICCO, Maria Cristina de. Direito ao esquecimento: luzes e sombras. *In*:SILVEIRA, Renato de Mello Jorge. (Org.). **Estudos em homenagem a IvetteSenise Ferreira**. São Paulo: LiberArs, 2015.

NETHER, Nicholas Augustus de Barcellos. **Proteção de dados dos usuários de aplicativos**. Curitiba: Juruá Editora, 2018.

OLIVIEIRA, L. **A importância histórico-social das redes.** Rio de Janeiro: Terceiro Setor, 2003.

ORGANIZAÇÃO DAS NAÇÕES UNIDAS. ASSEMBLEIA GERAL DAS NAÇÕES UNIDAS EM PARIS. **Declaração universal dos direitos humanos de 1948.** Disponível em: http://www.onu.org.br/img/2014/09/DUDH.pdf. Acesso em: 10 set. 2021.

REIMÃO, S. **Repressão e resistência:** censura a livros na ditadura militar. São Paulo: Fapesp, 2011.

RODOTÀ, Stefano. **A vida na sociedade de vigilância:** a privacidade hoje. Rio de Janeiro: Renovar, 2018. E-book.

SILVEIRA, C. M. **Regulação da mídia e liberdade de expressão:** análise da experiência alemã. Rio de Janeiro: EdPUC, 2016.

STALLINGS, W. **Criptografia e segurança de redes:** princípios e práticas. 6. ed. São Paulo: Pearson Education do Brasil, 2015.

STALLING, W. BROWN, L. **Segurança de computadores**. 2. ed. São Paulo: Pearson Education do Brasil, 2014.

SCHREIBER, Anderson**. Direito civil e constituição.** São Paulo: Atlas, 2013.

SCHREIBER, Anderson. **Direitos da personalidade**. 3. ed. São Paulo: Atlas, 2014.

VILLAS-BÔAS, Maria Elisa. O direito-dever de sigilo na proteção ao paciente. **Revista Biomédica,** São Paulo, n 23, a. 3, p. 13-23, 2015. Disponível em: https://www.scielo .Acesso em: 10 set. 2021.

BOLZANI, C. A. M. **Residências inteligentes.** São Paulo: Ed. LIVRARIA DA FISICA 2004.

BRASIL. Lei Geral de Proteção de Dados Pessoais**.**Lei **nº 13.709, de 14 de agosto de 2018.***In*: **VADE** Mecum. São Paulo: Saraiva, 2021.

BUZAN, B. New Pattern of Global Security. *In*: **Twenty-first century**. Ibadan: Affairs, Royal Institute of International Affairs, 1991.

CAPEL, V. **Home security:** alarms, sensors and systems. 2 ed. s. l. Newnes, 1997.

MONTEIRO, Silvana Drumond; VIGNOLI, RicheleGrenge; ALMEIDA, Carlos Cândido. Pós-humano como paradigma emergente na ciência da informação.

**Revista Informação, Estado e Sociedade,** João Pessoa, v. 30, n. 4, p. 1-28, out./dez. 2020.

MORAES, Paulo. **Mente Anti-hacker -** proteja-se! Rio de Janeiro: Brasport, 2011.

OLIVEIRA, Wilson. **Técnicas para hackers:** Soluções para Segurança. Portugal: Centro Atlântico, 2013.

SILVA, Antônio Everardo Nunes. **Segurança da informação.** Rio de Janeiro: Ciência Moderna, 2012.

WIENER, Norbert. **Cibernética**. São Paulo: Polígono 1970.