PUC-SP

PONTIFÍCIA UNIVERSIDADE CATÓLICA DE SÃO PAULO

MESTRADO EM DIREITO

GIOVANNA THAÍS DOS SANTOS MAROUF

CRIMES CIBERNÉTICOS NA ERA DO CONSUMIDOR DIGITAL E A ATUAÇÃO DO COMPLIANCE NA PRIVACIDADE DE DADOS PESSOAIS

SÃO PAULO

2024

GIOVANNA THAÍS DOS SANTOS MAROUF

CRIMES CIBERNÉTICOS NA ERA DO CONSUMIDOR DIGITAL E A ATUAÇÃO DO COMPLIANCE NA PRIVACIDADE DE DADOS PESSOAIS

Trabalho de Dissertação de Mestrado apresentado à Pontíficia Universidade Católica de São Paulo, como requisito para o recebimento do título de Mestre em Direito

Orientador: Dr. Motauri Ciocchetti de Souza

SÃO PAULO

2024

Discente: Giovanna Thaís dos Santos Marouf

Título: Crimes Cibernéticos na Era do Consumidor Digital e a Atuação do Compliance na Privacidade dos Dados Pessoais

Trabalho de Dissertação de Mestrado apresentado à Pontíficia Universidade Católica de São Paulo, como requisito para o recebimento do título de Mestre em Direito

Área de Concentração: Direitos Difusos e Coletivos

Aprovado em: ___/___/___

Banca Examinadora:

_____

Orientador:

Instituição:

_____

Orientador:

Instituição:

_____

Orientador:

Instituição:

DEDICATÓRIA

Primeiramente dedico esta Dissertação de Mestrado a minha avó Edith. Ela não somente me encorajou a me candidatar no Mestrado, como também me levou para fazer a primeira fase da OAB em seus últimos dias de vida. A advogada que me tornei devo todo ao meu amor eterno a ela.

Agradeço a Pirelli por me apresentar uma nova frente que até então nunca havia me sido apresentada: ao mundo dos departamentos jurídicos e a Copa Energia, meu primeiro emprego como advogada. O emprego que eu fui mais feliz até hoje e que me permitiu de maneira saudável conciliar meus estudos com o meu trabalho, além de me permitir realizar um sonho: meu intercâmbio em Barcelona para cursar o Programa de *Visiting Student* no *Advanced Master in Legal Sciences*.

Dedico este Mestrado à Universidade Pompeu Fabra – através dela pude ter uma experiência internacional no fim do meu Mestrado.

Sou eternamente grata a bolsa 100% que recebi pela CAPES para cursar o Mestrado na PUCSP e ao meu orientador por todos os ensinamentos e resiliência.

Agradeço também a minha família e aos meus amigos, graças a vocês a vida se torna mais leve para que eu possa tornar todos meus sonhos uma realidade.

BOLSISTA CAPES

O presente trabalho foi realizado com o apoio financeiro e educacional da Coordenação de Aperfeiçoamento de Pessoal de Nível Superior Brasil **("CAPES")** – Finance Code 001.

Agradeço imensamente a CAPES pela oportunidade de ter financiado meu Mestrado na PUCSP, quando recebi minha bolsa para cursar o Mestrado.

Sou grata também ao meu orientador que me auxiliou no meu projeto, o qual ficou em 4° lugar no setor de ampla concorrência, permitindo que eu fosse uma aluna bolsista.

Dedico todo este trabalho como forma e incentivo pela vida acadêmica, a educação gratuita, a pós-graduação *Stricto Sensu* e aos professores de todo Brasil.

AGRADECIMENTOS

Gostaria de utilizar deste espaço para agradecimentos, começando pela minha família que sempre foi minha base, desde a minha entrada na faculdade, como em todas as etapas da minha vida.

Sou eternamente grata à Pontifícia Universidade Católica de São Paulo que me acolheu desde a graduação, quando eu mais precisei ser acolhida, como por tudo que ela me proporcionou: amizades que levo para vida toda, conhecimento para que eu me tornasse advogada e agora futura mestre, esperança para dias melhores e oportunidade de vivenciar uma faculdade livre e humana como a PUC-SP.

Agradeço também aos meus amigos, chefes e a todos colegas de trabalho, que possibilitam uma jornada profissional leve e feliz.

RESUMO

Ao praticar crimes cibernéticos, os agentes infratores se utilizam dos meios tecnológicos para cometer condutas face a vítima, figura vulnerável, que tem sua vulnerabilidade ainda aumentada quando acometida por algum crime no mundo virtual.

Esta Dissertação inicia-se com a abordagem do conceito de consumidor e sua respectiva proteção jurídica, além dos meios digitais de consumo pelos quais se adequa. Durante o percurso da Dissertação, são abordados os crimes cibernéticos propriamente ditos no âmbito consumerista juntamente aos seus reflexos, destacando as diferenças entre crimes cibernéticos próprios e impróprios, em que o primeiro tem sua prática delituosa descrita pelo tipo penal delimitado ao meio virtual e os impróprios, em que apesar de serem praticados no meio informático, não possuem o os meios virtuais especificados no tipo penal.

A metodologia utilizada consistiu na investigação destes crimes cibernéticos e nos estudos das quatro principais esferas de conhecimento: Direito do Consumidor, Direito Penal, Direito Digital e Compliance.

Com a utilização destas quatro principais esferas, conclui-se que o Compliance e o Direito Digital ao estudarem sobre proteção de dados trazem um importante impacto a esta investigação dos crimes cibernéticos, já que, servem como instrumentos para prevenção do vazamento de dados pessoais, protegendo e garantindo segurança dos consumidores para que os mesmos não tenham suas informações vazadas e manuseadas impropriamente ao utilizarem-se do meio digital para efetuação de compras e serviços, fornecendo seus dados pessoais para as empresas de forma deliberada, sujeitando-se a um cenário passível para aplicação de golpes e fraudes por parte dos criminosos que invadem os meios digitais.

Com isto, o Compliance e o Direito Digital das empresas devem atuar para que fiscalizem e previnem o vazamento de dados pessoais, protegendo e garantindo segurança aos consumidores para que eles não tenham seus dados vazados e manuseados impropriamente.

Palavras – Chave: Crimes Cibernéticos – Dados Pessoais – Compliance – Direito do Consumidor – Direito Digital – LGPD

ABSTRACT

When committing cybercrimes, offending agents use technological means to commit conduct towards the victim, a vulnerable figure, whose vulnerability is further increased when they suffer consequences in the virtual world.

For this dissertation, it begins with an approach to the concept of consumer and its respective legal protection, as well as two digital consumer data that are adequate. During the course of the Dissertação, only cybercrimes specifically in the consumer field were addressed together with their reflections, highlighting the differences between proper and inappropriate cybercrimes, in which the former has its criminal practice described by the criminal type, which is limited to the virtual environment, and inappropriate ones, in which despite being carried out in the computer environment, they do not have the virtual means specified in the criminal type.

The methodology used consisted of the investigation of these cybercrimes and studies of four main areas of law enforcement: Consumer Law, Criminal Law, Digital Law and Compliance. With the use of these four main spheres, it is concluded that Compliance and Digital Law will study data protection and have an important impact on this investigation of cybercrimes, therefore, they serve as instruments to prevent the loss of personal data, protecting and guaranteeing security to consumers so that they themselves do not have their data stored and handled improperly or use digital media to carry out purchases and services, providing their personal data to companies in a deliberate manner, subjecting themselves to a passível cenário for application of beatings and frauds by two criminals who invade the digital media.

With this, Compliance and Digital Law of the companies must act so that we supervise and prevent the use of personal data, protecting and guaranteeing safety to consumers so that we ourselves do not have their data emptied and handled improperly.

Keywords: Cybercrimes – Personal Data – Compliance – Consumer Law – Digital Law – LGPD

SUMÁRIO

CAPÍTULO I

INTRODUÇÃO

O presente trabalho visa explorar o mundo digital com o advento da tecnologia com uma análise mais crítica do mercado de consumo.

Com a pandemia da COVID – 19 no Brasil, o mundo apresentou duas vertentes: o mundo físico, o qual estava impedido de realizar seu comércio e suas atividades de maneira habitual e o mundo digital que passou a ser o palco principal das relações em sociedade, já que os indivíduos passaram a executar suas atividades rotineiras de maneira virtual.

Dentre as atividades mencionadas, o mercado de consumo foi o que mais ganhou destaque, criando um espaço para que consumidores executem suas compras, realizem transações financeiras e executem suas atividades rotineiras de modo *online*, criando a figura do consumidor digital que executa suas tarefas e necessidades através dos meios digitais de consumo. Porém, juntamente com os benefícios trazidos, uma série de consequências foram apontadas, como os crimes contra as relações de consumo, sobretudo os crimes cibernéticos.

A ocorrência dos crimes cibernéticos gerou a necessidade dos indivíduos se protegerem contra estas práticas. Porém, tendo em vista que o consumidor é um ser vulnerável, tornou-se importante promover o Compliance como instrumento protetor dos dados pessoais dos indivíduos, juntamente a atuação da LGPD para garantir um respaldo jurídico na proteção dos dados do consumidor no ambiente virtual.

Em suma, o presente trabalho em seu primeiro capítulo aborda conceitos do direito do consumidor num contexto geral, suas regras e direitos atrelados, o segundo acerca do cenário aplicável aos meios digitais de consumo, o terceiro sobre crimes cibernéticos e o capítulo final sobre o papel do Compliance como forma de proteção do consumidor em face aos meios cibernéticos de consumo.

I. DIREITO DO CONSUMIDOR

Para existência de uma relação de consumo são necessários quatro elementos essenciais: a presença de um produto ou serviço, que seria o elemento objetivo, o fornecedor e o consumidor, correspondentes aos elementos subjetivos e por fim, um destinatário final, como elemento finalístico da relação de consumo.

O Código de Defesa do Consumidor é responsável por regularizar as relações de consumo e para tanto, protege os direitos difusos, direcionado a um grupo indeterminado de pessoas; coletivos ligados a um grupo determinado de pessoas e os individuais homogêneos, que também dizem respeito a um grupo específico de pessoas, mas de forma individualizada.

Para o referido Código, em seu artigo terceiro, "fornecedor é toda pessoa física ou jurídica, pública ou privada, nacional ou estrangeira, bem como os entes despersonalizados, que desenvolvem atividade de produção, montagem, criação, construção, transformação, importação, exportação, distribuição ou comercialização de produtos ou prestação de serviços", em que, serviço seria qualificado como qualquer atividade remunerada realizada no mercado de consumo com viés bancário, financeiro, securitário, de crédito, etc., e produto conceituado como qualquer bem, seja material/imaterial ou móvel/imóvel. [1]

Através da relação estabelecida, o Código de Defesa do Consumidor busca definir normas de proteção e defesa do consumidor, de ordem pública e interesse social.

1.1. ORIGEM

Criado pela Lei n° 8.078/1990, o Código de Defesa do Consumidor é o fruto da garantia dos direitos dos consumidores e é interligado a redemocratização e a criação da Constituição Federal que entendia cada vez mais a necessidade da existência de uma legislação típica para regularizar as relações de consumo.

Em 1970 foram criados os primeiros órgãos de defesa do consumidor e em meados de 1976 foram inaugurados alguns grupos como o PROCON (antigamente

[1] BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990.

denominado de Grupo Executivo de Proteção ao Consumidor), Associação de Defesa e Orientação do Consumidor de Curitiba **(“ADOC”)** e a Associação de Proteção ao Consumidor de Porto Alegre **(“APC”)**. Posteriormente, em 1985 foi inaugurado o Conselho Nacional de Defesa do Consumidor com o intuito de elaboração das políticas nacionais de Defesa do Consumidor.

A Constituição Federal desempenhou um importante papel nas garantias fundamentais, estabelecendo a proteção do consumidor como direito fundamental e como um dos princípios da ordem econômica, exigindo a necessidade de existir uma lei específica aos consumidores.

Em 11 de setembro de 1990 foi sancionada a Lei n° 8078, responsável por instituir o Código de Defesa do Consumidor, lei pela qual entrou em vigor em 11 de março de 1991, tornando-se um importante marco para relação consumerista.

1.2. PRINCÍPIOS DE PROTEÇÃO CONSTITUCIONAL

São os Princípios Fundamentais da Constituição Federal aplicáveis ao direito do consumidor que tutelam as relações consumeristas e que protegem não somente a Constituição como um todo, como também, todos os consumidores envolvidos.

Alguns princípios basilares que protegem a Constituição seriam o do Reconhecimento da Vulnerabilidade do Consumidor, em que o consumidor é a parte mais vulnerável, requerendo uma proteção e atenção especial do Estado; o Princípio do Intervencionismo do Estado pelo qual busca por adotar um conjunto de ações que trazem equilíbrio para as relações com o Estado interferindo na vida econômica, promovendo o bem estar social dos cidadãos; o Princípio da Harmonização de Interesses o qual promove de forma compatível a economia e o atendimento dos consumidores conforme suas necessidades; o Princípio da Boa Fé e o da Transparência, pois através deles, são garantidos o equilíbrio entre fornecedores e consumidores através de relações igualitárias que tomam suas ações baseadas na boa fé e pautadas pela transparência entre as partes e por fim o da Dignidade Humana, servindo como base para todos os direitos fundamentais, em que, pela Constituição, todos os consumidores deverão ter uma vida digna com os seus direitos garantidos.

1.2.1. RECONHECIMENTO DA NATUREZA PÚBLICA DO DIREITO DO CONSUMIDOR

A natureza pública do direito do Consumidor é reconhecida em diversos aspectos através de diversos mecanismos e contextos, como pela Constituição Federal, já que, a proteção ao consumidor, como direito fundamental, é um princípio que norteia a ordem econômica; o Código de Defesa do Consumidor ao reforçar a natureza pública do direito do consumidor quando define normas de ordem pública que atinge o interesse social; a Política Nacional das Relações de Consumo quando o Estado se responsabiliza pela defesa dos consumidores, etc.

Os direitos dos consumidores por serem direitos difusos e coletivos são direitos de titularidade indeterminada, vinculado a um grupo ou categoria de pessoas, e possuem seu viés de natureza pública em virtude da Ação Civil Pública ser um dos principais instrumentos utilizados para proteção dos direitos difusos e coletivos.

1.3. PRINCÍPIO DA VULNERABILIDADE

No Princípio da Vulnerabilidade, o Código de Defesa do Consumidor protege e reconhece que o consumidor é a parte mais frágil da relação de consumo, garantindo-lhe equilíbrio contratual perante o fornecedor. Como o fornecedor é a parte mais fortalecida da relação, cabe a ele o dever de informar as características e informações úteis com as devidas explicações necessárias ao consumidor dos produtos e serviços oferecidos, como prevê o Princípio do Dever da Informação.[2]

A vulnerabilidade é um traço característico de todos os consumidores, independentemente de classe social devido ao desequilíbrio técnico, jurídico, fático e informacional perante os fornecedores.

O aspecto técnico indica a fragilidade nas informações técnicas do produto e do serviço; a jurídica na fragilidade nos conhecimentos da esfera do Direito; a fática no aspecto econômico e a informacional aos dados correspondentes aos produtos e serviços.

[2] BAUDRILLARD, Jean. A sociedade de consumo. 2 ed. Portugal: Edições 70.

Dentre essa vulnerabilidade generalizada de todos os consumidores, identifica-se uma hipervulnerabilidade em alguns grupos sociais, como crianças, adolescentes, idosos, gestantes e pessoas com deficiências.

O princípio da vulnerabilidade é amplamente reconhecido, pois através deles, são pautadas leis e garantias aos indivíduos que prezam pelo equilíbrio socioeconômico entre as partes, tendo em vista que reconhecem que o consumidor é a parte mais fragilizada da relação.

1.3.1. DUPLA VULNERABILIDADE DO CONSUMIDOR

Como visto anteriormente, os consumidores por si só já são figuras mais vulneráveis frente aos fornecedores, por não possuírem tantos conhecimentos informacionais sobre os produtos e serviços ofertados.

No meio digital, os consumidores possuem sua vulnerabilidade potencializada devido à ausência de conhecimento sobre segurança digital, já que não sabem sobre os riscos e prevenções para garantir a segurança cibernética. Somado às questões da segurança digital, a vulnerabilidade digital é identificada a partir da desterritorialização, ou seja, ausência de um território delimitado onde a relação de consumo é estabelecida, juntamente a falta de contato com quem negocia, por não haver um meio físico ou material para se estabelecer a relação de consumo.[3]

A vulnerabilidade do Consumidor está presente em quatro vertentes: informacional, fática, técnica e jurídica.

Também denominada de vulnerabilidade socioeconômica, a vulnerabilidade fática relata uma superioridade do poder que o fornecedor possui face ao consumidor. Ademais, importante pontuar a vulnerabilidade jurídica, pois muitos consumidores não possuem conhecimentos básicos jurídicos que deveriam ter para se protegerem de abusividades executadas pelos fornecedores.

A vulnerabilidade informacional propõe a insuficiência de informações que os consumidores possuem do que estão adquirindo, relacionando-se também a vulnerabilidade técnica, já que os fornecedores possuem conhecimentos maiores

[3] BARROS, Flávio Monteiro de. Manual de Direito do Consumidor. São Paulo: Rideel. 2011.

acerca das especificidades dos produtos e serviços, quando comparados aos fornecedores dos produtos.

No meio virtual, a vulnerabilidade se mostra ainda mais acentuada, em virtude de mecanismos causadores de falhas no sistema informático pelos quais o consumidor *online* poderá estar sujeito.

A vulnerabilidade digital, com a automação das relações de consumo, existe um desequilíbrio entre as partes, em que o consumidor se encontra em uma situação de impotência, justamente por não terem mecanismos próprios de defesa para evitarem os ataques cibernéticos.

1.4. PRINCÍPIOS DE PROTEÇÃO DO CONSUMIDOR

O Código de Defesa do Consumidor não somente estabelece regulamentos, normas e conceitos através de seus artigos para proteger os consumidores, mas também as doutrinas desempenham um importante papel para proteção do consumidor em sociedade ao estabelecer princípios e informações que complementam o mencionado Código, como os princípios de defesa do consumidor. Dentre os quais seriam os principais: Princípio da Vulnerabilidade como foi citado anteriormente; do Dever de Informar; da Prevenção; da Transparência; da Boa Fé Objetiva; da Reparação Integral de Danos e da Solidariedade.

No Princípio do Dever de Informar, entende-se que as informações deverão ser repassadas ao consumidor do produto e serviço adquirido, como também, o Princípio da Prevenção determina quais cautelas o fornecedor deverá ter para evitar quaisquer tipos de danos ao consumidor, como, por exemplo, o fornecimento de informações ao consumidor sobre o manuseio de um produto ou serviço; o alerta de eventuais riscos e perigos existentes e a proibição de venda de produtos com periculosidade ou nocividade, informando os riscos do negócio de forma clara, sem ocultar nenhuma informação ao consumidor, apontando também características do produto e serviço, sua maneira de utilização e preço ofertado. Trata-se de uma obrigação imposta ao Estado e aos fornecedores, a transparência nas informações fornecidas, conforme o Princípio da Transparência.

Sempre caberá ao fornecedor ter uma conduta ética, respeitando os direitos dos consumidores nas relações estabelecidas, respeitando o Princípio da Boa

Fé Objetiva. Além da boa fé, todos consumidores possuem o direito de prevenção e reparação de danos patrimoniais, morais, coletivos e difusos e individuais pelos quais foram sujeitos, com base no Princípio da Reparação Integral de Danos e, havendo mais de um autor na ofensa, todos participantes responderão solidariamente na reparação de danos, independentemente da existência de culpa. Excepcionalmente, nos casos de responsabilidade por defeito ou acidente de consumo, o comerciante não responderá junto ao fornecedor do bem que causou o acidente, conforme o Princípio da Solidariedade.

Como dito anteriormente, além da doutrina, o Código de Defesa do Consumidor visa buscar por proteger o consumidor através da criação de normas e regulamentos, além de Regras de Responsabilidade Cíveis e Penais para garantir uma relação consumerista ideal.

1.5. CONCEITO DE CONSUMIDOR E SUAS INCIDÊNCIAS

Segundo o Código de Defesa do Consumidor, em seu artigo 29, nas práticas comerciais, equipara-se ao consumidor a coletividade de pessoas, ainda que indetermináveis, que hajam intervindo nas relações de consumo.

O conceito do consumidor previsto no artigo 29 não somente se aplica às relações de consumo, mas também às transações do mercado de uma forma geral, ou seja, também as empresariais e civis. O artigo 29 protege toda coletividade de pessoas, mesmo não sendo possível identificar o consumidor individualmente, justamente por tratarem das práticas comerciais abusivas que todos os consumidores estão expostos diariamente. A este conceito são aplicadas as regras dos artigos 29 a 54 e não a totalidade do Código de Defesa do Consumidor.[4]

Desta forma, cria-se uma rede protetora dos direitos difusos e coletivos dos consumidores, em que é prescindível o consumidor ter participado efetivamente da relação de consumo, bem como, estar suscetível a um evento danoso. O alcance da norma se dá para consumidores que diariamente são expostos às publicidades, práticas abusivas, cobrança de dívidas, dentre outros.

[4] KHOURI, PAULO R. ROQUE A. *DIREITO DO CONSUMIDOR*. DISPONÍVEL EM: MINHA BIBLIOTECA, (7TH EDIÇÃO). GRUPO GEN, 2020.

Somado ao artigo 29, o CDC traz em outros artigos outros conceitos de "consumidor", como previsto no artigo segundo, ao dispor que "consumidor é toda pessoa física ou jurídica que adquire ou utiliza produto ou serviço como destinatário final", equiparando ao consumidor a coletividade de pessoas, ainda que indetermináveis, que haja intervindo nas relações de consumo.[5]

Além dos artigos segundo e vigésimo nono, outro artigo que conceitua o termo de consumidor é o décimo sétimo do mesmo Código, pois analisa a figura do consumidor por equiparação refletindo sobre as vítimas de eventos danosos nas relações de consumo, independentemente se tiverem participado ou não da relação de consumo, adquirido qualquer produto ou contratado o serviço em questão, mas que sofreram alguma lesão e por este motivo serão resguardados pelo Código de Defesa do Consumidor.

No âmbito digital, conceitua-se como consumidor *online* todo aquele que executa compras ou adquire serviços via internet, sem optar e estar presente no ambiente físico. O perfil do consumidor *online* varia conforme questões culturais, econômicas e sociais, dividindo-se em três principais grupos: emergentes, ocasionais e digitais.

Consumidores ocasionais são os que consomem de forma esporádica; os emergentes são usuários de comércios *online* mas que preferem o comércio físico; e os digitais são pessoas que preferem realizar compras virtualmente.[6]

O perfil do consumidor digital é de ser um indivíduo imediatista, pois o comércio *online* ocorre a qualquer momento e em qualquer lugar, independemente da presença de um espaço físico de compra e venda de mercadoria. Ademais, caracteriza-se por ser um perfil pesquisador, pois diante da gama de variedades existentes no mercado virtual, há inúmeras fontes de venda imediata, promovendo a necessidade do pesquisador sempre estar buscando pelo produto/serviço com melhor custo-benefício. Referem-se aos consumidores que buscam praticidade, pois mesmo com a falta de tempo para se deslocar até o comércio presencial, a compra é efetuada.

[5] BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990.
[6] RIBEIRO, Gustavo Pereira Leite. O conceito Jurídico de Consumidor. Revista Trimestral de Direito Civil. Rio de Janeiro: Renovar, 2004. v. 18, abr./jun.

O usuário digital tem o hábito de pesquisar frequentemente realizando comparação de marcas, evitando burocracias e transtornos que teria em comércios presenciais, muitas vezes influenciados por redes sociais e propagandas que os direcionam aos sites de vendas.

Muitas das publicidades ofertadas proporcionam benefícios e descontos aos consumidores, tornando impactos positivos no consumo. Porém, podem trazer efeitos negativos quando se refletem em golpes pelos quais muitos indivíduos sofrem ao compartilhar dados pessoais ou bancários em sites inapropriados, ocasionando uma violação ao direito e a informática e propiciando a ocorrência dos crimes cibernéticos, tema alvo do presente trabalho.[7]

1.6. O DIREITO A INFORMAÇÃO COMO SUPERPRINCÍPIO

O Direito à Informação é um superprincípio, pois está consagrado na Constituição Federal e no Código de Defesa do Consumidor, definindo que a todos é assegurado o direito a informação, bem como, declarando que se trata de um direito básico de todos os consumidores.

O Direito à Informação é um instrumento crucial aos consumidores, pois através dele, é possível a tomada de decisões conscientes sobre a compra de produtos e serviços, sem que sejam enganados por terceiros.

Por serem importantes instrumentos aos consumidores, foram criados alguns órgãos como PROCON e Associações de Defesa do Consumidor, além do Ministério Público, para fiscalizar como está sendo o compartilhamento e o manuseio dessas informações com os consumidores.

Além de serem amparados pelas mencionadas instituições, são amparados pela busca da reparação judicial e administrativa quando não possuem informações claras sobre o que precisam.

O Direito à Informação é garantido através da transparência nas relações de consumo, a publicidade adequada que não induza o consumidor a erro, a presença de informações claras nos produtos e serviços ofertados, a disponibilidade de canais

[7] SANT'ANA, Armando. Propaganda: Teoria, técnica e prática. 7 ed. São Paulo: Thompson Learning, 2007.

de atendimento aos consumidores como o SAC, elaboração de Contratos de Adesão de forma clara e sem termos muito complexos etc.

Com o respeito ao Princípio do Direito à Informação há uma proteção dos consumidores na tomada de suas decisões, promovendo uma transparência nas relações de consumo estabelecidas.

2. REGRAS DE RESPONSABILIDADE NO CÓDIGO DE DEFESA DO CONSUMIDOR

2.1. REGRAS GERAIS DA RESPONSABILIDADE CIVIL NO CDC

Além dos princípios proferidos no Capítulo anterior, que servem como base para proteção dos consumidores, o Código de Defesa do Consumidor estipula em seus dispositivos regras gerais e peculiaridades acerca da Responsabilidade Civil em seu ordenamento.

No Código de Defesa do Consumidor, a Responsabilidade tem um caráter objetivo, tendo em vista que prescinde a comprovação de culpa para que o fornecedor seja responsabilizado.

Esta Responsabilidade Civil está prevista sobretudo nos artigos 12 e 14 do CDC, buscando a reparação dos danos causados aos consumidores por defeitos em seus produtos e serviços executados ou pela falta de transmissão de informações suficientes.

Destaca-se que, o fornecedor deverá se atentar para não inserir no mercado um produto ou um serviço que não ofereça uma segurança que dele legitimamente se espera, pois se assim ocorrer, deverá responder conforme Teoria do Risco do Negócio, pela qual determina que, qualquer pessoa a qual exerce alguma atividade cria um risco de dano para terceiros, devendo responder por esse risco, independentemente de culpa.

No sistema do Código de Defesa do Consumidor, a responsabilidade por vício do produto ou serviço como a responsabilidade pelo fato do produto possuem natureza objetiva, justamente por ser prescindível a verificação de culpa do fornecedor, excepcionalmente quando for constatado que o fornecedor não colocou o produto ou serviço no mercado ou que o defeito inexiste, atribuindo, exclusivamente, a culpa ao consumidor ou a terceiro.

O comerciante também se torna responsável quando não for identificado o fabricante, não for conservado os produtos perecíveis ou com produtos que não conterem descrições claras do seu fabricante, conforme previsto no CDC.

Também incorre na responsabilidade civil do CDC o diretor, administrador ou gerente da pessoa jurídica que aprove a oferta, o fornecimento, prestação de serviços.

Nos casos em que for exigido a comprovação de culpa ou dolo para responsabilizar o fornecedor de forma subjetiva, existem hipóteses pelas quais a responsabilidade deverá ser excluída, mesmo que a conduta praticada tenha sido acometida com culpa e dolo. As excludentes de responsabilidade subjetiva seriam essencialmente o caso fortuito e a força maior.

O caso fortuito faz referência ao evento sem previsibilidade e inevitável, ocasionado por causa externa e sem vontade das partes envolvidas. A força maior, diferencia-se do caso fortuito, por associar a eventos vinculados a ações humanas e causas internas, tratando-se também de um evento imprevisível e inevitável.

Divide-se o caso fortuito em interno e externo. Ambos são cenários imprevisíveis e inevitáveis, diferenciando-se a partir que, o interno faz referência a acontecimentos que ocorrem sob controle do agente, enquanto o externo está fora de controle.

Exemplo prático de força maior no contexto dos crimes cibernéticos seria numa situação concreta pela qual uma empresa sofre um ataque cibernético em massa e mesmo possuindo uma segurança cibernética, não conseguiu suprir com esta problemática, em virtude de ter sofrido um ataque cibernético por um grupo de hackers que superaram as suas expectativas de segurança.

Exemplos de casos fortuitos internos e externos no cenário cibernético podem ser exemplificados, indicando que no primeiro caso há um erro dentro da própria operação da empresa e o segundo a fatores externos à empresa. Exemplificando o caso fortuito interno, seria o caso de uma empresa que teve um erro no software de segurança em virtude de uma falha na atualização de seu sistema, dando abertura para vulnerabilidades no sistema e roubo de informações por terceiros, ocasião pela qual houve um problema técnico pelo próprio sistema da empresa, isto é, houve uma falha interna. Já o caso fortuito externo corresponde a

ataques globais, por exemplo, que afetam várias organizações simultaneamente, fora do controle interno.

2.2. REGRAS GERAIS DA RESPONSABILIDADE PENAL NO CDC:

A tutela penal do CDC foi concretizada face da necessidade em punir fornecedores por praticarem condutas inadequadas frente aos consumidores em que só seriam puníveis via sanções cíveis e administrativas

Ademais, muitas destas condutas ainda não estavam contempladas em leis esparsas, o que tornou necessário a atuação da seara penal para sanar este problema.

Estão dispostas nos artigos 61 ao 80 do Código de Defesa do Consumidor a estrutura penal do CDC. O bem jurídico do Direito Penal do Consumidor são as relações de consumo e todas as infrações penais previstas neste Código são de menor potencial ofensivo. O objetivo do direito penal do consumidor é proteger a integridade da relação de consumo e a Responsabilidade Penal vem justamente para punir condutas que seriam insuficientes serem punidas somente por indenização civil e sanção administrativa.

O sujeito ativo seria o fornecedor, fabricante, comerciante, prestador de serviço ou publicitário e o sujeito passivo o consumidor ou a coletividade dos consumidores.

No Código do Consumidor, em seu Título II na parte das “Infrações Penais”, uma série de dispositivos são responsáveis por enquadrar condutas que são puníveis no âmbito criminal. Porém, não apenas o Código de Defesa do Consumidor aborda sobre crimes nas relações de consumo, como também existem normas conexas no Código Penal.

O legislador busca criminalizar condutas contra a sociedade de consumo que envolvam publicidade enganosa ou abusiva, fraudes em ofertas, práticas abusivas, nocividade de produtos etc. Os bens tutelados são os princípios de proteção contratual e contra práticas comerciais abusivas, constituindo crimes de perigo, já que, não é exigido como elemento constitutivo de delito, ocorrer o dano efetivo aos consumidores.

CAPÍTULO II

OS MEIOS DIGITAIS DE CONSUMO

1. O SURGIMENTO DA INTERNET

A internet teve seu surgimento na década de 1960[8] após a união de algumas universidades para o desenvolvimento do *Advanced Research Projects Administration* (*ARPANET* – Administração de Projetos e Pesquisas Avançadas), cujo uso era exclusivamente das Forças Armadas Americanas que objetivavam promover a constituição e a continuidade de uma rede capaz de interligar computadores de todo o mundo, permitindo a interligação de sua comunicação mesmo em episódios de casos de calamidade como ataques nucleares.

Durante a Guerra Fria, o Departamento de Defesa Americano pretendia constituir uma rede de comunicação de computadores em pontos estratégicos com o intuito de descentralizar informações para que não fossem destruídos por bombardeios dados que estivessem localizados em um único servidor. Juntamente a isto, houve a implementação do Protocolo de Controle de Transferência/Protocolo de Internet, responsável pela interligação de diversos computadores, possibilitando sua atuação em grupo.

A integração dos países ocorre em virtude do surgimento da internet, essencialmente devido a criação e a popularização de diversas tecnologias que trouxeram um papel fundamental para o desenvolvimento da economia mundial quanto para o convívio em sociedade que depende a cada dia mais de tecnologia.

Graças a internet e ao mundo globalizado foram propiciadas a circulação de informações de forma instantânea e a comunicação em massa, a circulação de capitais, o crescimento de empresas multinacionais, dentre outros.

[8] Leite, George; S. e Ronaldo Lemos. Marco Civil da Internet. Disponível em: Minha Biblioteca, Grupo GEN, 2014.

1.1. DO MARCO JURÍDICO DA INTERNET NO BRASIL

A internet chegou ao Brasil em 1988 em virtude de iniciativas tomadas pela comunidade acadêmica de São Paulo – Fundação de Amparo à Pesquisa do Estado de São Paulo (“FAPESP”) e pela Universidade Federal do Rio de Janeiro e Laboratório Nacional de Computação Científica, juntamente com a criação pelo Ministério da Ciência e Tecnologia a Rede Nacional de Pesquisas a qual foi atribuída a responsabilidade de coordenar serviços de internet no Brasil. Em 1994, a Embratel iniciou um projeto para explorar a Internet para todos os brasileiros.

Posteriormente, surgiu um marco jurídico da constituição da internet que foi relevante no Brasil que se deu a partir da promulgação da Lei n° 12.965 de 2014, a qual estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, determinando diretrizes para atuação da União, Estados, Distrito Federal e Municípios atuarem.

A disciplina do uso da internet no Brasil tem como pilares o respeito à liberdade de expressão, a livre iniciativa, livre concorrência e a defesa do consumidor, bem como, a abertura e a colaboração, que buscam pela finalidade social da rede de reconhecer sua escala mundial, protegendo os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais.

Os princípios da proteção dos dados pessoais, da privacidade, da liberdade dos modelos de negócios promovidos na internet, bem como, a preservação da natureza participativa da rede e da garantia da neutralidade da rede buscam tornar a internet um ambiente seguro a todos seus usuários, visando não somente o direito ao acesso à todos, bem como, o acesso à informação, ao conhecimento e à participação na vida cultural dos indivíduos, buscando pelo pleno acesso à ampla difusão de novas tecnologias e de modelos de inovação.

Para o exercício da cidadania, é essencial o acesso à internet, tornando-se assegurados os direitos de inviolabilidade da intimidade, da vida privada e das comunicações privadas armazenadas, salvo por ordem judicial, bem como, o sigilo no fluxo de suas comunicações pela internet e aplicação das normas de proteção e defesa do consumidor nas relações de consumo idealizadas na internet.

Ocorre que, mesmo havendo uma proteção jurídica à internet, nem sempre a mesma é respeitada, já que, torna-se violada a partir do descumprimento dos seus direitos e princípios, colocando em risco os seus usuários e instituições vinculadas, diante da ocorrência dos chamados “crimes cibernéticos”, os quais violam principalmente o “direito e a informática”, em que os “consumidores digitais” são as vítimas, os quais serão abordados no presente trabalho.[9]

1.2. DIREITO E INFORMÁTICA

O direito esteve presente na informática [10]em suas diversas vertentes, como, por exemplo, no Direito Constitucional, em que a Constituição Federal aborda sobre a liberdade de comunicação, onde se defende a liberdade de pensamento na internet e fora dela; o Direito Civil abordando sobre o direito das obrigações e estipulando o Contrato, negócio jurídico, bilateral ou plurilateral, possuidor de uma norma jurídica individual reguladora de interesses privados perfeitamente aplicáveis aos meios eletrônicos, resultando em Contratos Eletrônicos; o Direito do Consumidor, em que há uma significativa movimentação do comércio pelos meios eletrônicos, o que representa a aplicabilidade do Código de Defesa do Consumidor para compras realizadas em ambientes eletrônicos; o Direito Tributário, pois há problemas jurídicos tributários que incidem sobre várias questões na internet, como é o caso do *software* e a mercadoria eletrônica, que conforme o STF, podem sofrer com a incidência do ICMS, ou a questão que foi amplamente discutida acerca da tributação do livro eletrônico ou até mesmo a incidência de tributos sobre os provedores de acesso à internet.

Menciona-se também o Direito Trabalhista ao desempenhar seu papel ao estudar acerca das relações de teletrabalho no qual o trabalhador desenvolve seu trabalho por intermédio da internet e há espaço, inclusive, para o Direito Administrativo, a partir dos serviços de E-CPF e E-CNPJ, arquivos eletrônicos que identificam os usuários, representando documentos de identidade e fornecendo garantias de integridade, privacidade e autenticidade na internet.

[9] Comer, Douglas E. Redes de computadores e internet. Disponível em: Minha Biblioteca, (6th edição). Grupo A, 2016.
[10] Paesani, Liliana M. Direito de Informática: Comercialização e Desenvolvimento Internacional do Software. Disponível em: Minha Biblioteca, Grupo GEN, 2015.

Assim, foram mencionados apenas exemplos de várias esferas do Direito pelas quais incidem sobre a internet e que se relacionam ao Direito Penal, sobretudo na prática dos denominados crimes cibernéticos.

2. SURGIMENTO DO COMÉRCIO ELETRÔNICO

O comércio eletrônico surgiu nos meados de 1970 nos Estados Unidos, quando foi registrada a primeira transação eletrônica com a venda de um computador por uma empresa dos Estados Unidos a uma Universidade da Califórnia.

A modalidade do comércio eletrônico ganhou força quando empresas de telefonia e internet se utilizaram do Intercâmbio Eletrônico de Dados para compartilhar arquivos entre as companhias. Posteriormente, a *Amazon* e a *eBay* demonstraram um grande interesse na ferramenta e apostaram seus conhecimentos para revolucionar o comércio eletrônico.

No Brasil, marco importante neste contexto ocorreu com a livraria *BookNet*, a qual era responsável por vender produtos via internet e aceitar o pagamento nas entregas, a qual posteriormente se tornou a Submarino, plataforma de comércio eletrônico muito reconhecida pelos brasileiros, que após alguns anos, fundiu-se juntamente com a Americanas.com, surgindo assim, a B2W, uma das maiores empresas do *e-commerce* do Brasil.

2.1. MECANISMOS

Os mecanismos do consumo digital são pautados pelo uso intensificado da internet ao longo dos anos. Com o advento da internet, são criados mecanismos que criam uma rede mundial pública de computadores, conectadas por tecnologias sem fio (*wireless*) e cabos que juntos produzem textos, sons e imagens gerando uma hipermídia para qualquer computador que esteja conectado a ela.

A *World Wide Web* também conhecido como as abreviaturas “www”, remete-se a um dos serviços oferecidos pela internet, incluindo uma interface de utilização a qual conecta os serviços de rede mundialmente.

A hipermídia faz referência a comunicação da internet que se molda através do uso das qualidades de multimídia, hipertexto juntamente com textos, ilustrações e gráficos com o uso de recursos de sons, vídeos e imagens.

Através do hipertexto que é um modelo de texto escrito de modo não sequencial, o usuário faz conexão de dados através de palavras que ilustram ligações denominadas de *hyperlinks* com documentos, textos e páginas, evidenciando que a linguagem padrão para escrever textos e páginas na internet é o *Hypertext Markup Language* **(“HTML”)**.

Assim, com o surgimento da Internet e dos mecanismos informáticos, surgem as relações comerciais digitais. O Direito surge como instrumento importante para regularizar essas relações, bem como, para assegurar os direitos dos indivíduos no meio digital.

3. CONVEÇÃO DE BUDAPESTE

Quando se discute sobre o surgimento do comércio eletrônico e da origem da internet, impossível deixar de mencionar acerca dos crimes digitais no âmbito internacional e acerca da Convenção de Budapeste.

Foi realizado a Convenção de Budapeste, a qual reuniu uma série de documentações vinculadas ao Direito Internacional Público com a atuação dos países signatários em seus respectivos comitês de especialistas responsáveis por implementar normas de direito material sobre crimes cibernéticos.

A Convenção de Budapeste estabeleceu um acordo internacional em 23 de novembro de 2001 entre países da União Europeia, com a adesão dos Estados Unidos, Japão e Austrália cujo papel foi fixar diretrizes às políticas nacionais, propondo uma harmonia nas legislações para o combate aos crimes digitais, como veremos adiante.

Os Estados membros do Conselho da Europa e os seguintes Estados Signatários possuem o objetivo de prosseguir com caráter prioritário uma política criminal comum a todos eles que protege a sociedade contra a criminalidade do ciberespaço tendo em vista as constantes mudanças oriundas da digitalização e pela globalização definitiva das redes informáticas. A Convenção desempenha um papel essencial para impedir os atos praticados contra a confidencialidade, disponibilidade e integridade dos sistemas informáticos, garantindo a incriminação desses comportamentos fraudulentos contra a internet, adotando poderes suficientes para detecção, investigação e procedimentos para combate as infrações.

A referida Convenção veio acompanhada de uma terminologia quanto aos seguintes conceitos:

- “Sistema informático”: execução de um programa para o tratamento automatizado de dados entre sistemas de dispositivos isolados ou interligados.

- “Fornecedor de serviço”: entidade responsável por processar ou armazenar dados informáticos.

- “Dados informáticos”: representação de informações em um processamento de sistema de computadores, incluindo um programa responsável por fazer um sistema informático executar uma informação.

- “Dados de tráfego”: todas as informações relacionadas a uma comunicação cibernética efetuada através de um sistema informático, gerado por um sistema como elemento de uma cadeia de comunicação.

A Convenção de Budapeste visou estabelecer medidas a nível nacional de direito penal material cujo teor almeja o combate de infrações contra a integridade, confidencialidade e disponibilidade de sistemas e dados informáticos.

Dentre as infrações mencionadas, existe a interceptação ilegítima em que cada parte será responsável por adotar as medidas legislativas que forem cabíveis para estabelecer como infração penal, em que, as partes exigem que a infração seja cometida com dolo ou que seja vinculada com sistemas informáticos interligados. Ademais, menciona-se sobre a interferência em dados, cuja atribuição é cada parte adotar medidas que se revelem necessárias para estabelecer como infração penal o ato intencional e ilegítimo de danificar, apagar ou deteriorar dados informáticos. A interferência em sistemas é causada pela obstrução grave, intencional e ilegítima ao funcionamento de um sistema informático através da danificação de dados da internet. O uso abusivo de dispositivos também é uma conduta familiar na Convenção de Budapeste, já que, cada parte adotará as medidas cabíveis para punir a produção/venda/importação/distribuição/disponibilização de um dispositivo concebido para prática de infrações, o uso de palavras-passe (códigos de acesso) que permitem o acesso a um sistema informático para o cometimento de condutas criminosas.

Algumas infrações abordadas pela Convenção de Budapeste estão relacionadas com o uso de computadores como a burla informática em que as partes

signatárias adotam medidas para o combate a introdução, eliminação ou supressão de dados informáticos ou de qualquer tipo de intervenção no funcionamento de um mecanismo informático com o objetivo de obter um benefício econômico ilegítimo para si ou para terceiros.

As infrações relacionadas ao conteúdo se destacam com a pornografia infantil com a sua difusão em sistema informático ou a sua simples posse deste tipo de conteúdo.

Quando se define a competência pela Convenção de Budapeste, foi estabelecido que cada parte adotará as medidas legislativas para estabelecer a sua competência relativamente a qualquer infração penal definida sempre que a mesma for cometida no território ou a bordo de um navio ou aeronave ou quando for ocasionada por um dos cidadãos nacionais, se a infração não for da competência territorial de nenhum Estado.

A referida Convenção não exclui qualquer competência penal exercida por uma parte, em conformidade com seu direito interno.

Os princípios gerais de cooperação internacional são aplicáveis aos instrumentos internacionais pertinentes a respeito da cooperação internacional em matéria penal, conforme acordos com base em legislações uniformes estabelecidas nos países.

Dentre os princípios gerais de cooperação internacional, destaca-se a extradição, cuja pena privativa de liberdade é definida por um período máximo de, pelo menos, um ano ou através de uma pena mais grave. Tratam-se de infrações passíveis de extradição em qualquer tratado de extradição existente ou que venha existir entre as partes. Torna-se responsabilidade das partes incluir estas infrações como passíveis de extradição em qualquer tratado de extradição a ser firmado entre as partes.

A partir do momento em que for exigida uma pena mínima diferente, baseado no tratado de extradição aplicável entre duas ou mais partes, será aplicada a pena mínima prevista no acordo pelo qual se aplica.

Havendo a condição de uma parte a extradição à existência de um tratado e acuse o recebimento de extradição de outra parte com a qual não havia celebrado

qualquer tipo de tratado de extradição, considera-se a Convenção de Budapeste como a base jurídica de apoio para temas relacionados a extradição.

Destaca-se que a extradição fica sujeita aos direitos internos da parte requerida ou pelos tratados de extradição aplicáveis, adicionando os fundamentos baseados nos quais a Parte requerida pode recusar a extradição.

Nos casos das extradições serem recusadas exclusivamente baseados na nacionalidade da pessoa procurada, ou no fato da parte requerida se considerar competente relativamente a essa infração, a parte requerida remeterá o processo, a pedido da parte requerente, às suas autoridades competentes para fins criminais, comunicando em tempo hábil, o resultado do processo a parte requerente.

Assim, as autoridades competentes tomarão iniciativas para condução da investigação.

Na mesma Convenção de Budapeste são estipulados os princípios gerais vinculados ao auxílio mútuo, já que as partes se auxiliaram quanto as investigações ou procedimentos relativos as infrações penais relacionadas com dados e sistemas informáticos ou para coleta de dados de forma eletrônica para o mapeamento de uma infração penal.

No auxílio mútuo os pedidos podem ser formulados através de fax e correio eletrônico, sempre condicionados as normas fixadas pelo direito interno da parte requerida ou pelos tratados de auxílio mútuo aplicáveis.

Dentre este auxílio, uma parte pode informar a outra informações obtidas no quadro de suas próprias investigações, desde que nos limites da sua própria legislação e na ausência de pedido prévio, sempre quando auxiliar a outra parte a iniciar investigações penais, tratando-se da informação espontânea.

Foi estabelecido na Convenção de Budapeste a Rede 24/7, cujo papel era designar um ponto de contato disponível 24 horas sobre 24 horas, 7 dias por semana, com o intuito de assegurar a prestação de assistência imediata a investigações vinculados a sistemas informáticos.

Desta forma, o objetivo desta Convenção é complementar os acordos multilaterais aplicáveis entre as partes, incluindo as disposições da Convenção

Europeia de Extradição, aberta para assinatura em Paris a 13 de dezembro de 1957, da Convenção Europeia de Auxílio Mútuo em Matéria Penal, aberta para assinatura em Estraburgo a 20 de abril de 1959 e do Protocolo Adicional à Convenção Europeia de Auxílio Mútuo em Matéria Penal, aberta para assinatura em Estrasburgo.

Destaca-se que se duas ou mais partes já tiverem firmado um acordo relativo às matérias tratadas pela presente Convenção ou se tiverem estabelecido relações a este respeito, terão a possibilidade da aplicação do referido acordo em substituição da Convenção. Porém, toda vez que as partes firmarem relações respeitando as matérias do objeto da presente Convenção de forma distinta daquela que é prevista, será feita de uma maneira que não seja incompatível com os objetivos e princípios desta Convenção.

Quanto a Resolução de Conflitos, o Comitê Europeu será conservado e informado sobre a interpretação e aplicação da presente Convenção para resolução de Problemas Criminais. Havendo litígio entre as partes quanto a interpretação da presente Convenção, as mesmas mediram esforços para encontrarem uma solução para o conflito por meio da negociação ou meio pacífico a sua escolha, possuindo a opção de submeter o conflito ao Comitê Europeu a um tribunal arbitral, sendo que as decisões estarão vinculadas as partes no litígio ou ao Tribunal Internacional de Justiça de comum acordo entre as partes envolvidas.

Qualquer parte pode denunciar a Convenção através de Notificação dirigida ao Secretário Geral do Conselho da Europa, produzindo efeitos no primeiro dia do mês seguinte ao termo de um período de três meses após a data de recepção da notificação pelo Secretário Geral.

O Secretário Geral, por sua vez, notificará ocasionalmente os Estados não membros, os Estados membros do Conselho da Europa que auxiliaram na elaboração da presente Convenção, assim como qualquer Estado aderente ou que tenha sido convidado a aderir à presente Convenção acerca do depósito de qualquer instrumento de aceitação, aprovação, ratificação ou adesão e a qualquer outro ato relacionado com a Convenção.

3.1. PROTOCOLO ADICIONAL À CONVENÇÃO SOBRE CIBERCRIME, REFERENTE AS PRÁTICAS RACISTAS E XENÓFOBICAS

O Protocolo tem o intuito de complementar as disposições referentes ao Cibercrime quanto aos assuntos ligados ao racismo e a xenofobia. Todo material racista e xenofóbico consiste na presença de qualquer imagem que incite ao ódio e a discriminação.

Considera-se e é incriminado como conduta a disponibilização de material racista e xenofóbico por meio de sistema de computadores. Quando há outros remédios eficazes, as partes podem não recrutar o sistema penal como responsável por resolver o conflito.

As partes adotarão as medidas legislativas cabíveis quando ocorreram ameaças, ofensas, racistas e xenofóbicas motivadas. Quanto a negação, minimização grosseira ou justificação do genocídio contra a humanidade consiste na disposição de material que minimize atos que justifiquem o genocídio ou crimes contra a humanidade através da utilização de sistema de computadores. As partes podem exigir que a negação seja cometida com o intuito de incitar o ódio contra um grupo de indivíduos com base na discriminação contra um indivíduo ou um grupo de pessoas com base na cor, raça, ascendência etc.

O presente Protocolo estará disponível para aqueles Estados que assinaram a Convenção, sendo que poderão expressar seu consentimento em ficarem vinculados por qualquer assinatura sem reservas quanto à ratificação, aceitação ou aprovação e a assinatura sujeita a ratificação, aceitação ou aprovação seguida de ratificação, aceitação ou aprovação.

Qualquer um dos Estados não pode assinar o Protocolo sem reserva de ratificação ou depositar um instrumento de ratificação, exceto se já tiver depositado um instrumento de ratificação, aprovação ou aceitação da Convenção, os quais serão depositados juntamente com o Secretário Geral do Conselho da Europa.

Destaca-se que o Protocolo entra em vigor quando há o primeiro dia do mês seguinte à expiração de três meses posteriores a data em que cinco Estados tenham expressado seu consentimento em se vincularem ao Protocolo.

Após a contextualização do surgimento da internet e do seu contexto internacional, o próximo capítulo irá descrever os crimes digitais pelos quais os consumidores estão sujeitos a serem vítimas, foco da presente Dissertação, como será observado em diante.

CAPÍTULO III

CRIMES CIBERNÉTICOS

1. CONCEITO

Apesar de muitos consumidores estarem sujeitos às condutas abusivas, nem todas os comportamentos são puníveis no Código de Defesa do Consumidor, porque possuem uma abrangência que não se restringe ao mundo digital.

Com o crescimento do mundo virtual, cada vez mais se mostrou necessário refletir acerca da proteção jurídica dos consumidores no ambiente digital.

Os denominados crimes cibernéticos[11]são condutas praticadas pelos agentes infratores que se utilizam de computadores ou de dispositivos eletrônicos para prática de atos ilícitos, ocasionando danos a indivíduos ou patrimônios, bem como, à reputação de vítimas, extorsão de recursos financeiros e danos à patrimônios.

São condutas antijurídicas, típicas e culpáveis praticadas contra ou com a utilização de sistemas de internet, onde o meio usualmente utilizado é o computador, não sendo o único recurso tecnológico propicio para tal prática, já que *tablets* e celulares também são meios de prática dessas infrações.

Crime digital é o fenômeno vinculado as transformações tecnológicas que a sociedade vivencia e que é estudado pelo Direito Penal e Direito Digital. Trata-se de comportamentos não autorizados, considerados ilegais que promovem o processamento automático de dados, transmitindo essas informações implicando na manipulação dos dados através do uso não autorizado de dispositivos eletrônicos, gerando assim, uma falsificação de programas.

Em decorrência da pandemia ocasionada pelo vírus *Covid-19* observou-se uma alteração no comportamento consumerista da população, a qual passou a consumir mais virtualmente do que presencialmente em razão do *lockdown* em vários lugares do mundo, onde comércios e instituições ficaram fechados para conter a circulação de pessoas pelas ruas e para combater o vírus e o comércio e as operações

[11] Crespo, Marcelo Xavier de F. Crimes digitais. Editora Saraiva, 2011.

financeiras virtuais entraram em vigor com mais força do que habitualmente, trazendo, por consequência, um maior índice de criminalidade virtual.

Uma Lei que trouxe impactos ao mundo jurídico brasileiro foi a 12.737 de novembro de 2012, também conhecida como “Lei Carolina Dieckmann”, a qual ganhou este nome em razão da repercussão pela qual se envolveu a atriz, quando a mesma teve seu computador invadido e seus arquivos pessoais furtados, tornando-se vítima do compartilhamento de uma série de documentos pessoais.

A referida Lei da Carolina Dieckmann dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências, como a invasão de dispositivo informático, a falsificação de documento particular e de cartão, além da interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública, dispositivos que serão abordados detalhadamente ao longo deste trabalho. [12]

Outra Lei de extrema importância para este tema é a 12.965/2014, estabelecendo princípios, garantias, direitos e deveres para o uso da internet no Brasil. Sua temática abrange sobretudo a inviolabilidade da vida privada, da intimidade, sigilo das comunicações privadas armazenadas e das comunicações pela internet, dentre outros.

Ressalta-se também a Lei Geral de Proteção de Dados, cujo objetivo principal é regular as atividades de coleta e tratamento de dados pessoais, dispondo sobre o manuseio desses dados nos meios digitais, por pessoas naturais e pessoas jurídicas de direito público ou privado, protegendo os direitos fundamentais de liberdade, privacidade e desenvolvimento da personalidade da pessoa natural também tem relação com a prática dos crimes digitais, pois o correto manuseio dos dados pessoais diminui as incidências de vazamento de dados e consequentemente, a prática do delito virtual.

O vazamento de dados ocasionado pelo não manuseio correto de informações pessoais e pelo acesso indevido a dados sigilosos por indivíduos não autorizados, ocorrendo de forma inesperada quando os sistemas de segurança *online*

[12] MALAQUIAS, Roberto Antônio Darós. Crime Cibernético e Prova: a investigação criminal em busca da verdade. 2. ed. Curitiba: Juruá, 2015.

não executam seu papel adequadamente ou quando há invasão de sistema por terceiros, não apenas afetam a violação de princípios, mas também, ocasionam espaços vulneráveis para o cometimento da ocorrência de crimes causadas pelo vazamento de dados pessoais, de forma que, abaixo serão citados alguns de seus exemplos:

Roubo de identidade: o roubo de identidade trata-se de um crime ocasionado por um agente infrator que absorve para si ou para terceiros, informações de um indivíduo, as utilizando como se fosse o detentor dos dados pessoais para realização de compras, contratação de serviços, realização de pagamentos e saques bancários, acessar redes sociais e contas bancárias de terceiros, dentre outros. O roubo de identidade pode ocorrer após ataques cibernéticos, de engenharia social, acessos indevidos a *emails*, contas bancárias, redes sociais etc.

Agentes infratores que cometem o crime de falsa identidade estão sujeitos à aplicação do artigo 307 do Código Penal, atribuindo uma pena de detenção de três meses a um ano ou multa, se o fato não constituir elemento de crime mais grave, para aqueles que atribuírem a si mesmo ou a terceiros a falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem.

Extorsão: muitas vítimas dos vazamentos dos dados pessoais estão sujeitas a extorsão, uma vez que os criminosos ameaçam o compartilhamento dos dados pessoais em troca de vantagens financeiras ou pessoais.

Segundo o Código Penal, a extorsão está interligada ao constrangimento de alguém, mediante violência ou grande ameaça, com o intuito de obter para si ou para alguém vantagem econômica, a fazer, tolerar que se faça ou deixe de fazer alguma coisa. A pena atribuída a este crime é de reclusão, de quatro a dez anos e multa. Associa-se também ao vazamento dos dados pessoais, a extorsão indireta, prevista no mesmo Código em seu artigo 160, pois exigir ou receber como garantia de dívida, abusando da situação de alguém, documento que pode dar causa a procedimento criminal contra a vítima ou contra terceiro, atribui-se uma pena de reclusão de um a três anos e multa.[13]

[13] SANTOS, Juarez Cirino dos. Direito Penal – Parte Geral, 3º edição. Curitiba: Editora Lumen Juris, 2008

Falsificação de documentos: os dados obtidos com as informações que foram compartilhadas de forma indevida, ocasionam na falsificação de documentos. Em relação aos documentos particulares, falsificar o documento todo ou em parte ocasiona ao infrator uma pena de reclusão de um a cinco anos e multa. Tratando-se de documentos públicos, são aplicadas penas de reclusão de dois a seis anos e multa.

Quebra de acordo de confidencialidade: se o vazamento de dados ocorrer em uma organização, resultará em uma quebra de acordo de confidencialidade ou até mesmo em um descumprimento contratual que ocasionará na aplicação de uma multa conforme previsto em Contrato ou no Termo de Confidencialidade.

Phishing: método em que alguns recursos servem como "iscas", sem que haja solicitação, para atrair que os consumidores sejam alvo de golpes cibernéticos, obtendo informações de usuários da internet. O *phishing* se distingue do *spam,* pois o primeiro invade dados de quem abre e reabre mensagens, enquanto o segundo visa oferecer um produto ou serviço.

Spooting: mascarar um usuário através da "camuflagem" do seu endereço de IP. Assim, criminosos produzem um IP falso, acreditando o consumidor que está utilizando uma fonte confiável, isto é, utilizando o site verdadeiro da empresa. As vítimas, por si, inserem seu CPF, RG, nome completo e endereço equivocadamente.

Ransomware: invasão de um sistema de um fornecedor de produto ou serviço por parte de um agente infrator, impedindo que o usuário tenha qualquer tipo de controle, tratando-se de um sistema perigoso para empresas e serviços públicos que dependem de sistemas de rede integrada para exercer suas atividades. *Ransom* em inglês significa a quantia paga a um sequestrador como resgate, desta forma, os invasores cobram o resgate para liberação do sistema.

Invasão à privacidade: invasão à privacidade significa o acesso não autorizado a contas ou dados pessoais de um indivíduo, com a intenção do cometimento de fraudes ou roubo de informações.[14]

[14] CRESPO, MARCELO XAVIER DE F. *CRIMES DIGITAIS*. EDITORA SARAIVA, 2011.

Existem quatro formas de invasão à privacidade: (i) vigilância: envolve o uso de câmeras ou dispositivos para monitorar as atividades de um indivíduo sem seu consentimento; (ii) *hacking* e roubo de identidade: invasão para roubo de dados; (iii) fotografia intrusiva: tirar fotos ou gravar vídeos intrusivos sem seu consentimento; (iv) publicação de informações privadas: publicação de dados não autorizados de informações privadas de uma pessoa.

As consequências por invasão à privacidade consistem em danos à reputação, já que, dependendo do que for compartilhado, as informações ocasionariam prejuízos a imagem do indivíduo perante a sociedade; perda financeira, pois o agente infrator poderia usar as informações roubadas para fins fraudulentos; sofrimento emocional; ações judiciais, já que, quem teve sua privacidade violada poderá ajuizar ação judicial buscando indenização por danos morais e materiais na esfera cível.[15]

As dicas para se proteger de invasão de privacidade são o uso de senhas fortes de difícil descoberta, monitoramento das contas, uso das configurações de privacidade, cautela com os dados pessoais, evitar utilizar Wi-Fi público ou redes abertas, dentre outros.

Cavalo de troia: trata-se de um mecanismo que oculta um *malware* em um arquivo que aparenta ser normal. Este mecanismo controla o computador de um usuário, roubando dados e inserindo outro *malware* no computador das vítimas. Afeta não somente computadores, como também dispositivos móveis. Os agentes criminosos colocam o cavalo de troia em mercados de aplicativos piratas para que usuários façam seu download.

Malware é todo tipo de software malicioso que ocasiona prejuízo, danificando sistemas, trazendo consequências financeiras negativas, interceptando dados etc.

O Cavalo de Troia possuí subdivisões, conforme abaixo:

[15] GALVÃO, Fernando. Direito Penal, Parte Geral – 5º edição. São Paulo: Saraiva, 2013.

- Cavalo de Troia de Porta dos Fundos: é criado uma “porta dos fundos” no computador do usuário, permitindo o acesso à máquina pelo invasor, a qual controla, carrega dados roubados, podendo fazer download de outro malware no computador.

- Cavalo de Troia de Acesso Remoto: concede ao invasor controle total do computador.

- Cavalo de Troia Downloader: responsável por fazer o download de outros conteúdos no computador infectado como partes adicionais de malware.

- Cavalo de Troia Infostealer: roubar dados do computador infectado.

- Cavalo de Troia de Ataque de DDos: execução de ataques de negação de serviço distribuído (DDos, Distributed Denial of Service) criados para derrubar a rede.

Para se manter protegido, os usuários de internet não devem acessar sites que não sejam seguros, já que a maioria dos programas de segurança para a internet possuem um componente que alerta para riscos de sites perigosos, devem utilizar de senhas complexas, realização de atualizações de softwares de sistemas operacionais assim que as atualizações forem dispostas pelo provedor de software, manutenção das informações pessoais em segurança com os firewalls.

***Worms*:** programa malicioso classificado como malware, atuando através de propagação em massa, criando cópias de si mesmo, infectando outras máquinas por meio do uso compartilhado de rede, tendo um alcance muito grande.

A melhor maneira de prevenir a ocorrência desses crimes citados ocasionados por vazamentos de dados pessoais, seria a criação de um Programa de *Compliance* pelas empresas voltado para obtenção de tratamento de dados pessoais, regulando as boas práticas da governança, bem como, o tratamento adequado para o sigilo e segurança de dados, mitigando possíveis riscos futuros do tratamento, coleta e armazenamento de dados.

2. PECULIARIDADES

2.1. SUJEITOS DOS CRIMES CIBERNÉTICOS

O agente que pratica os crimes cibernéticos seria qualquer pessoa comum sem grandes conhecimentos técnicos sobre informática, bem como, aquela pela qual possui informações técnicas que lhe possibilitam praticar condutas ilícitas mais facilmente.

Há dois conceitos de sujeitos usualmente reconhecidos, os denominados *hackers* – praticam ações lícitas com base nos conhecimentos tecnológicos que possuem e os *crackers* [16]– indivíduos que, geralmente, possuem a mesma cognição do que os *hackers*, porém que atuam ilicitamente.

Os *hackers* são pessoas que tem habilidades notórias de informática, utilizando-as para descobrir falhas de segurança em sistemas, dispositivos e redes de computadores para o desenvolvimento de soluções de tais falhas, não sendo criminosos. As empresas contratam os *hackers* para detectar possíveis brechas nos sistemas para desenvolvimento de alternativas mais seguras antes que os cibercriminosos tirem proveito destas vulnerabilidades. [17]

Os *crackers*, apesar de possuírem a mesma habilidade notória de informática que os *hackers*, eles utilizam destes conhecimentos para praticarem crimes, burlando sistemas operacionais, quebrando códigos de segurança de *softwares*. Desta forma, ambos possuem amplo conhecimento de tecnologia, porém, atuam de forma divergente: os *crackers* ilegalmente e ilicitamente e os *hackers* legalmente e de forma lícita.

Através do IP (*Internet Protocol*) é possível identificar tais agentes, pois o IP é um número pelo qual o computador detém quando alguém se conecta à internet, ocasionando a identificação do computador, promovendo o envio e recebimento de

[16] McClure, Stuart, et al. Hackers expostos: segredos e soluções para a segurança de redes. Disponível em: Minha Biblioteca, (7th edição). Grupo A, 2013.
[17] BARRETO, Alessandro Gonçalves; BRASIL, Beatriz Silveira. Manual de Investigação Cibernético à luz do Marco Civil da internet. Rio de Janeiro: Bransport, 2016.

dados, já que é constituída uma identidade virtual que fornece o perfil do usuário, tornando-se reconhecido o usuário como *hacker* ou *cracker.*

O sujeito ativo do crime cibernético, portanto, é todo aquele que comete a conduta ilícita. Sujeito passivo é reconhecido por ser o indivíduo que tenha um bem jurídico lesado por ações cometidas através de aparelhos eletrônicos, cabendo ser o papel de pessoa jurídica ou física.

A problemática envolvendo os sujeitos envolvidos nos crimes cibernéticos é o reconhecimento da autoria de quem praticou determinada conduta, pois tais indivíduos não se utilizam da sua identificação real, pois se passam por outra pessoa, a partir do momento que se utilizam de suas senhas pessoais. Por exemplo, ao se utilizar de uma rede de computadores, o usuário não conseguirá ser identificado, apenas o IP da máquina.

O IP é um número que todos os computadores possuem e através do provedor é permitido acessar à rede e fornece aos usuários um número de IP para sua conexão. Requisitando o número do IP, o provedor poderá fornecer acesso a informações sobre aquele usuário.

Desta forma, independentemente da identificação, os sujeitos ativos utilizam-se de sua inteligência para acessar outras máquinas ou da internet, como é o caso dos *hackers* e *crackers.*

Grande parte dos crimes digitais ocorrem em razão do despreparo das autoridades investigativas, e essencialmente a difusão de técnicas, banalização e instrumentos para aplicabilidade de golpes. Muitos dos criminosos digitais não praticariam crimes do mundo real, justamente por existir uma falsa sensação de anonimato e despreparo das autoridades em investigarem delitos.

Apesar de não existirem consensos entre o perfil do criminoso digital, pesquisas empíricas apontam que o perfil desses indivíduos indica jovens, do sexo masculino de faixa etária de 16 e 32 anos, com inteligência acima da média com sentimento de anonimato.

Por fim, além das expressões do *hacker* e *cracker*, uma série de denominações em outras vertentes são conhecidas como:

Carders: estelionatários especializados em fraudes de cartões;

Phreakers: conhecidos por ser os hackers da telefonia, os mesmos realizam interceptações, paralisam serviços e utilizam a telefonia em nome de terceiros;

White Hats: hackers éticos que utilizam das suas habilidades para o fortalecimento da segurança do sistema;

Black Hats: *crackers* são os indivíduos que possuem grandes conhecimentos em tecnologia para prática de atividades criminosas;

Após a identificação dos sujeitos e ao conceituar os crimes cibernéticos, mostra-se necessário identificar quem tem a competência para julgar tais condutas, ainda mais que a internet não ocupa nenhum espaço propriamente físico.

2.2. COMPETÊNCIA

Jurisdição é o poder de atribuição do Estado para aplicar a lei ao caso concreto para resolução de conflitos.

Competência é a delimitação desta jurisdição, a qual será baseada, conforme artigo 69 do Código de Processo Penal [18]com base no lugar da infração, domicílio ou residência do réu, natureza da infração, a distribuição, a conexão ou continência, a prerrogativa de função e a prevenção.

A regra é a competência ser determinada pelo local pelo qual se consumar a infração, ou no caso de tentativa, pelo lugar onde for praticado o último ato de execução. Em casos pelos quais for iniciada a execução no território nacional e a infração se consumar fora dele, a competência será baseada no último local de execução do Brasil. [19]

Não sendo conhecido o lugar da infração, a competência ficará regulada, subsidiariamente, pelo domicílio ou residência do réu. Destaca-se que nos casos de ações exclusivamente privadas, o querelante fica disposto a preferir o foro de domicílio ou residência do réu, ainda quando conhecido o lugar da infração.

[18] McClure, Stuart, et al. Hackers expostos: segredos e soluções para a segurança de redes. Disponível em: Minha Biblioteca, (7th edição). Grupo A, 2013.
[19] AVENA, Norberto. Processo Penal, 10ª edição. Rio de Janeiro: Forense, 2018.

No caso dos crimes cibernéticos o seu alcance poderá ser mundial, pois não há necessidade da presença territorial para efetuar uma conduta criminosa, já que, o território onde estes tipos de crimes são praticados possuem um caráter abstrato. Os crimes cibernéticos são praticados no denominado “ciberespaço”, o qual é definido como território do ambiente virtual onde os crimes são praticados por meio do uso da internet, pelo qual é ultrapassado os limites territoriais de um país.

Ao refletir sobre ciberespaço, a internet reside em várias jurisdições e as grandes adversidades ao pensarmos sobre crimes digitais consistem na efetiva responsabilidade de determinado território pelo crime cometido e a atribuição do poder de polícia para sanar eventuais problemas.

Ademais, ao refletirmos sobre ciberespaço, não se abrange a um espaço físico, mas trata-se de um meio onde são processadas as informações e destinadas a outro, podendo coincidir ou não, com o lugar de partida e o destinatário das informações recebidas.

Assim, ao determinar uma territorialidade implicaria em um juiz específico julgar e processar um crime informático.

No caso do crime cibernético, a competência é firmada pelo local onde partiu o ato delituoso, local de sede do provedor do site, de forma que, é indispensável a autorização judicial para identificação do IP de onde pode ter partido a ação delituosa e quando identificado, necessário a comprovação de quem, efetivamente, utilizou aquele computador para prática do crime.

Ressalta-se que, quando o provedor do site for internacional, acompanha-se o raciocínio do Código Penal, que determina competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado, quando o último ato de execução for praticado fora do território nacional. Já quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração concluída ou tentada nas divisas de duas ou mais jurisdições, a competência será com base na prevenção.

Quando se aborda acerca de competência, é importante observar qual seria o papel do tempo e do lugar no ciberespaço, como será visto adiante.

2.3. DO TEMPO E LUGAR DOS CRIMES NO CIBERESPAÇO

O ciberespaço não é propriamente um território, o que ganha importância o local da informação, a qual indica o território onde determinado crime foi cometido.

Porém, como os crimes cibernéticos podem ser praticados de forma parcial em diversos países, o *iter criminis* pode ser fragmentado.

Assim, questiona-se qual teoria deverá ser aplicada para ocorrência de delitos: teoria da atividade, da ubiquidade ou do resultado. Segundo a teoria da atividade, o local do crime é determinado pela sua ação ou omissão, ainda que o resultado seja produzido em outra localidade. A teoria do resultado implica em dar importância apenas no local onde foi produzido o resultado propriamente dito. A ubiquidade trata-se de uma mistura das duas teorias, já que, entende que o crime pode ser praticado tanto no local em que foi produzido o resultado quanto no lugar da conduta.[20]

O Direito Brasileiro em si, adota a Teoria da Ubiquidade,[21] havendo a aplicabilidade do artigo sexto e sétimo do Código Penal, informando que “o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado” e o sétimo aborda a extraterritorialidade onde são abordados crimes cometidos fora do território nacional.

Na internet, nem sempre é possível identificar o local onde está sendo praticado a conduta delituosa. No Brasil, muitas vezes alguns sites são identificados pelo prefixo “br”, significando que o site está registrado no Brasil, fator determinante para reconhecimento da origem do site. Porém nos casos internacionais, o Código Penal é determinante a competência do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.

Outro desafio a ser superado é o conflito de competência, já que, delitos desta natureza deverão ser analisados alguns critérios, como: local onde se encontra o sujeito ativo e passivo do crime, o local do servidor ou ainda, identificar casos pelos quais não é possível estabelecer onde ocorreu a infração, pois foi ocorrida em ambiente que não possui lugar definido.

[20] LOPES JR., Aury. Direito Processual Penal. 16. ed. São Paulo: Saraiva, 2019.
[21] Rangel, Paulo. *Direito Processual Penal*. Disponível em: Minha Biblioteca, (30th edição). Grupo GEN, 2023

3. CONDUTAS INFORMÁTICAS QUE PODEM CARACTERIZAR CRIME

A seguir serão listados uma série de condutas informáticas que contribuem para prática do crime digital por ofenderem a informática e o sistema digital:

Acesso ilegítimo: trata-se do acesso sem qualquer tipo de autorização em que geralmente ocorre em sistema informático, conceituado como um dispositivo isolado ou grupo de dispositivos interligados em que são desenvolvidos o tratamento automatizado de dados. Para legislar sobre o tema, as convenções internacionais acreditam que seja necessário indicar que o acesso teve intenção ilegítima. Já no Brasil, parte da doutrina acredita que o acesso ilegítimo ganha *status* de tipo penal essencialmente com o advento da Lei n° 12.737/2012 enquanto para outros autores, o Brasil pune com o artigo 154-A do Código Penal somente pelo fato da ocorrência da invasão.

Interferência de dados: faz referência a intenção ilegítima do agente de danificar, apagar, deteriorar, alterar ou eliminar dados informáticos. Se da invasão ocorre dano, incide o artigo 154 – B do Código Penal, nos termos da nova Lei n° 12.737/2012. Se não há invasão por parte do agente, mas apenas causa dano informático, é considerado o Código Penal de 1940 na subsunção do artigo 163.[22]

Interceptação ilegítima: Utilização de meios técnicos, em transmissões não públicas, para interceptação e captura de informações e dados, punida no Brasil pelo artigo 10 da Lei n° 9.276 de 1996.

Burla informática: conhecida como sabotagem informática, é o ato intencional e ilegítimo do qual origina o dano mediante alteração, introdução, eliminação de dados informáticos ou intervenção no sistema informático que almeja benefício econômico.

Envio de mensagens não solicitadas: é o famoso *spam*, em que são enviadas mensagens não solicitadas por qualquer meio, causando prejuízo de alguma forma.

[22] JUNQUEIRA, Gustavo, VANZOLINI, Patricia. Manual de Direito Penal. v. 1. 7.ed. São Paulo: Saraiva, 2021.

Uso indevido da informática: o uso indevido de sistemas informáticos, com prejuízo a cessionária do sistema ou a titular, causando prejuízo ao seu funcionamento ou a outras pessoas que utilizam do sistema.

Pichação informática: conhecido também como *defacement*, trata-se de condutas que alteram o *layout* e páginas na *web*, promovendo a pichação através da inclusão de textos ou figuras inapropriadas no código do *site* (html) ou no banco de dados. Parte da doutrina acredita se tratar crime de dano ou concorrência desleal.

Furto de dados ou vazamento de informações: é a cópia indevida de dados confidenciais. A conduta é análoga a "interceptação telemática" prevista na Lei 9276 de 1996 e outros doutrinadores acreditam na cópia indevida na concorrência desleal, ato ilícito identificado no artigo 195 da Lei 9.279 de 1996.

Uso abusivo de dispositivos: é o comportamento de produzir, vender, importar ou distribuir dispositivo ou programa informático para prática de condutas criminosas ou senhas, código de acesso e dados informáticos que promovem o acesso indevido a sistemas.

Falsidade ou fraude informática: é a produção de dados não autênticos com o objetivo que sejam utilizados legalmente como se fossem autênticos através da alteração de dados informáticos.

Após elencar algumas das condutas que contribuem para prática do crime digital, abaixo no próximo tópico constam os artefatos para sua prática. [23]

4. ARTEFATOS PARA A PRÁTICA DE CRIMES DIGITAIS

Existem técnicas que podem estar associadas e são meios para a prática de crimes digitais, conforme abaixo:

Vírus: programa de computador que altera dados ou sistemas, destruindo e alterando arquivos e programas para execução de funções em um sistema computacional ou dispositivo informático.

[23] ZAFFARONI, E. Raúl et al. Direito Penal Brasileiro. v. II, t. II. Rio de Janeiro: Revan, 2017.

Backdoor: código malicioso que permite fácil acesso a um sistema ou a uma máquina, burlando os mecanismos de autenticação através de um meio não documentado de acesso ao sistema.

Exploração do Kernel: Kernel é o núcleo de sistemas operacionais em que o criminoso digital se torna invisível a programas de segurança da informação, sistema de detecção de intrusos e etc.

SQL *injection*: altera parâmetros ou instruções que são executadas sobre uma ou mais tabelas de banco de dados através da linguagem *Structured Query Language* (“SQL”), possibilitando o acesso indevido a informações.

Rainbow table: quebra de senhas criptografadas.

Brute force: técnica para quebra de senhas e acesso a sistemas tentando todas as combinações possíveis.

Ataque de dicionário: teste de palavras do dicionário que podem fazer parte da composição de uma senha.

DNS poisoning: alteração dos endereços de resolução *DNS (Domain Name System)* de um serviço, direcionado a um acesso para um site falso.

Trojan: conhecido por ser “cavalo de troia” é um código malicioso geralmente ocultado em outro *software* que, quando instalado, provoca um sistema vulnerável no computador ou mesmo explora vulnerabilidades já existentes. Por meio desta técnica, é possível se tornar administrador e copiar informações confidenciais de um sistema.

Spyware: programa malicioso instalado em aplicativo baixado de fonte duvidosa, cuja função é coletar informações do usuário e enviá-las ao destinatário. As informações coletadas geralmente fazem referência a hábitos de consumo, informações de navegação e etc.

Sniffing: técnica consiste em capturar pacote de dados em que é possível realizar a interceptação do que é trafegado em uma rede.

Keylogging e screenlogging: artefato que monitora tudo que é digitado pela vítima, através da captura do teclado, armazenado em arquivo e remetido pelo atacante.

Connection back: é uma técnica pela qual a vítima é conectada diretamente com o atacante, o qual passa a ter acesso a máquina da vítima.[24]

Com a utilização dos artefatos que são os meios para a prática das condutas ilícitas, surgem os crimes cibernéticos. Porém, os crimes cibernéticos podem estar associados e combinados as diversas vertentes do Direito e as diferentes localidades, razão pela qual é importante estudar acerca do crime digital no âmbito internacional, como será observado abaixo.

5. CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

O Direito da informática pode ser classificado em duas vertentes: Direito Civil da Informática e Direito Penal da Informática.

Direito Penal da Informática é o conjunto de regulamentos e normas com o objetivo de repreender fatos criminosos que atinjam bens informáticos, enquanto o Direito Civil da Informática consiste nos entendimentos jurídicos cíveis vinculadas às relações privativas realizadas por intermédio da tecnologia da informação.

A classificação dos crimes informáticos se distingue conforme o entendimento de alguns autores, [25]como, por exemplo:

Klaus Tiedemann classificou os crimes digitais nos seguintes aspectos:

- *Manipulações:* afeta a saída e a entrada do processamento de dados;

- *Espionagem*: subtração de informações arquivadas;

- *Sabotagem*: destruição parcial ou total de programas

- *Furto de tempo*: utilização inadequada de instalações de computadores por empregados desleais ou estranhos.

Ulrich Sieber:

- *Violação à privacidade*

[24] ROSA, Fabrizio. Crimes de Informática. São Paulo: Bookseller, 2005.
[25] Jesus, Damásio, D. e José Antônio Milagre. Manual de crimes informáticos. Disponível em: Minha Biblioteca, Editora Saraiva, 2016.

- *Crimes econômicos* (*hacking*, espionagem, pirataria em geral, sabotagem e extorsão, fraude)

- *Conteúdos ilegais e nocivos*

- *Outros ilícitos* (contra a vida, crime organizado, guerra eletrônica)

Martine Briat: os crimes informáticos são divididos em:

- *Falsificação de dados dos programas*

- *Uso e acesso não permitido dos sistemas de informática*

- *Manipulação de dados e/ou programas para a prática de delitos já identificado pelas incriminações tradicionais*

Davara: apresenta a seguinte classificação:

- *Utilização de computadores com fins fraudulentos*

- *Acesso aos dados por quem não está autorizado*

- *Manipulação de dados contidos nos arquivos ou suportes informáticos alheios*

- *Introdução de programas em outros computadores para destruir informações*

- *Agressão à privacidade mediante o uso e processamento de dados com fim destinado ao autorizado*

Rovira del Canto: possui uma visão mais ampla da classificação dos crimes digitais:

- *Infrações à intimidade*

- *Ilícitos econômicos e de comunicação de conteúdos ilegais ou perigosos*

Porém, de todas as classificações expostas, a que mais se aproxima da realidade é a proposta pela diferença entre crimes informáticos pelos quais a informática é o meio para prática de agressões a bens jurídicos protegidos pelo Direito Criminal e crimes digitais pelo qual a informática é o bem jurídico protegido.

Desta forma, os crimes digitais são divididos em: [26]

a) **Crimes informáticos impróprios:** tecnologia da informação é o meio utilizado para agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Desta forma, trata-se daqueles crimes que já são tipificados no ordenamento jurídico. Alguns exemplos: a) falsa identidade ideológica; b) violação de direitos autorais etc. Desta forma, a internet é o meio para prática do crime e os efeitos repercutem na vida real.

b) **Crimes informáticos próprios:** o bem jurídico ofendido é a tecnologia da informação em si, de forma que, muitas práticas não poderiam ser enquadradas criminalmente. Assim, o objetivo é o sistema computacional em si, de forma que a prática e a consumação do fato apenas ocorrem no meio digital, como nos casos da invasão, modificação/alteração de *software* ou *hardware* de computadores.

c) **Crimes informáticos mistos:** a legislação protege tanto o bem jurídico informático, como a inviolabilidade de dados, como outro bem jurídico.

d) **Crimes informáticos mediato ou indireto:** é um crime digital praticado que traz como consequência um delito não informático consumado ao final.

Independentemente da classificação e do tipo de crime cibernético cometido, a prevenção da ocorrência de tais ilícitos é o principal instrumento de proteção à sociedade contra-ataques cibernéticos. Dentre os principais instrumentos preventivos, a estruturação de um programa de Compliance atua como um importante aliado para prevenção de tais crimes.

[26] TAVARES, Juarez. Teoria do Injusto Penal. 6.ed. São Paulo: Tirant Brasil, 2019.

CAPÍTULO IV

DA PROTEÇÃO DO CONSUMIDOR EM FACE DOS MEIOS CIBERNÉTICOS DE CONSUMO

1. DO COMPLIANCE

1.1. CONCEITO

O Compliance é a adoção de procedimentos internos [27]com o intuito de tornar determinada organização em conformidade com as leis, normas e regulamentos vigentes, garantindo um ambiente corporativo forte. Trata-se de um controle preventivo que promove com que a organização atue em conformidade com as leis e a forma ética de como a organização interage. Assim, há uma estrutura capaz de conter políticas, normas internas, códigos de ética e de conduta que mapeiam riscos para prevenção e respostas aos incidentes, monitorando pessoas, recursos e processos, desempenhando um papel importante que evita conflitos de interesses, análise do impacto da reputação da empresa e da perda de negócios em fraudes.

Para o Conselho Administrativo de Defesa Econômica, Compliance é “um conjunto de medidas internas que permite prevenir ou minimizar os riscos de violação às leis decorrentes de atividade praticada por um agente econômico e de qualquer um de seus sócios e colaboradores.”[28]

Os pilares do Compliance consistem em um suporte da alta administração, a avaliação de riscos, a implementação de um código de conduta e políticas de Compliance, com a adoção de todas políticas a serem adotadas em uma empresa, a criação de controles internos assegurando que os riscos sejam minimizados, realização de treinamento e comunicação, promovendo uma comunicação aos colaboradores dos objetivos do Compliance, criação de canais de denúncia sobre

[27] FRANCO, Isabel. *Guia Prático de Compliance*. Disponível em: Minha Biblioteca, Grupo GEN, 2019.
[28] MIRAGEM, Bruno. A Lei Geral de Proteção de Dados (Lei 13.709/2018) e o Direito do Consumidor. Revista dos Tribunais, São Paulo, v. 108, n. 1009.

violações as diretrizes do Código de Ética e de Prática de Conduta, realização de investigações internas, já que a empresa precisa tomar conhecimento e investigar qualquer tipo de comportamento antiético existente, promoção de uma *due diligence*, ou seja, avaliação do histórico de cada um dos fornecedores, representantes e distribuidores, antes de estabelecer uma relação contratual, preparo de uma auditoria e monitoramento, já que, é necessário monitorar se as pessoas estão comprometidas com as condutas adotadas pelo Programa de *Compliance* e por fim, a promoção da diversidade e da inclusão, pois não existe este programa sem respeito e igualdade entre os indivíduos.

Como dito anteriormente, o Compliance possui uma atuação preventiva, e quando se reflete sobre a sua atuação, é importante que as empresas possuam diferentes formas de se positivar a prevenção corporativa de ilícitos com o intuito de evitar a prática de crimes cibernéticos.

O Compliance digital é o mais apropriado para garantir a cibersegurança das corporações, pois é um mecanismo que garante a regulação dos processos para atender a normas e leis que incidem sobre o digital, garantindo um pleno tratamento às informações no ambiente digital. [29]

As três bases que os fundamenta é a autorregulação regulada, isto é, a regulação própria da empresa; a governança corporativa responsável por incentivar, monitorar e dirigir as empresas e suas relações entre sócios, diretoria, órgãos de fiscalização e conselho administrativo; e promoção de uma responsabilidade social e ética empresarial, já que, são tomadas ações para melhorar o bem-estar da sociedade e a promoção de princípios e valores transmitidos através da cultura interna empresarial.

Os princípios que orientam o Compliance e a ocorrência do vazamento de dados pessoais são:[30]

Princípio da Vulnerabilidade

[29] TASSO, Fernando Antonio. A responsabilidade civil na Lei Geral de Proteção de Dados e sua interface com o Código Civil e o Código de Defesa do Consumidor. Cadernos Jurídicos, São Paulo, v. 21, n. 53, jan./mar. 2020.

[30] ROCHA, Gustavo. Compliance digital e a Lei Geral de Proteção de Dados: LGPD. ADV Advocacia Dinâmica: informativo semanal, Rio de Janeiro, n. 15, abr. 2019.

O princípio da vulnerabilidade é um dos mais relevantes do CDC por reconhecer a fragilidade e o estado de risco do sujeito, estabelecendo, assim, um regime diferenciado para reequilibrar os poderes na relação de consumo.

A vulnerabilidade é identificada a partir do momento que o consumidor possui menos informações que o fornecedor, ou seja, tecnicamente é inferior e fática, por deter de menos recursos intelectuais e econômicos para reparação dos prejuízos oriundos do inadequado tratamento de dados.

Dentre esta vulnerabilidade, os dados pessoais também são informações vulneráveis a partir da sua dupla dimensão: (i) tutela de personalidade ao consumidor contra a tudo que sirva de ameaça a sua personalidade em virtude da coleta, processamento, utilização e circulação dos dados pessoais; (ii) responsabilidade do consumidor da garantia de controlar o fluxo de suas informações em sociedade.[31]

As duas dimensões em conjunto propiciam à autodeterminação informativa do consumidor e o controle objetivo do tratamento dos dados pessoais.

Quando é identificado o vazamento dos dados pessoais de um consumidor, identifica-se que a sua vulnerabilidade não foi respeitada, já que o mesmo foi vítima deste tipo de ocorrência, violando consequentemente o princípio da vulnerabilidade que deveria ser respeitado.[32]

Princípio da Privacidade:

Os dados pessoais, ao deixarem de ser sigilosos, acarretam a privacidade das pessoas, direito fundamental inviolável garantido em Constituição.

Princípio do Consentimento:

Quando são coletados dados pessoais pelas empresas, muitos dos usuários dos produtos e serviços adquiridos, assinam Termos de Consentimento. Nos casos pelos quais as informações pessoais ou sigilosas são compartilhadas com terceiros, viola-se a intimidade e o princípio do consentimento, uma vez que os

[32] ARTESE, GUSTAVO. COMPLIANCE DIGITAL: PROTEÇÃO DE DADOS PESSOAIS. IN: CARVALHO, ANDRÉ CASTRO ET AL. (COORD.). MANUAL DE COMPLIANCE. RIO DE JANEIRO: FORENSE, 2019.

consumidores inicialmente consentiram que compartilhariam de sua intimidade juntamente com a fornecedora de produtos/prestadora de serviços, que deveria ter a responsabilidade de guardar sigilo, não respeitando com o consentimento que também havia sido assinado.

Princípio da Transparência: todas as organizações possuem como responsabilidade a transparência sobre suas práticas de processamento e coleta de dados pessoais. Quando há o vazamento dos dados pessoais, as organizações não expressam detalhadamente seus processos de manuseio de dados pessoais. Ou seja, não há transparência e confirmação que todo procedimento de manuseio dos dados pessoais foi feito de forma confidencial.

Princípio da Confidencialidade: as fornecedoras de produtos e prestadoras de serviços, utilizam-se da ideia da utilização do Termo de Confidencialidade abordado na LGPD, que obrigam as empresas elaborem o documento garantindo sigilo entre as partes, já que, a quebra de sigilo ocasiona a realização de processos legais contra quem praticou o vazamento e divulgou as informações.

Princípio da Finalidade: os dados pessoais possuem finalidades específicas e legítimas, de forma que, o tratamento para manuseio dos dados pessoais deverá ser informado previamente ao titular, pois uma vez que há um desvio da finalidade dos dados obtidos, sobretudo no campo da esfera consumerista, há uma violação do princípio da finalidade.

Princípio da Adequação: os dados coletados necessitar estar adequados de acordo com a finalidade do tratamento previamente informado ao titular, de acordo com o contexto do tratamento.

Princípio da Necessidade: o princípio da necessidade prevê que apenas as informações mínimas necessárias deverão ser coletadas, já que o excesso de dados são indispensáveis e colocam os consumidores em risco, caso sejam divulgados de forma inapropriada.

Princípio da Segurança: é a necessidade de proteção dos dados de acessos não autorizados e de situações acidentais. A utilização de técnicas e meios que proporcionem a segurança destes dados são essenciais para que a segurança dos consumidores não seja violada.

1.2. PREVISÃO LEGAL

O Compliance e questões relacionadas às Proteções aos Dados Pessoais estão previstos essencialmente na Lei Anticorrupção n° 12.846/13 e Lei Geral de Proteção de Dados Pessoais n° 13.709/2018.[33]

Outras leis também vinculadas ao Compliance que podem ser citadas são às Leis de Acesso à Informação n° 12.527/11, Lei n° 9.613/98 de Lavagem de Dinheiro etc.

A Lei Anticorrupção visa, essencialmente, fazer com que as empresas fossem responsabilizadas, de maneira objetiva, pelos atos ilícitos contra a Administração Pública. A Lei Geral de Proteção de Dados, assegura a privacidade do indivíduo, protegendo os dados pessoais, à privacidade e a liberdade, garantindo as pessoas um maior controle em relação às suas informações pessoais.

2. DO TRATAMENTO DOS DADOS SENSÍVEIS

Dados sensíveis são todas as informações pessoais que, quando expostas ao público, poderão causar danos à privacidade e segurança do atingido, como, por exemplo, documentos de identidade, dados relativos à saúde do paciente, informações financeiras, dentre outros.

Para que haja o adequado tratamento das informações sensíveis, alguns princípios deverão ser seguidos, como o da Segurança, evitando acessos não autorizados ou perdas de informações confidenciais; o Princípio da Necessidade visando limitar o mínimo de informações necessárias em um contexto para atingir determinada finalidade; o Princípio do Consentimento em que o titular dos dados consinta explicitamente acerca do tratamento dos dados sensíveis (exceto no casos de cumprimento de obrigação da Lei); e o da Finalidade, pois todos os dados sensíveis, quando obtidos, deverão ter um objetivo específico.

As técnicas adotadas para o Tratamento de Dados consistem na realização da criptografia, impedindo que os dados sejam acessíveis mesmo em caso do

vazamento dos mesmos, pois tem o seu acesso impedido através de uma chave de segurança; monitoramento contínuo que garante a conformidade dos dados; auditoria; técnicas de anonimização para remoção e alteração de dados para que impeça a identificação do titular de dados; pseudonimização que substitue os identificadores por pseudônimos, removendo os identificadores pessoais repondo por valores de marcadores de substituição, etc.

2.1. A PROTEÇÃO DE DADOS DO CONSUMIDOR

Os dados pessoais são as informações relativas à identificação de um indivíduo que geralmente são fornecidas em um cadastro, como o RG, CPF, gênero, data de nascimento, dentre outros. Alguns dados, por mais que não sejam de conhecimento da população, também atuam como dado pessoal, exemplos: prontuário de saúde, endereço de IP, hábitos de consumo, retrato em fotografia etc.

A Lei que dispõe sobre este tema é a Lei Geral de Proteção de Dados Pessoais (“LGPD”) de n° 13.709 de 14 de agosto de 2018, destinada a União, Estados, Municípios e Distrito Federal. A mesma informa que na Lei há o tratamento de dados pessoais, inclusive nos meios digitais, referentes a pessoa física de direito público e privado ou pessoa natural, objetivando a proteção dos direitos fundamentais de liberdade, privacidade e o desenvolvimento da pessoa natural.

Assim, dado pessoal é a informação relativa tanto a pessoa natural, quanto a pessoa identificável, como nos casos de endereço de IP, geolocalização (GPS) e dentre outros.

A proteção dos dados pessoais tem como fundamentos a inovação, desenvolvimento econômico/tecnológico, respeito à privacidade, a inviolabilidade da imagem/honra/intimidade, livre iniciativa, livre concorrência, defesa do consumidor, direitos humanos e a autodeterminação informativa.

A LGPD menciona além do conceito de dados pessoais, os dados pessoais sensíveis que se tratam de informações sensíveis de crianças/adolescentes ou dados de pessoas naturais específicos quanto a sua origem racial ou étnica, convicção religiosa, opinião política, vinculação a sindicato, organização de caráter religioso, filosófico ou político, dado referente à saúde ou vida sexual, genético ou biométrico.

Conceitua-se, através da LGPD, o (i) titular como pessoa natural a quem se destina os dados pessoais; (ii) controlador como pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais, ou seja, é a empresa ou pessoa que coordena e define como o dado pessoal será tratado, desde sua coleta até a sua eliminação e (iii) o operador como pessoa natural/jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, tratando-se de pessoa ou empresa que trata e processa os dados pessoais sob as ordens do controlador. Destaca-se que o controlador tem responsabilidade sobre o operador, para que o tratamento de dados pessoais seja realizado conforme as diretrizes da lei. [34]

Nos casos dos tratamentos de dados pessoais das relações de consumo, inicialmente há a coleta de dados, pelos quais a empresa ou o controlador do banco de dados necessita obter as informações pessoais do consumidor, coletado pelo próprio consumidor através de compras online, preenchimento de contratos, transações comerciais ou por outras fontes.

As principais fontes de dados dos consumidores são: sorteios e concursos, censos e registros públicos, transações comerciais (cadastros dos consumidores no momento da compra ou da realização do serviço ou através de cartões fidelidade,), pesquisas de mercados, tecnologias de controle da internet e comercialização/cessão de dados.

Outra coleta de dados, especificamente no campo da internet, ocorre através da interação entre o consumidor e fornecedor pré contratualmente e antes que ocorra propriamente uma transação comercial virtual, já que podem ser realizadas por meio de tecnologias de controle da internet, como os cookies, os quais permitem checar a localização do usuário e a verificação de todos os seus movimentos online.

Cookies são marcadores digitais que são automaticamente inseridos por websites visitados responsáveis pela identificação e memorização dos movimentos do consumidor. Quando o computador está vinculado aos dados do indivíduo e com a divulgação das informações, esses marcadores ameaçam a privacidade do indivíduo, rastreando-os em outros sites. É necessário o consentimento prévio do usuário para qualquer tipo de coleta de informações, havendo uma obrigatoriedade

[34] AFONSO, Luiz Fernando. Responsabilidade civil dos provedores de internet e as relações de consumo.
São Paulo: Revista dos Tribunais, 2018.

no fornecimento de informações claras e completas sobre os objetivos do processamento de dados.

A legitimidade da coleta de dados está condicionada ao consentimento do consumidor ou previsão legal que autorize a coleta, uma vez que, seus dados serão processados.

A segunda fase é pautada pelo processamento de dados, os quais são submetidos a técnicas para transformações destes dados em informações úteis à empresa.

Algumas destas técnicas seriam a *Datawarehouse*, *Data mining*, *Online Analyticial Processing*, *Profililing* e *Scoring*. [35]

Datawarehouse significa depósito de dados, sistema informatizado responsável por armazenar diversas quantidades de informações que estão integradas orientadas pelo sujeito, não volátil, de forma que, os dados armazenados não sofrem alteração, nem podem ser cancelados. Trata-se da organização de dados de sistemas operativos e heterogêneos de acordo com a sua relevância para tomada de decisões estratégicas.

Data mining é a transformação de dados em informações úteis e valiosas para as empresas. Seu objetivo é a extração de inteligência significativa e de padrões de conhecimento, partindo de um banco de dados.

Online Analytical Processing (“OAP”), ferramenta que prevê tendências e prognósticos a partir da análise de uma determinada base de dados, de forma dinâmica e multidimensional.

Profiling é um registro baseado na reunião de inúmeros dados sobre uma pessoa, com a finalidade de se obter uma imagem detalhada visando à previsibilidade de padrões de comportamento, gostos, hábitos de consumo etc. A construção de um perfil pessoal possibilita a tomada de importantes decisões a respeito dos consumidores por parte das empresas.

Scoring é o sistema de avaliação que objetiva identificar os consumidores que possuem maior valor as empresas para que os mesmos sejam alvo de promoções para fidelização dos clientes.

[35] ARTESE, Gustavo. Compliance digital: proteção de dados pessoais. In: CARVALHO, André Castro et al. (coord.). Manual de compliance. Rio de Janeiro: Forense, 2019.

A terceira fase corresponde a difusão/cessão, identificando a legitimidade da difusão dos dados obtidos.

O manuseio inadequado do tratamento dos dados pessoais configura-se uma fragilidade aos consumidores, que poderão ser vítimas da violação de seus direitos, bem como, alvo de crimes cibernéticos decorrentes de vazamento de dados pessoais. Por este motivo, o Compliance e a LGPD devem ser utilizados como instrumentos essenciais para o combate aos crimes cibernéticos.

3. O PAPEL E A RESPONSABILIDADE DO COMPLIANCE NA PROTEÇÃO DE DADOS PESSOAIS

3.1. RESPONSABILIDADE CIVIL DOS AGENTES DE TRATAMENTO DE DADOS

O controlador é a pessoa jurídica ou natural, de direito público ou privado, a quem competem o tratamento de dados pessoais, responsável por elaborar um Relatório de Impacto à Proteção de Dados Pessoais (RIPD) no que se refere as operações de tratamento dos dados sensíveis e aos segredos das empresas. É de sua responsabilidade preocupar-se com todas as pessoas que poderão tratar os dados em seu nome; operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, sendo que ambos são agentes de tratamento de dados, os quais são responsáveis pela manutenção do registro das operações de tratamento de dados pessoais que efetuarem.[36]

O encarregado pelo tratamento dos dados pessoais é uma pessoa recomendada pelo controlador para atuar como canal de comunicação entre os titulares dos dados, a Autoridade Nacional de Proteção de Dados e o controlador. Suas principais responsabilidades são: tomar as devidas providências quanto ao recebimento de comunicações da autoridade nacional; prestação de esclarecimentos quanto as reclamações e comunicações dos titulares; orientação aos funcionários em relação as práticas a serem tomadas à proteção dos dados pessoais etc.[37]

---

[36] Kleindienst, Ana C. Grandes Temas do Direito Brasileiro: Compliance. Disponível em: Minha Biblioteca, (2nd edição). Grupo Almedina (Portugal), 2019.

[37] Neves, Edmo C. *Compliance Empresarial - o tom da liderança, 1ª edição*. Disponível em: Minha Biblioteca, Editora Trevisan, 2018.

3.2. RESPONSABILIDADE POR DANOS: SOLIDARIEDADE DO CONTROLADOR E OPERADOR

Sobre a responsabilidade solidária no âmbito da LGPD, o controlador e o operador podem ser responsabilizados pelos danos causados solidariamente diante dos titulares dos dados pessoais.

Responde solidariamente o operador quando houver o descumprimento da legislação de proteção de dados ou quando o mesmo não tiver obedecido as normas do controlador. No caso narrado, o operador é equiparado ao controlador. Ademais, os controladores que estiverem diretamente envolvidos no tratamento de dados que foram alvo de danos, respondem solidariamente. Os agentes de tratamento somente não serão responsabilizados quando provarem que o dano é culpa exclusiva do titular dos danos ou de terceiros, que não realizaram o tratamento de dados que lhes é atribuído ou que não ocorreu violação à legislação de proteção de dados pessoais.

3.3. EXCLUDENTE DE RESPONSABILIDADE

Como dito anteriormente, os excludentes de responsabilidade da LGPD são: quando for provado que o dano é culpa exclusiva do titular dos danos ou de terceiros, que não realizaram o tratamento de dados que lhes é atribuído ou que não ocorreu violação à legislação de proteção de dados pessoais.

Entende-se como culpa exclusiva da vítima a divulgação pública dos dados pessoais pelo titular em plataformas digitais; o armazenamento dos dados pessoais de forma insegura como *pen drives* e o mesmo for esquecido em público e etc. Enquanto a culpa por terceiro se refere a pessoa que não se identifique com o operador, titular de dados ou controlador, isto é, pessoa estranha ao tratamento de dados.[38]

Ao refletir sobre excludente da culpa exclusiva de terceiros no que se trata do tratamento ilícito de dados, torna-se impossibilitada a alegação sobre

[38] Viol, Dalila M. *Programas de Integridade e Combate à Corrupção:Aspectos teóricos e empíricos da multiplicação do compliance anticorrupção no Brasil*. Disponível em: Minha Biblioteca, Grupo Almedina (Portugal), 2021.

corrompimento do sistema quando for comprovado que as medidas de segurança adotadas pelo agente de tratamento não foram suficientes.

O caso fortuito e a força maior também são hipóteses de exclusão de responsabilidade no âmbito da tutela dos dados pessoais, sendo possível a aplicação do Código Civil como complemento à LGPD.

3.4. DANO COLETIVO E INVERSÃO DO ÔNUS DA PROVA

A inversão do ônus da prova, no contexto da LGPD, enquadra-se quando o juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação, houver hipossuficiência para fins de produção de prova ou quando a mesma for bastante onerosa.

Identifica-se que o dano poderá ser coletivo tratando-se da proteção de dados pessoais e que o pleito para deparação deste dano poderá ser feito coletivamente através de uma ação judicial, ou seja, a elaboração de uma demanda que atenda um grande número de interessados pela tutela dos dados pessoais.

4. RESPONSABILIDADE CIVIL NAS RELAÇÕES DE CONSUMO E A LGPD

Conforme o artigo 45 da LGPD, tem-se que: “as hipóteses de violação do direito do titular no âmbito das relações de consumo permanecem sujeitas às regras de responsabilidade previstas na legislação pertinente”, ou seja, prevalece o regime de responsabilidade previsto no Código de Defesa do Consumidor, por ser mais protetivo.

4.1. ANPD E PENALIDADES ADMINISTRATIVAS

A Autoridade Nacional de Proteção de Dados **(“ANPD”)** foi criada como uma autoridade de natureza jurídica transitória, em que primeiro momento servirá como órgão da administração pública federal, vinculado à Presidência da República, à partir de alterações e inclusões de vários dispositivos à LGPD.[39]

A ANPD atua de forma pragmática juntamente aos agentes de tratamento, objetivando uma mudança construtiva em relação a proteção de dados. O principal questionamento sobre a ANPD é acerca da sua indispensável autonomia, sendo

[39] Silva, Daniel, C. e José Roberto Covac. *Compliance como boa prática de gestão no ensino superior privado - 1ª edição*. Disponível em: Minha Biblioteca, Editora Saraiva, 2015.

necessária sua desvinculação com outros órgãos para garantir a segurança jurídica de suas decisões.

A referida autonomia no âmbito decisório e técnico fortalece sua atuação, focada na proteção de dados pessoais. O papel da ANPD é preservar o segredo empresarial, o sigilo das informações de forma que tenha prevalência sobre outras entidades e órgãos da administração pública que tenham competências correlatas, pois por ter um caráter transversal à proteção de dados pessoais, deverá ser harmonizada com outras disciplinas jurídicas já existentes, como o caso do direito do consumidor.

É função do artigo 52 da LGPD prever quais são as sanções de cunho administrativo a ser aplicáveis pela ANPD, não impedindo de serem impostas as sanções de caráter civil e penal.

Dentre as penalidades administrativas a serem consideradas, aplica-se a multa e também pode ser imposto ao controlador o bloqueio ou eliminação do banco de dados do infrator das informações pessoais relacionados à infração.

As penalidades administrativas não apenas visam punir o infrator, como também, evitar que os danos decorrentes do incidente possam se agravar, já que o titular dos dados não voltará ao *status quo ante*.[40]

Assim, dentre as penalidades aplicáveis decorrentes do vazamento dos dados pessoais que podem incorrer na ocorrência dos crimes cibernéticos, seriam: advertência, multa simples de até 2% do faturamento da pessoa jurídica do direito privado no seu último exercício limitada a 50 milhões de reais por infração, multa diária, eliminação dos dados pessoais a que se refere a infração, bloqueio dos dados pessoais a que se refere a infração até a sua regularização, proibição total ou parcial do exercício de atividades relacionadas a tratamento de dados, suspensão do exercício da atividade de tratamento de dados pessoais a que se refere a infração pelo período máximo de 6 meses, prorrogável por igual período, até a regularização da atividade de tratamento pelo controlador.

[40] Kleindienst, Ana C. Grandes Temas do Direito Brasileiro: Compliance. Disponível em: Minha Biblioteca, (2nd edição). Grupo Almedina (Portugal), 2019.

Existem algumas medidas sancionatórias para combater o vazamento de dados pessoais:[41]

01. **<u>Recomendação</u>:** a recomendação seria espécie de conselhos fornecidos por profissionais especializados em ilícitos corporativos. Tratam-se de condutas orientadas a serem seguidas, porém que não possuem caráter obrigatório de serem cumpridos, isto é, o seu não cumprimento não enseja na aplicação de sanção prevista em lei.

Exemplo disto é o artigo 9° da Lei 13.303/16, ao dispor que a empresa pública e a sociedade de economia mista adotorão regras de estrutura e prática de gestão de risco e controle interno, as quais deverão ser elaborados e divulgados no Código de Conduta e Integridade, porém, não há dispositivo abordando sobre a aplicação de sanção pela não adoção das recomendações que a Lei posiciona.

02. **<u>Obrigação mediante sanção</u>:** A obrigação mediante sanção é prevista em lei como dever geral da criação de um Programa de Compliance pelas empresas, as quais são aplicadas sanções caso ocorram seu descumprimento.

No Brasil, a Lei de Lavagem de Dinheiro (Lei 9.613/98), em seu artigo 10°, III, demonstra o exemplo de obrigação que deverá ser imposta mediante a aplicação de sanção, pois determina que as instituições financeiras deverão adotar políticas, procedimentos e controles internos compatíveis com seu porte e volume de operações, pois caso contrário, serão aplicadas sanções pelo Conselho de Controle de Atividades Financeiras.

03. **<u>Sanção ou condição de acordo</u>:** a sujeição à fiscalização de programas corporativos de prevenção de ilícitos poderá ser imposta legalmente como condição de acordo.

04. **<u>Exclusão de responsabilidade</u>:** existem leis que criam uma espécie de imunidade para aquelas empresas que possuem um programa de prevenção de ilícitos corporativos, contra consequências administrativas e/ou penais.

[41] Trennepohl, Terence, e Natascha Trennepohl. ESG e Compliance: interfaces, desafios e oportunidades. Disponível em: Minha Biblioteca, Editora Saraiva, 2023.

05. **<u>Interferência na aplicação da sanção</u>:** Os programas de *Compliance* possuem o poder de realizar modificações de acordo com o delito realizado.

4.2. RECEPÇÃO DA LGPD NO AMBIENTE CORPORATIVO:

A recepção da LGPD no ambiente corporativo se inicia à partir do regimento do Protocolo LGPD-BR o qual abrangerá os funcionários, prestadores de serviço, clientes e todos que fizerem parte de uma empresa.

À partir da atuação de profissionais de Compliance, identifica-se o cenário atual da empresa e a problemática envolvida em relação aos dados pessoais das pessoas que estão vinculadas a empresa, juntamente aos ditames da Lei Geral de Proteção de Dados Pessoais. Para isso, é necessário mapear seus processos internos, a forma de governança, as políticas existentes, a tecnologia contratada, o funcionamento de normas e regras internas.

O próximo passo é a avaliação do inventário de dados pessoais da empresa, mapeando se há sistema para utilizar os dados pessoais e como é realizado os tráfegos no sistema.

A auditoria do volume de dados pessoais deverá ser realizada, fazendo uma análise crítica do tratamento de todos os dados pessoais envolvidos, para que sejam filtrados apenas os dados cruciais para o tratamento efetuado pela empresa.

O controle tecnológico sob os dados pessoais que as empresas possuem devem ser identificadas pelo time de Compliance, para que seja mapeado o tratamento de dados, analisando a infraestrutura do seu suporte técnico, dentre seu armazenamento, territorialidade pelas quais os dados estão sendo armazenados, e etc.

O próximo passo seria a atualização das políticas de governança, privacidade dos termos de uso, NDA’s, além da auditoria interna de alguns documentos, dentre eles: regulamento interno do Contrato de Trabalho dos

funcionários, dos prestadores de serviço, dos colaboradores e o Contrato de Prestação de Serviços com os clientes.[42]

Todos os setores da empresa devem ser sistematizados, momento oportuno para um profissional da área de tecnologia da informação e segurança identificar as vulnerabilidades do sistema, através da execução de testes que verificam algum facilitador de meio pelo qual permita o *cyber* criminoso invadir o sistema operacional da empresa, vazando dados pessoais, ou até mesmo, visualizando dados que eram confidenciais.

Através destes testes, são emitidos relatórios que apontam falhas e lacunas para correção de vulnerabilidades do sistema através da utilização de *softwares*, ampliação de meios eletrônicos que garantem maior proteção ao tratamento dos dados pessoais.

Este cenário configura um espaço para adotar uma estratégia para implementação de um Programa de Compliance LGPD. A estratégia envolve a atualização/criação/edição de normas e regulamentos internos, mitigando os riscos de infrações para que a recepção da LGPD no ambiente corporativo seja feita de maneira satisfatória.

O protocolo de implementação da LGPD no Brasil é pautado pela consultoria jurídica; cibersegurança; auditoria; plano de estratégia; execução e administração do Programa de LGPD no Brasil.

4.3. PROTOCOLO DE LGPD NO BRASIL

O Protocolo de LGPD no Brasil consiste em ser orientado pela seguinte disposição: i. Identificação do cenário e Palestra; ii. Verificação de vulnerabilidades no sistema; iii. Criação do Setor de Controle; iv. Análise do Perfil DPO; v. Criação do Canal do Titular de Dados; vi. Realização do Fluxo de Dados; vii. Avaliação de Processos e Tecnologias; viii. Análise do cenário atual da empresa; iv. Elaboração da Política de Privacidade Externa; v. Confecção de Contratos, vi. Código de Ética, vii.

[42] Assi, Marcos. Compliance: como implementar, 1ª edição. Disponível em: Minha Biblioteca, Editora Trevisan, 2018.

Acordos Comerciais e Termo de Sigilo e Confidencialidade (NDA); e viii. Treinamentos para Conscientização da LGPD e suporte no relacionamento com os clientes.[43]

Inicialmente, o Protocolo de LGPD identifica o atual cenário da empresa, os regimentos existentes e as suas problemáticas, para que assim, seja efetuado a auditoria em diversos pontos da empresa. Em paralelo, são realizadas palestras por especialistas em LGPD, os quais participam os demais membros da companhia, onde são ouvidos os principais pontos de atenção por parte da equipe do Compliance.

Através do mapeamento do cenário da empresa, um profissional especialista em cibersegurança analisa a empresa de forma integral identificando seus processos, tecnologia e a forma de atuação do jurídico para que sejam emitidos relatórios técnicos que verificam a vulnerabilidade do sistema.

Para que seja emitido este relatório em sua plenitude, a empresa deverá consentir com o Termo de Sigilo e Confidencialidade para que seja criado um setor de controle, departamento responsável por supervisionar as atividades dos colaboradores ao cumprimento da Política de Privacidade Externa e Interna, além de promover na prevenção de incidentes que coloquem em ameaça o ambiente corporativo e auxiliar o Data Protection Officer **(“DPO”)** no cadastro dos titulares detentores dos dados pessoais.

O DPO é o profissional que se comunica com a Autoridade Nacional de Proteção de Dados **(“ANPD”)** e o titular de dados (cliente, colaboradores e fornecedores) e com os respectivos órgãos de Compliance (escritórios especializados, Poder Judiciário e etc).[44]

Posteriormente, há Criação do Canal de Dados, o qual será atribuída a função de entrar em contato com os titulares de dados para mapear as informações de todos os usuários que devem ter seus direitos cobertos pela LGPD. Através da criação deste Canal, são mapeados os fluxos de dados pessoais, identificando os procedimentos internos que são riscos à proteção de dados pessoais, orientando sobre as mudanças necessárias para que se adequem ao Protocolo de LGPD.

[43] Silva, Daniel, C. e José Roberto Covac. Compliance como boa prática de gestão no ensino superior privado - 1ª edição. Disponível em: Minha Biblioteca, Editora Saraiva, 2015.
[44] Teixeira, Tarcísio, e Ruth Maria Guerreiro. Lei Geral de Proteção de Dados Pessoais (LGPD): Comentada Artigo por Artigo. Disponível em: Minha Biblioteca, (4th edição). Editora Saraiva, 2022.

O próximo passo é a identificação das tecnologias utilizadas pela empresa, realizando questionamentos as lideranças de Departamento de Tecnologia, *Software*. Por meio desta identificação são conhecidos com mais afinco os processos internos como coleta, recepção, produção, classificação, utilização, acesso, reprodução, transmissão e modificação dos dados pessoais.

Assim, após a coleta dos dados pessoais e seus mecanismos de atuação, a equipe de Compliance já possui subsídios para dar seu parecer sobre a situação atual da empresa face à Lei 13.709/2018. O parecer conterá os pontos de avaliação de Processos e Mapeamento de Violações e Incidentes, com indicativos de falhas operacionais identificadas por profissionais especializados, como advogados atuantes em cibersegurança, os quais emitem um relatório com os processos e tecnologias aplicáveis.

Posteriormente, são confeccionadas Políticas de Privacidade e Códigos de Ética pautados pela LGPD e a atualização de alguns documentos em consonância com a LGPD, como: Contratos de Prestação de Serviço, Contratos de Trabalho com os Colaboradores; Regulamentos Internos com explicações das funções do tratamento dos dados pessoais de cada setor; e etc.

É papel essencial das empresas, juntamente com a atuação da equipe de Compliance, a realização de treinamentos e campanhas de conscientização sobre a importância da LGPD no ambiente corporativo.

Por fim, o suporte ao relacionamento com os clientes consiste em compor uma equipe de Compliance qualificada composta por conciliadores e árbitros para eventuais demandas contenciosas que envolvam temas de LGPD.

4.4. PROCEDIMENTOS PARA ADEQUAÇÃO DA LGPD NO AMBIENTE CORPORATIVO:

As etapas do programa de adequação do LGPD no ambiente corporativo ocorrem da seguinte forma:

Inicialmente, cria-se uma base legal que traz argumentos legais para a forma como os dados estão sendo tratados; após a apresentação da base legal, os processos são formas pelas quais são realizados os procedimentos para o tratamento

de dados, mapeando os agentes responsáveis e a segurança a ser implementada, já que, são identificados os incidentes já ocorrentes.

Posteriormente, a estruturação das atividades através da estipulação de um *design* cria um espaço para receptividade do titular e do mercado, já que, a transparência é um pilar essencial a adequação da LGPD no ambiente corporativo, pois por meio dela, são disponibilizadas de maneira acessível as informações aos titulares dos dados.[45]

A partir da obtenção destas informações preliminares, entender quais são os dados tratados, os fluxos da empresa e como os procedimentos são efetuados, são passos essenciais para o mapeamento dos dados pessoais relevantes a serem observados no cenário da LGPD.

O levantamento das bases legais é etapa importante para compreender as atividades da empresa, a estruturação da operação e a análise dos tratamentos dos dados pessoais executados.

Através deste levantamento, a equipe de Compliance posicionará qual é a maneira de tratamento de dados mais adequada ao caso concreto, através de uma análise de riscos.

A análise de riscos tem como pilar essencial a identificação das fraquezas do programa de adequação, isto é, seus pontos fortes e fracos a serem explorados.

Após a análise de riscos, a governança é o próximo passo para adequação de um programa de LGPD no ambiente corporativo, pois é definido a equipe responsável pela parte de LGPD, são traçados os planos de ação e as estratégias de como os dados pessoais serão governados dentro da empresa.

Posteriormente, a criação e adaptação de documentos são essenciais, pois são mapeados todos os Contratos e inseridos os clausulados LGPD nos documentos pertinentes.

A conscientização dos colaboradores da empresa e clientes também é projeto de adequação da LGPD, pois envolve os atos de treinamento e comunicação

[45] Marinho, Fernando. Os 10 Mandamentos da LGPD - Como Implementar a Lei Geral de Proteção de Dados em 14 Passos. Disponível em: Minha Biblioteca, Grupo GEN, 2020.

da LGPD. Para isto, deverão ser criadas campanhas institucionais, realizações de treinamentos, envio de comunicados, *workshops*, dentre outros.

4.5. DOCUMENTAÇÃO PARA IMPLEMENTAÇÃO DE UM PROGRAMA DE PROTEÇÃO DE DADOS PESSOAIS

O Compliance deverá recolher uma documentação para que seja implementado o Programa de Proteção de Dados Pessoais adequadamente. Os documentos seriam:[46]

a) *Recording of Processing Activities*: trata-se de um registro das operações de tratamento de dados, documento que aborda sobre os dados tratados, os agentes de tratamento, a finalidade, fundamentação jurídica, as hipóteses de compartilhamento e/ou transferência, medidas de segurança adotadas e etc. Este registro de operações deverá ser atualizado constantemente, identificando o fluxo de dados da empresa.

b) Relatório de Impacto à Proteção de Dados Pessoais: Documento do Controlador responsável por possuir a descrição dos processos de tratamento de dados pessoais que podem ocasionar riscos aos direitos fundamentais. Ademais, este relatório é responsável pela criação de mecanismos para mitigação de riscos. O documento conterá a descrição dos dados coletados; a metodologia utilizada para garantir a segurança das informações; avaliação do controlador em relação a mitigação de riscos.

c) Política de Privacidade: a função da Política de Privacidade é dar ciência aos titulares sobre o tratamento de dados efetuado pelo agente, formalizando todos os direitos e obrigações da LGPD. O documento traz um resumo do mapeamento dos dados usados, a fundamentação jurídica, o prazo, os direitos dos titulares, a forma de transferência de dados, as eventuais medidas de segurança tomadas e etc. Sua atribuição é estar disponível ao titular antes que o tratamento seja realizado.

d) Plano de Incidentes e Respostas: sua responsabilidade é de comunicar a ANPD e os titulares caso haja ocorrências de incidentes de segurança, ferramenta utilizada para diminuir a responsabilidade do agente diante a ANPD. Trata-se de um documento que prevê as etapas em caso de ocorrências de incidente de segurança.

46

e) Política de Proteção de Dados: criação de um manual sobre como a organização gerencia as questões relativas a proteção de dados;

f) Planos de governança e boas práticas;

g) Criação de Comitês de Proteção de Dados com membros de diversas equipes;

4.6. CONFORMIDADE

A instauração de um Programa de Conformidade no mundo corporativo promove políticas de segurança cibernética ao realizar controles de acessos, criptografia de dados, uso de software de segurança inovadores, avaliações e auditorias que corrigem vulnerabilidades do sistema.

Através da Conformidade são monitorados continuamente os sistemas e redes que detectam atividades suspeitas, gerindo adequadamente os dados, a criptografia de dados sensíveis permitindo que os dados não sejam facilmente acessíveis por terceiros.

A Responsabilidade Corporativa, a Mitigação Proativa, a Avaliação de Riscos são medidas que mitigam eventuais ameaças cibernéticas, de forma que, existe uma revisão contínua dos processos existentes e cada vez mais são adotadas novas tecnologias que fortalecem o meio virtual.

A Conformidade traz uma série de benefícios, dentre os quais estabelecem penalidades aos que não cumprirem as regulamentações cibernéticas, uma melhoria nas estruturas que proporcionam uma resposta eficiente, o aumento da confiança dos consumidores e partes envolvidas que se sentem satisfeitos com empresas que demonstram compromisso com a segurança, proporcionando, desta forma, uma cultura organizacional responsável e segura.

4.7. INTELIGÊNCIA ARTIFICIAL GENERATIVA

A inteligência artificial generativa é uma tecnologia que gera conteúdo em formato de textos, imagens, músicas etc. Este mecanismo serve para perpetrar e ao mesmo tempo defender os crimes cibernéticos.

Os crimes cibernéticos são facilmente executáveis através da inteligência artificial generativa pelos ataques automatizados consistentes à partir da criação de senhas e scripts que adivinham senhas; pela identificação de vulnerabilidades dos sistemas; pela engenharia social com a formulação de mensagens de texto ou reprodução de mídia que enganam os indivíduos que revelarem dados sensíveis; para criação de emails phishing que seriam convincentes ao público alvo; a automatização da criação de malware, dentre outros.

Outros pontos desfavoráveis seriam a criação de textos que simulem fraudes, modelos que expõem dados sensíveis etc.

Apesar da inteligência artificial generativa facilitar a execução de crimes cibernéticos, podem também serem aliados a promoção da segurança cibernética, já que, também possuem atributos que detectam e previnem a realização dos crimes cibernéticos, como a análise de anomalias, a elaboração de respostas a incidentes que afetem a segurança cibernética.

A Lei de Inteligência Artificial proposta pela União Europeia regulariza o tema no continente europeu. Alvo de debates pela Comissão da União Europeia em 2021, discute-se acerca dos riscos da utilização deste mecanismo.

Estudos foram realizados, classificando em níveis de risco acerca da utilização da inteligência artificial generativa, como, por exemplo, a proibição do uso deste mecanismo em usos que tragam ameaças à segurança da população ou que violem os direitos fundamentais, como é o caso da vigilância em massa.

Todo estudo da utilização da inteligência artificial é monitorado por Comissões da União Europeia e autoridades locais, de forma que, os usuários sempre são informados com transparência quando estiverem sujeitos a decisões automatizadas.

As classificações dos riscos são divididas em inaceitável, limitado, alto e mínimo. Toda vez que for classificado em alto risco, estarão sujeitos a critérios rigorosos de análise, como controles de conformidade antes de serem inseridos em sociedade.

É direito dos usuários almejar pela intervenção humana ao invés do uso da inteligência artificial e terem seus dados pessoais anonimizados ou pseudonimizados para se protegerem contra quaisquer vazamentos de informações.

A União Europeia visa promover constantemente a inovação, aumentando os investimentos neste setor, buscando a cooperações com outros países que propiciem recursos para o desenvolvimento dessa tecnologia.

Por outro lado, a inteligência artificial generativa dos Estados Unidos tem um viés setorial, pois possui diversas agências reguladoras por setores, como o de *Food and Drug Administration*, que regulamenta o uso dessa ferramenta em diagnósticos médicos; o *Department of Defense*, destinado para fins militares; o Federal Trade Commission, por regularizar questões vinculadas a publicidades, dentre outros.

Nos Estados Unidos não há uma lei federal para o assunto, mas existem agências que emitem orientações sobre o tema, juntamente com princípios orientadores do assunto que visam a não discriminação, a segurança e a transparência do mecanismo utilizado, princípios defendidos pelo Escritório de Política Científica e Tecnológica e pelo Instituto Nacional de Padrões e Tecnologia.

O governo americano busca por parcerias público-privadas e o desenvolvimento da inteligência artificial generativa de maneira ética, sem que seja preciso uma intervenção governamental rigorosa, incentivando a inovação, competividade e transparência.

Assim, enquanto a Europa possui uma regulação centralizada, prevenindo os riscos categorizando a inteligência artificial em níveis, o modelo americano possui um sistema descentralizado, sem lei federal específica, possuindo agências reguladoras sobre o tema.

O modelo europeu visa proteger os direitos fundamentais e a privacidade da proteção de dados através do Regulamento Geral de Proteção de Dados, enquanto os Estados Unidos priorizam por adotar diretrizes voluntárias e na autoregulamentação, em virtude de não existir uma lei federal, mas apenas a combinação de leis estaduais que protegem os dados pessoais dos indivíduos.

A Europa busca pela transparência das relações, dando ênfase na ética dos modelos de inteligência artificial diferentemente dos Estados Unidos, movido pela inovação em que a ética é voltada para mecanismos de autorregulação.

5.A PROPOSTA DE UM CÓDIGO PENAL DIGITAL

Uma das reflexões a serem propostas no presente trabalho dizem respeito a criação de um Código Penal Digital, a qual adaptaria e atualizaria as legislações criminais para abrangência dos delitos cometidos no ambiente virtual.

A importância da criação de um Código Penal Digital se manifesta à partir do crescimento dos crimes virtuais sem que haja legislação específica e outras fontes jurídicas existentes para suporte jurídico dos consumidores.

O novo Código Penal Digital exigiria a criação de Comitês de Especialistas para realização de um estudo prévio das leis a serem instituídas, como grupos formados por profissionais de direito, tecnologia, segurança cibernética, compliance, dentre outros e para revisão contínua, diante da constante mudança da evolução tecnológica em sociedade.

O Código Penal Digital promove a segurança no ambiente digital, pois ao estabelecer penalidades claras aos atos ilícitos cometidos, torna claro para sociedade sobre a ilicitude dos atos cometidos. Ademais, reduzem o risco de vazamento de dados pessoais, roubo de informações etc.

A criação do Código Penal Digital auxilia na uniformização das decisões judiciais, reduzindo eventuais interpretações que poderão ser divergentes, responsabilizando de forma mais eficaz todos os agentes infratores, já que, a partir da criação deste mecanismo, as vítimas dos crimes cibernéticos passam a ter meios para consulta de fontes jurídicas para sua defesa, garantindo um ambiente tecnológico e inovador.

A regulação jurídica atual não é suficiente para proteger os consumidores, justamente pelas lacunas existentes na lei que geram uma série de dúvidas as vítimas, aos agentes infratores e até mesmo ao próprio judiciário. Somado as lacunas existentes nas leis, a falta de uma fonte jurídica de consulta, bem como, a ausência de pareceres e discussões jurídicas acerca do tema que envolva crimes cibernéticos demonstra uma carência jurídica ao combate dos crimes cibernéticos, tendo em vista

que a regulação jurídica atual não supre as necessidades existentes. Para tanto, o Código Penal Digital demonstra uma enorme relevância de evolução sobre o assunto, já que, evidencia uma forma de combate a este tipo de crime, pois através deste mecanismo somado a adoção de uma Política de Compliance com incremento da LGPD e uma nova regulação jurídica relacionando a inteligência generativa constrói-se uma regulação jurídica mais fortificada sobre o tema.

CONCLUSÃO

O presente trabalho visa promover o conceito de consumidor, seus princípios relacionados e regras de responsabilidade civil e penal no Código de Defesa do Consumidor. Posteriormente, dialoga com o surgimento da internet que criou um grande espaço em sociedade.

À partir dos computadores interligados, a internet ganha uma nova proporção que lhe permitiu evoluir para outro patamar, já que através dela se constituiu uma sociedade da informação, a existência de uma sociedade global e o desenvolvimento de uma sociedade de riscos.

A internet chega ao Brasil quando faculdades estudaram trazer este mecanismo ao país e à partir da promulgação da Lei n° 12.965 de 2014, a qual estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil.

Após o surgimento e desenvolvimento da internet, e levando em conta as mudanças na sociedade global, surgiram algumas figuras importantes atuantes no meio informático, como é o caso do consumidor digital, já que, com o surgimento da internet não somente existia o mundo físico, mas o mundo digital ganhou cada vez mais espaço.

O consumidor digital, representado todo aquele que adquire produto ou serviço como destinatário final no espaço digital, passa a otimizar seu tempo ao ter facilidade em obter em instantes algum serviço ou produto, sem precisar se deslocar em espaços físicos para obter o que deseja.

Apesar das facilidades e benefícios que o mundo virtual trouxe à sociedade global, os consumidores também estão sujeitos a riscos na internet, em virtude das inúmeras pessoas que a acessam, já que, alguns indivíduos possuem uma má intenção ao usar a internet, já que promovem os denominados crimes cibernéticos.

Os crimes cibernéticos, caracterizados por serem crimes que ocorrem no ambiente virtual geram riscos as suas vítimas, por violarem direitos das vítimas e por através deles serem obtidos dados pessoais, dinheiro e outras informações relevantes

de forma indevida, já que a informática é o meio para prática de agressões a bens jurídicos protegidos pelo Direito Criminal.

Torna-se um desafio julgar o crime informático, pois além das suas inúmeras peculiaridades, definir uma competência para o ciberespaço é desafiador, pois a internet é capaz de ultrapassar os limites territoriais, alcançando diversas jurisdições. Para isso, foi definida a competência à partir do local onde partiu o ato delituoso, isto é, o local do provedor do site e a comprovação de quem utilizou o meio informático para prática do crime, além de trazer um estudo do funcionamento do mecanismo para o combate do crime cibernético no âmbito internacional.

A presente Dissertação buscou dar um enfoque no âmbito do Direito do Consumidor ao mencionar sobre os crimes cibernéticos, refletindo no cenário atual existente pelo qual os consumidores são as maiores vítimas de vazamento de dados pessoais resultantes destas infrações penais.

Ao serem vítimas de crimes digitais através de fraudes e outros mecanismos que configuram o fornecimento de dados indevidamente, muitos consumidores saem prejudicados devido a sua vulnerabilidade, incorrendo em crimes como omissão sobre a periculosidade/nocividade dos produtos e serviços prestados de maneira *online*, fraude em oferta virtual ou financeira virtual, venda de produtos falsificados pela internet e etc.

A prática dos crimes cibernéticos atrelados às práticas abusivas cometidas pelas empresas, somados a falta de prevenção com os dados pessoais dos usuários ou adquirentes dos produtos comercializados e serviços prestados, resultam na ocorrência dos crimes virtuais contra os consumidores, os quais tem seus dados pessoais vazados.

Para evitar o vazamento de dados pessoais, torna-se necessário se atentar a Lei Geral de Proteção de Dados a qual menciona quais são os riscos e as formas de se prevenir a divulgação das informações pessoais para fins ilícitos tanto por parte dos consumidores quanto por parte das empresas responsáveis pelo controle do ambiente virtual ao fornecerem seus produtos e serviços de maneira *online.*

A melhor maneira das empresas se prevenirem do vazamento dos dados pessoais seria manusear corretamente a forma pela qual ocorrem o tratamento destas informações.

A forma do tratamento dos dados pessoais se inicia com a coleta de dados corretos, seguida pelo processamento de dados em que são verificadas quais informações são realmente úteis às empresas, para, posteriormente, ocorrer a difusão/cessão identificando a legitimidade da difusão dos dados obtidos. Destaca-se que o manuseio incorreto destes dados pessoais se configura uma fragilidade aos consumidores, os quais acabam tendo seus direitos violados.

O manuseio incorreto dos dados pessoais incorre em ameaças, roubo de identidade para fins ilícitos, fraudes, quebra de acordos de confidencialidade, dentre outros.

Assim, para evitar o vazamento de dados pessoais, o papel dos fornecedores se baseia em proteger os consumidores, que são mais vulneráveis, contra-ataques cibernéticos. Para isto, mostra-se crucial investir no Compliance das empresas, já que, através dele são adotados procedimentos internos com o intuito de tornar determinada organização em conformidade com às leis, normas e políticas da Companhia.

Com o Compliance, existem recursos que monitoram pessoas e processos, evitando perda do negócio em virtude de fraudes e conflitos de interesses. O principal objetivo é mitigar os riscos da Companhia e de eventuais consumidores que estejam sujeitos à ataques cibernéticos em virtude do vazamento de dados pessoais.

Desta forma, o Compliance por ter uma atuação preventiva, positiva a prevenção corporativa de ilícitos afim de evitar a prática de ataques cibernéticos. O Compliance se mostra à partir da recepção da LGPD no ambiente corporativo com o regimento do Protocolo LGPD-BR, pautado pela cibersegurança, auditoria, consultoria jurídica e parametrização dos processos afim de propiciar o ambiente mais seguro com o intuito de evitar com que os consumidores sejam alvo de ataques cibernéticos por indivíduos que acessam os sites dos fornecedores com má-fé.

Quando o Compliance e o manuseio dos dados pessoais pelos fornecedores não conseguem desenvolver seu pleno papel, pois ataques cibernéticos

estão presentes, torna-se importante mencionar acerca da responsabilidade civil dos agentes de tratamento de dados (operador e controlador).

Considera-se como responsabilidade solidária do operador, quando houver o descumprimento da legislação de proteção de dados ou quando o mesmo não tiver obedecido as normas do controlador, caso pelo qual há equiparação entre operador e controlador diante dos dados pessoais tratados.

A exclusão da responsabilidade se daria quando, comprovadamente, o dano é culpa exclusiva do titular dos danos ou de terceiro, que não realizaram o tratamento de dados que lhes é atribuído ou que não ocorreu violação à legislação de proteção de dados pessoais.

Considera-se culpa exclusiva da vítima a divulgação pública dos dados pessoais pelo titular em plataformas digitais; o armazenamento dos dados pessoais de forma insegura como *pen drives* e o mesmo for esquecido em público e etc. Enquanto a culpa por terceiro se refere a pessoa que não se identifique com o operador, titular de dados ou controlador, isto é, pessoa estranha ao tratamento de dados, dentre outros.

Desta forma, tendo em vista a promoção da cibersegurança entre os consumidores e fornecedores, mostra-se evidente que criar um ambiente seguro para que os consumidores possam adquirir seus produtos e serviços é essencial para evitar a ocorrência de crimes virtuais, bem como, poupar o vazamento de dados pessoais.

Com isto, cabe ao consumidor atentar-se ao compartilhar seus dados pessoais e ao manusear a internet para não cair em golpes, fraudes, clicar em links suspeitos, dentre outros e cabe ao Compliance das empresas criar um espaço seguro para ofertar seus produtos e serviços, visando a maior segurança ao consumidor, que se torna vulnerável não somente nas relações de consumo, mas também no ambiente virtual, já que, a não preocupação da cibersegurança dos mesmos acarretaria em penalidades aplicáveis pela ANPD.

BIBLIOGRAFIA

ALVES, CLEBER FRANCISCO; GONZÁLES, PEDRO. DEFENSORIA PÚBLICA NO SÉCULO XXI: NOVOS HORIZONTES E DESAFIOS. RIO DE JANEIRO: LUMEN JURIS.

ARTESE, GUSTAVO. COMPLIANCE DIGITAL: PROTEÇÃO DE DADOS PESSOAIS. IN: CARVALHO, ANDRÉ CASTRO ET AL. (COORD.). MANUAL DE COMPLIANCE. RIO DE JANEIRO: FORENSE, 2019.

ASSI, MARCOS. COMPLIANCE: COMO IMPLEMENTAR, 1ª EDIÇÃO. DISPONÍVEL EM: MINHA BIBLIOTECA, EDITORA TREVISAN, 2018.

AVENA, NORBERTO. PROCESSO PENAL, 10ª EDIÇÃO. RIO DE JANEIRO: FORENSE, 2018.

BARRETO, ALESSANDRO GONÇALVES; BRASIL, BEATRIZ SILVEIRA. MANUAL DE INVESTIGAÇÃO CIBERNÉTICO À LUZ DO MARCO CIVIL DA INTERNET. RIO DE JANEIRO: BRANSPORT, 2016.

BRASIL. Lei Nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Brasília, DF: Diário Oficial da União, 1990.

BLUM, RITA PEIXOTO F. *O DIREITO À PRIVACIDADE E A PROTEÇÃO DOS DADOS DO CONSUMIDOR*. DISPONÍVEL EM: MINHA BIBLIOTECA, (2ND EDIÇÃO). GRUPO ALMEDINA (PORTUGAL), 2022.

BUSATO, PAULO CÉSAR. DIREITO PENAL- PARTE GERAL. 3ª EDIÇÃO- EDITORA: ATLAS, V.1.

CAPEZ, FERNANDO. CURSO DE DIREITO PENAL.13ª EDIÇÃO. EDITORA: SARAIVA JÚNIOR, 2018.

CARVALHAES NETO, EDUARDO HAYDEN; COUTINHO, KAREN MENTZINGEN. ENFORCEMENT DA LEI GERAL DE PROTEÇÃO DE DADOS E SANÇÕES. IN: BEPPU, ANA CLAUDIA; BRANCHER, PAULO MARCOS RODRIGUES (COORD.). PROTEÇÃO DE DADOS PESSOAIS NO BRASIL: UMA NOVA VISÃO A PARTIR DA LEI Nº 13.709/2018. BELO HORIZONTE: FÓRUM, 2019.

COMER, DOUGLAS E. *REDES DE COMPUTADORES E INTERNET*. DISPONÍVEL EM: MINHA BIBLIOTECA, (6TH EDIÇÃO). GRUPO A, 2016.

CRESPO, MARCELO XAVIER DE F. *CRIMES DIGITAIS*. EDITORA SARAIVA, 2011.

DIDIER JR, FREDIE. CURSO DE DIREITO PROCESSUAL CIVIL. 9. ED. BAHIA: JUSPODIVM, 2008.

FIORILLO, CELSO ANTÔNIO, P. E CHRISTIANY PEGORARI CONTE. *CRIMES NO MEIO AMBIENTE DIGITAL.* DISPONÍVEL EM: MINHA BIBLIOTECA, (2ND EDIÇÃO). EDITORA SARAIVA, 2016.

FRAGOSO, HELENO CLÁUDIO. LIÇÕES DE DIREITO PENAL: PARTE GERAL. 10. ED. REV. POR FERNANDO FRAGOSO. – RIO DE JANEIRO: FORENSE, 1986.

GARRIDO, PATRICIA P. PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD). DISPONÍVEL EM: MINHA BIBLIOTECA, (4TH EDIÇÃO). EDITORA SARAIVA, 2023.

GONÇALVES, VICTOR EDUARDO RIOS. SINOPSES JURÍDICAS, DIREITO PENAL. VOLUME 7 – 25ª EDIÇÃO. EDITORA SARAIVA, JUR.

JESUS, DAMÁSIO E. DE. DIREITO PENAL, VOLUME 1: PARTE GERAL. 28 ED. REV. – SÃO PAULO: SARAIVA, 2007.

JESUS, DAMÁSIO, D. E JOSÉ ANTÔNIO MILAGRE. MANUAL DE CRIMES INFORMÁTICOS DISPONÍVEL EM: MINHA BIBLIOTECA, EDITORA SARAIVA, 2016.

JÚNIOR, ALBERTO DO A. DIREITO INTERNACIONAL E DESENVOLVIMENTO. DISPONÍVEL EM: MINHA BIBLIOTECA, EDITORA MANOLE, 2005.

JUNQUEIRA, GUSTAVO, VANZOLINI, PATRICIA. MANUAL DE DIREITO PENAL. V. 1. 7.ED. SÃO PAULO: SARAIVA, 2021.

KHOURI, PAULO R. ROQUE A. *DIREITO DO CONSUMIDOR*. DISPONÍVEL EM: MINHA BIBLIOTECA, (7TH EDIÇÃO). GRUPO GEN, 2020.

KLEINDIENST, ANA C. *GRANDES TEMAS DO DIREITO BRASILEIRO: COMPLIANCE*. DISPONÍVEL EM: MINHA BIBLIOTECA, (2ND EDIÇÃO). GRUPO ALMEDINA (PORTUGAL), 2019.

LEITE, GEORGE, S. E RONALDO LEMOS. *MARCO CIVIL DA INTERNET*. DISPONÍVEL EM: MINHA BIBLIOTECA, GRUPO GEN, 2014.

LEONARDI, MARCEL; “RESPONSABILIDADE CIVIL DOS PROVEDORES DE SERVIÇOS DE INTERNET”.

LIMA MARQUES, CLÁUDIA. CONTRATOS NO CÓDIGO DE DEFESA DO CONSUMIDOR. O NOVO REGIME DAS RELAÇÕES CONTRATUAIS. SÃO PAULO: REVISTA DOS TRIBUNAIS, 2011.

LIMA, CÍNTIA ROSA PEREIRA D. ANPD E LGPD: DESAFIOS E PERSPECTIVAS. DISPONÍVEL EM: MINHA BIBLIOTECA, GRUPO ALMEDINA (PORTUGAL), 2021.

LOPES JR., AURY. DIREITO PROCESSUAL PENAL. 16. ED. SÃO PAULO: SARAIVA, 2019.

LUCCA, NEWTON DE E ADALBERTO SIMÃO FILHO; “DIREITO E INTERNET”. ASPECTOS JURÍDICOS RELEVANTES.

MALAQUIAS, ROBERTO ANTÔNIO DARÓS. CRIME CIBERNÉTICO E PROVA: A INVESTIGAÇÃO CRIMINAL EM BUSCA DA VERDADE. 2. ED. CURITIBA: JURUÁ, 2015.

MARINHO, FERNANDO. OS 10 MANDAMENTOS DA LGPD - COMO IMPLEMENTAR A LEI GERAL DE PROTEÇÃO DE DADOS EM 14 PASSOS. DISPONÍVEL EM: MINHA BIBLIOTECA, GRUPO GEN, 2020.

MARQUES, CLAUDIA L. DIREITO DO CONSUMIDOR - 30 ANOS DE CDC. DISPONÍVEL EM: MINHA BIBLIOTECA, GRUPO GEN, 2020.

MCCLURE, STUART, ET AL. *HACKERS EXPOSTOS: SEGREDOS E SOLUÇÕES PARA A SEGURANÇA DE REDES*. DISPONÍVEL EM: MINHA BIBLIOTECA, (7TH EDIÇÃO). GRUPO A, 2013.

MIRAGEM, BRUNO. A LEI GERAL DE PROTEÇÃO DE DADOS (LEI 13.709/2018) E O DIREITO DO CONSUMIDOR. REVISTA DOS TRIBUNAIS, SÃO PAULO, V. 108, N. 1009

NETO, FRANCISCO MAIA. ARBITRAGEM: A SOLUÇÃO EXTRAJUDICIAL DE CONFLITOS – 2. ED.

NEVES, EDMO C. *COMPLIANCE EMPRESARIAL - O TOM DA LIDERANÇA, 1ª EDIÇÃO*. DISPONÍVEL EM: MINHA BIBLIOTECA, EDITORA TREVISAN, 2018.

NORONHA, MAGALHÃES; DIREITO PENAL, VOLUMES 1 A 4.

NUCCI, GUILHERME DE SOUZA. CURSO DE DIREITO PENAL – VOL.1 – 4ª EDIÇÃO- EDITORA FORENSE.

NUCCI, GUILHERME DE SOUZA. MANUAL DE DIREITO PENAL: 3 ED. REV. ATUAL. E AMPL. 2. TIR. – SÃO PAULO: EDITORA REVISTA DOS TRIBUNAIS, 2007B.

PAESANI, LILIANA M. DIREITO DE INFORMÁTICA: COMERCIALIZAÇÃO E DESENVOLVIMENTO INTERNACIONAL DO SOFTWARE. DISPONÍVEL EM: MINHA BIBLIOTECA, GRUPO GEN, 2015.

PAULINO, JOSÉ ALVES; “CRIMES DE INFORMÁTICA”.

PRADO, LUIZ RÉGIS. CURSO DE DIREITO PENAL BRASILEIRO; PARTE GERAL. 7A .ED., SÃO PAULO: REVISTA DOS TRIBUNAIS, 2007.

PRUDÊNCIA DO SUPERIOR TRIBUNAL DE JUSTIÇA. REVISTA DE DIREITO RENOVAR, RIO DE JANEIRO, N. 29, P. 1-11, MAIO/AGO., 2004.

QUEIROZ, PAULO. DIREITO PENAL; PARTE GERAL. 3ª. ED., SÃO PAULO: SARAIVA, 2006.

RANGEL, PAULO. *DIREITO PROCESSUAL PENAL*. DISPONÍVEL EM: MINHA BIBLIOTECA, (30TH EDIÇÃO). GRUPO GEN, 2023.

REIS, MARIA HELENA JUNQUEIRA; “COMPUTER CRIMES”. A CRIMINALIDADE NA ERA DOS COMPUTADORES.

REVISTA E AMPLIADA – BELO HORIZONTE: DEL REY, 2008.

RIBEIRO, GUSTAVO PEREIRA LEITE. O CONCEITO JURÍDICO DE CONSUMIDOR. REVISTA TRIMESTRAL DE DIREITO CIVIL. RIO DE JANEIRO: RENOVAR, 2004. V. 18, ABR./JUN.

ROCHA, GUSTAVO. COMPLIANCE DIGITAL E A LEI GERAL DE PROTEÇÃO DE DADOS: LGPD. ADV ADVOCACIA DINÂMICA: INFORMATIVO SEMANAL, RIO DE JANEIRO, N. 15, ABR. 2019.

SANT’ANA, ARMANDO. PROPAGANDA: TEORIA, TÉCNICA E PRÁTICA. 7 ED. SÃO PAULO: THOMPSON LEARNING, 2007.

SANTANNA, GUSTAVO. DIREITO DO CONSUMIDOR. DISPONÍVEL EM: MINHA BIBLIOTECA, GRUPO A, 2018.

SANTOS, JUAREZ CIRINO DOS. DIREITO PENAL – PARTE GERAL, 3º EDIÇÃO. CURITIBA: EDITORA LUMEN JURIS, 2008.

SILVA, DANIEL, C. E JOSÉ ROBERTO COVAC. *COMPLIANCE COMO BOA PRÁTICA DE GESTÃO NO ENSINO SUPERIOR PRIVADO - 1ª EDIÇÃO*. DISPONÍVEL EM: MINHA BIBLIOTECA, EDITORA SARAIVA, 2015.

SILVA, JOSEANE SUZART LOPES DA. DIREITO DO CONSUMIDOR CONTEMPORÂNEO: ANÁLISE CRÍTICA DO CDC E DE IMPORTANTES LEIS ESPECIAIS. RIO DE JANEIRO: LUMEN JURIS, 2020.

TARTUCE, FLÁVIO, E DANIEL AMORIM ASSUMPÇÃO NEVES. *MANUAL DE DIREITO DO CONSUMIDOR: DIREITO MATERIAL E PROCESSUAL. VOLUME ÚNICO*. DISPONÍVEL EM: MINHA BIBLIOTECA, (12TH EDIÇÃO). GRUPO GEN, 2023.

TARTUCE, FLÁVIO; NEVES, DANIEL AMORIM ASSUMPÇÃO. MANUAL DE DIREITO DO CONSUMIDOR. DIREITO MATERIAL E PROCESSUAL. 5 ED. RIO DE JANEIRO: FORENSE. 2016.

TASSO, FERNANDO ANTONIO. A RESPONSABILIDADE CIVIL NA LEI GERAL DE PROTEÇÃO DE DADOS E SUA INTERFACE COM O CÓDIGO CIVIL E O CÓDIGO DE DEFESA DO CONSUMIDOR. CADERNOS JURÍDICOS, SÃO PAULO, V. 21, N. 53, JAN./MAR. 2020.

TAVARES, JUAREZ. TEORIA DO INJUSTO PENAL. 6.ED. SÃO PAULO: TIRANT BRASIL, 2019.

TEIXEIRA, TARCÍSIO, E RUTH MARIA GUERREIRO. LEI GERAL DE PROTEÇÃO DE DADOS PESSOAIS (LGPD): COMENTADA ARTIGO POR ARTIGO. DISPONÍVEL EM: MINHA BIBLIOTECA, (4TH EDIÇÃO). EDITORA SARAIVA, 2022.

THEODORO JÚNIOR, HUMBERTO. DIREITOS DO CONSUMIDOR: A BUSCA DE UM PONTO DE EQUILÍBRIO ENTRE AS GARANTIAS DO CÓDIGO DE DEFESA DO CONSUMIDOR E OS PRINCÍPIOS GERAIS DO DIREITO CIVIL E DO DIREITO PROCESSUAL CIVIL. 6. ED. REVISTA E ATUALIZADA DE ACORDO COM O CÓDIGO CIVIL DE 2002. RIO DE JANEIRO: FORENSE, 2009.

TRENNEPOHL, TERENCE, E NATASCHA TRENNEPOHL. ESG E COMPLIANCE: INTERFACES, DESAFIOS E OPORTUNIDADES. DISPONÍVEL EM: MINHA BIBLIOTECA, EDITORA SARAIVA, 2023.

VARGAS. JOSÉ CIRILO DE. DO TIPO PENAL. 3ª. ED., RIO DE JANEIRO: LÚMEN JÚRIS, 2008.

VIANNA, TÚLIO LIMA; “FUNDAMENTOS DE DIREITO PENAL INFORMÁTICO”. DO ACESSO NÃO AUTORIZADO A SISTEMAS COMPUTACIONAIS.

VIOL, DALILA M. *PROGRAMAS DE INTEGRIDADE E COMBATE À CORRUPÇÃO:ASPECTOS TEÓRICOS E EMPÍRICOS DA MULTIPLICAÇÃO DO COMPLIANCE ANTICORRUPÇÃO NO BRASIL*. DISPONÍVEL EM: MINHA BIBLIOTECA, GRUPO ALMEDINA (PORTUGAL), 2021.

WALD, ARNOLD. O DIREITO DO CONSUMIDOR E SUAS REPERCUSSÕES EM RELAÇÃO ÀS INSTITUIÇÕES FINANCEIRAS. REVISTA DOS TRIBUNAIS, SÃO PAULO: RT 666/7-

WOLFGANG, HOFFMANN-RIEM. TEORIA GERAL DO DIREITO DIGITAL. DISPONÍVEL EM: MINHA BIBLIOTECA, (2ND EDIÇÃO). GRUPO GEN, 2021.

ZAFFARONI, E. RAÚL ET AL. DIREITO PENAL BRASILEIRO. V. II, T. II. RIO DE JANEIRO: REVAN, 2017.