**Centro Universitário do Planalto Central Apparecido dos Santos - UNICEPLAC**

**Curso de Direito**

**Trabalho de Conclusão de Curso**

# Um estudo sobre o estelionato virtual e o impacto da superexposição de dados

Gama-DF

2022

**MYLENA KETLEY BORGES DE MELO**

# Um estudo sobre o estelionato virtual e o impacto da superexposição de dados

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Orientador: Prof. Me. Antônio Roger Pereira de Aguiar.

Gama-DF

2022

**MYLENA KETLEY BORGES DE MELO**

# Um estudo sobre o estelionato virtual e o impacto da superexposição de dados

Artigo apresentado como requisito para conclusão do curso de Bacharelado em Direito pelo Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac.

Gama, 12 de novembro de 2022.

**Banca Examinadora**

---

Prof. Antônio Roger Pereira de Aguiar

Orientador

---

Profa. Me. Caroline Lima Ferraz
Examinador

---

Profa. Me. Risoleide de Souza Nascimento
Examinador

# Um estudo sobre o estelionato virtual e o impacto da superexposição de dados

Mylena Ketley Borges de Melo[1]

**Resumo**
É notório o aumento de usuários conectados à internet. Dessa forma, a prática de crimes virtuais expandiu significativamente. Nesse contexto, surge o objetivo deste artigo, cuja finalidade é fornecer uma explicação sobre os crimes executados na rede mundial de computadores, principalmente os que envolvem a prática de estelionato atrelados à superexposição de dados. Dessa forma, a presente pesquisa traz à baila a Lei Geral de Proteção de Dados, tema atual e relevante para reflexão jurídica. Ademais, o estudo centra-se em duas das mais importantes ferramentas virtuais utilizadas pelos criminosos, quais sejam o uso das redes sociais e o *whatsapp* usados na prática delituosa de crimes com invasões informáticas. O estudo também versará sobre a aplicabilidade do *data protection officer*.

**Palavras-chaves:** estelionato; internet; crimes; redes sociais; whatsapp; LGPD.

**Abstract:**
The increase in users connected to the internet is notorious. In this way, the practice of virtual crimes has expanded significantly. In this context, the objective of this article arises, whose purpose is to provide an explanation about the crimes carried out on the world wide web, especially those involving the practice of embezzlement linked to the overexposure of data. In this way, the present research brings up the General Data Protection Law, a current and relevant topic for legal reflection. Furthermore, the study focuses on two of the most important virtual tools used by criminals, namely the use of social networks and whatsapp used in the criminal practice of crimes with computer invasions. The study will also address the applicability of the data protection officer.

**Keywords**: embezzlement; internet; crimes; social networks; whatsapp; GDPR.

[1] Graduando(a) do Curso de Direito, do Centro Universitário do Planalto Central Apparecido dos Santos – Uniceplac. E-mail: mylena1798@gmail.com.

## 1 INTRODUÇÃO

O estelionato virtual é um crime no qual a pessoa utiliza os meios fraudulentos para obter uma vantagem injusta, usa os dados da vítima, fotos, número de telefone. Os agentes do ilícito mandam mensagens para as pessoas próximas das vítimas e começam a praticar o eventual crime.

Uma eventualidade comum nos acontecimentos que envolvem o crime de estelionato é o uso de *sites* falsos para obtenção de dados dos usuários. Por conseguinte, dessa espécie, os golpistas organizam uma página de internet com as empresas meramente conhecidas para aplicar o crime que está tipificado no art.171 do Código Penal, porém na plataforma *fake* criada por eles. A vítima insere seus dados bem como as senhas e as numerações do cartão de crédito, tendo assim os dados expostos para os estelionatários cometerem qualquer tipo de fraude contra as vítimas no mundo virtual. Para tratar dos crimes virtuais, foi promulgada em 2021 a Lei 14.155, que inseriu vários parágrafos ao art. 171 do Código Penal e mudou algumas regras relativas à concorrência judicial.

Diante do caso em tela, é importante salientar que existem vários tipos de crimes que podem ocorrer por meio eletrônico e também por meio de canais digitais, nos quais são envolvidas a honra e a imagem das pessoas vítimas de tais ilícitos cometidos.

A expressão estelionato vem da palavra latina *stellio*, que quer dizer "[...] o camaleão que muda de cor para escapar da detecção ou passar despercebido". Quem efetua estelionato não tem dificuldade em se adaptar ao ambiente em que se encontra porque, disfarçando muito bem e possuindo seus meios, ilude a vítima com seus enganos e má-fé. Estelionato é um dos delitos mais enganadores do Código Penal Brasileiro, pois podem ser desempenhados de diversas formas.

Nesse contexto, surgiu a Lei Geral de Proteção de Dados Pessoais (LGPD 13.709/2018, publicada para resguardar os direitos fundamentais à liberdade e à privacidade, bem como ao livre desenvolvimento da personalidade de cada indivíduo. A lei disciplina sobre o tratamento de dados pessoais armazenados em meio físico ou digital, seja feito por pessoa física ou jurídica de direito público ou privado e inclui um amplo leque de operações que podem ocorrer em meio manual ou digital.

Com o intuito de garantir a proteção dos dados do cidadão em território nacional, a LGPD passou a vigorar a partir de 2020. Para tanto, a LGPD prevê a presença de profissional responsável pela responsabilidade do DPO *(data protection officer)* pela segurança de dados no art. 5º, inciso VIII, da Lei 13.853/2019. (BRASIL, 2019)

O crime de “invasão de equipamentos de informática” foi inserido no Código Penal pela Lei 12.737, de 30 de novembro de 2012, e é definido como “[...] invasão de equipamentos eletrônicos, interligados ou não a rede de computadores, com objetivo de obter, sem o consentimento expresso ou tácito do proprietário do equipamento, alterar ou destruir dados ou informações, ou instalar vulnerabilidades para ganho ilícito. (BRASIL, 2012)

Outrossim, o presente artigo mostra-se como pesquisa aplicada, descritiva e explicativa às características do *data protection officer* para enfrentamento de possíveis invasões de dispositivos informáticos e estelionatos virtuais em face da superexposição de dados à luz da LGPD. Para melhor entendimento, foi usado o livro do Guilherme de Souza Nucci do Curso de Direito Penal - Parte Especial - Vol. 2, como também do Rogério Greco Curso de Direito Penal - Vol. 3 para exemplificar melhor sobre o tema de estelionato. Já no tema da LGPD, foi usado como uma das principais doutrinas que é a Lei Geral de Proteção de Dados (LGPD) Guia de implantação de Lara Rocha Garcia com o intuito de ter um aprimoramento do assunto, deixando claro para os leitores de como ocorre. Vários outros livros foram empregados para uma abordagem descritiva.

O *data protection officer* é um profissional que tem o objetivo de garantir a proteção de dados de cada indivíduo nas empresas. Nesse sentido, a problemática será: quais as características do DPO para enfrentamento de possíveis invasões de dispositivos informáticos e estelionatos virtuais em face da superexposição de dados à luz da LGPD? Uma característica a ser salientada sobre o DPO é garantir de forma independente que uma organização específica cumpra as leis que protegem os dados pessoais dos indivíduos, tornando-o assim, de difícil acesso para possíveis invasões de dispositivos informáticos e crimes de estelionatos virtuais.

Por conseguinte, serão abordados no presente artigo cientifico três capítulos principais sendo que no primeiro tópico será abordado sobre a disposição do estelionato e a Lei de Proteção de Dados; no segundo as características e conceito sobre o DPO e a importância desse profissional para evitar invasões e crimes virtuais, e por conseguinte, a pesquisa versará sobre as formas de cometimento do crime de invasão de dispositivos informáticos e as formas de evitá-lo.

## 2 DISPOSIÇÃO SOBRE ESTELIONATO E LEI PROTEÇÃO DE DADOS

A temática do crime de estelionato é uma das mais interessantes dentre os diversos crimes descritos no Código Penal, tanto por sua estrutura congênita quanto pelo infinito número

de formas de fazê-lo. Trata-se de crime patrimonial em que não tem a gravidade de crimes violentos como roubo (art. 157 CP), extorsão (art. 158 CP), ou extorsão por sequestro (art. 159, CP) não está presente, nem a singeleza de furto (art. 155 CP) ou extorsão por sequestro (art. 159 e 168 CP).

O Código Penal disciplina que esse crime em tela, está tipificado no art.171 do Código Penal com pena reclusão de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis (Vide Lei 7.209 de 1984). Estelionato, muitas vezes conhecido como o "crime 171", é um crime contra a propriedade que pode ser cometido por qualquer pessoa que queira tirar vantagem de outra. Alguns exemplos desse crime incluem a clonagem de contas do WhatsApp e a invasão de contas pessoais para obter os dados.

Para Gonçalves (2020, p. 502), o estelionato é um crime marcado pelo emprego de fraude, uma vez que o agente, valendo-se de alguma artimanha, consegue enganar a vítima e convencê-la a entregar-lhe algum bem e, na sequência, locupleta-se ilicitamente com tal objeto. Ao iniciar a execução do estelionato, o golpista emprega artifício, ardil ou qualquer outra fraude.

O erro é uma representação mental da realidade que está incorreta. Não implica ignorância, mas sim uma falsa compreensão de qualquer coisa. Como tal, o que se discute é uma contradição entre a verdade aparente e a verdade real. Trata-se, portanto, de um desvio da verdade". Colocar alguém em erro é fazer com que essa falsa noção surja em suas mentes, e manter alguém em erro (PRADO, 2021, p. 436). Segundo o STJ no que diz respeito ao assunto sobre o estelionato enfatiza que na Súmula 48, STJ compete ao juízo do local da obtenção da vantagem ilícita processar e julgar crime de estelionato cometido mediante falsificação de cheque (BRASIL, 1992).

Já na Súmula 244, STJ ressalta que compete ao foro do local da recusa processar e julgar o crime de estelionato mediante cheque sem provisão de fundos (BRASIL, 2001). Por conseguinte, a Súmula 107, STJ compete à Justiça Comum Estadual processar e julgar crime de estelionato praticado mediante falsificação das guias de recolhimento das contribuições previdenciárias, quando não ocorrente lesão à autarquia federal (BRASIL, 1994). Segundo Nucci (2021, p. 431) é incomparável a diferença entre uma representação de teatro bem produzida assim como é contada uma história inventada ou baseada em fatos reais é um estelionatário. O estelionato é um crime artístico porque envolve representação, persuasão, discursos embelezados, cenários montados, figurantes e todas as outras ferramentas necessárias para ludibriar alguém.

É aceitável no âmbito do estelionato o crime de bagatela, bem como em outros crimes

patrimoniais, desde que não haja violência ou ameaça grave. Não há necessidade de discutir o crime organizado se o bem-estar jurídico da vítima não for significativamente prejudicado. Certamente, todos os demais requisitos para a aceitação da teoria de crime sem importância devem ser observados, incluindo a primariedade, os bons precedentes, o objeto de interesse pessoal protegido, o valor do dano causado (NUCCI, 2021, p. 434).

Por sua vez Bitencourt (2018, p. 287) conceitua o estelionato, crime que requer a cooperação da vítima, o início de sua execução se dá com o engano da vítima. Quando o agente não consegue enganar a vítima, o simples emprego de artifício ou ardil caracteriza apenas a prática de atos preparatórios, não se podendo cogitar a tentativa. Geralmente a conduta é composta, visto que para obter uma vantagem injusta armando para alguém ou mantendo-o errado. Obter um benefício ou lucro ilícito como resultado da armadilha da vítima. Esse é o conteúdo do artigo 171 do CP, pois ela coopera com o agente sem perceber que está perdendo o domínio aos seus pertences (NUCCI, 2021, p. 431).

Há controvérsia doutrinária sobre a punição do agente pelo crime de estelionato quando ocorre a chamada torpeza bilateral no caso concreto. Reconhecemos que, nessas circunstâncias, não seria possível punir o agente pelo crime de extorsão sem incorrer em absurdas legalidades, uma vez que, como se depreende da leitura do artigo 883 do CC, o direito privado de ação civil não se aplica a essas questões envolvendo a torpeza da suposta vítima (GRECO, 2021, p. 358).

A ação típica do estelionato é desenvolver uma conduta fraudulenta usando um artifício, um teste de detector de mentiras ou qualquer outro método análogo ao induzir ou manter o erro da vítima com o objetivo de obter uma vantagem injusta para si ou para outra pessoa (do básico/simples/ tipo anormal/incongruente). Como a lei está escrita atualmente, é impossível tirar qualquer outra conclusão além de que o ato é de natureza criminosa. Esta conclusão só pode ser tirada quando o agente obtém com sucesso a vantagem ilícita.

É evidente que o estelionato tem um duplo efeito a vítima sofre danos, enquanto o agente se beneficia. Esses resultados geralmente seguem um ao outro, embora seja possível que a vítima sofra danos enquanto o agente não consegue obter a vantagem desejada; nesse cenário, o crime é visto como tentado. Por exemplo, é o que acontece quando alguém publica um anúncio falso de venda de um veículo em um jornal e convence a vítima a fazer um depósito em determinada conta bancária para concluir a transação.

Assim esclarece Gonçalves (2020, p. 504) que o artigo 171 revisto está redigido e proíbe tirar qualquer outra conclusão que o estelionato é material para um crime, o que só ocorre quando o agente obtém com êxito a vantagem ilícita. É evidente que um estelionato pressurizado tem dois resultados: a vítima sofre dano e o agente se beneficia.

Conforme Prado (2021, p. 436) esclarece, o erro é uma representação mental da realidade que está incorreta. Não implica ignorância, mas sim uma falsa compreensão de qualquer coisa. Como tal, é "uma contradição entre verdade aparente e fato; portanto, um desvio da verdade" que está sendo discutido. Colocar alguém em erro é fazer com que essa falsa noção surja em suas mentes, e manter alguém em erro é impedir que o lesado descubra a verdade devido à operação do truque astuto.

O furto por fraude e a apropriação não autorizada são outros dois tipos de crimes patrimoniais dos quais o estelionato se diferencia. Ao começar a realizar o estelionato, o golpista utiliza um meio artificial, um ardil, ou qualquer outra forma de fraude. O crime de estelionato surge como representação gráfica de certas formas jurídicas de cooperação ou relacionamento artificial: a conduta ofensiva não termina, como, por exemplo, em um roubo ou agressão unilateral do agente, mas requer algum tipo de complemento e funciona com a cooperação passiva da vítima (PRADO, 2021, p. 435).

O artifício torna-se aparente quando o agente utiliza algum tipo de artifício para ajudá-lo no aprisionamento da vítima, como lançar a mão de algum tipo de artefato. Por exemplo, na história do bilhete premiado, ele prende a vítima com um bilhete falso. Ardil é uma conversa envolvente em que o agente manipula verbalmente a vítima. Saber que uma televisão deve ser removida de um local específico por uma pessoa, por exemplo. (GONÇALVES, 2020 p. 502).

Assim, entende-se que a presença de três elementos é fundamental, fraude (ardil ou engano), erro e disposição prejudicial de bens patrimoniais é necessária para certo tipo de finalidade injusta do estelionato. É importante notar que se não há fraude, mas há um erro e uma disposição patrimonial prejudicial, então não há crime. A jurisprudência do STJ há muito tempo sustenta que o cometimento desse crime em sua totalidade ocorre quando o agente obtém uma vantagem injusta, pois, como dito anteriormente, isso leva à produção do resultado naturalístico.

> Ementa HABEAS CORPUS. ESTELIONATO TENTADO. PRINCÍPIO DA INSIGNIFICÂNCIA. ABSOLVIÇÃO EM PRIMEIRO GRAU. REFORMA PELO ACÓRDÃO IMPUGNADO. TROCA DE ETIQUETA DE PREÇO ENTRE MERCADORIAS DE SUPERMERCADO. MÍNIMO DESVALOR DA AÇÃO. IRRELEVÂNCIA DA CONDUTA NA ESPERA PENAL. CIRCUNSTÂNCIA PESSOAIS DO AGENTE NÃO IMPEDEM O RECONHECIMENTO DA ATIPICIDADE. PRECEDENTES DO STF E DO STJ. 1. A conduta perpetrada pelo agente? tentar obter vantagem indevida, em prejuízo de estabelecimento comercial, colocando em mercadoria mais cara, etiqueta de preço de outra, trinta e cinco reais mais barata? Insere-se na concepção doutrinária e jurisprudencial de crime de bagatela, já que a ação não resultou em perigo concreto e relevante, de modo a lesionar ou colocar em perigo bem jurídico tutelado pela norma penal. 2. As circunstâncias de caráter eminentemente pessoal não interferem no reconhecimento do delito de

> bagatela, uma vez que este está relacionado com o bem jurídico tutelado e com o tipo de injusto, e não com a pessoa do acusado, que não pode ser considerada para a aplicação do princípio da insignificância, sob pena de incorrer no inaceitável direito penal do autor, incompatível com o sistema democrático. 3. Ordem concedida para anular a decisão condenatória. Decisão Vistos, relatados e discutidos estes autos, acordam os Ministros da QUINTA TURMA do Superior Tribunal de Justiça, na conformidade dos votos e das notas taquigráficas a seguir, por unanimidade, conceder a ordem, nos termos do voto da Sra. Ministra Relatora. Os Srs. Ministros Arnaldo Esteves Lima, Napoleão Nunes Maia Filho, Jorge Mussi e Felix Fischer votaram com a Sra. Ministra Relatora. (BRASIL, 2008).

Em alguns casos, a partir do ano de 2016, o STJ passou a reconhecer que o crime seria cometido não no momento em que a vítima recebesse a vantagem injusta, mas sim no momento em que a vítima realmente sofria o dano. O Tribunal, no entanto, reafirmou o entendimento anterior no sentido de que o consumo ocorre no momento e no local em que se obtém uma vantagem injusta (posição que nos parece acertada), o que foi previamente fixado (ESTEFAM, 2021, p. 230).

O Regulamento Geral de Proteção de Dados, Lei 13.709, de 14 de agosto de 2018, também conhecida como LGPD, causou certa comoção no meio jurídico e empresarial ao trazer uma série de previsões sobre a necessidade de diversos participantes do mercado terem cautela quanto aos dados e informações que são responsáveis por proteger sob a ameaça de consequências graves como multas ou, pior, impossibilitando a operação. (BRASIL, 2018)

Em poucas palavras, um dado pessoal pode ser um nome, um endereço, até mesmo a placa de um carro, o site de um restaurante favorito, um link de mídia social, o tamanho da roupa etc.19, dependendo de sua contextualização, organização, manuseio adequados, e interpretação para que possa se tornar informação quando carrega um significado ou mesmo apenas tem algum tipo de sentido (SOLER, 2022, p. 12).

O objetivo da LGPD é proteger direitos fundamentais como privacidade, intimidade, honra e direito à reputação e à dignidade. Também é possível argumentar que a necessidade de leis específicas para proteção de dados pessoais cresceu com o rápido avanço e expansão tecnológica mundial, que surgiu como resultado dos efeitos negativos da globalização, que resultou, entre outras coisas, no aumento da importância da informação. Isso significa que a informação evoluiu para uma atividade altamente relevante para políticos e empresários: quem tem acesso aos dados também tem acesso ao poder (PINHEIRO, 2021, p.29).

A LGPD possui regras para a coleta e processamento de dados pessoais para evitar o vazamento deles e garantir sua privacidade e proteção. O objetivo da lei é garantir a transparência na relação entre pessoas físicas e jurídicas, em particular no que diz respeito à

forma como os dados pessoais dos titulares (cidadãos) são coletados, armazenados e utilizados.

O ex-presidente Michel Temer aprovou a Lei 13.709/2018, também conhecida como Lei de Proteção de Dados. Ela foi criada com o propósito de determinar os princípios, deveres e direitos que as empresas devem seguir ao lidar com dados de clientes. A Lei se baseou no GPDR (Regulamento Geral de Proteção de Dados) que surgiu na Europa após escândalos envolvendo grandes corporações que passaram a divulgar dados de clientes sem autorização. Sua proposta era garantir transparência aos cidadãos sobre o uso de seus dados (ROCHA¸ *et al* 2020, p. 19).

Para proteger os direitos fundamentais, incluindo a privacidade, a intimidação, a honra e o direito à reputação e à dignidade, foi criada a LGPD. Em decorrência dos efeitos negativos da globalização, que resultaram no aumento da importância da informação, também é possível argumentar que a necessidade de leis específicas para proteção de dados pessoais aumentou junto com o rápido desenvolvimento e disseminação da tecnologia pelo mundo (PINHEIRO, 2021, p. 29).

Dada a importância dos dados pessoais, o *caput* do art. 46 da LGPD expressa a exigência de prestadores de tratamento implementarem salvaguardas de segurança, técnicas e administrativas apropriadas para proteger os dados pessoais de acessos não autorizados (como invasão de servidores) e situações em que possam ser perdidos, alterados, comunicados ou submetidos a outro tratamento impróprio ou ilegal (TEIXEIRA, 2021, p. 94).

A LGPD é um padrão forte que contém disposições sobre como os dados pessoais são, sejam eles tratados fisicamente ou digitalmente, por pessoas físicas ou jurídicas com direitos públicos ou privados. Por isso, é aplicável a todos os entes federativos (SOLER, 2022, p. 10). Outrossim, a segurança da informação está intimamente relacionada à proteção de dados pessoais, pois exige organização e medidas técnicas razoáveis para atingir esse objetivo, (ou seja, garantir que os dados pessoais de um usuário não sejam destruídos, alterados, divulgados ou acessados inadequadamente em um ambiente de internet aberta.

Dessa forma, devido a um problema relacionado ao mercado, muitas corporações multinacionais já utilizavam tecnologias de segurança para proteger as informações que coletavam de seus usuários. Por consequência disso, com a implementação da LGPD, essas empresas devem agora tomar medidas adicionais para garantir que essas tecnologias de segurança possam proteger os dados pessoais de qualquer pessoa, mesmo em seguida da finalização de seu tratamento.

Segundo Lima (2021, p. 90**)** a LGPD, por sua vez, destaca a necessidade de realizar um Relatório de Impacto à Proteção de Dados Pessoais, documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades

civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco, conforme o art. 5º, XVII, da LGPD.

Um documento significativo para a regularidade do tratamento de dados pessoais foi anteriormente disponibilizado pela LGPD em seu artigo 5º, inciso XVII o Relatório de Impacto à Proteção de Dados Pessoais RIPD (OLIVEIRA, 2021, p. 21). De acordo com o referido artigo, a RIPD é uma documentação do controlador que contém uma descrição dos processos de tratamento de dados pessoais que podem resultar em riscos aos direitos fundamentais e liberdades civis, bem como medidas, salvaguardas e mecanismos de mitigação de riscos.

Pela sua própria natureza, o RIPD é uma autoavaliação portanto, ainda que possa ser apresentado a terceiros, não pretende ser um documento "homólogo" perante a ANPD (Autoridade Nacional de Proteção de Dados ou qualquer outra autoridade). Tanto no ambiente físico quanto no digital, a segurança é um tema de extrema importância. Ataques que podem tornar os servidores indisponíveis podem resultar em sérias consequências para as empresas, especialmente aquelas envolvidas no comércio eletrônico. Portanto, a segurança da informação é fundamental (LIMA, 2021, p. 93).

Pode-se dizer que a ANPD foi gerada para dar mais segurança e estabilidade à implementação do Regulamento Geral de Proteção de Dados. Cabe à autoridade efetivar os ajustes necessários para que a lei tenha maior conformidade com a realidade social e econômica no caso específico do Brasil, onde se prevê que diversos dispositivos da Lei sejam objeto de regulamentação futura (PINHEIRO, 2021, p. 20).Primeiramente, é notável observar que a ANPD será responsável por fornecer orientações gerais sobre a adequação e aplicação da Lei Geral de Proteção de Dados Brasileira, definindo as regras para tratamento de dados no Brasil e tendo competência para alterar a Lei 13.709/2018. As determinações de penalidades e multas da LGPD também serão implementadas pela ANPD, que também será responsável pela fiscalização dos tratamentos.

Por sua vez Garcia (2020, p. 22) relata que de forma simples, as autoridades públicas podem recolher e tratar os dados, com exceção da realização de interesses públicos; no entanto, eles devem obter o consentimento para exercer sua autoridade legal ou cumprir suas obrigações. Em outras palavras, com ou sem o consentimento do proprietário, o governo pode coletar os dados necessários para cumprir qualquer obrigação legal.

Portanto, isso não exclui o direito do titular em termos de transparência, ou seja, ele pode exigir a declaração de todos os dados acessíveis aos poderes públicos, qual o tratamento que é feito e o compartilhamento, mas não pode exigir a exclusão ou o bloqueio do tratamento se for fornecido na forma prevista. Caberá à ANPD fazer valer quaisquer abusos ou enganos

futuros do Poder Público no que diz respeito ao uso dos dados, assim como caberá à ANPD fazer valer quaisquer julgamentos técnicos futuros sobre disputas judiciais que não sejam abrangidos pela lei.

É considerável ter em mente que o peso da evidência é decidido pelo tribunal. De acordo com o Direito, quem faz a acusação, ou a pessoa que inicia um processo judicial, deve demonstrar que a outra parte é responsável e lhe causou danos. No entanto, a instituição do investimento do ônus da prova permite que a acusação seja feita sem provas, mas obriga o acusador a se defender. A LGPD permite que isso aconteça quando se constata que a acusação é verdadeira e o Titular não tem recursos suficientes, ou quando uma das partes carece de recursos econômicos e financeiros adequados (GARCIA, 2020, p. 23).

Ressalta a importância da ANPD para o *enforcement* da própria LGPD, que se tornou evidente na União Europeia a partir da década de 1960. Não é apenas uma organização que faz as regras a ANPD também compete para equilibrar interesses comerciais com proteção humana. A Organização para a Cooperação e Desenvolvimento Econômico (OCDE) já evidenciou tal preocupação ao elaborar as Diretrizes sobre Proteção da Privacidade e Circulação Transfronteiriça de Dados Pessoais do OCDE *(Guidelines on the Protection of Privacy and Transborder Flows of Personal Data)* de 1980, ratificando que um sistema de proteção de dados pessoais eleva o Brasil a outro patamar no contexto do capitalismo informacional, pois o nível de proteção passa a estar adequado ao europeu (LIMA, 2020, p. 378).

Isso se deve ao fato de que, em 28 de janeiro de 1981, foi realizada a Convenção sobre Proteção de Dados Pessoais, também conhecida como Convenção Nº 108, com vistas ao processamento automatizado desses dados. Neste caso, destacou-se que a criação de uma organização reguladora e fiscalizadora era necessária para o adequado cumprimento das leis de proteção de dados pessoais, garantindo a independência e autonomia da organização para o desempenho de suas funções (LIMA, 2020, p. 378).

A lei também permite a inversão do ônus da prova na apresentação de provas visto que o suporte é muito pesado. Nesse sentido, laudos e provas referentes ao tratamento e arquivamento de dados de acordo com as diretrizes legais passam a ser a base para os processos processuais e para o exame final pela ANPD. Isso restaura a base para a proteção do consumidor proposta no artigo 2º.

## 3. DATA PROTECTION OFFICER

Denominamos de *data protection officer*, ou simplesmente DPO, o responsável pela

salvaguarda dos dados pessoais e das organizações dos clientes. No ambiente de trabalho, ele auxilia a empresa ajustando os processos para formar um programa de *compliance* que evidencia o aumento da segurança dos dados que ela é responsável por proteger.

A descrição de um DPO é um perfil profissional híbrido que, independentemente do local de origem, precisará ampliar seus conhecimentos para ter sucesso em outra área. Essa demanda é uma razão por trás de uma certificação como DPO, que abrange segurança da informação, legislação e o estabelecimento de um sistema de gestão para garantir que a privacidade e a proteção dos dados sejam parte regular do negócio e não apenas um projeto especial. *Data protection officer* ou diretor de proteção de dados é o nome usado para descrever a função do profissional responsável pela proteção de dados dentro de uma organização, garantindo a segurança das informações de clientes, fornecedores e internos da empresa.

Segundo (Lima, 2021, p. 46) ressalta que nada impede que o operador também tenha um responsável pela proteção de dados (DPO), designado para compartilhar e complementar o controlador para garantir a segurança dos dados ponto a ponto, dependendo do tamanho e complexidade das operações comerciais do operador. O DPO é uma pessoa nomeada pelas empresas que sejam responsáveis ou que atuem como subcontratadas para o tratamento de dados pessoais e a sua função será supervisionar e aconselhar a empresa a respeito das obrigações contidas no Regulamento.

O principal objetivo do funcionário nomeado é observado em sua definição, que é atuar como ponto de referência para que fique claro a quem devem ser dirigidos os pedidos de tratamento de dados pessoais. A finalidade do legislador é clara quando se trata de tratamento de dados, não deve haver dúvidas sobre quem deve agir, o responsável é o encarregado pelo recebimento das solicitações internas (OLIVEIRA, 2021 p. 16).

A presença e o trabalho de um *Data Protection Officer* estão se tornando cada vez mais essenciais nas empresas que armazenam e lidam com dados diariamente. De acordo com o art. 51, IV, da LGPD, o profissional deve exercer todas as demais atribuições que lhe forem estabelecidas pela autoridade controladora ou por normas complementares. O profissional deve ter conhecimento técnico e jurídico, ser capaz de acompanhar de perto todo o ciclo de vida das informações e apoiar todas as equipes organizacionais em questões que envolvam proteção de dados e privacidade.

Dessa forma, o ciclo interno de indicação, aprendizado e prática pode ser difícil e prolongado, levando muitas empresas a optar pela terceirização desse serviço. Dada a natureza multidisciplinar do trabalho que o titular desempenha, ele precisa ter conhecimento de direito, tecnologia, gestão e comunicação, portanto, encontrar alguém com todos esses conhecimentos

e habilidades pode ser uma tarefa assustadora. Também leva tempo para preparar alguém. Se o responsável for uma empresa, ela pode contar com a soma dos conhecimentos de seus funcionários para realizar todas as tarefas que lhe são atribuídas por lei.

Por outro lado, nenhuma empresa entende o negócio de outra empresa e seus gestores, e alguns detalhes administrativos e organizacionais geralmente não são revelados a nenhum outro parceiro, por mais estratégico que seja. Portanto, esse argumento sustenta a proposta de que o principal deve ser um empregado (GARCIA, 2020 p. 19). Falta um entendimento unificado. De outro modo, discute-se se o encarregado poderá ser qualificado como pessoa coletiva quando a palavra singular for retirada, como foi referido anteriormente, e foi acrescentada a frase "pessoa designada pelo responsável pelo tratamento e operador. Assim, o legislador afirma que é necessário um consenso entre o operador e o responsável pelo tratamento, independentemente de o responsável pela execução da tarefa ser uma pessoa singular ou coletiva.

Como resultado, a designação do encarregado poderia levar a conflito entre o controlador e o operador, pois qualquer um deles poderia sentir que seus interesses não eram levados em consideração. Isso porque o papel do encarregado é crucial para ambas as partes, principalmente em ações que envolvam potenciais crises ou correções de horários que exijam agilidade, abertura e trabalho cooperativo (GARCIA, 2020, p. 20).

De outro modo a ter em conta é que o encarregado não pode ser alguém que detenha um cargo de chefia (nesse caso, seria o responsável por supervisionar os seus pares), mas sim uma pessoa que se mantenham diretamente relacionado com o CEO/Presidente ou com o Conselho. Para gerenciar o registro das atividades de processamento, a LGPD exige que os DPOS priorizem suas tarefas e concentrem seus esforços nas questões que representam os maiores riscos à proteção de dados.

O GDPR reserva o art. 4° para pontuar as definições dos principais termos utilizados no documento. É notável como a lei brasileira se espelhou no modelo adotado pelo documento europeu. Embora alguns termos e expressões possam diferir, as páginas e as funções de cada assunto ou processo são as mesmas nas versões brasileira e europeia da publicação. Como ilustração, considere como o termo "controlador/processador" do GDPR foi alterado para "controlador/operador" na LGPD, com as ações, funções e responsabilidades sendo as mesmas.

É fundamental notar que, no caso do Brasil, o controlador de dados (DPO) recebeu um termo ao mesmo tempo amplo e abrangente (permitindo a personalidade física e jurídica), e há também o entendimento de que, como função de comunicação, poderia ser realizado por um comitê (um grupo de pessoas representando diversos setores ou áreas sob uma presidência), de

acordo com o modelo de governança específico de cada instituição. (PINHEIRO, 2021, p. 31).

O GDPR estabelece diretrizes sobre quem deve atuar como DPO, o que significa que uma autoridade ou organização pública pode nomear um único DPO para várias dessas autoridades ou organizações, levando em consideração a estrutura e as dimensões organizacionais de cada organização. O DPO é escolhido com base nas suas qualificações profissionais, particularmente no seu conhecimento especializado da lei e das práticas de proteção de dados. Levando em conta, que o profissional pode ser um membro do quadro de funcionários da organização responsável pelo tratamento, como um funcionário do controlador ou pode exercer suas funções de acordo com um contrato de prestação de serviços, caso em que o controlador contrata uma empresa especializada em proteção de dados para fornecer esse suporte (LIMA, 2020, p. 290).

O controlador, operador e encarregado são os três indivíduos listados como "agentes de tratamento de dados pessoais" na Lei Geral de Proteção de Dados. A primeira pessoa, física ou jurídica, com direito público ou privado, toma as decisões sobre como tratar os dados pessoais. O segundo, por outro lado, realiza operações de tratamento de dados em nome do controlador e de acordo com as instruções escritas deste último. Por fim, a pessoa designada como “encarregado” pelo crítico será o canal de comunicação entre estes, os titulares dos dados, e a ANPD. Assim, a pessoa designada pode ser um membro do pessoal do responsável pelo tratamento ou um advogado que o responsável pelo tratamento tenha contratado para o efeito (LIMA, 2020, p. 295).

Nos termos do art. 41, caput, o encarregado de dados é a pessoa indicada pelo controlador, entretanto, de acordo com o art. 5º, VIII, o encarregado é indicado pelo controlador e pelo operador. Trata-se, portanto, de um equívoco do legislador. No fundo, na redação original do art. 5º, VIII, a indicação era apenas do controlador, sendo a alteração promovida pela Lei n. 13.853/2019 (TEIXEIRA, 2021, p. 2021). A Lei nº 13.709/2018, também conhecida como Lei Geral de Proteção de Dados (LGPD), foi publicada em 15 de agosto de 2018 e entrará em vigor em 1º de agosto de 2020. Introduziu um novo posicionamento com total relevância para a gestão de dados, o Encarregado, cuja principal responsabilidade é atuar como canal de comunicação com os titulares dos dados e com a Autoridade Nacional de Proteção de Dados (ANPD).

Por outras palavras, a função da Lei do Encarregado ou mais popularmente designada por Encarregado de Proteção de Dados (DPO), passa por acolher reclamações e comunicações dos titulares, prestar esclarecimentos e implementar disposições, receber comunicações da autoridade nacional, dirigir colaboradores e contratantes da organização no que diz respeito as práticas a serem priorizadas no que diz respeito à proteção de dados pessoais, e cumprir as

demais atribuições estabelecidas pelo controlador ou estabelecidas por lei.

Para obter maior proteção de dados nas redes de computadores, a Lei 13.709/2018 estabeleceu restrições e direitos que devem ser observados pelos responsáveis pela manutenção de informações de terceiros. Fruto destas medidas de segurança e em resposta à procura do mercado, surgiu o cargo de *Data Protection Officer*, que ficaria encarregue de sustentar a segurança das empresas e dos seus clientes. De acordo com a legislação em vigor, qualquer empresa, pública ou privada, que trate de um número significativo de registros de dados deve obter a nomeação de um profissional responsável pela proteção de dados, neste caso um encarregado conforme previsto no artigo 5.º desta Lei.

Para o autor, a função DPO pode ser realizada através da prestação de serviços que podem envolver até mesmo tarefas automatizadas utilizando a aplicabilidade do uso dos bots, conhecido como o DPO Bots. Além disso, é possível fornecer serviços de DPO Share quando uma associação contrata um DPO para atender às necessidades exclusivas de um determinado setor da indústria e divide essas necessidades entre seus membros (PINHEIRO, 2021, p. 56).

Para cumprir essa função, com o mais alto nível de responsabilidade, foi desenvolvida no Brasil uma nova categoria de seguro, levando em consideração os recentes incidentes cibernéticos que afetaram os negócios. Posto isto, a contratação de um agente de seguros visa proporcionar ao segurado o ressarcimento dos prejuízos sofridos em decorrência de um ataque, bem como a indenização dos prejuízos causados a terceiros.

## 4. CRIMES INFORMÁTICOS

Levando em conta o avanço tecnológico nas últimas duas décadas, o mundo digital oferece vantagens incomparáveis para alguns e até previsíveis para outros. No entanto, com as melhorias trazidas pela evolução em vários campos, a internet forneceu uma plataforma para o cometimento de diversos crimes que prejudicam o bem-estar moral e financeiro, impactando pessoas físicas e jurídicas. É sabido que dados e informações estão se tornando recursos cada vez mais valiosos para as corporações. Hoje, a informação é a mais crucial das atividades. Desta forma, sabe-se que uma "atividade de informação" é qualquer aconselhamento ou informação que agregue valor a uma transação comercial. Um crime de tecnologia da informação é qualquer delito que tente violar o estado natural de dados e recursos fornecidos por um sistema de processamento de dados, seja por meio de compilação, armazenamento ou transmissão de dados.

O que antes exigia o uso do contato visual direto agora é realizado com o anonimato

proporcionado pelas conexões de internet, eliminando a necessidade de proximidade física para atuar como barreira à atividade criminosa. Existem inúmeros termos e classificações para crimes ligados às novas tecnologias, incluindo crimes de computador, crimes cometidos usando computadores, crimes de informação, criminalidade relacionada a computadores, crimes cibernéticos e assim por diante. No entanto, parece mais adequado utilizar o termo “crimes informáticos” dada a sua amplitude, que permite a expansão da área de estudo para ter em conta toda a atividade criminosa relacionada com as tecnologias de informação e tecnologias mais recentes (FIORILLO, 2016, p.61).

Em outras palavras, podemos classificar os crimes cometidos pela internet ou com o seu auxílio e que resultem em algum tipo de dano à vítima como crimes informativos. Assim, as situações em que um computador é utilizado para atividades ilícitas, bem como atos criminosos cometidos contra computadores ou em relação aos dados que eles contêm, estão incluídos na definição ampla de crime informacional. A partir dessas considerações, é possível dividir os crimes de informática em três categorias: "puros", "mistos" e "comuns" entre as infinitas classificações possíveis.

Os únicos crimes virtuais puros são aqueles que visam o *software* (ou programa) do sistema de computador, *hardware* os componentes físicos do computador, como CPU, monitor, teclado e circuito, dados, sistemas e métodos de armazenamento, entre outros. Relativamente a crimes semelhantes, o computador é uma condição necessária para a sua prática, como a movimentação não autorizada de fundos através do *home banking* ou a prática de "*salemislacing*" (saque diário de pequenos montantes de milhões de contas, também conhecido como saldo retirados. Os crimes comuns seriam aqueles já reconhecidos pela legislação brasileira, tornando a rede mundial de computadores apenas mais um meio de realização desses crimes, como é o caso dos seguintes crimes já designados como tal pela legislação penal, o estelionato (art. 171 do CP), a ameaça (art. 147 do CP), os crimes contra a honra (arts. 138-140 do CP), o homicídio (art. 121 do CP), a veiculação de pornografia infantil (Estatuto da Criança e do Adolescente – ECA – Lei n. 8.069/90), o crime de violação ao direito autoral (art. 184 do CP) (FIORILLO, 2016, p. 62).

O maior desafio que se coloca em relação aos crimes informáticos diz respeito, nomeadamente, aos crimes informáticos que são designados como crimes informáticos “puros” e não têm justificação legal, como quando há violação de informação considerada juridicamente significativa. Tendo em conta o princípio da legalidade ser tido como protetor do direito penal, torna-se impossível punir comportamentos que, embora possam prejudicar a vítima e constituir, por si só, um delito, carecem da típica equivalência jurídica.

A proteção das atividades informacionais pode ser proativa, por exemplo, usando medidas técnicas para impedir uma crise informacional. Por outro lado, é impossível garantir que um sistema seja 100% seguro no momento em que valorizamos proteções reativas ou recuperativas que visam responder a incidentes específicos ou mesmo reparar algum dano ocorrido. O direito penal está presente nesse sentido. Mais do que isso, a Lei Contra Crimes Cibernéticos pode ser vista como um tipo de proteção desmoralizante para a segurança da informação, pois permite que os criminosos saibam que serão responsabilizados por seus crimes caso sejam identificados (JESUS, 2016, p. 51).

Aspectos de segurança da informação são impactados pela alteração da lei. 12.737/2012. Inúmeras atividades criadas por pesquisadores e empresas devem ser examinadas à luz da nova Lei de Crimes de Informação. Vários controles, planos e políticas precisam ser revistos. Passamos a delinear as principais questões relativas ao crime previsto no artigo 154-A do Código Penal, traduzido pela Lei 12.737/2012, que trata de aspectos de segurança da informação e crimes cibernéticos na esperança de auxiliar na interpretação e esclarecimento da lei por seus usuários.

Para Damásio (2016, p. 57) a lei conforme alterada, não se aplicará a quem entrar em um dispositivo por meio de uma invasão ou violação de segurança ordenada por terceiros. Em uma invasão de computador, o observador digital pode precisar identificar o agente invasor e, em ordem cronológica, os endereços IP daqueles que posteriormente acessaram a invasão. Portanto, crimes de informação que incluem dados e outros benefícios legais são aqueles para os quais o legislador deve fornecer proteção.

É importante notar que a polícia tem investigado indivíduos que usaram cassinos online e até corridas de cavalos virtuais, alertando-os para possíveis violações legais dos artigos 50 e 58 do Decreto-Lei 3.688/41 (Lei das Contravenções Penais). Isso sugere que o termo "cibercrime" precisa ser revisto. Para isso, foi escolhido o termo "fraude informática". Os crimes informáticos são crimes frequentes como resultado, eles normalmente envolvem conduta antijurídica e criminal e são cometidos usando a tecnologia da informação como ferramenta, enquanto outros meios teriam sido igualmente apropriados para a tarefa em questão. Portanto, esses crimes são cometidos livremente (SYDOW, 2015 p. 34).

Os demais agentes decidiram não entrar neste momento porque acreditavam que o sistema já era seguro ou tinha um mecanismo de segurança que havia sido desligado. É importante avaliar a relação entre o invasor e aqueles que foram afetados por ele acessando o dispositivo em nossa teoria. Consciente da lacuna legal, o crime organizado pode pedir a um "laranja" que atua fora do país para realizar a invasão para que os demais no país possam entrar

e obter ou alterar as informações (JESUS, 2016, p. 57).

Conclui-se que as precauções de bom senso devem ser praticadas por todos os indivíduos com um computador conectado, como evitar o uso de software pirata, manter sistemas de correção corrigidos e ter um bom programa antivírus, todavia, mais importante, ser cauteloso ao clicar e evitar curiosidade. O proprietário de uma máquina "zumbi" utilizada em um crime digital que, segundo as provas, não utilizou nenhuma das medidas acima estabelecidas assumiu o risco de fazê-lo e pode até ser responsabilizado. Embora não seja culpado, o usuário pode ter que testemunhar em um processo legal ou investigação sobre a proteção de suas atividades eletrônicas (JESUS, 2016, p. 59)

De outro modo, apurou-se que o agente encarregado do zumbi não sabia que estava sendo contratado para o crime, dessa maneira ele não pode crime ou invasão cometido pelo agressor *(handler*). Isso porque o computador da vítima respondeu automaticamente ao comando remoto do criminoso de forma óbvia para o dono da atividade e nunca começou a executar a invasão em momento algum. Um crime cibernético deve ser avaliado sob vários ângulos devido às suas características únicas.

Um dos maiores problemas para punir crimes cometidos em ambiente digital é a evidência da materialidade do crime e as fontes de autoridade que fornecem o mínimo de justificativa para uma ação penal proposta. Neste sentido, os óbices descobertos ao longo da investigação criminal, bem como os potenciais processos judiciais vão desde a identificação de um potencial autor e a sua localização bem como a identificação do endereço IP, ou protocolo de internet, que identifica a máquina de origem da conduta, que não implica necessariamente a identificação do sujeito penal, à validade e legalidade das provas recolhidas e, por fim, aos desafios de rastrear a conduta no momento da sua realização.

O avanço da criminalidade e seu rápido desenvolvimento nos últimos anos causaram preocupação em escala global. Como resultado, muitas nações têm tomado medidas para reduzir os efeitos desse tipo de atividade criminosa em seus territórios, seja por meio da ratificação de acordos de cooperação internacional, da adoção de leis específicas para lidar com comportamentos criminosos emergentes, ou ainda, de acordo com nossas pesquisas sobre o tema, certas condutas no Brasil são protegidas pela lei tal como está. Notadamente, essas são as condutas para as quais a internet tem se tornado cada vez mais um meio de realização do crime. Por outro lado, os avanços tecnológicos também facilitaram o surgimento de novas práticas criminosas que exigem previsão legal que adquiram tipicidade, sobretudo, quando estamos diante dos crimes informáticos ditos puros (FIORILLO, 2016, p. 69).

A segurança da informação refere-se ao processo de defesa da informação contra

ameaças à sua confidencialidade, disponibilidade e integridade. O papel da segurança da informação é preservar as atividades relacionadas à informação enquanto garante confidencialidade que é o acesso à informação é restrito a quem precisa tê-la, integridade: a precisão, autenticidade e consistência das informações. Acessibilidade que é a informação esteja disponível para quem precisa tê-la. Uso legítimo é usado para as informações somente de acordo com a permissão.

## 5. CONSIDERAÇÕES FINAIS

À luz da exposição, pode-se afirmar que a internet foi um marco significativo para a humanidade. Ela revolucionou a vida humana ao possibilitar maior interação interpessoal, facilitar a execução de tarefas diárias, afetar a economia, proporcionar lazer, fomentar relacionamentos, ampliar o acesso à informação, entre muitas outras coisas. No entanto, apesar de todas as vantagens, conveniências e benefícios que a internet trouxe para a sociedade moderna no decorrer dos anos, ela também causou uma série de questões problemáticas, entre as quais se destaca o uso injustificado da internet para fins de prática de atos ilícitos, também conhecidos como crimes cibernéticos.

As pessoas mal intencionadas usam as redes sociais para prejudicar outras pessoas é quando há uma perda parcial de privacidade, a falsa sensação de impunidade e as conveniências que elas proporcionam. Inquestionavelmente, os métodos utilizados para a realização de crimes na internet evoluíram e mudaram em função dos avanços trazidos pelo seu desenvolvimento. Nesse sentido, foi possível observar que, com o passar do tempo, os crimes virtuais principalmente o estelionato virtual foi se tornando progressivamente mais prevalentes.

Ficou estabelecido que o crime de estelionato cometido em ambiente virtual tem início quando os indivíduos possuem dispositivos eletrônicos conectados à internet com o intuito de obter vantagem indevida para si ou para outrem, induzindo ou mantendo a vítima em erro, e fazendo-o por meio de engano, fraude ou qualquer outro meio desonesto que prejudique a vítima.

A prevalência desse tipo de crime online aumentou drasticamente com a chegada da pandemia de Covid-19, pois as pessoas passaram mais tempo em casa e, portanto, passaram mais tempo online. Com o intuito de tornar mais severas as penas para os crimes cometidos em ambiente virtual, foi criada a Lei 14.155/21 se fez necessária para tentar coibir tal conduta. No entanto, apesar de a referida lei ter sido aprovada em boa hora, não foi suficiente para diminuir a prática. Mesmo após a implementação da regra no ordenamento jurídico brasileiro, o número

de casos envolvendo o crime virtual continua aumentando. Diante disso, pode-se dizer que os modelos da nova legislação acerca dos crimes virtuais não se mostraram eficazes ou são insuficientes para reprimir o crime online.

## REFERÊNCIAS BIBLIOGRÁFICAS


BITENCOURT, Cezar Roberto. **(Tratado de direito penal, v. 3, p. 287)**. São Paulo, Editora Saraiva, 2018. E-book. ISBN: 9788547224714 Disponível em: http://biblioteca2.senado.gov.br:8991/F/?func=itemglobal&doc_library=SEN01&doc_number=001140622 Acesso em 13 set. 2022.

BRASIL**.** Superior Tribunal de Justiça. **Súmula Vinculante. Súmula Vinculante n.48.** Plenário. Brasília, data. 25 de agosto de 1992 Disponível em: https://www.coad.com.br/busca/detalhe_16/833/Sumulas_e_enunciados Acesso em 25 set. 2022.

_____ Superior Tribunal de Justiça. **Súmula Vinculante. Súmula Vinculante n.107** Plenário. Brasília, 22 de junho de 1994 Disponível em: https://www.coad.com.br/busca/detalhe_16/775/Sumulas_e_enunciados Acesso em 25 set. 2022.

_____ Superior Tribunal de Justiça. **Habeas Corpus. HC 118702 / MG** QUINTA TURMA, Impetrante: Leandro César Correa. Impetrado: Tribunal de Justiça do Estado de Minas Gerais. Relator (a): Ministra Laurita Vaz. Brasília, 18 de dezembro de 2008 Disponível emhttps://processo.stj.jus.br/processo/revista/inteiroteor/?num_registro=200802296201&dt_publicacao=16/02/2009 Acesso em: 12 set. 2022.

_____ Superior Tribunal de Justiça. **Súmula Vinculante. Súmula Vinculante n.244** Plenário. Brasília, 01 de fevereiro de 2001 Disponível em: https://www.coad.com.br/busca/detalhe_16/641/Sumulas_e_enunciados. Acesso em 25 set. 2022.

ESTEFAM, André. **DIREITO PENAL V 2 - PARTE ESPECIAL (ARTS. 121 A 234-B)**. São Paulo, Editora Saraiva, 2021. *E-book*. ISBN 9786555590180. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555590180/.Acesso em: 12 set. 2022.

GARCIA, Lara R. **Lei Geral de Proteção de Dados (LGPD): Guia de implantação**. São Paulo, Editora Blucher, 2020. *E-book*. ISBN9786555060164. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555060164/. Acesso em: 12 set. 2022.

FIORILLO, Celso Antônio P.; CONTE, Christiany P. **Crimes no meio ambiente digital**. São Paulo, Editora Saraiva, 2016. *E-book*. ISBN 9788547204198. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788547204198/. Acesso em: 01 out. 2022.

GONÇALVES, Victor Eduardo R. **Esquematizado - Direito penal - parte especial**. São Paulo, Editora Saraiva, 2020. p. 502 *E-book*. 9788553618927. Disponível em:

https://integrada.minhabiblioteca.com.br/#/books/9788553618927/. Acesso em: 21 ago. 2022.

GRECO, Rogério. **Direito Penal Estruturado**. São Paulo, Grupo Gen. 2021. *E-book*. ISBN 9788530993412. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788530993412/. Acesso em: 08 set. 2022.

JESUS, Damásio D MILAGRE, José A. **Manual de crimes informáticos.** São Paulo, Editora Saraiva, 2016. *E-book*. ISBN 9788502627246. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 09 set. 2022.

LIMA, Ana Paula Moraes Canto D. LGPD Aplicada. p.93 São Paulo, GEN, 2021. *E-book.* ISBN 9788597026931. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788597026931/. Acesso em: 08 set. 2022.

LIMA, Cíntia Rosa Pereira D. **Comentários à Lei Geral de Proteção de Dados.** Lisboa – Portugal, Almedina, 2020. *E-book.* ISBN 9788584935796. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788584935796/. Acesso em: 24 set. 2022.

NUCCI, Guilherme de Souza. **Curso de Direito Penal - Parte Especial - Vol. 2.** São Paulo Grupo GEN, 2021. *E-book*. ISBN 9786559640157. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559640157/. Acesso em: 08 set. 2022.

OLIVEIRA, Ricardo. **LGPD: Como evitar as sanções administrativas**. São Paulo, Editora Saraiva, 2021. E-book. ISBN 9786553623262. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553623262/. Acesso em: 09 set. 2022.

PRADO, Luiz R. **Tratado de Direito Penal Brasileiro - Parte Especial - Vol. 2**. São Paulo, GEN, 2021. E-book. ISBN 9786559640416. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786559640416/. Acesso em: 08 set. 2022.

PINHEIRO, Patrícia P. **PROTEÇÃO DE DADOS PESSOAIS: COMENTÁRIOS À LEI N. 13.709/2018 (LGPD).** São Paulo, Editora Saraiva, 2021. E-book. ISBN 9786555595123. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555595123/. Acesso em: 10 set. 2022.

SYDOW, Spencer T**. Crimes informáticos e suas vítimas**. São Paulo, Editora Saraiva, 2015. E-book. ISBN 9788502229488. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502229488/. Acesso em: 29 set. 2022.

SOLER, Fernanda G. **Proteção de dados: reflexões práticas e rápidas sobre a LGPD**. São Paulo, Saraiva, 2022. E-book. ISBN 9786553622500. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786553622500/. Acesso em: 09 set. 2022.

TEIXEIRA, Tarcísio. **A LGPD e o e-commerce**. São Paulo, Editora Saraiva, 2021. E-book. ISBN 9786555598155. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555598155/ . Acesso em: 25 set. 2022.

_____, Victor Eduardo R.; LENZA, **Pedro. Esquematizado - Direito Penal - Parte Especial.** São Paulo, Saraiva, 2022. *E-book*. ISBN 9786555597738. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9786555597738/. Acesso em: 12 set. 2022.

## AGRADECIMENTOS

Agradeço a Deus, primeiramente, que me deu força para concluir esta etapa da minha vida iluminando o meu caminho e por ter me proporcionando a chegar até aqui.

Agradeço minha família, em especial meus avós que sempre me deram apoio para não desistir dos meus sonhos, ao meu avô por me apoiar também financeiramente.

A professora Caroline, pelas correções e os ensinamentos para construção desse trabalho, e em especial ao meu orientador Antônio Róger que me permitiu apresentar um bom desempenho durante o processo desse trabalho.

Por fim, a palavra gratidão me define nesse momento tão especial.