FACULDADE DE INHUMAS
CENTRO DE EDUCAÇÃO SUPERIOR DE INHUMAS

CURSO DE DIREITO

JOÃO PEDRO DE CASTRO VIEIRA

CIBERSEGURANÇA E LGPD: A APLICABILIDADE NO CASO “INVASÃO DO SUPERIOR TRIBUNAL DE JUSTIÇA”

INHUMAS-GO
2022

JOÃO PEDRO DE CASTRO VIEIRA

CIBERSEGURANÇA E LGPD: A APLICABILIDADE NO CASO “INVASÃO DO SUPERIOR TRIBUNAL DE JUSTIÇA”

Monografia apresentada ao Curso de Direito, da Faculdade de Inhumas (FACMAIS) como requisito para a obtenção do título de Bacharel em Direito.
Professor (a) orientador (a): Maressa Melo Santos

INHUMAS – GO
2022

Dados Internacionais de Catalogação na Publicação (CIP)

BIBLIOTECA FACMAIS

V658c

VIEIRA, João Pedro de Castro
CIBERSEGURANÇA E LGPD: A APLICABILIDADE NO CASO “INVASÃO DO SUPERIOR TRIBUNAL DE JUSTIÇA”/ João Pedro de Castro Vieira. – Inhumas: FacMais, 2022.
47 f.: il.

Orientador (a): Maressa de Melo Santos

Monografia (Graduação em Direito) - Centro de Educação Superior de Inhumas - FacMais, 2022.

Inclui bibliografia.

1.STJ; 2. Hacker; 3. Cibersegurança. I. Título.

CDU: 34

JOÃO PEDRO DE CASTRO VIEIRA

CIBERSEGURANÇA E LGPD: A APLICABILIDADE NO CASO “INVASÃO DO SUPERIOR TRIBUNAL DE JUSTIÇA”

AVALIAÇÃO DE DESEMPENHO DO(S) ALUNO(S)

Monografia apresentada ao Curso de Direito, da Faculdade de Inhumas (FACMAIS) como requisito para a obtenção do título de Bacharel em Direito.

Inhumas, 29 de novembro de 2022.

BANCA EXAMINADORA

_____

Prof .Maressa de Melo Santos – FacMais
(orientador(a) e presidente)

_____

Prof Wendell Pereira Gonzaga – FacMais
(Membro)

AGRADECIMENTOS

Agradeço primeiramente a Deus pela oportunidade de vivenciar toda essa jornada, agradecer a minha esposa e meus pais que me deram todo o suporte para vivenciar tais momentos sem que me deixasse abater ou pensasse em desistir. Aos professores que puderam fazer dessa jornada uma longa caminhada de conhecimento e aos colegas desses anos que acabaram por tornar tudo mais fácil com companheirismo e amizade.

O espírito humano precisa prevalecer sobre a tecnologia. - Albert Einstein

LISTA DE ABREVIATURAS E SIGLAS

STJ - Superior Tribunal de Justiça

CF - Constituição Federal

LGPD - Lei Geral de Proteção de Dados

ANPD - Autoridade Nacional de Proteção de Dados

CNPD - Conselho Nacional de Proteção de Dados

OCDE - Organização para a Cooperação e Desenvolvimento Economico

GDPR - Regulamento Geral sobre a Proteção de Dados

RESUMO

Em um mundo cada vez mais digitalizado e conectado, recursos que protejam os usuários em ambientes virtuais se tornam cada vez mais indispensáveis, dentro disso o conceito de cibersegurança se faz muito importante, visto que o mesmo constitui uma série de ferramentas e práticas que visam a proteção do usuário em ambiente virtual, porém mesmo com esses dispositivos de proteção acontecem com cada vez mais frequência crimes em ambientes virtuais, se fazendo necessário a existência de legislações que abarque tais problemas. Um caso famoso de crime cibernético que será abordado neste trabalho foi o ataque ao Superior Tribunal de Justiça, onde os servidores ficaram inoperantes por dias, sendo considerado o pior ataque cibernético a um órgão público. Dentro desse contexto de legislações se faz presente a Lei Geral de Proteção de Dados (LGPD) que visa estabelecer parâmetros para a segurança da captação, armazenamento e manuseio de dados dos usuários de quaisquer plataformas digitais. Assin sendo esse trabalho visa apresentar a aplicabilidade da LGPD no contexto do ataque cibernético sofrido pelo STJ.

Palavras-chave: STJ. Hacker. Cibersegurança.

ABSTRACT

In an increasingly digitized and connected world, resources that protect users in virtual environments become increasingly indispensable, within this the concept of cybersecurity becomes very important, since it constitutes a series of tools and practices that aim to user protection in a virtual environment, but even with these protection devices, crimes in virtual environments are happening with increasing frequency, making it necessary to have legislation that covers such problems. A famous case of cyber crime that will be addressed in this work was the attack on the Superior Court of Justice, where the servers were inoperative for days, being considered the worst cyber attack on a public body. Within this context of legislation, the General Data Protection Law (LGPD) is present, which aims to establish parameters for the security of capturing, storing and handling data from users of any digital platforms. Thus, this work aims to present the applicability of the LGPD in the context of the cyber attack suffered by the STJ.

Keywords: Hacker,. STJ,. Cybersecurity.

SUMÁRIO

INTRODUÇÃO

Diante da insegurança causada por diversos casos de vazamentos de dados e procurando se manter alinhado com as políticas internacionais de proteção e tratamento de dados, tais como o Regulamento Geral sobre a Proteção de Dados Europeia, o Brasil se viu em um ambiente onde deveria criar uma lei que regulamenta como é feito o tratamento de dados em nosso país. Assim seguindo o modelo europeu da GDPR foi criada a LGPD, publicada em 14 de agosto de 2018, mas que entrou em vigência somente no dia 17 de setembro de 2020. A lei é composta de 64 artigos que visam regulamentar o tratamento de coleta de dados pessoais com o intuito principal de resguardar os direitos básicos de honra, privacidade e liberdade de cada cidadão:

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural (BRASIL, 2018).

Dentro da temática cibersegurança também pode-se acrescentar o termo segurança da informação, que foram mecanismos que surgiram com o advento da internet e sua modernização, proporcionado pelo o crescente número de usuários e dadas as altas taxas de transferências de arquivos e consequentemente dados, foram necessárias a criação de mecanismos que assegurem a integridade destes e de seu compartilhamento dentro da rede mundial de computadores:

> São características básicas da segurança da informação os atributos de confidencialidade, integridade e disponibilidade, fazendo com que esta segurança esteja restrita somente a sistemas computacionais, informações eletrônicas ou sistemas de armazenamento. (OLIVEIRA; 2012, s/p).

Dentro disso, a cibersegurança encontra alguns pilares sendo eles a capacidade proteger os computadores, garantir a integridade e segurança de dados e mecanismos para recuperação dos mesmos após algum incidente. Como dito por Louise Marie Hurel:

> Como ISO/IEC 27032:2012, o termo se refere à preservação da confidencialidade, integridade e disponibilidade de informações no ciberespaço, ou seja, aos princípios que norteiam as atividades de segurança (HUREL, 2020, p. 6).

A relação entre a Cibersegurança e a LGPD consiste no fato de que a lei traz inúmeros mecanismos quanto a prática de segurança em ambiente digital e prevê diversas medidas administrativas e técnicas que aprimoram a cibersegurança, podemos citar um desses mecanismos como sendo o artigo 46 que traz o seguinte texto:

> Art. 46. Os agentes de tratamento devem adotar medidas de segurança, técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito. (BRASIL, 2018).

Dentro deste conceito um caso se tornou bastante notório, quando no dia 03 de novembro de 2020 os sistemas do Superior Tribunal de Justiça foram invadidos causando a interrupção de diversos procedimentos do órgão público e gerando uma enorme tensão a respeito do possível vazamento de dados referentes aos processos em andamento da casa.

Diante disso tem se como problema de pesquisa a relação entre a cibersegurança e a Lei Geral de Proteção de Dados diante do caso concreto da invasão do Portal do Supremo Tribunal de Justiça, fato este que ocorreu no dia 03/11/2020.

1. A CONJUNTURA HISTÓRICA, ECONÔMICA E SOCIAL QUE ORIGINOU A LEI GERAL DE PROTEÇÃO DE DADOS

A atual conjuntura da sociedade remodelou e muito as relações humanas, muitas coisas migraram do meio físico para o digital de uma forma assustadoramente veloz, o que acabou por criar um gigantesco mercado de dados. Onde os mesmos se tornaram um valioso produto sendo incessantemente comercializados entre empresas visando diversos fins:

> Antes dessas inúmeras mudanças, as atividades e situações eram sempre concretizadas pessoalmente, hoje, porém, muitas migraram para a forma virtual, transformando a maneira como nos relacionamos. Nessa nova configuração social, onde a troca de informações e de dados é constante, estes começaram a ser o cerne de um sistema econômico virtual gigantesco. (TEIXEIRA; FARIA; SILVA; OLIVEIRA, 2021, p. 236).

As relações comerciais também foram drasticamente afetadas, onde o modelo econômico predatório e o consumismo assumiram papel principal nessa geração digital, o que de certa forma tornou as tecnologias criadas posteriormente a esse movimento cada vez mais invasivas.

> Hoje estamos diante de um modelo econômico que desconsidera totalmente os limites planetários, esta crescente busca por bens de consumo levou ao uso descontrolado de tecnologias cada vez mais invasivas, o que tem levado o planeta Terra a reagir a esta economia global com choques ambientais que temos presenciado recorrentemente. (AMAYA, 2017, p. 88).

Em uma análise fria podemos comparar essa digitalização e modernização a uma nova revolução industrial, porém essa de forma muito mais invasiva no que diz respeito a privacidade dos indivíduos, trazendo à tona diversas novas problemáticas.

> Se estamos em uma nova Revolução Industrial, muito mais ampla, dinâmica e que irá revolucionar a organização das cadeias globais de valor, este é o momento para decidirmos se faremos da era das acelerações uma oportunidade ou não, este é o momento, o ponto de inflexão. (AMAYA, 2017, p. 89).

Dentro deste cenário, se fez necessário a criação de mecanismos que viessem a garantir os direitos fundamentais dos cidadãos quanto a forma que seus dados são manipulados, comercializados, utilizados e afins:

> O espírito da lei foi proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, trazendo a premissa da boa-fé para todo o tipo de tratamento de dados pessoais, que passa a ter que cumprir uma série de princípios, de um lado, e de itens de controles técnicos para governança da segurança das

> informações, de outro lado, dentro do ciclo de vida do uso da informação que identifique ou possa identificar uma pessoa e esteja relacionada a ela, incluindo a categoria de dados sensíveis (PINHEIRO, 2018, p. 11).

Tais mecanismos são de suma importância pois são eles que vem a garantir que todos os direitos dos usuários do espaço cibernético serão protegidos de forma integral.

1.1 Cenário Internacional e Nacional

Fazendo uma análise onde se traz o olhar crítico do macro para o micro, no que diz respeito às tratativas quanto a legislação que zelem por assuntos relacionados a segurança de dados em âmbito internacional, as mesmas começaram a ser tratadas de forma mais concisa a partir do crescimento desenfreado do ambiente virtual, e a expansão da internet e da rede mundial de computadores.

> O motivo que inspirou o surgimento de regulamentações de proteção de dados pessoais de forma mais consistente e consolidada a partir dos anos 1990 está diretamente relacionado ao próprio desenvolvimento do modelo de negócios da economia digital, que passou a ter uma dependência muito maior dos fluxos internacionais de bases de dados (PINHEIRO, 2018, p. 13).

Desde então o assunto é pauta frequente, sendo assinado em 2016 o General Data Protection Regulation, ou apenas GDPR, que consiste no cuidado com a pessoa física no que diz respeito à proteção de dados:

> A liderança do debate sobre o tema surgiu na União Europeia (UE), em especial com o partido The Greens, e se consolidou na promulgação do Regulamento Geral de Proteção de Dados Pessoais Europeu n. 679, aprovado em 27 de abril de 2016 (GDPR), com o objetivo de abordar a proteção das pessoas físicas no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, conhecido pela expressão “free data flow”. O Regulamento trouxe a previsão de dois anos de prazo de adequação, até 25 de maio de 2018, quando se iniciou a aplicação das penalidades(PINHEIRO, 2018, p. 13).

A legislação criada na Europa fez com que o Brasil, que possui desejo antigo de adentrar a Organização para a Cooperação e Desenvolvimento Econômico (OCDE), fez com promulgasse sua própria legislação a respeito da matéria de dados.

> Um dos fatores que levaram à promulgação da LGPD brasileira de forma tão veloz é sem dúvida essa motivação política, uma vez que possuir uma lei específica de proteção de dados pessoais é um dos requisitos para os membros da OCDE. (PANEK, 2019, p. 19).

Assim sendo fica explícito que o crescimento exponencial das interações em ambientes virtuais, foi o principal catalisador para a criação das legislações que versam a respeito da proteção de dados, e garantias de que o usuário estará seguro realizando qualquer tipo de ação em ambiente virtual.

1.2 Princípios, Fundamentos e Objetivos

A Lei Geral de Proteção de Dados elenca em seu segundo artigo todos aqueles que serão seus princípios norteadores, aqueles que trarão o ponto de ancoragem de todas as ações da mesma.

> Art. 2º 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;
> VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais. (BRASIL, 2020).

O primeiro fundamento elencado é o respeito à privacidade, direito esse garantido pela Constituição Federal de 1988 em seu artigo 5º, mais precisamente nos incisos X, XI e XII que primam pela inviolabilidade da honra, imagem e vida privada de todos os indivíduos sendo assim um dos direitos fundamentais. Tal garantia por parte da LGPD se dá pois a privacidade é diretamente atingida dentro das interações sociais que ocorrem no universo digital, sendo assim matéria que deva ser resguardada.

> Com o passar dos anos, com os avanços tecnológicos e a inserção de novas tecnologias, como câmeras fotográficas portáteis, por exemplo, e a crescente invasão da vida privada pelas mídias, viu-se a necessidade de se consagrar um direito à privacidade com uma abrangência maior, ou seja, não respaldando apenas os meios físicos, conforme na época da Constituição do Império, mas sim uma extensão, em que esses direitos fossem um direito geral do indivíduo. (SOARES, 2020, p. 9).

O segundo fundamento elencado foi a autodeterminação informativa que consiste basicamente no direito individual de cada cidadão de definir o que será feito com seus dados pessoais e para quem irá fornecê-los.

> Por sua vez, a terceira geração de normas de proteção dos dados pessoais alterou-se para absorver o princípio de liberdade, a fim de que o titular pudesse ter uma autodeterminação, referente à maneira a qual seus dados seriam coletados e tratados.(PANEK,2019,p. 19)

O próximo e terceiro pilar da lei que é trazido tende a liberdade de expressão, informação, comunicação e opinião outro princípio fundamental trazido na Constituição Federal de 1988

> Infere-se, do texto da Lei, que essas limitações buscam consigo, contribuir para um melhor equilíbrio entre a proteção da privacidade e da segurança pública, ou seja, há sempre a busca do equilíbrio, do que é benéfico para o indivíduo quanto aos seus dados pessoais, nunca ultrapassando, porém, a barreira de se tornar um perigo para o Estado e toda a sociedade. (SOARES, 2020, p. 22).

O quarto fundamento é a inviolabilidade da intimidade, da honra e da imagem, intimamente ligados ao que está disposto no primeiro fundamento básico da lei, pois é abordado no artigo 5º da constituição como sendo um direito fundamental

> Art. 5º 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, nos termos seguintes:
> X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação (BRASIL, 1988).

Assim sendo, vê-se que a Constituição defende o direito à inviolabilidade da vida íntima, honra e imagem das pessoas, o que se replica em ambiente virtual. Os dois próximos fundamentos trazidos pela lei incorrem em matéria semelhante, o primeiro trata da defesa ao desenvolvimento econômico, tecnológico e a inovação que consiste na defesa e no fomento dos mesmos no meio digital, porém respeitando tudo aquilo que é defendido pela LGPD, enquanto o sexto fundamento defende que a livre iniciativa, a livre concorrência e a defesa do consumidor.

> A LGPD visa um equilíbrio entre o direito à privacidade e o uso massivo das informações pessoais. Sua missão, portanto, não é outra, senão proteger direitos fundamentais, tais como a liberdade, a privacidade, o livre desenvolvimento e a personalidade.(SOARES, 2020, p. 27).

Por fim, o último fundamento defende os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais, como já foi visto em outros dos fundamentos da LGPD, a mesma versa em cima de matérias em suma constitucionais, trazendo pra si assuntos que são tidos como princípios fundamentais dentro da CF.

> Como fundamentos da LGPD podemos destacar o respeito à privacidade, liberdade de expressão, inviolabilidade da intimidade, livre iniciativa, defesa do consumidor, direitos humanos, dignidade e exercício da cidadania. Na prática, a LGPD se aplica aos governos e às empresas, tendo que garantir maior segurança aos dados pessoais, sempre observando a finalidade, adequação, necessidade, livre acesso, qualidade, transparência, segurança, prevenção, responsabilização e a prestação de contas de tudo que se refere aos dados pessoais, conforme bem explicado durante o presente trabalho.(SOARES, 2020, p. 27).

Além dos fundamentos podemos encontrar disposto dentro da Lei Geral de Proteção de Dados em seu artigo 6º todos os seus princípios, sendo estes aqueles que serão utilizados como norteadores para a execução do dispositivo.

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
> VII - 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, 2020).

Simplificando o entendimento em cima dos princípios elencados temos, finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, resposabilização e prestação de contas.

> O consentimento por parte do titular dos dados da mesma forma deve ser compreendido de tal maneira que sigam os princípios regidos no artigo mencionado acima. O uso de tais princípios na análise de dados têm por finalidade orientar quanto ao uso destes dados. (TEIXEIRA, 2020, p. 40).

Tais princípios trazem mais clareza nas relações que envolvam dados, fazendo com que o usuário do meio virtual e a pessoa em ambiente físico se resguarde do mau uso de suas informações pessoais em qualquer espécie de situação:

> O princípio da adequação contido no art.6º, inciso II, da LGPD, delibera que o trato de dados pessoais precisa ser coadunável com os devidos fins pré estabelecidos com o contratante, isto é, os dados obtidos pelo contratado necessariamente devem guardar referência com o objetivo definido com o cliente. (TEIXEIRA, 2020, p. 41).

Por fim temos os objetivos específicos da LGPD quais fins a mesma deseja alcançar, fins esses que se mostram explícitos em seus fundamentos e princípios onde podemos concluir que a mesma irá abarcar diversas áreas das ações humanas dentro do ambiente virtual.

1.3 Direito à privacidade e a proteção de dados

A privacidade consiste a grosso modo a tudo aquilo que está ligado à intimidade do ser, ao que lhe é secreto de certa forma, e a proteção jurídica a privacidade consiste em garantir a inviolabilidade da pessoa e de seus bens e pensamentos.

> A privacidade, o “direito de estar só” do direito americano, foi consolidado no Estado Moderno, estritamente vinculado ao indivíduo. Ao direito, importava

> proteger o domicílio do sujeito e a inviolabilidade de seus bens e propriedades. O conceito da privacidade e liberdade no século XX, por outro lado, adquire uma preocupação com a intimidade da vida privada, inspirado pelos direitos de personalidade constitucionais europeus.(PANEK, 2019, p. 14).

O Direito à privacidade e a proteção de dados pessoais, em especial aquela oferecida pela LGPD acabam por se entrelaçar a partir do momento que toma se de princípio que a referida lei visa a garantia do direito fundamental de privacidade estipulado na Constituição Federal em seu artigo 5º inciso X: “X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação”. (BRASIL, CF, 1988).

Com a franca expansão do universo digital, fazendo com que cada vez mais a coleta de dados seja realizada e esses dados sejam utilizados de forma indiscriminada a privacidade passou a ser matéria jurídica a ser analisada de forma mais cautelosa, visto que a mesma se coloca em posição delicada nesse universo digital com alta taxa de transferência de dados a todo momento, sendo assim dispositivos como a LGPD se mostram extremamente necessários para a regulação desse tipo de assunto.

> As bases de dados eletrônicas, nos últimos anos, tiveram uma enorme expansão, tanto na utilização pelos usuários como pelos fornecedores e desenvolvedores. A coleta de dados acontece a todo o momento, seja de forma online ou offline, e adquiriu capacidades quase infinitas de processamento e armazenamento. Não é à toa que, com esse cenário, surge uma preocupação com a privacidade do indivíduo, e o direito assume uma tarefa complicada devido à complexidade do tema e todas relações jurídicas advindas desse princípio. (PANEK, 2019, p. 8).

O que ocorre é que a velocidade com que as mudanças ocorrem na atual conjuntura da sociedade faz com que o Direito não seja ágil o suficiente para acompanhar todas essas alterações, fazendo com que se gere inúmeras inseguranças jurídicas.

> Dado a velocidade das criações tecnológicas e da disseminação desenfreada das informações, o direito não tem capacidade de acompanhar as mudanças, muitas vezes deixando lacunas na tutela da era digital e ignorando a profunda alteração no tecido social e econômico causado pela circulação de informações. (PANEK, 2019, p. 10).

Assim sendo a Lei Geral de Proteção de Dados visa a proteção da privacidade, e consequentemente dos usuários da internet, visto que a mesma atua fortemente neste âmbito sendo assim ela traz em seu primeiro artigo a garantia da defesa da privacidade:

> A LGPD, assim como a GDPR, visa garantir maior controle e proteção aos cidadãos sobre suas informações pessoais perante empresas que lidam com dados pessoais ou frente ao Poder Público, também detentor de numerosas informações presentes em bancos de dados sobre os cidadãos. (MOURA 2019, p. 62).

O projeto de lei ainda estabelece a criação da Autoridade Nacional de Proteção de Dados (ANPD) e do Conselho Nacional de Proteção de Dados Pessoais e da Privacidade, porém a parte do projeto que faria esta função foi vetada pelo presidente da República sob alegação de vício constitucional. No entanto posteriormente, no ano de 2018 foi editada a medida provisória nº 869/18, criando assim a ANPD sendo ele um órgão da administração federal associada à presidência da República.

1.4 Impactos Sociais da Lei

A Lei Geral de Proteção de Dados trouxe inúmeros impactos na sociedade e diretamente no trabalho de diversas categorias que têm por meio a captura e trativa de dados. Pois esses ambientes de trabalho por sua vez terão que respeitar e seguir tudo aquilo que a LGPD traz enquanto fundamentação base, seus princípios e fundamentos de uma forma geral.

> A LGPD tem por fundamentos principais a segurança e a privacidade e, além disso, ela também assegura a livre iniciativa e a liberdade de expressão do indivíduo de ceder ou não seus dados pessoais. Ademais se destaca também que o fator preponderante de tais fundamentos está no consentimento do titular dos dados, ele deve ser abordado de forma clara e correto, para autorizar, tendo, ainda, a liberdade de aceitar ou não, o uso de suas informações pessoais por parte de terceiros, sejam eles agentes físicos, públicos ou privados. (SILVA; JALES, 2022, p. 14).

Essas empresas lidam com um volume de dados imensurável, o que faz com que a LGPD impacte diretamente em tudo aquilo que elas produzem, visto que a lei regulamenta a forma como os dados são tratados e captados.

> Essas empresas lidam diariamente com milhões de dados pessoais de seus inúmeros clientes, por isso, não resta dúvida do quão impactadas serão pela LGPD. Arriscamos dizer que será necessária toda uma reestruturação na sua forma de organização interna ao cuidarem desses dados sensíveis, devendo ser passada toda nova ética aos seus colaboradores, a fim de evitar no futuro as possíveis sanções estabelecidas na nova legislação.(SILVA; JALES, 2022, p. 8).

Para elucidar melhor um modelo de negócio que foi severamente afetado pela LGPD, o que por consequência gera um impacto social considerável, temos o modelo de negócio dos Call Center. Um modelo de negócio que possui diversos empregados no brasil e que foi severamente afetado pela LGPD, pois teve que se adaptar em diversas partes de seu operacional para que se adequasse a lei foi o setor de Call Center. O setor de call center é responsável de certa forma por uma revolução na forma de se comunicar e de vender produtos e serviços ao cliente final.

> Os serviços de Call Center revolucionaram a comunicação, o atendimento e o comércio pelo mundo. Trazendo a velocidade das ligações telefônicas (e posteriormente ainda mais velocidade com o surgimento da internet), a modalidade afetou fortemente a indústria e o mercado de trabalho mundial. (SOUZA, OLIVEIRA JUNIOR, 2021, p. 7).

Assim sendo com a implantação da LGPD muita coisa mudou no que tange a forma do serviço de call center agir para com seu cliente. Pois anteriormente a falta de regulamentação de certa forma fazia com que as tratativas fossem feitas de maneira informal, algo que veio a ser padronizado com a chegada da Lei Geral de Proteção de Dados, que trouxe diversos padrões e regras para com a forma que as tratativas são executadas e os dados coletados.

> Isso se dá porque as empresas de Call Center, sejam de serviços receptivos ou ativos, trabalham com uma quantidade enorme de dados pessoais. Aqueles que já são clientes precisam cadastrar dados como nome completo, CPF, telefone e até endereço, para efeitos comerciais, como recebimento de novas ofertas, vantagens, etc., tanto para medidas de segurança, como confirmação de titularidade e garantias contratuais. (SOUZA, OLIVEIRA JUNIOR, 2021, p. 8).

Visto que a LGPD traz punições no que diz respeito ao mau uso e tratamento dos dados, isso fez com que as empresas de call center dessem suma importância para a forma como os dados são coletados e tratados e a forma cuja a qual tratavam seus clientes, visto que a mesma teria que ser o mais transparente possível, isso tudo visando a não punição dos órgãos reguladores.

1.5 Impactos da Lei no meio digital

Os impactos da implementação da Lei Geral de Proteção de Dados não foram sentidos somente no que diz respeito ao meio social e trabalhista físico. Os meios sociais e trabalhistas no que tange ao ambiente virtual da internet também foram extremamente afetados com essa nova normativa. O contexto no qual a LGPD entrou em vigor, fez com que a sua atividade causasse ainda mais impacto, pois o país passava pelo advento da pandemia, o que fez com que muitas atividades que antes eram exercidas de forma física passassem a ser virtuais.

> Ademais, cumpre ressaltar que quando a lei fora promulgada em 2018, o mundo já enfrentava grandes impactos tecnológicos no âmbito digital e fora dele, como por exemplo, compras onlines, envio de currículos via e-mail para locais que estão com oportunidades de empregos, as próprias empresas de Call Center que armazenam todos os dias milhões de dados pessoais, entre outras. Podemos dizer, contudo, que a pandemia da Covid -19 fez com que todo esse processo acelerasse ainda mais, pois ficamos completamente à mercê desses serviços, inclusive, tivemos que nos adaptar ao trabalho de forma remota e principalmente ao home office. (SOUZA; OLIVEIRA JUNIOR, 2021, p. 6).

Assim sendo, pode-se inferir que as mudanças que ocorreram afetaram e muito o ambiente virtual e mostra com a inserção da LGPD que o Direito está atento às mudanças que ocorrem na sociedade e como isso afeta os ambientes de convivência social e no que diz respeito aos negócios.

> Nesta perspectiva, faz-se notório que o direito está em constante adaptação aos fatos ocorridos em sociedade, como cita o doutrinador Miguel Reale em sua obra “A Teoria Tridimensional do Direito”, logo, se faz necessária uma evolução legislativa para acompanhar as demandas remanescentes de tais avanços. Por conseguinte, não poderia ser diferente quanto à regulação no armazenamento de dados. (SILVA E JALES, 2022, p. 10).

Neste panorama podemos ver o quão o Direito tenta se adequar aos novos panoramas da sociedade, e assim também impacta diretamente as relações, nesse ponto a LGPD se faz necessária é de suma importância pois o ambiente virtual se tornou uma extensão da vida de cada cidadão, pois nele se concentram compras, vendas, relacionamentos e tudo que de certa forma é realizado no meio físico.

> Inspirada na legislação europeia General Data Protection Regulation (GDPR) de 2018, a qual está sendo a principal marca para evolução no âmbito de regulamentações de proteção de dados pessoais ao redor do mundo, a Lei Geral de Proteção de Dados (LGPD) – Lei 13.709/2018 – foi criada para trazer maior segurança aos dados pessoais, durante a era da informação digital, onde a internet se tornou o principal meio em que as pessoas se relacionam, compram, vendem, estudam, ensinam, informam, etc. (SOUZA, OLIVEIRA JUNIOR, 2021, p. 3).

Dentro disso mostra-se que a implantação da LGPD fez ser alterada diversas tratativas no ambiente virtual pois o mesmo demonstra ser uma extensão do meio físico. Assim sendo o meio digital sofreu inúmeras alterações no que tange às relações interpessoais que envolvem captação de dados e armazenamento dos mesmos.

2. MUNDO DIGITAL: SURGE A CIBERSEGURANÇA

Além dos mecanismos jurídicos, se faz necessária a existência de dispositivos de segurança dentro do meio virtual, para que assim os usuários tenham a seguridade de que estão em um ambiente onde seus direitos não possam ser violados ou roubados. Nesse contexto surge a cibersegurança, mecanismo de defesa do usuário dentro do ambiente virtual.

> Atualmente, o avanço tecnológico e a quantidade de sistemas e redes conectadas à Internet estão crescendo vertiginosamente, além de sofrerem repentinas mudanças, entendidas por atualizações e/ou evoluções à tecnologia já existente. Com isso, aumenta-se a preocupação quanto a segurança desses sistemas "conectados"e requer-se mecanismos que possam normatizar proteções e mitigar vulnerabilidades. (TEIXEIRA, 2021, p. 41).

Nesse aspecto presume-se a importância da cibersegurança e seu papel indispensável para a manutenção das relações em ambiente virtual. Assim sendo o que se decorre nesse trabalho terá a missão de elucidar conceitos importantes a respeito desses mecanismos.

2.1 O que é cibersegurança

Não existe definição padrão para o termo cibersegurança que seja aceito, dentro disso temos diversas definições porém contendo o mesmo cerne, assim como definido por Jussara de Oliveira que cibersegurança é:

> Cibersegurança é o ramo do ciberespaço que visa proteger computadores e servidores, dispositivos móveis, sistemas eletrônicos, redes e dados, contra ataques maliciosos. Também é chamada de segurança da tecnologia da informação ou segurança de informações eletrônicas. (POLESEL, 2021, p. 11).

Em consonância com essa definição existe o conceito apresentado por Lauren Bernat que define a cibersegurança como:

> O termo “cibersegurança” tem sido utilizado para se referir a qualquer elemento associado aos perigos de se usar as tecnologias de informação e comunicação (TIC): desde roubos on-line até possíveis conflitos armados que ocorrem no “domínio cibernético”, espionagem, exércitos de trolls que desestabilizam eleições ou disseminam fake news e violações de dados que prejudicam a privacidade de indivíduos.(BERNAT, 2020, p. 14).

Ou seja, a cibersegurança é a encarregada por garantir através de seus elementos componentes a segurança dos usuários em ambiente virtual, para que estes não sofram nenhuma espécie de violação de seus direitos, em uma comparação simplista, podemos atrelar a cibersegurança à polícia em ambiente físico. Sendo assim ela se torna algo essencial à sociedade como um todo. Com o avanço da tecnologia a cibersegurança se tornou indispensável, visto que cada vez mais as relações humanas são feitas em ambientes virtuais, sendo assim, a existência de mecanismos de defesa para que haja boa convivência em tal ambiente se faz de extrema necessidade. A Agência Nacional de Telecomunicações define cibersegurança como sendo:

> A segurança cibernética são ações voltadas para a segurança de operações, de forma a garantir que os sistemas de informação sejam capazes de resistir a eventos no espaço cibernético que visam comprometer a disponibilidade, a integridade, a confidencialidade e a autenticidade dos dados armazenados, processados ou transmitidos e dos serviços que esses sistemas ofereçam ou tornem acessíveis. (ANATEL, 2021, s/p).

A partir do que é descrito pela ANATEL podemos entender que a cibersegurança ou segurança cibernética como é descrito pela mesma consiste basicamente em todo dispositivo e ação que tem por fim garantir a segurança daqueles que residem no espaço cibernético. Assim sendo faz se extremamente necessário para que a internet não se torne um perímetro desregrado e suscetível aos mais diversos tipos de golpes e crimes.

> Enquanto a segurança, a nível militar, sempre fora um tema de extrema relevância no cenário internacional, a nível virtual, enquanto cibersegurança, ganhou destaque após a globalização. A justificativa reside na necessidade de proteção dos dados confidenciais de órgãos governamentais, organizações e também de cidadãos comuns diante da ação dos hackers. (RIGAMONTE, 2017, p. 27).

Com o advento da globalização a integração via internet se tornou cada vez mais comum, fazendo com que ferramentas de proteção a todos os dados que trafegam na mesma seja de extrema importância para que sejam evitados diversos transtornos causados pelos hackers.

2.2 O papel da cibersegurança na sociedade

No início da internet, onde a mesma era utilizada meramente para comunicação e estava retida a uma classe mais abonada da sociedade, o quesito de cibersegurança não era uma preocupação de tamanha importância como é hoje. Contudo, com a evolução da sociedade e a inserção de atividades comerciais e consequentemente monetárias no meio virtual, a presença de elementos que possam suprimir condutas nocivas se tornou essencial para que se possa evitar um colapso virtual além de ondas e mais ondas de crimes.

> Por forma a permitir que os direitos, liberdades e garantias constitucionalizados sejam respeitados nas plataformas digitais, um número crescente de pessoas tem vindo a trabalhar no sentido de travar a expansão do nível de ameaças. Desta forma criou-se um conceito de segurança do ciberespaço, habitualmente conhecido por “cibersegurança”(TELES, 2015, p. 14).

Então vê se que a cibersegurança surgiu muito mais por um estado de necessidade, visto que hoje milhões de reais, dólares e euros, circulam pela rede mundial de computadores, necessitando assim de tais dispositivos. Nestes espaços assentam todas as redes de telecomunicações vitais, de transporte e de distribuição de energia das quais dependem o comércio global, a segurança energética e a prosperidade das sociedades modernas.

Como o caminho da sociedade humana tende a ser cada vez mais virtual e tecnológico, mais e mais se faz necessário a criação de mecanismos virtuais e proteção aos usuários, garantindo um ambiente seguro e estável sem comprometer a prosperidade humana.

> Tal cenário traz inúmeras transformações em todos setores da vida humana. O progresso tecnológico é evidente, agora é impossível processar, armazenar, recuperar e comunicar informação em qualquer formato, sem interferência de fatores como distância, tempo ou volume.(ROSA; SILVA; PALHARES, 2005, p. 3).

A rápida mudança das tecnologias faz com que grandes impactos sejam sentidos na sociedade, dada a velocidade cuja as quais as relações humanas são afetadas pela evolução de tais tecnologias, o que antes levava-se dias, hoje faz-se

em segundos, a comunicação, o formato de compra e venda e o jeito de se fazer toda espécie de negócio foi drasticamente afetado pelo advento da internet.

> É inegável que as tecnologias de informação exigem mais especialização e melhor capacitação do indivíduo, modificando sua forma de educação e, via de consequência, tanto sua habilitação para ingresso no mercado de trabalho como seu desempenho na realização do mesmo, propiciando-lhe assim, maior vantagem competitiva. (COSTA, 1995, p. 7).

Nesse contexto a cibersegurança em uma comparação pueril, tende para o ambiente virtual tão qual o policia tende ao meio social, pois esses mecanismos são construídos essencialmente para a proteção do indivíduo enquanto o mesmo utiliza a internet. Os ataques a dados de pessoas e instituições existem a muito tempo, por aqueles chamados de “hackers”.

> Os primeiros relatos de ataques cibernéticos realizados a partir de uma rede de computadores são da década de 80. Nesta década, Cliff Stoll realizou um dos primeiros casos de investigação de ataque cibernético que levou à prisão de Markus Hess em 1990. Serge Schmemann publicou uma matéria relatando um ataque hacker que resultou em vazamentos de dados da NASA e Brian Reid relatou ataques realizados a sistemas Unix na área de São Francisco comprometendo alvos conectados na ARPANET. (CILENTO, 2021, p. 12) .

Como elucidar os problemas com ataques a dados de instituições governamentais e pessoas não é um problema atual, porém com a expansão constante da internet ferramentas de contenção e proteção contra tais ataques se fazem de extrema importância para que seja mantida a seguridade em ambiente virtual.

2.3 O que são hackers?

É comumente associado a todo crime cometido em ambiente virtual a ação de um Hacker, mas afinal, o que são hackers e porque suas atitudes acabam por lesar diversas pessoas que muitas das vezes estão a quilômetros de distância do mesmo. Mas antes disso temos que apresentar aqui que existe um erro de consenso popular quanto às nomenclaturas, e que na verdade o Hacker pode não ser o vilão que descrevem, para isso, será utilizada a definição de Hacker dada por José Bosco da Mota Alves que assim diz:

> Hacker. possui profundos conhecimentos de programação e de sistemas operacionais, principalmente Unix e Linux. Tem conhecimento das falhas de

> segurança dos sistemas e está sempre em busca de novos desafios, mantendo-se fiel aos códigos éticos de sua comunidade (BACH, 2001, p. 4).

Como está na definição pode se ver que o Hacker não é a figura malévola e perversa que se prega, muito pelo contrário. Mas quem são os malfeitores do ambiente virtual, que causam danos e prejuízos milionários a empresas e governos. Esses são chamados de Cracker, como também definido por José Bosco da Mota Alves:

> Cracker: apesar de muitos possuírem conhecimentos similares aos hackers, os crackers têm intenções criminosas e rompem a segurança de um sistema em busca de informações confidenciais, com o objetivo de causar danos ou obter vantagem pessoal (BACH, 2001, p. 4).

Assim sendo, sabe-se que o Cracker é o real vilão cuja a qual a cibersegurança tenta a todo custo evitar suas ações, mas como cabe no consenso comum de que a palavra hacker é a que dá significado ao criminosos a mesma será mantida ao longo deste trabalho a fim de não complicar a compreensão do público alvo do mesmo e simplificar seu entendimento.

> A palavra hacker assusta a maioria das pessoas desinformadas, pois julgam um hacker como sendo aquele indivíduo que invade os computadores, apaga os arquivos, toma o controle da máquina e, ainda, envia mensagens à vítima. Este conceito que a maioria das pessoas tem a respeito dos hackers foi criado, possivelmente, pela publicidade negativa gerada pelos filmes que tratam do assunto, como por exemplo; “Jogos de Guerra”, e com o mais recente: “A rede e os Hacker”. A partir destes filmes e das notícias que a mídia difunde, cria-se a muitas pessoas uma confusão de sentimentos antagônicos, como a aversão e, ao mesmo tempo, a admiração aos piratas cibernéticos.(BACH, 2001, p. 19).

Vê se que erroneamente foi se difundindo ao longo do tempo a falácia de que os hackers são os criminosos cibernéticos, quando na verdade essa atribuição é de detenção do Cracker. É um fato que crackers e hackers possuem uma enorme fonte de conhecimento a respeito de informática e tecnologia da informação, mas a sutil diferença entre um e outro é que o hacker utiliza seus conhecimentos de forma ética e moral a fim de fortalecer e ajudar a comunidade de profissionais que ali estão, tentando construir uma rede mais segura e instável para os usuários.

> Os hackers direcionam seu potencial para construir, não destróem ou roubam dados de forma intencional, compartilham informações deixando

> rastros de passagem abertas para que administradores de rede possam fazer correções; eles têm como objetivo aprender mais, pois são autodidatas e gostam de desafios (BACH, 2001, p. 5)

Por outro lado o cracker utiliza de seus conhecimentos para destruir, invadir e cometer crimes em ambientes virtuais, o mesmo não tem interesse em construir ou beneficiar qualquer que seja a comunidade, pensando somente na vantagem que obterá com suas ações, com isso é capaz de roubar dados, violar a privacidade de terceiros, chantagem, pedidos de resgate de dados importantes, seja isso feito com personagens civis ou grandes empresas, existem diversos relatos de empresas que sofreram com o “sequestro” de seus dados.

> Alguns jovens, que não faziam parte do meio acadêmico e aprenderam a programar de forma autodidata, utilizaram seus conhecimentos para invadir sistemas por diversão e, em casos extremos, roubar dados e dinheiro via computador. Um destes grupos, chamado The 414s, ganhou destaque no início dos anos 80 e a Cultura Hacker foi parar na mídia, ainda que retratada de forma equivocada. (SOUSA, 2013, p. 8)

Assim sendo nota-se que os hackers acabaram por levar a culpa de tudo aquilo que realmente é feito pelos crackers, por questões midiáticas os mesmos acabaram por carregar em seu nome a alcunha que não lhes pertence, e sim pertence a uma classe cuja a qual quase não se fala nos veículos de comunicação.

2.4 Crimes cibernéticos

Crimes são algo que estão inseridos na sociedade a milênios, então não é de se espantar que a medida que a sociedade avance e se modernize os crimes façam o mesmo, acompanhando tendências e fases:

> No limiar dessa evolução tecnológica é possível constatar que, atualmente, o Código Penal de 1940 tende a lidar com situações criminosas que vão além do plano físico. Hoje, o agente delituoso não necessita ir às ruas para cometer determinados ilícitos como furto, racismo, crimes contra à honra, dentre outros. (ROCHA, 2013, p. 1).

Há de se esclarecer que quanto a definição de crime cibernético, não existe um consenso sobre uma definição padrão, um problema que notamos nessa área digital é justamente a falta de consensos sobre as definições a serem utilizadas, seja no que diz respeito a cibersegurança, crimes cibernéticos e afins, mas utilizemos a definição dada por Matsuyama e Lima:

> De maneira objetiva, pode-se conceituar crimes cibernéticos como sendo condutas ilegais que se efetivam mediante a utilização de dispositivos informáticos, conectados ou não a rede mundial de computadores, bem como as ações criminosas contra equipamentos tecnológicos, sistemas de informação ou banco de dados (MATSUYAMA; LIMA, 2016, p. 2).

Sendo assim os crimes cibernéticos acabam por ser de uma forma resumida, condutas nocivas e ilegais praticadas mediante uso de equipamentos eletrônicos, dentro disso temos uma gama enorme de tais dispositivos, como desktops, notebooks, tablets, smartphones e até mesmo os novos smartwatches. Ou seja, em um mundo cada vez mais digitalizado, tudo pode ser utilizado de arma para o cometimento de ações delituosas.

> No início do milênio, o mundo digital, embora extremamente fascinante, era ainda enigmático e obscuro para o homem comum. Com a popularização e amplo uso da internet nas mais variadas atividades, ressurgiu também aquela familiar e genuína preocupação em relação à segurança das informações que eram compartilhadas online, não somente para os governos, mas a todos que faziam uso dela (ROCHA, 2017, p. 10).

Nesse contexto, nota-se a migração dos crimes que antes eram somente cometidos em ambiente físico para o ambiente virtual, visando o fato de que o ambiente virtual possui uma amplitude muito maior de alcance a possíveis vítimas.

Dentro disso a existência de dispositivos de regulação e defesa em ambiente virtual se tornam indispensáveis. Mas mesmo com o constante desenvolvimento da cibersegurança os crimes em ambiente virtual seguem causando enormes estragos e prejuízos a pessoas e empresas.

2.5 O Impacto dos crimes cibernéticos da atualidade

Os crimes cibernéticos conseguem impactar de forma considerável a sociedade, visto que os ambientes virtuais permitiram a propagação de crimes que antes eram tidos em focos isolados, exemplo a pedofilia, algo que antes era focal se tornou descentralizado e com distribuição em massa de material graças a internet, o mesmo pode se dizer do tráfico, da piratária que hoje é amplamente difundida e também ataques terroristas, visto que diversos ataques a escolas feitos por jovens tem suas partes de planejamento realizados em foruns online, mostrando que os crimes cibernéticos vem se tornando a mais nova mazela da sociedade.

> Todo o tipo de conduta delituosa é praticada online, desde pedofilia, prostituição, tráfico, pirataria, até sabotagem e terrorismo. A digitalização dos métodos de trabalho tem causado em muitos países, inclusive ao Brasil, transtornos provocados por uma nova onda de crimes cibernéticos. Só neste ano foram registrados inúmeros sequestro de informações de empresas e hospitais por todo mundo. (ROCHA, 2017, p. 10).

Essa nova modalidade de crimes vem trazendo inúmeros transtornos e prejuízos para pessoas e instituições, visto que pela não existência de barreiras físicas o criminoso pode realizar tais atos a quilômetros de distância da vítima, fazendo com que geograficamente seja muito difícil mapear tais criminosos. Além dos crimes que surgiram exclusivamente em ambiente virtual, houve a potencialização daqueles que são existentes em ambiente físico, fazendo com que o alcance desses também seja potencializado, tais como extorsões, sequestros, exploração sexual de menores e afins.

> A criminalidade informática não trouxe apenas como consequência o surgimento de novas condutas ilícitas, além daquelas já previstas no ordenamento jurídico brasileiro, praticadas com o auxílio do computador. Outras particularidades foram trazidas com o advento da internet, já que as novas condutas atingem aos mais variados bens e interesses da sociedade tais como a violação de bens jurídicos até então não atingidos com a prática de um crime.(RAMOS, 2017, p. 19).

Outro ponto a ser levado em consideração não é somente a alteração dos crimes já existentes ou criação de novas condutas criminosas, mas também a alteração do bem jurídico atingido por tais condutas, visto que as possibilidades trazidas para a internet de formas de lesar o usuário são diversas, desde bens físicos, dinheiro e afins até mesmo lesões a moral e imagem da pessoa a depender de que fato foi realizado contra ela.

> Não se trata apenas do surgimento de novas condutas ilícitas não tipificadas no ordenamento brasileiro, promovidas pelo desenvolvimento da internet, mas também de uma alteração dos bens jurídicos atingidos com a nova criminalidade. A criminalidade da informática passou a atingir também os bens jurídicos difusos em contrapartida aos bens jurídicos individuais atingidos pela criminalidade não informática.(RAMOS, 2017, p. 21).

Dentro desse contexto pode se ver que essa nova modalidade de crime trouxe consigo diversas inseguranças tanto aos usuários quanto jurídicas, o que faz com que os dispositivos legais de regulamentação e punição para tais crimes se façam de extrema importância.

2.6 Por que os dispositivos legais são tão importantes para o combate dos crimes cibernéticos?

A pandemia trouxe um aumento expressivo do fluxo de ações realizadas em ambientes virtuais, muitas empresas transferiram seus modos de operação para a internet o que ocasionou uma mudança massiva na forma de se trabalhar e viver. No mesmo ritmo os crimes cibernéticos também ganharam maior notoriedade, visto que o número de possíveis vítimas aumentou expressivamente, o que faz imprescindível a existência de dispositivos legais de caráter coercitivo e punitivo no que se refere a tais práticas delituosas.

> Na pandemia as pessoas precisaram acessar mais a internet para resolver as demandas e ficaram mais vulneráveis nesse período, os crimes virtuais afetaram tanto as pessoas naturais como as pessoas jurídicas, assim causando de tal maneira, prejuízos a imagem, quanto prejuízos financeiros. (FILGUEIRA; JUNIOR, 2021, p. 6).

Deste modo observa-se que a existência de dispositivos legais que protejam os usuários em tal ambiente é algo indispensável, Na Europa por exemplo, a preocupação com tal matéria é um tanto mais antiga, culminando na criação do GDPR (General Data Protection Regulation ou em tradução livre temos o nome como “Regulamento Geral de Proteção de Dados”), tal dispositivo teve influência direta para que o Brasil tivesse seu próprio regulamento a respeito da regulamentação da forma de coletar e tratar dados.

> Trata-se de lei que determina regras para o gerenciamento de informações as quais, de alguma forma, possam identificar dados de clientes, colaboradores, parceiros de negócio e fornecedores, sem que exista o consentimento prévio destes últimos para que seus dados sejam compartilhados com quem quer que seja. (SIVIERI, 2021, p. 16).

Tal normativa surgiu por lá em resposta à subsequentes eventos de vazamento de dados por parte de grandes empresas, o que comprometeu e expôs por diversas vezes a população a ter seus dados nas mãos de terceiros sem sua autorização. Sendo assim se fez necessário que tal norma fosse criada a fim de

forçar as empresas detentoras dos dados a investir em proteção e segurança dos mesmos.

> Como uma resposta direta da comunidade europeia em relação a preocupação quanto a privacidade dos dados de seus cidadãos (anterior ao caso Facebook®), resposta está acelerada pelos escândalos de vazamento de dados, notadamente protagonizados por empresas do continente americano, em 25 de maio de 2018, entra em vigor a GDPR (General Data Protection Regulation n. 679 ou “Regulamento Geral de Proteção de Dados”). (SIVIERI, 2021, p.16).

Dentro desse cenário internacional surge no Brasil a LGPD, impulsionado pelo amplo crescimento do mercado digital e o fato das novas gerações serem totalmente digitalizadas faz com que a movimentação em ambiente cibernético se torne cada vez maior. Sendo assim, é crescente, assim como na europa, a necessidade de proteção dos dados dos usuários nesse ambiente.

> No Brasil, não diferentemente do que se verifica em outros países, a preocupação com a privacidade dos dados dos seus cidadãos também veio, ao longo do tempo, tomando forma e importância. O crescer da economia digital e o apetite das novas gerações pelo uso das mídias sociais e interativas aceleraram as iniciativas governamentais para que a promulgação de uma lei que tornasse claras as regras para a utilização de dados pessoais. (SIVIERI, 2021, p.19).

Nesse contexto surge a Lei Geral de Proteção de Dados, mais um instrumento de regulamentação e proteção ao usuário, trazendo assim uma maior instabilidade e segurança para todos os usuários.

3. ANÁLISE DO CASO “INVASÃO HACKER AO STJ” E A RELAÇÃO ENTRE A LGPD E A CIBERSEGURANÇA

Como já discorrido anteriormente, a existência de meios e mecanismos que resguardem as pessoas em ambiente virtual se tornou algo indispensável, assim sendo esses mecanismos e meios de resguardo precisam dialogar entre si de forma a que um não invada o espaço de ação do outro e assim não tenhamos inseguranças criadas de forma desnecessárias. Neste contexto surge a LGPD em consonância com a cibersegurança.

> A internet transformou as relações sociais e econômicas estabelecidas pelos indivíduos, assim, houve a necessidade de evolução também por parte da legislação brasileira, para que esta possa abarcar as novas relações jurídicas derivadas deste novo campo (BARRETO, 2019, p. 31)

Sendo assim, veremos qual a relação entre cibersegurança e LGPD, além de entender a relação prática de ambas no caso de invasão dos servidores do Superior Tribunal De Justiça, no ano de 2020. Dentro disso é necessário analisar que existe todo um contexto histórico em torno da criação da Lei Geral de proteção de dados, algo que foi fortemente influenciado por uma cultura internacional que preza cada vez mais por uma política forte de proteção de dados em ambientes virtuais.

> No cenário europeu, a matéria sobre proteção de dados é mais desenvolvida, sendo que diversos países europeus produziram normas sobre a matéria já nos anos 70 e 80, com a principal atenção no princípio da dignidade humana. Temos também a consolidação europeia de outros princípios como pertinência, proporcionalidade, finalidade e necessidade, que vieram a ser efetivamente aplicados na elaboração da Lei Geral de Proteção de Dados brasileira. (PANEK, 2019, p.18)

Dentro desse contexto podemos ver que a Europa vem a bastante tempo se preocupando com a disponibilidade dos dados e da forma como eles são tratados, o que culminou na criação da RGPD, ou, Regulamento Geral Sobre a Proteção de Dados Europeia, regulamento que foi aprovado em 2016 e criou sobre todos os demais países uma certa pressão para que se criassem normativas que viessem a se preocupar com a manipulação e obtenção de dados.

> Quando o RGPD entrou em vigência, criou-se uma influência internacional para que outros países também passassem a normatizar o tema de proteção de dados. Somado a isso, e provavelmente o fator mais concreto, foram o surgimento de barreiras de países sem previsão legal do tema, nas

> negociações internacionais econômicas com a União Europeia. (PANEK, 2019, p.18)

Assim sendo, nota-se que houve uma pressão internacional muito grande para que os países iniciassem suas políticas de proteção e tratamento de dados, visando assim uma maior segurança no que tange ao assunto entre todos os países.

Entretanto a importância de dispositivos como a Lei Geral de proteção de dados se mostra de extrema importância quando ocorrem casos práticos onde sua aplicabilidade se faz necessária, demonstrando assim a sua eficácia perante as mazelas da vida cotidiana, desde o ataque a um perfil de uma rede social de um civil, até a invasão dos servidores do Supremo Tribunal de Justiça que foi o caso que será aprofundado neste trabalho.

3.1 Análise do caso “Invasão Hacker ao STJ”

Um dos objetivos principais deste estudo é associar a correlação entre o ataque sofrido pelo Superior Tribunal de Justiça e a Lei Geral de Proteção de Dados, utilizando-se das definições existentes na cibersegurança para tal. Mas para que a contextualização se torne mais simplista, é necessário trazer toda a situação que culminou neste estudo. Assim sendo, será apresentado os pormenores da forma como foi realizado o ataque ao STJ.

> A invasão detectada na rede de informática do Superior Tribunal de Justiça (STJ), considerada o “pior ataque cibernético realizado contra a rede de tecnologia da informação de uma instituição pública brasileira” (SOUZA, 2021, p.13)

Como apresentado o ataque é considerado o maior a redes de serviço público no Brasil, o que expôs diversas pessoas, visto que nos sistemas do STJ circulam milhares de dados pessoais por segundo, dentro de processos, arquivos e afins. Sendo assim, é possível notar a periculosidade que esse tipo de ataque representa, visto que pode atingir milhares e até milhões de pessoas de uma só vez.

> O Superior Tribunal de Justiça (STJ) detectou, no dia 3 de novembro de 2020, um ataque hacker durante o período da tarde, quando ocorriam sessões de julgamento. Verificou-se que um vírus estava circulando na rede de informática do tribunal e, como medida de precaução, os links para a rede mundial de computadores foram desconectados, o que implicou no cancelamento das sessões de julgamento e impossibilitou o funcionamento dos sistemas de informática e de telefonia da Corte (MARTINS, 2020, s/p)

Os danos causados pelo ataque foram notórios, durante determinado período não houve acesso aos dados disponíveis nos servidores do STJ, dados esses que por precaução já estavam alocados em um backup seguro, porém os danos não foram piores pois no servidores em questão existiam mecanismos e equipes especialistas em de cibersegurança que logo se prontificaram a repelir a ameaça vindoura, fazendo com que assim os danos não fossem ainda maiores e viessem a prejudicar ainda mais pessoas e o andamento dos processos da casa.

> Em paralelo, a equipe da STI do STJ, juntamente com empresas prestadores de serviços de tecnologia do tribunal, a exemplo da Microsoft, iniciou os procedimentos de recuperação dos ambientes dos sistemas de informática do Tribunal da Cidadania. As empresas designaram equipes especializadas para auxiliar o STJ na recuperação do ambiente tecnológico.(MARTINS, 2020, s/p)

A ação rápida das equipes evitou que mais dados fossem vazados, e que os estragos pudessem ser ainda maiores derivados desse ataque, após passado o ataque, as equipes responsáveis pela manutenção dos sistemas deram início ao balanço dos estragos e as manutenções necessárias para fazer com que tudo retornasse ao seu antigo estado. O primeiro passo foi o retorno dos serviços tidos como essenciais para o funcionamento da casa.

> O restabelecimento dos sistemas está sendo executado pela equipe da Secretaria de Tecnologia da Informação e Comunicação do tribunal e das empresas Microsoft e Atos Brasil, com o apoio do Comando de Defesa Cibernética do Exército brasileiro e o Serpro. Cabe salientar a magnitude do trabalho dessa equipe na última semana – foi necessária a criação de um novo ambiente para o carregamento dos dados – estes, integralmente preservados no backup – com os cuidados para blindar ao máximo a infraestrutura.(MARTINS, 2020, s/p)

A resposta em pouco tempo foi um dos fatores essenciais para que os estragos não fossem ainda maiores, assim como ter uma equipe especializada no assunto para fazer da forma correta as tratativas necessárias para a garantia do mínimo dano possível. No dia 14 de novembro de 2020 seguiam se as tratativas para reparos dos sistemas que ainda se encontravam inoperantes e correção de possíveis falhas nos sistemas que já estavam em produção, assim garantindo que o que havia voltado a funcionar não parasse e dando celeridade para o retorno das funcionalidades que se encontravam inoperantes desde o dia 3.

> Seguem sendo realizados ajustes pontuais em aplicações administrativas que ainda apresentam instabilidade, a exemplo do Acesso Remoto (RDS), sistema disponível aos usuários internos para a realização de trabalho remoto, inclusive em finais de semana, fundamental durante o período da pandemia. (MARTINS, 2020, s/p)

Um ponto que merece destaque é que todo esse transtorno se deu em meio a pandemia ocasionada pela covid-19, o que tornou o mundo ainda mais digital, fazendo com que todas as atividades que antes eram realizadas de forma presencial se tornassem digitais, aumentando assim o fluxo de acessos inclusive aos servidores do STJ, visto que as audiências passaram a ser realizadas de forma remota e online, aumentando ainda mais o transtorno vivenciado com o ataque sofrido pela casa. Durante o processo de restauração dos sistemas, foi também promovida a implementação de novas ferramentas de cibersegurança, fazendo assim com que o risco de um futuro ataque cibernético não seja iminente ao STJ.

> As orientações quanto às trocas das chaves de acesso por senhas fortes e com procedimentos de dupla autenticação – necessárias para o uso dos sistemas – estão sendo seguidas por todos, numa demonstração de compreensão da importância do papel de cada um para o reforço da segurança da infraestrutura. (MARTINS, 2020, s/p)

Esse tipo de ataque a um órgão público causa muito mais transtornos do que a danificação de bens materiais, ele traz consigo receios no que diz respeito aos ambientes virtuais, e como ataques desse nível podem afetar a soberania de os alicerces de um Estado Democrático de Direito, fazendo com que seja gerado um temor nos usuários de modo a que os faça pensar que tais ferramentas não lhe podem dar garantias de segurança quanto a si e seus dados.

> O STJ não se intimidou e superou, com a participação e o apoio de empresas e instituições, o desafio que se impôs. Judiciário, Executivo e Legislativo se fizeram presentes para prestar solidariedade e auxiliar o Tribunal da Cidadania a enfrentar a crise que se apresentou, numa demonstração robusta de que as instituições do Estado Brasileiro não se curvam nem se intimidam diante de ataques que pretendem atingir os sólidos alicerces da democracia brasileira. (MARTINS, 2020, s/p)

Dentro disso é possível compreender que esses tipos de ataque vão muito além do que danos matériais, eles acabam por ferir e vilipendiar direitos tidos como basilares para os cidadãos brasileiros, causam transtornos dentro dos mais variados sistemas públicos caso esses sejam os alvos, sendo assim se faz extremamente necessário a existência de mecanismos coercitivos e punitivos para tais demandas,

dentro disso é onde se encaixa a Lei Geral de Proteção de Dados, que visa definir os modos como esses dados devem ser coletados e tratados e estabelecer o que venha a ocorrer em caso de não cumprimento de suas estipulações.

3.2 Relação prática entre LGPD e Cibersegurança

Podemos estabelecer uma relação prática entre cibersegurança e LGPD a partir do momento em que uma consegue complementar a outra no que diz respeito à segurança do usuário em ambiente virtual. Enquanto a cibersegurança visa a utilização de ferramentas para evitar qualquer espécie de ataque criminoso, como é especificado Marcelo Vandré:

> Posto isso, devemos entender o conceito de cibersegurança como sendo o conjunto de estratégias e habilidades para redução de riscos nas operações realizadas através do meio virtual, protegendo os usuários e fornecedores de ataques de hackers ou qualquer tipo de outro acesso não autorizado. (BARRETO, 2019, p.26).

Não obstante podemos trazer a definição de que a LGPD é um mecanismo jurídico voltado à proteção de dados e manipulação de dados, elucidando as maneiras como desde sua entrada em vigor as maneiras como os dados serão coletados, tratados e distribuídos, como definido por Matheus Braga Benedito:

> A Lei Geral de Proteção de Dados (LGPD), aprovada em agosto de 2018 e com vigência a partir de setembro de 2020, propõe uma padronização de normas e práticas, para assegurar o direito à privacidade e à proteção de dados pessoais dos usuários, de forma igualitária dentro do país e no mundo, não importando se a sede de uma organização ou o centro de dados dela estão localizados no Brasil ou no exterior: se há o processamento de conteúdo de pessoas, brasileiras ou não, que estão no território nacional, a LGPD deve ser cumprida (BENEDITO, 2021, p.6)

Um exemplo de tal relação ocorreria quando uma pessoa realiza o cadastro em uma plataforma online de cursos. A plataforma utiliza de ferramentas de cibersegurança para garantir que os dados de seus alunos não serão vazados, enquanto o aluno tem a segurança de saber que a empresa de cursos não pode disponibilizar ou comercializar seus dados pois este se encontra resguardado pela LGPD.

> É notório que o texto da Lei identifica, de forma clara, o objeto necessário de proteção que é o dado em sua essência elementar, quando este de alguma

> forma possa identificar a pessoa natural, de maneira direta ou indireta. (SIVIERI, 2021, p.19)

Pode-se inferir que a LGPD é o mecanismo jurídico pelo qual se personifica os bens pelos quais a cibersegurança zela pelos seus mecanismos de segurança e protocolos. A lei define bem qual é seu objeto primário de proteção e o intuito das quais sua existência se justifica. Somente a entrada da LGPD em vigor foi responsável por inúmeras bruscas mudanças em diversas empresas, que tiveram que buscar mecanismos para se adequar aos requisitos estipulados pela lei.

> Portanto, na busca por conformidade, as organizações deverão definir estratégias de proteção de dados com apoio de pessoas e tecnologias que permitam aos seus gestores e colaboradores, alcançarem o nível adequado de governança em privacidade e segurança da informação exigido pela Lei. (VASCONCELOS; SALIB; 2020; p.3)

Assim sendo, podemos notar que as ferramentas de cibersegurança, com o advento da LGPD tiveram que se adequar à nova legislação, o que requisitou das empresas uma disponibilidade em fazer mudanças em sistemas já vigentes para a adequação a tal. Tirando o fato do esforço despendido podemos dizer que a vigência da lei acabou por forçar as empresas a realizarem investimentos na área de cibersegurança, garantindo assim a sua conformidade com a nova lei, algo que acabou por ser um efeito adjacente muito interessante, gerando assim diversas vagas de trabalho na área além de criar um ambiente mais seguro para os usuários de quaisquer que sejam os serviços, evitando assim que tivessem seus dados expostos de alguma maneira.

> Ademais, estar em compliance com os requisitos da LGPD exigirá, entre outros aspectos, adequação dos processos organizacionais existentes, demandando, via de regra, investimentos em consultoria especializada, em capacitação de pessoal, em ferramentas de segurança, no mapeamento de dados7 (data mapping), na melhoria de procedimentos e nos fluxos internos e externos acerca de dados pessoais, bem como, na implementação de uma cultura organizacional voltada para a segurança da informação e privacidade (VASCONCELOS; SALIB, 2020, p.3)

Tais alterações fizeram com que todas as empresas revisem suas políticas de tratamento de dados, e com isso foi necessária diversas alterações para que as políticas de cada empresa entrassem em conformidade com a lei, fazendo assim com diversos processos e ferramentas de cibersegurança fossem revistas, visando

assim a conformidade com a nova legislação. Dentro disso pode se dizer que as ferramentas de cibersegurança ganharam parâmetros cujo os quais tem que ser projetadas e ter suas finalidades bem delimitadas, para que assim possam trabalhar em consonância com a Lei Geral de Proteção de Dados.

3.3 Aplicação prática da relação entre LGPD e Cibersegurança no caso do STJ

Vale ressaltar antes da associação prática dos assuntos mas já se valendo da mesma que a LGPD tem um enfoque muito forte no que diz respeito a privacidade do cidadão, o que faz com que uma ação criminosa desse porte seja um ataque direto à privacidade de todos que tenham dados envolvidos na situação em questão.

> Art. 1º Esta Lei dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. (BRASIL, 2018, s/p)

Como é expressamente descrito em seu artigo primeiro, a lei refere-se à proteção da privacidade, liberdade e demais direitos fundamentais, sendo assim, agressões como a ocorrida com a invasão dos servidores do STJ fazem com que o dispositivo jurídico tenha seu valor confirmado em casos práticos.

> Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais e garantidos os direitos fundamentais de liberdade, de intimidade e de privacidade, nos termos desta Lei.(BRASIL, 2018, s/p)

O caso em questão ocorreu no dia 3 de novembro de 2020, quando foram detectadas anormalidades nos servidores do Superior Tribunal de Justiça (STJ), diante do caso, medidas de contenção foram tomadas para tentar impedir que dados fossem vazados dos servidores da casa, como foi especificado em nota da mesma:

> O Superior Tribunal de Justiça (STJ) detectou, no dia 3 de novembro de 2020, um ataque hacker durante o período da tarde, quando ocorriam sessões de julgamento. Verificou-se que um vírus estava circulando na rede de informática do tribunal e, como medida de precaução, os links para a rede mundial de computadores foram desconectados, o que implicou no cancelamento das sessões de julgamento e impossibilitou o funcionamento dos sistemas de informática e de telefonia da Corte.(MARTINS, 2020)

A equipe responsável por investigar o ocorrido levou 6 dias para que pudesse restabelecer os danos causados, isso tudo pois todo o acervo de dados da casa foi criptografado, atitude comum em casos onde os cibercriminosos “sequestram” os dados da empresa ou órgão público em questão e posteriormente pedem uma espécie de resgate, geralmente pagado em criptomoedas para que os dados sejam liberados novamente, uma prática que vem se tornando comum nos últimos anos, principalmente em um período pós pandemia onde as empresas se tornaram cada vez mais digitalizadas da mesma forma que os orgãos públicos também, visto que esse foi o método adotado por eles para continuarem suas atividades em meio a pandemia da covid-19.

> Brasil. O site do STJ ficou fora do ar no dia 03 de novembro de 2020, quando foi identificado o ataque e no dia 05 de novembro de 2021 foi identificado que o hacker responsável por invadir o sistema do STJ criptografou todo o acervo de processos do tribunal, além de ter bloqueado o acesso às caixas de e-mail de ministros, além dos backups de dados da corte que também foram criptografados (BOSCO, 2020, s/p).

Perante tais fatos o que podemos inferir é que mais uma vez o poder de devastação e transtorno que pode ser causado por crimes cibernéticos, pois foi montada uma força tarefa para que as atividades da casa pudessem voltar ao normal funcionamento. Essa é uma característica que podemos definir como sendo exclusivamente do mundo cibernético, onde grandes estragos e transtornos podem ser causados por um grupo pequeno de pessoas, ou até mesmo por uma só, visto que o impacto causado por uma invasão em um sistema público é as vezes irreversível além de fazer com que diversos serviços que impactam diariamente a vida de milhões de pessoas fique indisponível.

> O Superior Tribunal de Justiça (STJ) informa que o restabelecimento dos sistemas de informática do tribunal está em andamento e que houve importantes progressos nesta segunda-feira (9).
> O Sistema Justiça e suas funcionalidades foram restaurados, bem como o Sistema Justiça Web – ambos são essenciais para a retomada dos julgamentos e das sessões de julgamentos no STJ. Nos próximos dias, haverá a estabilização dos módulos, para que eventuais falhas momentâneas sejam corrigidas.(MARTINS, 2020)

O ataque em questão foi classificado pelo então presidente da casa como o pior ataque cibernético a um órgão público brasileiro na história, e destacou a importância da constante reavaliação das políticas de segurança da informação:

> No dia 3 de novembro, o Superior Tribunal de Justiça (STJ) sofreu o pior ataque cibernético já empreendido contra uma instituição pública brasileira, em termos de dimensão e complexidade. Até então, nossa equipe não havia experimentado algo similar e, apesar de estarmos preparados, fomos levados a transformações que vão aperfeiçoar a forma como o Tribunal trata a segurança da informação. (MARTINS, 2020)

Dentro desse contexto podemos ver que tanto a cibersegurança quanto a Lei Geral de Proteção de Dados se fizeram presentes. A cibersegurança contou com os mecanismos de detecção, que vieram a acusar a presença de um vírus dentro do sistema, o que permitiu a rápida ação das equipes responsáveis, podendo assim evitar maiores danos.

Já a LGPD se enquadra nesse assunto se levantarmos a hipótese de que tenha havido danos consideráveis durante o ataque. Sendo assim surge a incógnita de que se o responsável pelo tratamento dos dados, no caso o STJ, seria penalizado em caso de vazamento. E caso isso tivesse ocorrido, conforme está tipificado no artigo 43 da Lei Geral de Proteção de Dados, o Superior Tribunal de Justiça não seria responsabilizado pelos danos sofridos provenientes de vazamento:

> Art. 43. Os agentes de tratamento só não serão responsabilizados quando provarem:
> I - que não realizaram o tratamento de dados pessoais que lhes é atribuído;
> II - que, embora tenham realizado o tratamento de dados pessoais que lhes é atribuído, não houve violação à legislação de proteção de dados; ou
> III - que o dano é decorrente de culpa exclusiva do titular dos dados ou de terceiro.(BRASIL, LGPD, 2018).

Como explicitado no parágrafo segundo da referida lei, no caso do STJ que realiza todo o tratamento dos dados de forma a seguir a Lei Geral de Proteção de Dados, caso houvesse danos e dados fossem vazados a mesma não poderia ser responsabilizada por estes, e utilizando este caso como parâmetro é possível dizer que será um problema de todas as empresas que não se adequarem às normas da Lei Geral de Proteção de Dados, visto que em caso de ataque e vazamento de dados, se a empresa referida não estiver em conformidade será punida pela negligência na adequação das referidas normas. A única implicação seria a disposta no artigo 48 da LGPD, onde com está especificado em caput:

> Art. 48. O controlador deverá comunicar à autoridade nacional e ao titular a ocorrência de incidente de segurança que possa acarretar risco ou dano relevante aos titulares.

Sendo assim, como foi feito, o órgão deverá comunicar sobre o fato ocorrido a fim de que se torne público quando casos assim aconteçam. A publicidade dos casos onde ocorre vazamento de dados acaba sendo de fundamental importância pelo fato de trazer ao conhecimento de todos uma possível exposição de suas informações, fazendo com que os envolvidos monitorem através de ferramentas de cibersegurança qualquer comportamento estranho envolvendo seus dados.

4. CONSIDERAÇÕES FINAIS

Dentro daquilo que foi apresentado durante todo o discorrimento deste projeto, podemos inferir algumas questões pontuais cujas as quais o mesmo se propôs a levantar de modo que trouxesse a elucidação de como a Lei Geral de Proteção de Dados, um dispositivo deveras novo em nosso ordenamento visto que tem apenas 4 anos de existência, pode influenciar e auxiliar no que tange a casos criminosos como a invasão dos servidores do Superior Tribunal de Justiça visto que tal tipo de ação criminosa.

Nesse cenário foi possível entender o que é cibersegurança e o quão enraizado esse termo está na conjuntura atual da sociedade, visto que a realidade atual é cada vez mais tecnológica e imersa em um mundo cada vez mais digitalizado. Algo que acentuou-se fortemente com a pandemia da Covid-19, que fez com que diversos serviços públicos e privados migrassem do ambiente físico para o virtual, alguns deles mesmo após a liberação por parte dos órgãos sanitários acabaram por optar manter-se de forma virtual visto que esse mecanismo gera diversas espécies de economia além da praticidade. Neste caso a cibersegurança se tornou um mecanismo essencial visto que esse aumento gigantesco no tráfego de dados em ambiente virtual propiciou um crescimento igual no que diz respeito ao número de criminosos cibernéticos.

Assim sendo a realidade cada vez mais virtual a criminalidade acabou por acompanhar tal tendência aumentando assim o número de crimes cometidos em ambientes cibernéticos, gerando assim aquilo que é rotineiramente chamado de hacker, mas ao qual vimos que é uma terminologia adotada de forma erroneamente, cujo o qual o termo certo é cracker e o mesmo acaba por ser um criminoso que atua em meios cibernéticos.

Além da cibersegurança se fez necessário e foi difundido através dos estudos apresentados neste trabalho a importância de dispositivos jurídicos que dêem sustentação e venham a agir de forma coercitiva para com os criminosos em ambiente virtual.

Tudo isso quando aplicado ao ataque sofrido pelo Superior Tribunal de Justiça, cujo o qual foi classificado como sendo o pior ataque cibernético a uma instituição pública no Brasil, faz com que se entenda a importância da LGPD no que

diz respeito ao modo de agir para com os dados e a forma com que se deve resguardar todos aqueles que fornecem dados de alguma forma seja para com instituições públicas ou empresas privadas, além de mostrar o árduo papel que é efetuado pela cibersegurança e suas ferramentas, no caso do STJ, identificando o mal potencial e assim dando margem de tempo para uma ação efetiva que veio a coibir danos ainda maiores dos que aconteceram.

Conclui-se que a parceria desenvolvida pelas ferramentas de cibersegurança que vem a desempenhar um papel dentro do ambiente online, prevenindo de mitigando danos e os dispositivos jurídicos no caso a LGPD que agende forma coercitiva além de oferecer toda uma base comportamental da forma cuja a qual deve-se captar, tratar e distribuir os dados, mostra que esse é um caminho a ser vastamente explorado nos próximos anos visto a expansão cibernética pela qual passamos.

REFERÊNCIAS

AMAYA, Ornella Cristine. **A SOCIEDADE DE CONSUMO NA ERA DIGITAL**: OS DESAFIOS DO DESENVOLVIMENTO SUSTENTÁVEL NA ERA DA QUARTA REVOLUÇÃO INDUSTRIAL. 2017. Dissertação (Mestrado Direito) - Universidade do Vale do Itajaí, [*S. l.*], 2017.

BACH, Sirlei Lourdes. **Contribuição do Hacker para o desenvolvimento da informática.** 2001. 135 f. Tese (Doutorado) - Curso de Ciência da Computação, Universidade Federal de Santa Catarina, Florianopolis, 2001.

COSTA, Sely Maria de Souza. **Impactos Sociais das Tecnologias de Informação**. 1995. Dissertação (Biblioteconomia) - UNB, [*S. l.*], 1995.

CILENTO, Lucas Geraldo. **Modelos de previsão de vulnerabilidades de sistemas operacionais baseados no modelo ARIMA e Redes Neurais**. 2021. Monografia (Bacharelado Engenharia da Computação) - UFPE, [*S. l.*], 2021.

FILGUEIRA, Danielle Polyanna; JÚNIOR, Vicente Celeste de Oliveira. **CRIMES DIGITAIS**: A EFICÁCIA DO ORDENAMENTO JURÍDICO BRASILEIRO EM COMBATER OS CRIMES PRATICADOS NO AMBIENTE VIRTUAL. 2022. Dissertação (Direito) - UNP, [*S. l.*], 2022.

HUREL, Louise Marie. CIBERSEGURANÇA NO BRASIL: uma análise da estratégia nacional. **Instituto**
Igarapé A Think And do Tank, Rio
de Janeiro, v. 1, n. 54, p. 6-12, abr. 2021.

MOURA, Natalia Mirella Melo de. **A EFETIVAÇÃO DO DIREITO À PRIVACIDADE DIGITAL E PROTEÇÃO DE DADOS NO BRASIL**. 2019. Monografia (Bacharelado Direito) - UFP, [*S. l.*], 2019.

MATSUYAMA, Keniche Guimarães; LIMA, João Ademar de Andrade. **CRIMES CIBERNÉTICOS: ATIPICIDADE DOS DELITOS**. 2016. Dissertação (Direito) - UNIFACISA, [*S. l.*], 2016.

OLIVEIRA, Gabrielle Domingos de. **Gestão da segurança da informação**:
perspectivas baseadas na tecnologia da informação. 2012. 12 f. Tese (Doutorado)- Curso de Biblioteconomia, Ufal, Juazeiro do Norte, 2012.

PINHEIRO, Patrícia Peck. **Proteção de Dados Pessoais Comentários à Lei n. 13.709/2018 LGPD**. São Paulo: Saraiva Jur, 2018. 97 p.

PANEK, Lin Cristina Tung. **Lei Geral de Proteção de Dados nº 13.709/2018**: uma analise dos principais aspectos e do conceito de privacidade na sociedade informacional. 2019. 35 f. Tese (Doutorado) - Curso de Direito, Universidade Federal do Paraná, Curitiba, 2019.

POLESEL, Jussara de Oliveira Machado. **Cibersegurança, privacidade e proteção de dados pessoais no brasil à luz do direito comparado e dos standards internacionais de regulamentação**. 2021. 141 f. Tese (Doutorado) - Curso de Direito, Universidade de Caxias do Sul, Caxias do Sul, 2021
RIGAMONTE, Fernando Lira. **A soberania na era cibernética**. 2017. 37 f. Tese (Doutorado) - Curso de Direito, Universidade Federal de Lavras, Lavras, 2017.

ROSA, ROSEMAR; SILVA, RACHEL INÊS DA; PALHARES, MÁRCIA MARIA. **AS NOVAS TECNOLOGIAS: INFLUÊNCIAS NO COTIDIANO**. 2005. Dissertação - UFBA, [*S. l.*], 2005.

ROCHA, Carolina Borges. A evolução criminológica do Direito Penal: Aspectos gerais sobre os crimes cibernéticos e a Lei 12. 737/2012.Revista Jus Navigandi, ISSN 1518-4862, Teresina, ano 18, n. 3706, 24 ago. 2013.

RAMOS, EDUARDO DULCETTI. **CRIMES CIBERNÉTICOS**: ANÁLISE EVOLUTIVA E LEGISLAÇÃO PENAL BRASILEIRA. 2017. Monografia (Bacharelado Direito) - UFRJ, [*S. l.*], 2017.

SOARES, Rafael Ramos. **Lei Geral de Proteção de Dados - LGPD**: Direito a Privacidade no Mundo Globalizado. 2020. Monografia (Bacharelado Direito) - PUC Goiás, [*S. l.*], 2020.

SILVA, INDIRA DAYANA OLIVEIRA TRAJANO; JALES, JOSÉ LEONARDO DE ARAÚJO. **O IMPACTO DA NOVA LGPD (LEI GERAL DE PROTEÇÃO DE DADOS) NO ÂMBITO EMPRESARIAL**. 2022. Monografia (Bacharelado Direito) - Universidade Potiguar, [*S. l.*], 2022.

SOUZA, GIOVANNA LARA AZEVEDO; OLIVEIRA JUNIOR, LUIZ HENRIQUE CAETANO DE. **OS IMPACTOS DA LGPD**: LEI GERAL DE PROTEÇÃO DE DADOS – NAS EMPRESAS DE CALL CENTER. 2021. Dissertação (Bacharelado Direito) - ANIMA, [*S. l.*], 2021.

SOUSA, DIEGO GOMES DE. **A ÉTICA HACKER NA ERA DO SIGILO DA INFORMAÇÃO**. 2013. Monografia (Bacharelado em Comunicação Social) - UFRJ, [*S. l.*], 2013.

SIVIERI, EDSON VICENTE. **ESTRUTURAÇÃO DO DEPARTAMENTO DE SEGURANÇA DA INFORMAÇÃO PARA ATENDER A GESTÃO DE DADOS EM CONFORMIDADE À LEI GERAL DE PRIVACIDADE DE DADOS (LGPD)**. 2021. Monografia (Direito) - UNISUL, [*S. l.*], 2021.

TEIXEIRA, Ana Clara Campos; FARIA, Evânia Gizele Rodrigues de; SILVA, Fabiana Maria da; OLIVEIRA, Jhenniffer Cristiny. **Lei geral de proteção dos dados**: lgpd para mídias sociais. 2021. 6 f. Tese (Doutorado) - Curso de Direito, Faculdade de Pará de Mina, Pará de Minas, 2021.

TELES, Tiago Miguel Fonseca Paiva de Sousa. **Cibersegurança**: detecção de outliers. 2015. 263 f. Tese (Doutorado) - Curso de Ciências Militares, Escola Naval, Alfeite, 2015.