UNIVERSIDADE PRESBITERIANA MACKENZIE

MATEUS CARRIJO CUTTI

CRIMES VIRTUAIS NO ORDENAMENTO JURÍDICO E AS SUAS DIFICULDADES DA IDENTIFICAÇÃO DO AGENTE

São Paulo

2023

MATEUS CARRIJO CUTTI

CRIMES VIRTUAIS NO ORDENAMENTO JURÍDICO E AS SUAS DIFICULDADES DA IDENTIFICAÇÃO DO AGENTE

Trabalho de graduação interdisciplinar apresentado como requisito para obtenção de título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

ORIENTADOR (A): FABIANO AUGUSTO PETEAN

São Paulo

2023

MATEUS CARRIJO CUTTI

CRIMES VIRTUAIS NO ORDENAMENTO JURÍDICO E AS SUAS DIFICULDADES DA IDENTIFICAÇÃO DO AGENTE

Trabalho de graduação interdisciplinar apresentado como requisito para obtenção de título de Bacharel no Curso de Direito da Universidade Presbiteriana Mackenzie.

Aprovado em:

BANCA EXAMINADORA

Examinador(a)

Examinador(a)

Examinador(a)

Dedico esse trabalho a Deus, minha família e meus amigos que contribuíram de forma significativa para que eu concluísse mais uma etapa importante em minha vida.

AGRADECIMENTO

Agradeço a minha família que é fonte de inspiração para o meu sucesso, me ajudando durante toda a jornada acadêmica. Ao meu professor e orientador Fabiano Augusto Petean, por sua paciência e incentivo, sem ele não seria possível a conclusão deste trabalho. E agradeço a todos que de alguma forma colaboraram e me ajudaram para que eu pudesse chegar até aqui.

“O Sucesso é a soma de pequenos esforços repetidos dia após dia.”

Robert Collier

RESUMO

No cenário atual em que vivemos, é notável a presença da tecnologia em grandes avanços de utilização, fazendo com que a interatividade e facilidade de informações sejam acessíveis para diversos fatores intuitivos, assim ocasionando convenções sobre os crimes na internet. Mediante a isso, o objetivo da pesquisa é abordar sobre a legislação que trata do estelionato virtual, com ênfase nas abordagens de aplicações penosas sobre quem comete os crimes nesses casos. As considerações acerca desse tema são de discursos novos, vez que,pelo fato da maior quantidade de acessos à internet, vir a se tornar frequente esses tipos de "golpes", pode se encontrar no ordenamento jurídico, no Código Penal, na Lei 12.737, Constituição Federal e ademais textos disposto por legisladores que justificam as causas que levam a esses atos. Como resultado constado nesse trabalho, verificou-se muitas questões de má-fé, influências e coações, sendo de prejuízo ocasionado pela vantagem ilícita do coator, com enfoque também nas repercussões de mídia. Por fim, pode-se enfatizar sobre as implicações das disposições gerais que se baseiam no artigo 141 do Código Penal.

Palavras-chave: Crimes Virtuais; Código Penal; Internet.

ABSTRACT

In the scenario in which technology is making, it is notable in advances in use, withinteractivity and ease of information being current for several intuitive factors, as well as concessions on internet crimes. In view of this, the objective of the research is to address the virtual legislation that deals with embezzlement, emphasizing the approaches of painful applications on who commits the crimes in these cases. As considerations on this topic are from speeches, since the greater amount of new types of access, become frequent in "coups", can be found in the legal system, in the Penal Code in Law 12.737, Federal and Legal Constitution in addition, texts provided by legislators that justify the causes that lead to these acts. As a result of this work, many issues of bad faith, influences and coercion were noted, with the damage caused by the unlawful advantage of the coercer, also focusing on the repercussions of the media. Finally, it can be emphasized on the provisions of the general provisions that are based on article 141 of the Penal Code.

Keywords: Virtual Crimes; Penal Code; Internet.

SUMÁRIO

1 INTRODUÇÃO

O direito é uma ciência que está em constante evolução, se moldando de acordo com o próprio desenvolvimento da sociedade ao longo do tempo com a necessidade de acompanhar as demandas econômico-sociais, sendo assim, dinâmico. Com o passar dos anos, as formas de como os criminosos praticam os delitos também vem mudando, tendo como uma de suas principais formas os crimes virtuais/cibernéticos.

O crescimento tecnológico vem a ser marcado por diversas invenções, tornando os resultados mais práticos e resultantes em fatores econômicos. Isso se origina da participação de grande giro que coloca a comunicação como um dos principais fatores sociais e culturais da atualidade.

O potencial da internet faz com que os alcances sejam amplos, tendo como base interações e disponibilidades que advém de ferramentas práticas para os crimes virtuais, assim inseridas informações que podem não ser condizentes com a realidade do indivíduo, criando perfis aleatórios para conquistar algo.

Esses atos são praticados como crime de imagem e honra, pois utilizam-se da vantagem ilícita do coator. Relata a prática frequente de acontecimentos nas atuações que se voltam no intuito de praticar a impunidade.

Dessa forma, tem-se como problema de pesquisa, que aqui é apresentado, “Como o Direito Penal se aplica aos casos de quem sofre os cibercrimes? ”

2 CRIMES CIBERNÉTICOS

A internet é capaz de propiciar facilidade e dispor benefícios, como conectividade para compra de produtos, redes sociais e outros, o que modificou significativamente a forma de se relacionar na sociedade. No entanto, essa facilidade de acesso e a possíveis relações que emergem no ambiente virtual podem causar também diversos malefícios, dado que os cibercriminosos se aproveitam para obter vantagem ilícita, valendo-se da fragilidade dos indivíduos e, muitas vezes, do pouco conhecimento das tecnologias.

Com isso, o crime cibernético, também conhecido como crime informático, ou cyber crimes, são aqueles cometidos de forma indevida pelo acesso da internet. Esses crimes digitais são descritos como furto, falsidade ideológica, invasão de sistema e entre outros. Destaca-se a concepção de Pacheco (2011), quando define que:

> O crime digital é modalidade de delito perpetrado por intermédio de meio eletrônico digital, ou que afete o objeto tutelado e protegido pelo Direito Penal (...). Ante a ampla possibilidade de ataques digitais, os instrumentos docrime podem ser dos mais variados, tais como computadores de mesa (Desktops), computadores portáteis (notebooks e notebooks), telefones celulares com funções integradas (smartphones), ou dispositivos mais singelos tecnologicamente, tais como circuitos integrados (processadores ou chips), dispositivos de armazenamento de dados (pendrives ou hard disks) ou outros dispositivos similares que processem dados, além dos recursos empregados por meio de engenharia social (PACHECO, 2011, p. 4).

Esses conceitos têm grandes mudanças pertinentes ao uso, pois, com o tempo, a facilidade de ultrapassar fronteiras faz com que se torne mais “comum” esse tipo de ato, sendo consequências que definem esses crimes, como a intenção de atingir o sistema, obter dados e cometer algo para vantagem própria. Quando esses crimes são relatados como comuns, enquadram-se na Lei Penal, pois é quando distribuem as informações que são invadidas.

De acordo com as quantidades exuberadas e dificuldade de tratamento nos atos

criminosos ocorridos, destaca-se que foi criada em 2014 a Lei nº 12.965, conhecida como Marco Civil da internet, com preceitos que estabelecem princípios, garantias e direitos sobre o uso da internet. Sendo eles, destacados pelo artigo 3º que dispõe:

> **Art. 3º** A disciplina do uso da internet no Brasil tem os seguintesprincípios:
> I - Garantia da liberdade de expressão, comunicação e manifestação depensamento, nos termos da Constituição Federal;
> II - Proteção da privacidade;
> III - Proteção dos dados pessoais, na forma da lei; IV - Preservação e garantia da neutralidade de rede;

> IV Preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
> V- Responsabilização dos agentes de acordo com suas atividades, nos termosda lei (BRASIL, 2014).[1]

Quanto às características dos crimes cibernéticos, percebe-se que funcionam de modo diverso, sendo adotadas as teorias que se aplicam pelo processamento do julgado, nos fatos de fronteiras, faz com que o objeto tutelado possa vir a ser de outros locais, em que se dá à ubiquidade de competência. Mas, nas ferramentas assumidas sobre as utilizações inaptas, será enfatizado sobre o Estelionato virtual.

Embora as práticas já venham a ser discutidas desde os anos 60, a modernização fez com que a utilização de rede seja um ambiente ideal para o crime cibernético, pois muitas pessoas que utilizam não têm conhecimento aprofundado sobre sistema e acabam se tornando vulneráveis a ataques.

Por fim, cabe dizer que o surgimento da internet e as facilidades para executar atividades diárias fazem com que a interação seja ampla e traga submissão aos usuários, como assim analisado no tópico a seguir sobre o estelionato Virtual.

2.1 Criação de perfis falsos

A criação de um perfil falso, configura crime, então no anonimato isso ocorre para que haja interação entre as pessoas e estabeleça diálogos que vão trazer algum lucro para quem faz.

A responsabilidade para esses casos vigora no crime de falsa identidade, disposto no artigo 307 do Código Penal, que relata:

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obtervantagem, em proveito próprio ou alheio, ou para causar dano a outrem: Pena - detenção, de três meses a um ano, ou multa, se o fato não constituielemento de crime mais grave (BRASIL, 1940).[2]

Essa vantagem através do proveito alheio é uma comprovação de dolo, vez que se cria um perfil já com o intuito de cometer esses atos. Mesmo que viole as diretrizes de dados e de segurança nos termos de serviço da rede social, o abuso é bem comum nos dias atuais, pois é

[1] BRASIL. Marco Civil da Internet: comentários à lei n. 12.965, de 23 de abril de 2014. São Paulo: Saraiva, 2014.
[2] BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

elemento subjetivo que implica no direito de personalidade da vítima.

O agente, que faz isso, deve ser inserido como declaração falsa, para que o fato seja juridicamente julgado como crime de falsidade ideológica e, assim, não cometa vantagens que tipifique o estelionatário.

> I- Superior Tribunal de Justiça entende que o estelionato absorve a crime falsidade documental, caso esta tenha sido usada como crime meio para o delito de estelionato;
> II- Supremo Tribunal Federal entende que há concurso formal de crimes, visto que esses delitos atingem bens jurídicos diferentes. Além disso, o crime de falsidade de documento público é mais severamente punido do que o segundo, afastando a teoria de absolvição dos crimes;
> III- Há concurso material de crimes, pois há uma pluralidade de comportamentos;
> IV- O crime de falsidade de documento público prevalece sobre o estelionato(CAPEZ, 2020).

O entendimento do Superior Tribunal de Justiça foi feito pela súmula 17, que relata o teor de: "Quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido", sendo necessário comprovar o fato que identifique o ato de estelionato, pois, caso contrário, prevalece o julgamento Federal que tipifica o concurso formal de crimes, em junção da falsidade e estelionato.

2.2 Fraude Recíproca

Nos crimes cibernéticos e de estelionato, é concedido que a vantagem ilícita seja um estudo de casos recíprocos, nos exemplos que ocorrem a torpeza bilateral, como dito aos atos que o agente e a vítima visam obter a vantagem indevida, prejudicando ou não o outro. Como fato estudado, a base disso é quando a vítima é enganada, mas ainda assim contribuí parao feito.

Nesse posicionamento, tem-se a concepção de que pode não haver o crime, pois a vítima já não reage com boa-fé e, assim, o direito não pode amparar a má-fé desta. Já em outra cirscunstância, pode ser julgado como boa-fé que não constitui subjetividade, sendo de dolo do agente fazer algo com a vítima, pois só nessa intenção já caracteriza o estelionato.

Diante dos fatos, o que prevalece é que: "não há possibilidade de compensação de condutas no direito penal, devendo ser punido o sujeito ativo e, se for ocaso, também a vítima, quando praticada a conduta ilícita" (CAPEZ, 2020, p. 25).

De acordo com Guaracy Moreira (2010), em seu código comentado, caracteriza fraude

e estelionato da seguinte maneira:

> 1.1 Fraude eletrônica majorada, § 2º B – A pena prevista no § 2º A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 a 2/3), se o crime é praticado mediante a utilização de servidor mantido forado território nacional. Não são raros os golpes e as fraudes provindos de hackers e cibercriminosos que atuam e são mantidos fora do nosso território.
>
> 1.2. Estelionato obtido com emprego de documento falso. O tema é tormentoso na doutrina e na jurisprudência. São várias orientações e inúmeros julgados a respeito do assunto. Predomina, porém, o entendimento de que o crime de estelionato absorve o delito de falso. Adota-se o chamado princípio da consunção. Trata se, pois, de crime único. A falsidade foiapenas um meio para o agente alcançar vantagens ilícitas, um meio deexecução do estelionato.
>
> A Súmula nº 17 do STJ estabelece que "quando o falso se exaure no estelionato, sem mais potencialidade lesiva, é por este absorvido". Assim, se o agente, por exemplo, utilizar-se de documento falso e realizar diversas compras de eletrodomésticos em vários estabelecimentos mediante a falaciosa promessa de pagamento, responde apenas pelo crime de estelionato, aplicando se o princípio da consunção. O falso praticado visou unicamente à obtenção de vantagens ilícitas. A falsidade, na espécie, é mero delito meio para a prática do estelionato, delito fim. Os delitos dos arts. 297 e304 estarão absorvidos pelo art. 171 todos do CP.

Magalhães Noronha (1954), que defende o concurso formal de crimes (art. 70 do CP), diz que "há unidade de ação, de atuação e multiplicidade de bens jurídicos violados". Nesse sentido, é a jurisprudência do Superior Tribunal Federal, em que o descaminho não envolve o crime de falsificação. Há uma disputa formal quando a falsificação é um meio de cometer outro crime, como o desaparecimento.

Uma terceira posição, minoritária, entende que o fato deve ser resolvido de acordo com as próprias regras do jogo. Qualquer pessoa que danifique a propriedade de alguém usando um documento falso afeta dois objetos legais separados, propriedade e fé pública.

Portanto, a punição deve ser aplicada. Como as penas neste caso se tornam muito altas, razões de política criminal têm levado a jurisprudência a decidir pela absorção de mentiras por ofuscação. No entanto, isso é comum no folclore e na jurisprudência estrangeira. Seguimos o livro, aliás, a ação é autônoma e atinge não apenas dois bens jurídicos distintos, mas também dois contribuintes distintos: na fraude a pessoa, na falsa o Estado.

Decisão do Superior Tribunal Federal tendo como relator o Min. Moreira Alves assinala que:

> Se além da falsificação do documento público, há assunção de identidade falsa para o levantamento do dinheiro, não há que se pretender que o falsum tenha sido o único meio fraudulento empregado pelo agente. Existência de concurso material

de crimes de falsidade material e estelionato (STF – HCno 55.248 – RTJ 85/491).[3]

3 CRIMES POR MEIO VIRTUAL

A partir do entendimento de que a prática de crimes na Internet tornou-se possível, o direito penal deve agora compreender quais são os crimes mais importantes cometidos no século XXI, dos quais é possível introduzir medidas preventivas e leis que amparem esses crimes.

A Internet é um dos meios tecnológicos usados por criminosos cibernéticos para quebrar dados pessoais na Internet, usando formas sofisticadas de atacar os direitos humanos e insultar os direitos por meio de calúnia e difamação.

Com o desenvolvimento da tecnologia, a conexão com a World Wide Web tornou-se cada vez mais acessível, ainda mais com a popularização dos smartphones, computadores, que possuem recursos que permitem diversos acessos.

Os ataques dos cibercriminosos às suas vítimas são silenciosos, a arma utilizada costuma ser um computador, tablet, smartphone ou outro meio tecnológico surpreendente. O dano à imagem de uma pessoa que é agredida por esse tipo de criminoso é imensurável (LIMA; XAVIER, 2015).

Além disso, possuem sistemas e estratégias intimamente ligados aos crimes-cibernéticos, nos quais, mesmo com o investimento e evolução constante no campo da tecnologia, muitos ataques ainda ocorrem e são eficazes, principalmente devido à educação social, na qual convence o usuário para, sem perceber, instalar programas que serão perigosos para o computador e que podem coletar dados de pessoas, infringindo os princípios desegurança da informação. Alguns dos ataques são descritos como exemplos: *malware*, *spyware* e *ransomware.*

Malwares podem ter muitas funções, dependendo da programação e do tipo de serviço. Spyware *Keylogger* -. Uma das atividades mais comuns desse tipo de ataque é a criação de máquinas zumbis, uma botnet. - Botnets são máquinas que realizam tarefas controladas remotamente por seus criadores, na maioria das vezes, são utilizadas para realizar ataques em grande escala, em que vários computadores podem destruir computadores e servidores governamentais e sites, também conhecido como ataque DDOS (denial of service attack). Eles trabalham em conjunto com *phishing* para induzir as vítimas a acessar sites clonados sem seu conhecimento e repassar informações pessoais (OLIVO, 2010).

Desde *spyware* instalando spyware, na maioria dos casos, sem que a vítima perceba, para que ela possa monitorar seu computador. Por meio da conexão feita P2P (Per-to-Per), ou seja, seu computador é conectado diretamente ao computador do criminoso cibernético, todos os documentos, fotos, vídeo, webcam podem ser compartilhados entre ambos. Com isso, o

invasor pode instalar mais softwares maliciosos, ou ameaçar e chantagear a vítima ao receber um documento ou foto (PEREIRA; MARTINS, 2014).

E *ransomware* que consiste em sequestrar o computador, ou seja, quando roda na máquina da vítima, seu código malicioso codifica todas as informações do computador e depois apresenta uma tela com os procedimentos a serem seguidos para restaurar os arquivos. Na maioria dos casos, o dinheiro costuma ser solicitado para recuperação do computador, quando a vítima recebe a senha, retira a criptografia feita, o que novamente dá acesso aos arquivos (CABRAL, 2015).

A Internet permite uma utopia onde as pessoas mesmo em distâncias físicas conectam as mais distantes como se estivessem perto um do outro. Para que a participação e contribuição da pessoa sejam efetivas no chamado espaço cibernético, é preciso que o Estado ajude a protegê-lo direitos e garantias fundamentais e as novas tecnologias não podem ser um só significa violar esses direitos (PANNAIN; PEZZELLA, 2015).

3.1 Crimes Contra honra

A honra é protegida pela constituição, que tem disposição de lei fundamentado no art. 5º, X, Constituição Federal. São crimes de honra conhecidos de longa data do ordenamento jurídico brasileiro. Honra é um direito a identidade prevista na constituição é necessária para proteção da dignidade e reputação pessoal de uma pessoa (BARROSO, 2004).

A dignidade, segundo os ensinamentos brasileiros, divide-se em dignidade objetiva e dignidade subjetivo. Primeiro, depende da reputação do ambiente social em que vive. Em segundo lugar para homenagear e constituição pessoal da vítima, o julgamento que cada um tem de si mesmo (CUNHA,2014).

Para Guilherme de Souza Nucci (2017) a honra objetiva também pode ser chamada de objeto jurídico, que será a reputação ou a imagem de uma pessoa perante terceiros, enquanto a honra subjetiva é chamada de objeto material. Dentro do tema dos crimes contra a honra, na legislação direito penal específico, existem três tipos de crimes separados: difamação, calúnia e injúria.

Na legislação, distinguem-se os tipos de crimes e penas, que são os seguintes:

> Calúnia Art. 138 Caluniar alguém, imputando-lhe falsamente fato definido como crime: Pena - detenção, de seis meses a dois anos, e multa. Difamação

> Art. 139 Difamar alguém, imputando-lhe fato ofensivo à sua reputação: Pena - detenção, de três meses a um ano, e multa. Injúria
> Art. 140 Injuriar alguém, ofendendo-lhe a dignidade ou o decoro: Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940, online).

Caluniar é apontar um fato falso para alguém, a difamação, por outro lado, é definida como atribuir a alguém criminoso, mas um insulto à sua reputação e, no final, injurias, ao contrário dos outros comportamentos de "imputação", que é determinado pela atribuição de qualidades negativas ou deficiências (NORONHA, apud CUNHA, 2014).

O Código Penal brasileiro permite em concordância ao § 3º, a chamada exceção a verdade que se caracteriza por provar a verdade da definição, generativo comportamento anormal (expressar comportamento que é falsamente insultante):

> Exceção da verdade § 3º - Admite-se a prova da verdade, salvo: I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível; II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141; III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível (BRASIL, 1940, online). (Grifo nosso)

Tendo em conta a tipificação da exclusão da verdade prevista no Código, o Código Penal é entendido como a própria lei que traz pressupostos seguros para essas exceções, ou seja, se o ato criminoso especificado estiver correto, o tipo de crime é excluído, assim prevê a proibição de punição exceção à verdade que deve ser seguida. Como calúnia, em difamação, protege-se a honra objetiva da vítima, o que está descrito na atribuição o fato de que, mesmo não sendo crime, a reputação da vítima diante de terceiros (CUNHA, 2014).

Caluniar é expor alguém publicamente, avaliar algo de sua reputação com uma vontade específica *(animus difamandi),* bem como que a denúncia chegue a informações de terceiros (NUCCI, 2017).

Tal como no estudo do crime anterior, denominado de exceção da verdade, mas apenas nos casos em que a vítima é um funcionário público e a ofensa está relacionada com o exercício de funções e é responsabilidade do infrator prová-la a veracidade da acusação, excluindo a ilicitude de sua conduta (CUNHA, 2014).

> Exceção da verdade Parágrafo único –
> A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções (BRASIL, 1940, online)

Na injuria, ao contrário dos crimes anteriores, o direito tutelado é a dignidade subjetiva do ofendido, caracterizada pela conduta ou omissão como delito; existe pessoa específica que

insulta sua dignidade, via de regra, não existe avaliação de provas concretas, mas conceituação negativa da vítima (CUNHA, 2014).

É um insulto que macula a própria dignidade subjetiva, capaz de alcançá-la sua dignidade, dano à sua imagem, com vontade específica (*animus difamandi*), no momento em que o insulto à atenção ofensa, apesar do conhecimento de terceiros, não reconhecendo a exceção verdade (NUCCI, 2017).

Não há como falar sobre esses comportamentos sem entrar no assunto liberdade de expressão. A liberdade de expressão é baseada no respeito à autonomia e a dignidade humana, o que exige o respeito pelos direitos fundamentais do outro. As tecnologias digitais estão redefinindo a liberdade de expressão aumentando positivamente as oportunidades de participação social e cultural, ampliando o acesso à verdadeira democracia (PANNAIN; PEZZELLA, 2015).

É livremente exercido e é necessário exercer o direito de se expressar como tomar os direitos dos outros e os agressores devem responder por seus excessos. No entanto, comportamento feito pela internet nem sempre é punível, é devido à dificuldade de provar o verdadeiro criminoso (não o nomear) por falta de prontidão do estado para lidar com tal situação (COELHO; BRANCO, 2016).

A identidade deve ser considerada na análise de um crime de ameaça da vítima. Portanto, idade, gênero, raça, cor, orientação sexual, etc. Características são fatores que devem ser analisados em uma situação específica, é preciso analisar se o comportamento como promessa de causar dano injusto a alguém (CUNHA, 2014).

3.2 Crimes contra a inviolabilidade o patrimônio - Estelionato

O estelionato é o termo dado para artifícios de iludir alguém, com concepção que decorre de palavra com origem grega, na qual identifica “lagarto que engana as presas”, assim se assemelha ao sentido descrito pelas fraudulências de coagir as vítimas (RIBEIRO, 2019)

Ao longo dos anos a repressão da conduta por prejuízo alheio em tentar ter vantagem ilícita e utilizar a boa-fé como princípio do erro, foi se aperfeiçoando e demandando de discussões legislativas que punisse quem cometesse. Assim, para Andreucci (2014), o estelionato é a indução do erro, na fragilidade da pessoa, sendo extraído pelo poder psicológico que manipula.

Para isso, o estelionato é tipificado como a vantagem patrimonial, que receberá da vítima a entrega de bens e de valores, sendo entregas baseadas pela coação antes fundada pela boa-fé, como ilusão e a demonstração de confiança e respeito sobre o outro.

Em suma, o estelionato é quando ocorre a entrega voluntário do bem, sob a supostaboa índole de quem a manipulou, cabendo a vantagem ilícita e o prejuízo alheio, sendo prescrito no artigo 171 do Código Penal, que descreve em sua redação:

> Art. 171. Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer meio fraudulento: Pena – reclusão, de 1 (um) a 5 (cinco) anos, e multa. (BRASIL, 1940)

A fraude é dada como o principal delito no estelionato, pois os elementos entregam em conduta direcionada na vantagem e na utilização da fraudulência, assim como descrito acima, sendo que as verificações desses elementos sejam notadas pela vontade do coator de se beneficiar em pró ao terceiro.

O objeto pode tutelar pela confiança e credibilidade, sendo precedido aos desejosque reprimem a fraude. Feito, tipo como o caso de sua própria natureza, por que é juridicamente ilícita. Por isso, o estelionatário é dito como criminoso, mesmo que pela forma simples da ação.

É importante ressaltar que ocorre a distinção entre o estelionato aos demais crimes patrimoniais, pois não é utilizada a força, assim descrito por Greco, em sua citação sobreo estelionato:

> Desde que surgiram as relações sociais, o homem se vale da fraude para dissimular seus verdadeiros sentimentos e intenções para, de alguma forma, ocultar ou falsear a verdade, a fim de obter vantagens que, em tese, lhe seriam indevidas. (GRECO, 2010)

Pode-se dizer mediante a isso, que é o crime de estelionato é conceituado pela vantagem ilícita, em prejuízo da vítima, por meios de fraudes e de indução incorreta por meios frágeis de conseguir as coisas, é ato tipificado e protegido pelo ordenamento penal, como inviolabilidade do patrimônio. Os sujeitos são divididos em passivo e ativo: sendo o ativo o coator e o passivo quem sofre todo esse engano. É considerado crime doloso, pois é advinda da vontade de auferir a vantagem ilícita, admitindo sua vontade para a consumação e obtenção do ato.

Essa supremacia desses fatos é introdutória sobre o preceito que será abordado a seguir no tópico de estelionato virtual, sabendo que é julgado por intermédio dessa lei, como

desdobramentos dos fundamentos aqui descritos.

3.2.1 Estelionato virtual

Quando se trata de estelionato virtual, é induzido ao erro na vantagem patrimonial ilícita, em que os métodos são executórios por amplas possibilidades do ato. Sabendo que quem pratica, tem diversos conhecimentos na área tecnológica, sendo que atua operando ao meio eletrônico, perceptíveis sobre os pontos que pode facilmente enganar a outra pessoa.

É infundado que esse crime é crescente e se tornou mais ainda após a pandemia do covid-19, pois entre as características que mais se tornam frequentes aos golpes serão descritos como a invasão nas técnicas da internet.

Os hackers que são os que praticam esse tipo de conduta, é definido como aquele que utiliza as habilidades para alcançar benefícios, criando configurações que consiga o acesso em bancos, empresas, redes de acesso e entre outros. Sendo de costume a invadir os sistemas para apontar a vítima que deve ser melhorado algo no processo visto. Para isso, existem programas que são utilizados para coletar informações e fazer o trafego da rede que foi interceptada.

Dessa forma, o estelionato virtual acontece quando os infratores criam ou acessam alguma rede de dados, criando perfis falsos para não ser identificados e fazendo promessas de troca para obter a vontade pecuniária. É aproveitado por meio digital, brechas que permite a obtenção dos anseios.

Para Recorda Freitas (2009), o virtual traz vantagens, mas com a facilidade que dispõe, é possível fácil acesso e golpes, como compras online, que são realizadas pelo computador, assim como outros meios que eles coagem para conseguir.

Essa proporção faz com que ocorra a invasão dos dados da vítima, sujeita a diversos fraudes e em especifico ao que acontece muito, além do citado acima das compras, é a conta bancaria. Pois através do internet-banking, eles têm como fazer com que a vítima acesse e deixe os dados inseridos na página, como nos casos da nova funçãode transferência “pix”.

Nas palavras de Junior (2008), o crime de estelionato virtual é descrito da seguinte maneira:

> Quem comete crime de estelionato é aquele que cria página em ambiente virtual ou faz anúncios em sites, simulando por exemplo, a venda de produtos com o objetivo de induzia a vítima em erro para queessa efetue

> pagamento antecipado para a compra de produtos, na ilusão de que irá recebe-los posteriormente, quando, em verdade, se trata de um golpe empregado pelo agente para obter vantagem indevida, aproveitando-se da boa-fé de pessoas para enganá-las e provocar prejuízo patrimonial a elas.

Essas hipóteses configura o crime, pois faz com que a pessoa pague antecipado por produtos que não existe, esse exemplo é visado como a boa-fé do comprador para com o prejuízo patrimonial de forma aludida feita pelo estelionatário.

Diante a esses fatos, a diferença do estelionato em ambiente virtual para o estelionato comum, é que a pessoa vai operar em um sistema, um pela plataforma digital e a outra por ambiente físico, mesmo sabendo que o virtual vem a ter maiores índices de acontecimentos.

3.2.2 Estelionato virtual no ordenamento jurídico

O estelionato virtual não tem previsão no texto do estelionato, descrito no artigo 171 do CP, sendo diploma que o delito feito pela obtenção da vantagem ilícita já traz um entendimento sobre o caso, mesmo que questão de ser na internet ou não. Em tese, é relatado as semelhanças para a mesma penalização, pois os objetos resultam o mesmo intuito.

Os debates de tipificação do crime, entra também em contexto ao visto na Constituição Federal, pelo artigo 5º, inciso XXXIX, em que se dá o disposto do princípio da legalidade, isso conta como limitação preventiva do Estado para defesa desse conceito de crime.

Por ser tema ainda recente os tribunais discutem com atenção sobre os princípios modernos dos crimes cibernéticos, pois são milhares de vítimas diariamente, como aplicação que possibilita maior entendimento aos casos. Isso contempla que pelo fato de muitas vezes os casos se repetirem, o Ministério Público e poder judiciário, tendem a impunidade, dado a inexistência da lei que cuide desse tipo de crime.

Isso induz que as pessoas julgam como não procedente nenhuma punição ao crime, pois nao é notado a norma regulamentadora especifica que ampare as ilicitudes criminais que é acometida, ainda mais pela dificuldade de localizar o autor, para determinar a competência do julgamento.

De acordo com Cruz e Rodrigues (2018), a tipificação legal é conceituada da seguinte forma:

> os crimes praticados por meio da internet possuem tipificação legal e quando se consegue identificar os autores do delito há a sanção penal. O

> que faz com que as pessoas acreditem na impunidade do fato é a ausência de previsão legal especifica que contenha no seu texto a palavra “internet”. Muito embora o preambulo do dispositivo legal não faça menção ao termo “internet”, o fato dos sujeitos se utilizarem da rede mundial de computadores para praticar o ilícito, tem-se que a consumação possui tipificação, devendo ser aplicadas as sanções previstas (CRUZ e RODRIGUES, 2018).

Diante disso, como “omissão” do ordenamento jurídico em razão a esse tema, os pontos norteadores para uso da internet, são condutas que se baseiam nas análises prescritas pelo Código Penal, visto que todo o objeto relata a ilicitude do ato doloso, em necessário atendimento de punição que use como alicerce as condutas do estelionato comum tipificado.

3.3 Crime de invasão de privacidade e da intimidade

Existem proteções constitucionais à privacidade e intimidade, ambas consagradas no artigo 5º, X da Constituição Federal, que integram o rol dos direitos fundamentais, instituída pela Lei nº 12.737 de 2012 (conhecida como Lei Carolina Dieckmann), há uma previsão legal no artigo 154-A do Código Penal sobre invasão de dispositivos informáticos, ou seja:

> 154-A. Intrometer-se em dispositivo de computador alheio, conectado ou não a uma rede de computadores, violando um mecanismo de segurança e com o objetivo de obter, degradar ou destruir dados ou informações sem a permissão expressa ou implícita do proprietário do dispositivo ou instalação causando danos ao obter lucro ilícito: Pena - reclusão, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL, 1940, online). [4]

Os objetos jurídicos protegidos são a privacidade, a vida pessoal e o direito à privacidade nos dados contidos no dispositivo informático, sendo a principal parte do primeiro tipo de crime "intrusão", ou seja, entrar sem permissão, aberta ou secretamente.

O segundo tipo é caracterizado pela visão de “instalação” e se configura apenas com a instalação de uma vulnerabilidade que não é necessária para efetivamente obter uma vantagem ilegal e, portanto, é um crime oficial (CAPEZ, 2016).

[4] BRASIL. Decreto-Lei 2.848, de 07 de dezembro de 1940. **Código Penal.** Diário Oficial da União, Rio de Janeiro, 31 dez.

A atriz Carolina Dieckmann foi vítima de um ataque ao seu computador e do compartilhamento de arquivos pessoais, e suas fotos íntimas vazaram na internet. O objeto jurídico do crime descrito no artigo 154-A é a privacidade pessoal e/ou profissional armazenada em dispositivo informático, que pune por ataque a dispositivo informático alheio, violação dos seus mecanismos de segurança ou instalação de dispositivo vulnerável (CUNHA, 2014).

No § 3º, o legislador apresentou os atributos essenciais do crime, que está diretamente relacionado à invasão da vida pessoal da vítima. Neste caso, a violação conduz à aquisição do conteúdo de comunicações eletrônicas privadas, informação confidencial (entre outras coisas), exceto nos casos de descumprimento em caso de crime mais grave, a pena é aumentada de seis meses para dois anos. (CAPEZ, 2016).

Da mesma forma, o § 4º indica um elemento principal do crime relacionado com o anterior e estipula que a pena "é aumentada de uma para duas partes se for descoberta, negociada ou transferida a terceiro, qualquer que seja o caso, capacidade de dados ou informações obtidas" (BRASIL, online).

3.4 Crime contra a liberdade sexual com menores

É muito importante abordar a questão da liberdade sexual, principalmente no envolvimento de menores. O Estatuto da Criança e do Adolescente fornece uma descrição básica dos crimes contra crianças e adolescentes e tenta prever as diferentes condutas que podem ser realizadas (CAPEZ, 2016).

Ao contrário dos comportamentos descritas a esse crime, geralmente ocorrem em segredo. Alguns aplicativos de celular facilitam o compartilhamento de informações e mensagens instantâneas, o que faz com que muitos usuários compartilhem informações sem perceber que necessariamente estão cometendo um crime (CUNHA, 2014).

Além disso, um tema que não é muito abordado, mas que merece atenção – é a *deep web* (rede profunda). Esta plataforma é praticamente desconhecida pela maioria dos utilizadores, permitindo a prática de comportamentos ilegais através de sites considerados "invisíveis" por não serem encontrados nos motores de busca tradicionais como o Google. Diversas situações ilegais são encontradas nessa plataforma, como tráfico de drogas, pedofilia, tráfico de pessoas, tráfico de órgãos e outras condutas (GLOBO.COM, 2016, online).

O artigo 241 do Estatuto da Criança e adolescente descrevem comportamentos ilegais, conforme descrito: Comercializar ou expor à venda foto, vídeo ou outra gravação contendo

cena sexual ou pornográfica envolvendo criança ou adolescente: Pena - reclusão de 4 (quatro) a 8 (oito) anos e multa (BRASIL, 1990). [5]

As condutas que mais se diferenciam no ambiente virtual são as previstas nos artigos 241-A e 241-B da Lei da Criança e do Adolescente. O artigo 241-A prevê punição ao comportamento ilícito de compartilhamento de qualquer processo de distribuição de identidades sexuais ou pornografia com a participação de crianças e adolescentes. 241-B pune quem, de qualquer forma, obtiver ou guardar qualquer imagem/foto de qualquer natureza com sexo aberto ou aspecto pornográfico com criança e/ou adolescente (TAVARES, 2012).

Em relação ao crime cometido no ambiente virtual, a jurisprudência é rígida na aplicação da punição, mesmo considerando que os crimes cometidos pela rede global são de natureza transnacional/internacional. A propósito, é mencionado que a decisão do Supremo Tribunal de Justiça sobre esta questão:

> **HABEAS CORPUS Nº 413.069 - SP (2017/0208680-6) RELATOR: MINISTRO JOEL ILAN PACIORNIK IMPETRANTE: DEFENSORIA PÚBLICA DA UNIÃO ADVOGADO: DEFENSORIA PÚBLICA DA UNIÃO IMPETRADO: TRIBUNAL REGIONAL FEDERAL DA 3A REGIÃO PACIENTE: MICHAEL LEME DE QUEIROZ DECISÃO** Cuida-se de habeas corpus substitutivo de recurso próprio, com pedido de liminar, impetrado em benefício de MICHAEL LEME DE QUEIROZ, contra acórdão do Tribunal Regional Federal da 3ª Região (APC n. 2016.61.14.002516-6). Consta dos autos que o paciente foi condenado em primeiro grau pela prática dos crimes do arts. 241-A e 241-B, do Estatuto da Criança e do Adolescente c.c. art. 69 do Código Penal, à pena de 4 (quatro) anos de reclusão, em regime aberto, consistentes em prestação de serviços à comunidade e prestação pecuniária. O Tribunal Regional Federal da 3ª Região, por sua vez, negou provimento ao recurso defensivo e deu parcial provimento ao recurso ministerial, conforme ementa a seguir transcrita: DIREITO PENAL. PROCESSO PENAL APELAÇÕES CRIMINAIS. PORNOGRAFIA INFANTO-JUVENIL. LEI 8.069/90. ARTIGOS 241-A E 241-B. PROGRAMA DE COMPARTILHAMENTO DE DADOS. USO. COMPETÊNCIA. JUSTIÇA FEDERAL. DOLO CARACTERIZADO NO COMPARTILHAMENTO DOS ARQUIVOS ILÍCITOS. AUTORIA E MATERIALIDADE INCONTROVERSAS. ABSORÇÃO. INOCORRÊNCIA NO CASO CONCRETO. CONDENAÇÃO MANTIDA. DOSIMETRIA. ALTERAÇÕES. 1. Réu flagrado em posse de acervo de fotografias e vídeos de pornografia Infanto juvenil, acervo este armazenado digitalmente em discos rígidos de sua propriedade. Teria, ainda, compartilhado arquivo do mesmo teor anteriormente. [...] em outros termos: ao disponibilizar arquivos de conteúdo pornográfico infanto-juvenil em servidor mundialmente acessível, o que há é a disponibilização/divulgação de pornografia infanto-juvenil além das fronteiras nacionais, o que torna claro seu caráter transnacional. [...] 3. Por sua vez, a constatação da internacionalidade do delito demandaria apenas que a publicação do material pornográfico tivesse sido feita em "ambiência virtual de sítios de amplo e fácil acesso a qualquer sujeito, em qualquer parte do planeta, que esteja conectado à internet" e que "o material pornográfico, envolvendo crianças ou adolescentes tenha estado acessível por alguém no estrangeiro, ainda que não haja evidências de que esse acesso realmente ocorreu" [...] Publique-se. Intime-se. Brasília (DF), 23 de fevereiro de 2018.

[5] Lei 8.069, de 13 de julho de 1990. Dispõe sobre o **Estatuto da Criança e do Adolescente** e dá outras providências. Diário Oficial da União, Brasília, 16 jul. 1990

(STJ - HC: 413069 SP 2017/0208680-6, Relator: Ministro Joel Ilan Paciornik, Data de Publicação: DJ 28/02/2018) (grifos nossos)

O ato, previsto como crime nos referidos artigos, tem condão de proteger a dignidade e a liberdade sexual de crianças e adolescentes. São crimes dolosos que requerem danos potenciais e não requerem danos materiais reais (NUCCI, 2016).

Com a popularidade de aplicativos como o Whatsapp, a conduta do artigo 241-B aumentou. Ao introduzir os tipos de crimes previstos neste artigo, deve punir o agente que tiver em seu poder imagens de menores de 18 anos envolvidos em pornografia. Um objeto material é uma foto, vídeo ou imagem que contenha pornografia ou sexo explícito com a participação de uma criança ou adolescente, objeto legal para proteger o desenvolvimento moral de uma criança ou adolescente (NUCCI, 2016).

4. ORDENAMENTO JURÍDICO PARA OS CRIMES VIRTUAIS

4.1 Lei Caroline Dieckmann (LEI Nº 12.737/12)

No Brasil, não existiam leis de combate ao cibercrimes até 2012, quando uma lei foi introduzida, demonstrando o primeiro sinal do movimento da advocacia criminal para apoiar a população contra o cibercrime. A Lei nº 12.737/12, conhecida como Lei Carolina Dieckmann, surgiu graças a um projeto da deputada federal Paula Teixeira (PT-SP), que buscou regular os crimes cometidos no ambiente virtual, que até então era uma brecha legislativa.

O motivo do nome "Carolina Dieckmann, deve-se ao envolvimento da atriz em um crime cibernético na época, onde suas fotos íntimas foram *hackeadas* e expostas na internet, o que teve muitas repercussões na mídia e nas redes sociais. Para se ter uma ideia do reflexo do caso ocorrido em 4 de maio de 2012, foram divulgadas 36 fotos íntimas da atriz. As fotos rapidamente viraram assunto na internet, pois era o assunto mais falado no *Twitter,* e segundo dados da ONG *Safernet*, as imagens tiveram mais de 8 milhões de acessos únicos em apenas 5 dias (ROMANI, 2012).

Este evento acelerou a entrada em vigor da lei, que foi promulgada em dezembro de 2012 e entrou em vigor em 3 de abril de 2013. De modo geral, a lei contribui para a Código Penal, Seções 154-A e 154-B. O motivo do aditamento ao artigo 154 refere-se à sua descrição dos crimes de violação do segredo profissional, que sugere:

> Art. 154 - A revelação por alguém, sem justa causa, de segredo que conhecia por direito à sua função, serviço, ofício ou profissão, e cuja revelação pudesse causar prejuízo a outrem: pena - detenção, de três meses a um ano, ou 'multa de um conto dez contos de arroz. (Vide Lei nº 7.209, de 1984) Parágrafo único - somente em caso de representação (Brasil, 1940).
> Art. 154-A. Invadir equipamentos informáticos de outras pessoas, independentemente de estarem ou não ligados à rede informática, violar indevidamente um mecanismo de segurança e com o objetivo de obter, adulterar ou destruir dados ou informações sem a autorização expressa ou implícita do proprietário do dispositivo ou da instalação. Vulnerabilidades para obtenção de vantagem ilícita: pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (Brasil, 2012).

Segundo Capez (2014), a lei permite a classificação adequada do que pode ser considerado crime, pois nela toda pessoa pode ser sujeito ativo, referindo-se ao crime comum. O sujeito passivo não é o proprietário do dispositivo informático. Os dados sobre o bem jurídico protegido estão relacionados ao que se define como o nível de crime perigoso, ou seja, a partir do qual os documentos descobertos são importantes.

Dessa forma, sua abordagem pode ser caracterizada como crime formal, devido ao acesso, modificação ou destruição de dados e informações importantes. E, por fim, um impacto sobre o perigo abstrato mais importante ao bem jurídico tutelado, que é a privacidade.

Entender que o bem jurídico tutelado é a liberdade individual do usuário do aparelho informático é fundamental, pois este é o primeiro impacto de qualquer tipo de crime cibernético. A liberdade é um dos direitos e garantias fundamentais impostos no artigo 5º da Constituição Federal de 1988, portanto, na esfera penal, encontram-se os crimes a que ela incide.

Foi criado o tipo penal "invasão de equipamentos de informática", conforme art. 154-A e sua respectiva modalidade de ação penal, para a qual o art. 154-B.

> Art. 154-B. Nos crimes previstos no art. 154-A, procede apenas por representação, salvo se o crime for cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou municípios ou contra concessionárias de serviços públicos. (Brasil, 2012)

Com o artigo 154-B, torna os crimes cometidos no 154-A de conduta criminal pública dependentes da representação da vítima, pois sua intimidade e vida privada são os bens disponíveis que são violados. Assim, a vítima também tem o direito de considerar se deseja evitar o processo legal, na forma de uma ação pública incondicional. A atuação direta do Ministério Público neste tipo de crime ocorre apenas nos casos em que o crime for cometido contra a administração pública direta ou indireta de qualquer dos poderes da União, Estados, Distrito Federal ou Municípios ou contra concessionárias de serviços públicos (PAGANOTTI, 2013).

Assim, mostra como o que aconteceu com a atriz Carolina Dieckmann aumentou a vulnerabilidade da população na internet, pois temiam que algo semelhante acontecesse com eles. Um dos motivos do temor e da maior celeridade na aprovação das leis apareceu na mídia, que tem muita reflexão neste caso, destacando a falta de legislação penal pertinente ao assunto e direto sobre os perigos da exposição na rede. Com isso, não foram apenas os políticos que se envolveram, mas também um clamor bastante popular em favor de uma legislação que tratasse de crimes cibernéticos (GRANATO, 2015).

Isso mostra que para solucionar um problema de crime ainda não legalizado, às vezes é necessário a ação popular para que determinada lei seja atualizada, demonstrando que apenas a ação legislativa pode ser postergada para que o feed de atualização seja efetivo, à medida que o projeto de lei é processado. Congresso, algo que pode levar até anos, como aconteceu com o Marco Civil da Internet que será descrito a seguir.

4.2 Marco Civil da Internet (LEI Nº 12.965/14)

O Marco Civil da Internet era uma lei que estava em discussão desde 2007, após muitas consultas e debate público e seguido por um período de incerteza e inação após sua apresentação à Câmara dos Deputados. Quando muitos crimes internacionais foram divulgados sobre vigilância em massa não autorizada pelos EUA.

Souza e Lemos (2016), descrevem que o Marco Civil da Internet (Lei nº 12.965/2014) foi a primeira iniciativa do Poder Executivo brasileiro totalmente dedicada às especificações e eventos ocorridos na rede. No entanto, este foi um processo gradual, se não fosse o tratado internacional de segurança na Internet, esse projeto seria esquecido no Senado. Assim, o escândalo serviu de catalisador, acelerando o processo que continuava mostrando mais uma vez sobre a atualização das leis sobre tecnologia da informação que só aconteceu por causa da disseminação da mídia.

Tomasevicius Filho (2016), em sua leitura do Marco Civil, destaca a crítica de que a censura pode ser restabelecida no país, desde que se legalize ao ambiente que até então era totalmente "livre". No entanto, em seu artigo 2º, caput, afirma-se que o uso da Internet no Brasil se baseia no respeito à liberdade de expressão. E a seção 19 afirma que:

> Art. 19. Para garantir a liberdade de expressão e evitar a censura, o provedor de aplicativos de Internet somente poderá ser responsabilizado civilmente pelos danos decorrentes de conteúdos gerados por terceiros se, por meio de ordem judicial específica, não tomar providências no âmbito e em os limites Técnicos de seu serviço e no tempo indicado, torna indisponível o conteúdo identificado como infrator, salvo disposição legal em contrário (Brasil, 2014).[6]

Com este artigo, os provedores de Internet estarão protegidos da responsabilidade pelas ações de terceiros que utilizam seus serviços, evitando assim reclamações ou cobranças que prejudiquem a liberdade. Na qual prevê o princípio da Constituição Federal sob as "garantias da liberdade de expressão, comunicação e expressão do pensamento, nos termos da Constituição Federal" (TOMASEVICIUS FILHO, 2016).

Preservar os direitos fundamentais e garantir que o desenvolvimento tecnológico seja indispensável, pois a legislação deve se basear nas melhores condições para a população, tornando o Marco Civil um instrumento que melhora o desenvolvimento das condições econômicas e sociais de indivíduos e grupos.

---

[6] BRASIL. Lei no 12.965, de 23 Abril de 2014. **Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil**. Brasília, 2014.

Essa lei, considerada pela mídia como a “Constituição da Internet”, buscou disciplinar todas as questões existentes quanto ao uso da rede no território nacional com base em princípios como neutralidade, privacidade e liberdade de expressão, bem como os artigos 32. Que abordam os princípios de uso da Internet, os direitos e garantias dos usuários, o fornecimento de conexões e aplicativos de Internet, a atuação governamental e as disposições finais.

O usuário da rede tem a garantia de que sua privacidade não será violada, a qualidade da conexão estará de acordo com o contratado e que seus dados serão repassados apenas a terceiros com seu consentimento ou em questões legais. Nesse sentido, a lei regulamenta o monitoramento, filtragem, análise e fiscalização de conteúdo para garantir o direito à privacidade no contato com outras pessoas, bem como o direito de impedir que terceiros acessem informações pessoais (Amaral, 2008, p. 306).

A não disponibilização de dados pessoais recolhidos através da Internet a terceiros sem o consentimento prévio do utilizador, bem como o estabelecimento da obrigação de informar os utilizadores sobre a recolha de dados sobre si próprios, quando houver justificação para tal.

Descrito no art. 10 da Lei 12.965/14, determinou que a preservação e disponibilização de registros de conexão e acesso a aplicativos de Internet devem ser realizadas com respeito à intimidade, vida privada, honra e imagem das pessoas direta ou indiretamente envolvidas. Com isso, possibilitou que provedores de Internet e de serviços só sejam obrigados a fornecer informações aos usuários caso recebam ordem judicial. No caso de logs de conexão, os dados devem ser armazenados por pelo menos um ano, enquanto os logs de acesso às aplicações são armazenados por seis meses (MPSP, 2018).

Esta atribuição é complementar ao art. 14, em que os provedores de conexão à Internet não podem manter registros de acesso a aplicativos de Internet sem o consentimento prévio do usuário, nem dados pessoais desnecessários para esse fim. Isso se chama neutralidade de rede, que também proíbe as operadoras de vender pacotes de internet de acordo com o tipo de uso, ou seja, não é permitido criar obstáculos para determinado tipo de conteúdo em prol de uma vantagem econômica. Dessa forma, o tráfego de quaisquer dados deve ser feito com a mesma qualidade e velocidade, sem qualquer discriminação (MPSP, 2018)

O Marco Civil da Internet foi um marco para a legislação de tecnologia da informação, mostrando que a lei pode ser atualizada nessa questão, e que uma constituição voltada para as práticas criminosas nessa área também pode ser criada com estudos e o estabelecimento de objetivos diretos para a proteção do usuário.

4.2.1 Lei Geral de Proteção de Dados (Lei nº 13.709/2018)

A última lei da Internet entrou em vigor em agosto de 2020, a Lei Geral de Proteção de Dados Pessoais (Lei nº 13.709/2018), já conhecida como LGPD. A criação visa reduzir os riscos associados ao uso indevido e/ou tratamento indevido de dados pessoais e, ao mesmo tempo, permitir o desenvolvimento de novos negócios e tecnologias em um ambiente juridicamente seguro. A aplicação da LGPD afetará não apenas os negócios das empresas brasileiras, mas também todos os países, empresas estrangeiras ou domicílios que forneçam produtos e/ou serviços ao mercado brasileiro e monitorem o comportamento dos titulares dos dados no Brasil, independentemente de sua nacionalidade.

A lei define informações sobre o que são considerados dados pessoais, dados sensíveis e dados anônimos, representando informações pessoais (GPF, ID, endereço IP, etc.), dados relacionados à saúde, vida sexual, orientação política, etc. Não permitem a identificação, direta ou indireta, de seu titular respectivamente.

Desta forma, a lei pretende gerir o tratamento dos dados das pessoas que têm acesso à Internet, podendo referir-se a "recolha, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, tratamento, arquivamento, armazenamento ou para extrair dados pessoais" (DANIEL IP, 2019).

Segundo a LGPD as atividades relativas ao tratamento de dados serão realizadas seguindo o princípio da boa-fé. (Art. 6 da LGPD) e em demais princípios que serão mais bem expressados em breve.

Tendo-se em vista o conceito de boa-fé, deve-se ressaltar que está se subdivide em duas formas as quais se apresenta sendo elas: a boa-fé objetiva e a boa-fé subjetiva. A boa-fé Objetiva corresponde a verdadeira regra de comportamento ético e jurídico sendo está determinada de um conceito jurídico indeterminado, encontra-se ligada a equidade do processo, ou seja, considera-se que faz parte da ética do direito.[7]

No âmbito jurídico é aplicado a boa-fé objetiva uma função tripla a qual seria a função interpretativa dos negócios jurídicos; a função que restringe os direitos e a função que cria os deveres. "Como se vê, a definição do conteúdo exato da boa-fé objetiva não é tarefa da qual tenha se desincumbido o legislador. Tal tarefa é reservada ao intérprete, mas não deixada ao seu mero arbítrio".

Cada decisão exige do juízo uma decisão especifica pensando não só na decisão, mas

[7] GAGLIANO, P. S.; FILHO, R. P. Manual de direito civil. 7. ed. São Paulo: Saraiva, 2023. E-book.

também no âmbito social, sendo necessário não esquecer o princípio da boa-fé quando faz determinada decisão. Sendo assim o juiz necessita analisar a boa-fé do ato praticado pelo sujeito e no caso concreto como essa se encaixa para ser uma decisão tão importante para o direito.

Na boa-fé subjetiva o sujeito acredita que está agindo de forma legitima e de acordo com a lei, diferente da boa-fé objetiva onde este tem que estar agindo legitimamente.

Outro princípio mencionado na LGPD é o da finalidade, também tratado no art. 6º desta lei que compõe na "realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;" "pode-se relacionar o princípio da finalidade com o uso dos dados pessoais inseridos no contexto para o qual foram coletados, devendo, portanto, permanecerem adstritos a ele."[8] Sendo assim, os dados não podem ser usados para algo que não seja a finalidade para a qual esses foral coletados.

O princípio que subsegue o da finalidade é o da adequação e se fundamenta da seguinte forma no artigo 6º da LGPD "adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento; "Além disso, trata-se de um princípio limitador relativamente ao modo de coleta dos dados, determinando que "deve haver limites à coleta de dados pessoais e todos os dados devem ser obtidos por meios leais e justos, onde seja adequado, com o conhecimento ou consentimento do sujeito dos dados"[9]

No princípio da necessidade que também está fundamentado no artigo 6º da LGPD "necessidade: limitação do tratamento ao mínimo necessário para a realização de finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;" sendo assim través do contrato formalizado, apenas os dados necessários para a preparação deste documento são coletados e a política de retenção de dados e o horário são definidos, para que, uma vez que os dados pessoais não sejam necessários, eles possam ser eliminados.[10]

A finalidade, adequação e a necessidade são princípios que somados resultam no que se chama de mínimo essencial, algo como saber qual a menor quantidade de dados pessoais necessária para que se chegue ao fim pretendido de forma adequada. No momento da coleta é primordial que se esteja atento à real necessidade de se obter determinado dado pessoal para se atingir a finalidade pretendida. Sobre o princípio do livre acesso a LGPD diz que "livre acesso:

---

[8] GUERREIRO, R.; TEIXEIRA, T. Lei Geral de Proteção de Dados Pessoais: Comentado artigo por artigo. 4. ed. São Paulo: Saraiva, 2022. E-book.

[9] MENKE. Fabiano; DRESCH. V. F. Rafael. LEI GERAL DE PROTEÇÃO DE DADOS aspectos relevantes. Indaiatuba-SP: editora FOCO, 2021. E-book.

[10] LIMA, A.; D. S.; BARONOVSKY, T. LGPD para contratos. São Paulo: Saraiva, 2021. E-book.

garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;"[11]

Princípio do livre acesso vem do princípio da transparência e aumenta o direito à informação, a comunicação e consulta de dados pessoais e comunicação para que seja fácil encontrar e compreender estes, devem então ser claros, simples e objetivo. Devem estes estar de forma acessível para o titular deve podendo encontrar-se fisicamente ou digitalmente, essa forma ainda deve permitir a utilização posterior destes dados essas respostas devem ser encaminhadas dentro de 05 dias para o titular de acordo com a regulamentação legal. (Artigo 19 da LGPD).

O princípio da qualidade dos dados encontra-se conceituado no artigo 6º da LGPD da seguinte forma, "qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;" portanto esse princípio tem por objetividade que sejam mantidos os dados de forma que estes possam ser atualizados, claros e que sejam relevantes, ajustado com a finalidade para qual servira esse tratamento.[12]

Já o princípio da transparência efetiva que as informações devem ser claras, não podendo essas causarem confusão em quem as recebem, precisam estas serem facilmente acessíveis a respeito de seu tratamento com os agentes.

O princípio da segurança tem por finalidade tratar de como é assegurado que esses dados não serão utilizados de forma ilícita, e que esses dados estão protegidos e seguros de meios que possam acarretar a utilização destes com má-fé. Já a LGPD traz também em seu texto um breve conceito sobre o mesmo "segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão".

Princípio da "prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; " (art. 6º da LGPD). O princípio da prevenção possui o objetivo de proteger contra futuros danos que possam ocorrer aos dados e aos seus possuidores.

Outro princípio tratado no artigo 6º é o "não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos; " a função principal desse princípio é para que não ocorra a discriminação de determinados usuários por motivos de

[11] Lei nº 13.709, de 14 de agosto de 2018. Institui a LGPD.
[12] SOLER, F. G. Proteção de Dados: reflexões práticas e rápidas sobre a LGPD. São Paulo: Saraiva, 2021. E-book.

seus dados, como por exemplo escolher apenas um gênero para entrevistas de emprego pelos dados que estão descritos em seus currículos discriminando assim o outro gênero.

O último princípio é "responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas". (Art. 6º LGPD)

É necessário que seja verificado que as medidas de segurança estão sendo tomadas de forma correta, e se estão seguros os dados os quais o agente tem acesso e está utilizando sobre os sujeitos.

4.3 Projetos de Lei

As sociedades modernas caracterizam-se pela rápida dinâmica de inovação e adaptação social, os fluxos tecnológicos e o desenvolvimento de novos mecanismos de convivência iluminam a cada dia novas formas de convivência e cooperação entre as pessoas, a consequência prática dessa realidade é a necessidade de avaliação constante e aperfeiçoamento da legislação.

Como em todos os vetores da sociedade, em sentido estrito, a interação das pessoas na internet (WWW) está mudando principalmente devido à criação de novos aplicativos, novos dispositivos e novas funções já existentes. Nesta ferramenta, as condições legais em vigor, é tarefa quotidiana das forças de investigação e das autoridades judiciárias, por sua vez, estes elementos reportam constantemente ao legislador com vista ao aperfeiçoamento do normativo. (TOMASEVICIUS FILHO, 2016)

> O crescente desenvolvimento das tecnologias de informação e o uso massivo da Internet têm facilitado o acesso das pessoas a mais conhecimento e maior agilidade nos processos de tomada de decisão. Por outro lado, a informatização tem sido utilizada para fins criminosos, usualmente chamados de "crimes virtuais" ou "cibernéticos" (SENADO FEDERAL, 2012). [13]

Se for desenvolvido um novo código que defina os crimes virtuais e abranja todos os seus aspectos, e seja criada uma área de segurança especial sobre o assunto com alto nível de

[13] _____. Senado Federal. "O Senado e os Crimes cibernéticos". Rev. Em Pauta. Ano V - nº 235 - Brasília, 10 de setembro de 2012

conhecimento de informática, para que o conflito seja solucionado de forma hábil, obtendo uma maneira de ajudar a encontrar um criminoso virtual.

Nota-se que o ordenamento jurídico não está totalmente preparado para coibir tais condutas, portanto, se as regras relacionadas ao mesmo assunto pudessem ser aprimoradas, poderíamos esperar que o nível de crimes cibernéticos diminuísse devido à eficácia de suas respectivas leis. (SIQUEIRA, 2017, p. 128)

Com foco nesse fenômeno social, as Câmaras Legislativas Federais do Brasil, o Senado e a Câmara e, nesse sentido, a maioria de seus legisladores têm envidado esforços e trabalhado para produzir legislação com tema de crimes virtuais.

No Senado Federal, o jornal "Em Pauta - Processo Legislativo do Senado no Serviço Público" Ano V - nº 235 - Brasil, 10 de setembro de 2012, tramitando diversas leis com assuntos correlatos, destacando-se o Projeto de Lei do Senado (PLS) nº 427 de 2011, que apresentou pelo senador Jorge Viana (PT-AC), o Projeto de Lei na Câmara nº 35 (PLC) de 2012, de autoria do deputado federal Paulo Teixeira (PT-SP), está em votação no Plenário do Senado Federal depois de pronto para aprovação nas comissões temáticas desta câmara, bem como o PL do SENADO nº 236 de 2012 de autoria do senador José Sarni (PMDB-AP).

O Projeto de Lei do Senado (PLS) nº 427 de 2011, pendente de parecer para apreciação da Comissão de Constituição e Justiça da Câmara, visa alterar o Código Penal para incluir o "crime de atentado contra a segurança de meio ou serviço de comunicação informatizado) (SENADO FEDERAL)

Já no Projeto de Lei da Câmara (PLC) nº 35 de 2012, que já foi aprovado naquela casa, com a tipificação penal de vários crimes de informática está incluído no Código Penal. Com aprovação nas comissões temáticas. (SENADO FEDERAL, 2012)

Na Câmara dos Deputados, as iniciativas dos legisladores ocorreram em clima extremamente construtivo após os intensos debates que se estabeleceram no âmbito da CPI dos crimes cibernéticos em 2016. (CÂMARA DOS DEPUTADOS, 2016)

Dentre as propostas de lei decorrentes da referida CPI, destaca-se o projeto de lei da Câmara dos Deputados sobre "perda de instrumentos do crime doloso destinados à prática de crimes reincidentes", incluindo computadores, telefones celulares e seleciona aparelhos eletrônicos usados em crimes virtuais. Outra proposta visa ampliar a abrangência do crime de invasão de dispositivo de computador e incluir os crimes cometidos contra ou por meio de computador, conectado ou não a rede, aparelho de comunicação ou sistema de telecomunicações, ao rol de delitos com repercussão interestadual ou internacional, que requeiram a mesma repressão. (CÂMARA DOS DEPUTADOS, 2016)

Ainda, dentre as proposições anteriormente mencionadas, o Relatório da CPI dos Crimes virtuais propôs alterações no Marco Civil da Internet, Lei nº 12.965, de 23 de abril de 2014, que reconhece a ausência de cópia idêntica do conteúdo infrator, sem a necessidade de novo mandado judicial e de nova regra que permita o banimento de programas de internet por mandado judicial nas hipóteses nela previstas. (CÂMARA DOS DEPUTADOS, 2016)

Todas as propostas legislativas são discutidas em comissões temáticas junto com inúmeras outras propostas de projetos de lei. Esforços legislativos recentes em ambas as câmaras foram significativos, mas várias iniciativas têm lutado para serem aprovadas devido às questões usuais do processo legislativo, incluindo uma sobrecarga de projetos de lei em andamento e as questões políticas inerentes a isso.

5. ANÁLISES JURISPRUDÊNCIAS DOS CRIMES VIRTUAIS

No âmbito do processo penal, a persecução e repressão de crimes virtuais devem ser determinadas para os processos e julgamentos de aplicação da lei, tendo em conta que o ambiente virtual se faz presente em vários países de forma virtual e não está sujeito a limitações físicas.

Segundo Távora (2017, p. 387), “a autoridade torna-se norma jurídica para a gestão efetiva das atividades dos órgãos subordinados, o que previamente determinava a margem de atuação de cada um, ou seja, além dos limites do poder”.

No caso, os principais aspectos da jurisdição material que devem ser analisados são o o de competência material, dada pelo nome de *ratione materiae* e *ratione loci*, que de acordo com o artigo 69 do Código Penal "a competência determina: I - local da infração: II - local de residência ou domicílio do o réu e III - a natureza da infração."

A justiça é residual, permanecem e têm competência para apreciar todas as questões que não sejam de competência geral ou especial. Por outro lado, os critérios para a instauração da justiça federal são mais limitados, pois o processo só pode ser transferido da justiça estadual para a federal nos casos em que se trate de grave violação de direitos humanos, dispositivos constitucionais e tratados das convenções que o Brasil subscreve. Assim diz o artigo 109 CF/88:

> Aos juízes federais compete processar e julgar:
> I - As causas em que a União, entidade autárquica ou empresa pública federal forem interessadas na condição de autoras, rés, assistentes ou oponentes, exceto as de falência, as de acidentes de trabalho e as sujeitas à Justiça Eleitoral e à Justiça do Trabalho;
> II - As causas entre Estado estrangeiro ou organismo internacional e Município ou pessoa domiciliada ou residente no País;
> III - as causas fundadas em tratado ou contrato da União com Estado estrangeiro ou organismo internacional;
> IV - Os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral;
> V - Os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;
> V-A as causas relativas a direitos humanos a que se refere o § 5º deste artigo;
> VI - Os crimes contra a organização do trabalho e, nos casos determinados por lei, contra o sistema financeiro e a ordem econômico-financeira;
> VII - os habeas corpus, em matéria criminal de sua competência ou quando o constrangimento provier de autoridade cujos atos não estejam diretamente sujeitos a outra jurisdição;
> VIII - os mandados de segurança e os habeas data contra ato de autoridade federal, excetuados os casos de competência dos tribunais federais;

> IX - Os crimes cometidos a bordo de navios ou aeronaves, ressalvada a competência da Justiça Militar;
> X - Os crimes de ingresso ou permanência irregular de estrangeiro, a execução de carta rogatória, após o "exequatur", e de sentença estrangeira, após a homologação, as causas referentes à nacionalidade, inclusive a respectiva opção, e à naturalização;
> XI - a disputa sobre direitos indígenas. (...) § 5º Nas hipóteses de grave violação de direitos humanos, o Procurador-Geral da República, com a finalidade de assegurar o cumprimento de obrigações decorrentes de tratados internacionais de direitos humanos dos quais o Brasil seja parte, poderá suscitar, perante o Superior Tribunal de Justiça, em qualquer fase do inquérito ou processo, incidente de deslocamento de competência para a Justiça Federal.

Portanto, não é o simples fato de um crime ser cometido pela Internet que por si só atrai a competência do judiciário federal para processar e julgar tal crime.

O artigo 70 do Código Processual Penal [14]estabelece que "a competência, em regra, é determinada pelo lugar onde foi cometido o crime, ou tratando-se de tentativa, pelo lugar onde foi praticado o último ato de execução".

Assim, considera-se como foro de jurisdição territorial o local onde foi cometida a infração, uma vez que o CPP adota a teoria consequencial para determinar tal competência. O conhecido cientista Nestor Távora explica que "a teoria da consequência se torna importante em crimes multidimensionais, onde as ações de execução ocorrem em outro local de consequência, sempre dentro das fronteiras nacionais". (TÁVORA, 2017, p. 389)

No entanto, de acordo com Távora (2017), a legislação brasileira, a fim de adequar as regras do processo penal à criminalidade moderna, teve como discussão dada pelo Superior Tribunal de Justiça, que firmou o entendimento de que o juízo competente para processar e julgar o crime de roubo por meio de fraude na Internet, o ambiente onde a conta da vítima foi retirada ilegalmente, de acordo com a aplicação artigo 70 do CPP, é da competência do local da conta fraudulenta.

Segundo a legislação do Superior Tribunal de Justiça, os crimes de difamação praticados por meio eletrônico, seja em chats ou sites de redes sociais, mesmo sediadas no exterior, têm competência para processar e julgar o juiz de direito do estado. Justiça. Nesse sentido, a referida decisão publicada no Diário Eletrônico da Justiça, da Terceira Seção do Supremo Tribunal de Justiça, julga o seguinte caso:

> **CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER. AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.** 1 - O simples fato de o suposto delito ter sido cometido por meio da

[14] BRASIL. **Código de Processo Penal.** Decreto lei nº 3.689, de 03 de outubro de 1941.

> rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais "Orkut" e "Twitter", não atrai, por si só, a competência da Justiça Federal. 2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da Constituição Federal. 3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal, as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual. 4 - Conflito conhecido para declarar a competência do Juízo de Direito do Juizado Especial Cível e Criminal de São Cristóvão/SE, o suscitado. (CC 121.431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012)[15]

Constatou-se que não houve violação do artigo IV do art. 109 da CF e bem ao inciso V do mesmo diploma legal, haja vista que o crime de dano não está previsto em tratados ou convenções internacionais que o Brasil se obrigue a tutelar.

A autoridade competente do Brasil para julgar crimes praticados por estrangeiro residente no Brasil será a capital do estado em que tenha residido pela última vez, mas nunca tenha residido no Brasil, nos termos do artigo 88 do CPP, será a capital da República.

Com o aumento do uso de computadores e da Internet, os crimes virtuais aumentaram o número de vítimas de fraudes, crimes contra a honra, racismo, disseminação de pornografia infantil e outros crimes.

Com essas grandes e populares mudanças sociais ocorridas em decorrência da globalização da Internet, criou-se uma nova forma de comunicação e modificou as relações sociais em todo o mundo, mas junto com tais benefícios surgiram também novos riscos, criando a necessidade de controle legal.

O dinamismo e a universalidade inerentes à Internet tornaram-se foco de preocupação do poder legislativo, que aprovou as Leis nº 12.735/12 e nº 12.737/12 e nº 12.965/14. Quando se trata de jurisdição para julgar crimes cometidos pela Internet, algumas questões devem ser consideradas, como o local de transmissão e se o crime é ou não transnacional.

O Supremo Tribunal Federal, com decisão do Recurso Extraordinário nº 628.624[16], decidiu por maioria de votos que a competência do Ministério Público e acórdão relativos à publicação do crime na Internet, imagens contendo conteúdo pornográfico com a participação de crianças e / ou adolescentes é da justiça federal. O

[15] JUSBRASIL. CC 121.431/SE, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 11/04/2012, DJe 07/05/2012.

[16] JUSBRASIL. Recurso Extraordinário nº 628.624. STF. Julgado em 29/10/2015

O tribunal de primeira instância sustentou a seguinte tese: "Os tribunais federais são encarregados de processar e condenar crimes envolvendo o acesso ou aquisição de material pornográfico infantil ou adolescente por meio da rede mundial de computadores".

5.1 Competência do Direito Penal

O Código Penal adotou em seu artigo. 6º, a Teoria da Ubiquidade mista, que dispõe que, para os efeitos da jurisdição nacional, o lugar do crime pode ser tanto o lugar do fato ou do resultado, quanto ainda o lugar do interesse legítimo ameaçado ou lesado para evitar conflitos jurisdicionais adversos.

Nesse sentido, constata-se incidentalmente que os crimes virtuais são praticados de forma dentro da jurisdição nacional. Para determinar o tempo e o local em que a ação ocorreu, o principal tipo de verbo do dispositivo acusativo deve ser examinado. Assim, difamação, injúria (crimes contra a honra), publicação, distribuição (pornografia infantil), danificar (crimes de danos causados por vírus), falsificação (crimes contra a fé pública), lucro por meio do desvio de outrem (absorção), são comportamentos praticados quando no mundo material, diz-se que houve uma prática a que se referem.

A mesma coisa acontece com os crimes cibernéticos, exceto que são cometidos por meio de um computador e acesso à Internet. O agente comete um crime quando entra no computador, acessa a Rede e armazena nela coisas ilegais. Por exemplo, usa-se uma mentira ideológica quando se cria uma identidade falsa dentro de uma comunidade virtual usando a Internet por meio de um computador.

Com base nesse fato, é fácil entender que os crimes virtuais de que trata a justiça brasileira são praticados quase em sua totalidade no território nacional, pois a natureza dos crimes virtuais era a condenação ou o recurso para eles, o que está relacionado com a realidade (não há relatos de grupos cometendo roubo eletrônico transnacionalmente através de fraude, quando alguém é desacreditado, o autor é conhecido da vítima, etc.).

De resto, a teoria compreensiva da miscigenação leva os pressupostos mais longínquos ao determinar que o Estado brasileiro é competente quando, ainda que o crime “aqui” não seja cometido, suas consequências aqui são produzidas ou previstas. Ou seja, sempre que um cidadão é ofendido ou lesado por um crime virtual e os legítimos interesses nacionais são insultados ou lesados, os tribunais têm competência para tomar as medidas cabíveis, porque o resultado está dentro do território nacional.

O fato de existir jurisdição brasileira para resolver esses tipos de disputas não significa que uma sentença penal brasileira possa resultar eficiência, isso significa que, teoricamente, na maioria das vezes, a eficácia da Lei é testada, pois uma vez identificado o autor do crime, ele pode ser punido. Caso contrário, pelas hipóteses de que o autor do crime resida em outro país, quando observadas as condições do art. 7º do Código Penal juntamente com os acordos bilaterais e multilaterais que o Brasil celebrou com o país estrangeiro.

5.2 Justiça Estatal

Há um equívoco de que todos os delitos criminais na Internet são da competência dos tribunais federais. Essa ideia parte de dois pressupostos: 1) A rede não tem fronteiras e, portanto, será um crime de caráter internacional e 2) A Internet será um serviço público da União (VIANNA, 2003, p.95).

Embora a Internet esteja disponível em todo o mundo, as consequências do crime são confirmadas em uma comunidade, uma determinada localidade (na verdade, quando os bens jurídicos protegidos não estão em mais de um país). Além disso, o crime é cometido a partir de um local específico, não de um local indefinido, embora possa parecer à primeira vista.

Em relação ao segundo argumento, a União não administra ou é responsável pela Internet, e a Rede não faz parte dela, é utilizada apenas ocasionalmente. Deve ficar claro que os serviços públicos prestados pela União são aqueles definidos pela Carta Magna. Conforme mencionado acima, os crimes praticados na Internet, de competência da Justiça Federal, são os crimes mencionados no artigo. 109 da Constituição Federal. Em inciso IV, a Carta Magna especifica que os crimes praticados contra bens, serviços ou interesses da Comunidade, de suas entidades autárquicas ou empresas públicas são de competência federal e os crimes eletrônicos praticados contra entes da Administração Federal são abrangidos por esta cláusula.

O artigo V do referido aparato constitucional é o que contempla o extenso rol de crimes eletrônicos de competência do judiciário federal. A Constituição determina que os crimes previstos em tratado e convenção nacional serão investigados pelo judiciário federal quando sua execução se iniciar no País e o resultado tiver ocorrido ou houver previsão de ocorrência no exterior.

O mais proeminente desses crimes são os comportamentos descritos no art. 241 do ECA e lei antirracismo 7.716/8918. Ressalvadas as presunções de competência da justiça eleitoral, tais como os crimes descritos no art. Artigos 289 a 354 do Código Eleitoral (Lei 4.737/65) – e

da Justiça Militar (Lei nº 1.001/69), o restante cabe à Justiça Geral. Nesse sentido, o Superior Tribunal de Justiça se posicionou da seguinte forma:

> **PENAL. CONFLITO DE COMPETÊNCIA. CRIME DE INFORMÁTICA. INEXISTÊNCIA DE TRATADO ENTRE OS PAÍSES. NÃO-INCIDÊNCIA DO DISPOSTO NO ART. 109, V, DA CF/88. COMPETÊNCIA DA JUSTIÇA ESTADUAL.** 1. Para a incidência da regra de fixação da competência do art. 109, V, da CF/88, é imperativa a análise da existência ou não de tratado ou convenção internacional entre os países envolvidos na prática criminosa. 2. A qualidade do órgão policial conducente da investigação é irrelevante para a fixação da competência do Juízo, pois a Carta da República prevê regras distintas na fixação das competências jurisdicional e policial. 3. Conflito conhecido para declarar a competência do Juízo de Direito da 1ª Vara Criminal da Comarca de Santa Cruz do Sul/RS, suscitado. (CC 33.871/RS, Rel. Ministro ARNALDO ESTEVES LIMA, TERCEIRA SEÇÃO, julgado em 13.12.2004, DJ 01.02.2005 p. 403)[17]

A fim de exercer de forma sistemática e efetiva a autoridade para dizer qual Lei se aplica em um caso concreto, a sentença e a aplicação da pena correspondente - se necessário - o juiz separou o estado em várias jurisdições ordinárias, estabelecendo regras para determinar qual a jurisdição e tribunal competente.

Assim, *verbi gratia*, a competência da justiça comum é dividida em cada matéria da federação e distribuída entre os vários distritos (foros) existentes. Nestes casos, há sempre juízos (varas) que se debruçam sobre determinados temas e estes devem apenas tratá-los de forma específica e individual.

Dessa forma, as regras que tornam determinada infração penal passível de revisão por foro predeterminado e para determinada pena ou tipo de penas, devem ser mais resolvidas, pois ao se tratar de crimes virtuais permanecem, ao menos inicialmente, um pouco difícil.

Cabe enfatizar que com efeito, no sistema processual penal, o legislador ordinário decidiu estabelecer o local onde o crime foi cometido como foro competente da ação penal *(locus delicti commissi).* É o que estabelece o art. 70 do Código de Processo Penal.

Uma vez que o início do crime ocorre pelo surgimento de elementos de sua definição legal, com base nas propriedades da Internet, é possível estabelecer critérios comuns para todos os crimes nela cometidos, a fim de avaliar a cena do crime e, portanto, o foro competente.

---

[17] JUSBRASIL. CC 33.871/RS, Rel. Ministro ARNALDO ESTEVES LIMA, TERCEIRA SEÇÃO, julgado em 13.12.2004, DJ 01.02.2005 p. 403

De antemão, é necessário verificar se o crime sob investigação é material, oficial ou de comportamento ordinário. Os crimes materiais (ou consequenciais), segundo Paulo Queiroz (3ª ed., 2006, p. 171), "são aqueles em que o tipo de crime descreve condutas cuja consumação se entende como a ação completa dos elementos do tipo, só ocorre criando o resultado nele previsto".

De fato, quando se trata de roubo por fraude na Internet, o comportamento compete ao artigo 155, parágrafo 4º do Código Penal, por se tratar de crime material, é necessário pela culminância de crime em que o agente ativo se apropria de bens alheios.

5.3 Responsabilidade Civil e Danos Morais no âmbito virtual

O Código Civil de 2002, garante que a indenização por danos morais prevista no artigo 186, que aquele por ação ou omissão causa dano, é exclusivamente moral e configura ato ilícito.

Pensando nisso, Carlos Roberto Gonçalves (2009, p.3) aborda a questão da responsabilidade civil: "Aquele que pratica ação ou omissão que cause danos deve arcar com as consequências de seus atos. Esta é a regra elementar do equilíbrio social, que resume essencialmente o problema da responsabilidade". Portanto, percebe-se que a responsabilidade é um fenômeno social.

O artigo 5º, [18]incisos V e X da Constituição Federal dispõe: "Todos são iguais perante a lei e garante aos brasileiros e aos estrangeiros residentes no País a inviolabilidade dos direitos à vida, à liberdade, à igualdade, X - Importância, à vida pessoal, à dignidade e à imagem das pessoas, direito à indenização por danos materiais ou morais danos como resultado de sua violação".

O Código Civil Brasileiro garante a possibilidade de indenização por calúnia, difamação e injúria, e a obrigação de indenizar a vítima. Conforme estipulado no Código Civil: "art. 953. A indenização por injúria, calúnia ou calúnia consiste na reparação dos danos por elas causados à vítima. Parágrafo único. Se a vítima não puder provar danos materiais, o juiz determinará o valor da indenização justa dependendo das circunstâncias do caso."

A indenização por dano moral decorrente de crimes contra a honra é uma forma de ressarcir o dano psicológico, violação da reputação sofrida pela vítima em decorrência de humilhação pública em ambiente público ao qual têm acesso milhares de usuários.

[18] BRASIL. Constituição (1988). Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República

A lei de Marco Civil e Direito da Internet, Lei 12.965/2014, dispõe no artigo 7: “O acesso à Internet é imprescindível para o exercício da cidadania e são assegurados ao usuário os seguintes direitos: I- inviolabilidade da vida privada e pessoal, sua proteção e indenização por danos materiais ou morais decorrentes de sua violação;"

A reparação por ofensa é feita à integridade moral de uma pessoa, o que requer punição criminal e civil, para compensar a vítima pelo dano que afetou a dignidade objetiva e subjetiva. Nesses casos, o autor Arnaldo Rizzardo (2009, p.32) declara que as indenizações devem decorrer do fato de o bem jurídico ter sido lesado para proteger os interesses das provas que demonstrem termos injuriosos usados pela ré contra a autora.

De acordo com o tribunal de Justiça de São Paulo, descreve a devida indenização por danos morais da honra, quando violado:

> RESPONSABILIDADE CIVIL - Insurgência do autor contra injúrias publicadas pela ré em sítio eletrônico de relacionamento - Prova documental a demonstrar os termos pejorativos e depreciativos utilizados pela ré em referência ao autor - Evidente a intenção de difamar e insultar - Não configurada hipótese de legítima defesa dos interesses dos filhos da ré - Limites da mera crítica extrapolados - Honra e imagem do autor violadas - 37 Dano moral caracterizado - Indenização devida - Cabível, por outro lado, a redução do valor da condenação - RECURSO PARCIALMENTE PROVIDO.

No caso citado, ficou claramente demonstrado que a conduta ilícita do ente atuante pode ofender e atentar contra a dignidade do autor, portanto, o Tribunal entendeu pela necessidade de indenizar por danos morais.

Como na lei 12.965/2014, em seu artigo 18, que os provedores de conexão à internet não são responsáveis por danos causados por conteúdo gerado por terceiros. No entanto, o artigo 19 da mesma lei garante que o prestador pode ser responsabilizado civilmente se houver ordem judicial específica.

Nesse viés, o Tribunal de Justiça do Estado de São Paulo reconheceu a obrigação do Facebook de indenizar pelas mensagens ofensivas postadas pelo usuário:

> RECURSO – APELAÇÃO – AUSÊNCIA DE PREPARO – DETERMINAÇÃO DE COMPROVAÇÃO DA HIPOSSUFICIÊNCIA DO APELANTE NÃO ATENDIDA - DESERÇÃO DECRETADA – RECURSO DO CORRÉU NÃO CONHECIDO. **INDENIZAÇÃO - INJÚRIA - DIVULGAÇÃO DE MENSAGENS OFENSIVAS EM REDE SOCIAL – AÇÃO PARCIALMENTE PROCEDENTE EM RELAÇÃO AO FACEBOOK – TUTELA ANTECIPADA PARA A EXCLUSÃO DAS POSTAGENS E COMENTÁRIOS ANEXADOS À INICIAL MANTIDA** PELA R. SENTENÇA PROFERIDA – SUCUMBÊNCIA RECÍPROCA EM FACE DA MESMA - RECURSO DO AUTOR PROVIDO. (sem grifos no original)

Portanto, a divulgação de mensagens injuriosas e ofensivas é ato grave passível de indenização por danos morais, onde se viola o direito à privacidade. Segue um trecho do RESP (Recurso Especial), que cobre muito bem esta situação:

> "Na fixação da indenização por danos morais, recomendável que o arbitramento seja feito com moderação, proporcionalidade ao grau de culpa, ao nível socioeconômico dos autores, e, ainda, ao porte da empresa recorrida, orientando-se o juiz pelos critérios sugeridos pela doutrina e pela jurisprudência, com razoabilidade, valendose de sua experiência e do bom senso, atento à realidade da vida e às peculiaridades de cada caso" (Resp 135.202-0-SP, 4ª T. rel. Min. Sálvio Figueiredo).[19]

Sem dúvida, o progresso tecnológico cria oportunidades e grandes mudanças na sociedade. No entanto, a obrigação do Estado é garantir a proteção de direitos fundamentais, trazendo assim responsabilidade e indenização a todos os usuários que utilizam o ambiente virtual – redes sociais – para propagar palavras ofensivas e discriminatórias.

[19] JUSBRASIL. Resp 135.202-0-SP, 4ª T. rel. Min. Sálvio Figueiredo. São Paulo, 2020.

6. CONCLUSÃO

De acordo com o que foi constatado em base do tema, pode-se dizer que a internet vem tendo constantes avanços, aderindo fatores de muitos acessos e interação com as pessoas. São inegáveis os acessos e as facilidades que isso dispõe. Mas em contrapartida,pode vir a ser um meio de muitos crimes virtuais, golpes advindos pela maldade e oportunidade em se beneficiar pelos dados e bens de outros

Como observado, a principal razão para a atualização do Código Penal sobre as leis de apoio à segurança do crime virtual ocorre principalmente nos casos de repercussão na mídia, seja nacional ou internacional, sendo as duas principais alterações a Lei Caroline Dickmann e o Marco Civil da Internet.

No entanto, o Marco Civil não regulamenta adequadamente o aspecto penal, o tema é pouco elaborado, e com diversas leis em outros contextos regulatórios, sem uma "constituição" voltada para essa área específica.

Os métodos de prevenção de ataques devem ser lidos, compreendidos, aplicados e testados diariamente, o que é essencial para aumentar as informações. As pessoas devem estar atentas e não ser inocentes quando abrem determinado site ou aplicativo, seja em um computador ou celular. Os golpes podem acontecer a qualquer hora, lugar e equipamento, seja por meio hardware, software ou pessoas, então saber que esses problemas são possíveis com qualquer pessoa representa o que é preciso para aprender a combater esses males, tornando a Internet um espaço seguro para todos.

Por fim, é preciso evolução das leis para o crime virtual, focada na segurança e típica de todos os crimes de informática, trazendo uma organização mais precisa e focada no que já está regulamentado, permitindo um melhor entendimento do que novas leis precisam ser analisadas e legisladas para se tornarem vigentes.

Em suma, os resultados contam com ações efetivas em meio do conhecimento e habilidades em manusear os instrumentos tecnológicos, que vem a ser base de pesquisa aser mais aprofundado e relatado para conscientização das pessoas. Sabe-se que em os crimes cibernéticos, é a forma de causar dano a outro, por meio da fraudulência.

REFERÊNCIAS BIBLIOGRÁFICAS

ALEXANDRE JÚNIOR, J. C. Cibercrime: um estudo acerca do conceito de crimes informáticos. **Revista Eletrônica da Faculdade de Direito de Franca**, v. 14, n. 1, jun. 2019.

ANDREUCCI, Ricardo Antonio. **Manual de Direito Penal.** 10 ed. São Paulo: Saraiva, 2014.

ATAÍDE, Amanda Albuquerque de. **Crimes Virtuais: uma análise da impunidade ed os danos causados às vítimas.** Maceió, 2017.

BARRETO, A. G.; KUFA, K.; SILVA, M. M. **Cibercrimes e seus reflexos no direito brasileiro**. Salvador: JusPODIVM, 2019.

BARROSO, LUÍS ROBERTO. Estado, Sociedade e Direito: Diagnósticos E Propostas para o Brasil. **In: XXII Conferência Nacional dos Advogados**. Rio de Janeiro, 2014.

BEZERRA, Clayton da Silva; AGNOLETTO, Giovani Celso. **Combate às fake News: doutrina e prática.** 1.ed. São Paulo: Posteridade, 2019.

BITENCOURT, Cezar Roberto. **Penal comentado.** 7 ed. São Paulo: Saraiva, 2012.

BRASIL, **Lei geral de proteção de dados pessoais.** Lei nº 13.709, de 14 de agosto de 2018.

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil. Brasília, DF: Senado,1988

BRASIL. **Decreto-Lei 2.848, de 07 de dezembro de 1940.** Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez.

BRASIL. **LEI 14.155,** de 27 maio de 2021. Lei de violação de disposto informático.

BRASIL. **LEI Nº 12.737,** DE 30 DE NOVEMBRO DE 2012. Lei de Invasão a Dispositivo Informático [Internet].

CABRAL, Ismael et al. **Segurança da informação em bibliotecas universitárias federais: um levantamento sobre ferramentas e técnicas utilizadas.** 2015.

CAMPOS, Pedro Franco de [et al.]. **Direito penal aplicado: parte geral e parte especial do Código Penal.** - 6ª. Ed. – São Paulo: Saraiva, 2016.

CAPEZ, Fernando. **Rapto Violento ou Mediante Fraude: Inexistência de Abolitio Criminis na Visão do STF.** 2010.

CAPEZ, Fernando. **Curso de Direito Penal-Volume 1-Parte Geral**. Saraiva Educação SA, 2020.

COELHO, Ivana Pereira; BRANCO, Sérgio. **Humor e Ódio na Internet.** Cadernos Adenauer XV, Rio de Janeiro, s/n, out/2016.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** São Paulo: Saraiva, 2011.

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral.** Salvador: Juspodivm, 2014.

DE LIMA, Pedro Rogério Melo; DE OLIVEIRA XAVIER, Lidia. O fenômeno do cybercrime sob a perspectiva do direito a privacidade. **Hegemonia**, n. 16, p. 4-21, 2015.

GONÇALVES, Victor Eduardo Rios. **Direito penal esquematizado: parte especial do Código Penal. -** 8. ed. – São Paulo: Saraiva Educação, 2018.

GRECO, Rogério. **Curso de Direito Penal: parte especial.** v. III. 7. ed. Rio de Janeiro: Ed. Impetus, 2010.

JESUS, Damasio de; MILAGRE, José Antonio. **Manual de Crimes Informáticos.** São Paulo: Saraiva, 2016.

LIMA, P. R. M. de; XAVIER, L. de O. O fenômeno do cybercrime sob a perspectiva do direito a privacidade. **Revista Eletrônica de Relações Internacionais do Centro Universitário Unieuro**, n. 16, p. 4-21. 2015.

MONTEIRO, Renato Leite. **Crimes eletrônicos: uma análiseeconômica e constitucional.** Fortaleza, 2010.

MOREIRA FILHO, Guaracy. Código penal comentado. **São Paulo: Rideel**, 2010.

NORONHA, Edgard Magalhães. Dos crimes contra a economia popular. **Revista da Faculdade de Direito UFPR**, v. 2, 1954.

NUCCI, Guilherme de Souza. **Manual do Direito Penal.** 7. ed. São Paulo: Revista dos Tribunais, 2011.

OLIVO, CLEBER KIEL; SANTIN, A. O.; OLIVEIRA, L. E. S. Avaliação de Características para Detecção de Phishing de E-mail. **Pontifícia Universidade Católica do Paraná, Curitiba–PR, Brasil**, 2010.

PANNAIN, Camila Nunes; PEZZELLA, Maria Cristina. **Liberdade de Expressão e Hate Speech na Sociedade da Informação.** Revista Direitos Emergentes da Sociedade Global, Santa Maria, v. 4, n.1, p. 72-87, 2015.

PACHECO, Gisele Freitas–COSTA; LOPES, Renato. Crimes **Virtuais e a Legislação Penal Brasileira.** 2011.

PEREIRA, Arthur Martins et al. **Ciber segurança na indústria 4.0: criação de website informativo**. 2014

SIQUEIRA, Marcela Scheuer et al. **Crimes virtuais e a legislação brasileira.** (Re)Pensando o Direito – Rev. do Curso de Graduação em Direito da Faculdade CNEC Santo Ângelo. v. 7, n. 13 (2017).

SILVA, Aurélia Carla Queiroga; BEZERRA, Margaret Darling; SANTOS, Wallaz Tomaz. **Relações Jurídicas Virtuais: Análise de Crimes Cometidos com o Uso da Internet.** Revista Cesumar Ciências Humanas e Sociais Aplicadas, v.21, n.1, p. 7-28, jan./jun. 2016.

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a** perspectiva **vitimodogmática.** 2009

TAVARES, José de Farias. **Comentários ao Estatuto da Criança e do Adolescente.** Rio de Janeiro: Forense, 2012.

TOMASEVICIUS FILHO, Eduardo. **Marco Civil da Internet: uma lei sem conteúdo normativo.** Estud. av., São Paulo , v. 30, n. 86, p. 269- 285, Abr. 2016.

VIEIRA, Jair Lot. **Crimes na Internet Interpretados pelos Tribunais.** 1.ed. São Paulo: Editora Edipro . 2009, 344p.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação.** Rio de Janeiro: Brasport, 2012.

WIGERFELT, Anders S.; WIGERFELT, Berit. DAHLSTRAND, Karl Johan. Online Hate **Crime – Social Norms And The Legal System.** Revista Quaestio Iuris. v. 8, n. 3, Rio de Janeiro, p. 1859-1878, 2015.