UNIVERSIDADE PRESBITERIANA MACKENZIE

GIOVANNI PERCIDIO FERRI

CRIMES VIRTUAIS:
UMA ANÁLISE CONCEITUAL E PROCEDIMENTAL NA ATUALIDADE

São Paulo
2023

GIOVANNI PERCIDIO FERRI

CRIMES VIRTUAIS:
UMA ANÁLISE CONCEITUAL E PROCEDIMENTAL NA ATUALIDADE

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie, como parte dos requisitos necessários à obtenção do título de Bacharel em Direito.

Orientador: Prof. Dr. Carlos Eduardo Nicoletti Camillo

GIOVANNI PERCIDIO FERRI

São Paulo
2023

CRIMES VIRTUAIS:
UMA ANÁLISE CONCEITUAL E PROCEDIMENTAL NA ATUALIDADE

Trabalho de Conclusão de Curso apresentado à Faculdade de Direito da Universidade Presbiteriana Mackenzie, como parte dos requisitos necessários à obtenção do título de Bacharel em Direito.

Aprovado em: _____

BANCA EXAMINADORA:

_____

Examinador(a):

_____

Examinador(a):

_____

Examinador(a):

CRIMES VIRTUAIS:
UMA ANÁLISE CONCEITUAL E PROCEDIMENTAL NA ATUALIDADE

Giovanni Percidio Ferri[1]

RESUMO

O tema principal do trabalho são os crimes virtuais, sua classificação e os procedimentos necessários à sua adequação de jurisdição e competência além da classificação dos dados segundo a Lei Geral de Proteção de Dados e a importância do correto tratamento destes.
Objetiva-se repassar informação técnico-jurídica de forma acessível e descomplicada além de sintetizar os principais crimes virtuais da atualidade incluindo uma breve contextualização sobre a sociedade da informação e a sua origem.
O método utilizado para desenvolvimento deste trabalho foi de pesquisa bibliográfica por meio de artigos, livros, publicações além da letra de lei que possibilitou estabelecer parâmetros e conectar a legislação ao caso concreto tanto quanto o caminho a ser percorrido para adaptar leis existentes a nova forma em que a sociedade da informação se relaciona, destacando também a necessidade de uma atualização das normas complementares preenchendo as lacunas necessárias para estabelecer segurança jurídica ao ordenamento jurídico brasileiro neste tópico.

Palavras-chave: Crimes Virtuais; Sociedade da Informação; Lei Geral de Proteção De Dados; Tratamento de Dados; Crimes Virtuais Próprios; Crimes Virtuais Impróprios; Direito Penal.

ABSTRACT

The main topic of this academic work are cybercrimes, its classification and the necessary procedures to its correct adequation in terms of jurisdiction and competency apart from disclosing the meaning and importance of what is data and its correct treatment from the perspective of LGPD.
One of the objectives of this paper is spreading technical law knowledge in a simpler and accessible way besides of synthetizing the main cybercrimes of our current times including a brief background on the origin of informational society.
Bibliographic research was the chosen method to develop this paper utilizing articles, books and publication forums alongside the letter of the law which provided a well-established gathering of information, opinions and technical analysis that could connect the posited law to real cases. Also provided the path to adapt existent laws to the new ways of living that the informational society acquired. Highlighting the concern of updating the complementary laws to fill up the existent gaps on the current Brazilian juridical ordination.

Keywords: Cybercrimes; Informational Society; LGPD; Brazil Law; Data treatment.

[1]Graduando em Direito pela Universidade Presbiteriana Mackenzie

INTRODUÇÃO

O presente trabalho tem como objetivo explanar os principais crimes virtuais no ordenamento jurídico brasileiro, os crimes cometidos por meio dos dispositivos tecnológicos sob o viés do Direito Penal e as adaptações de leis complementares a este ao longo do recente desenrolar das inovações tecnológicas e cibernéticas e as suas implicações na sociedade e consequentemente no âmbito jurídico.

A motivação para escrever sobre tal tema origina-se na observância do crescente e repentino desenvolvimento das tecnologias cibernéticas e suas inovações que ocorreram na última década e das inúmeras influências destas no cotidiano de cada um; transcendendo as barreiras jurídicas e as distinções que este faz, modificando a nossa forma de nos comunicar, trabalhar e relacionar. Alterando também os meios que utilizamos para buscar informações, a rapidez e eficiência que estes novos meios nos propiciam, diminuindo distâncias e rompendo barreiras que os tempos anteriores à sociedade da informação jamais poderiam sequer imaginar.

Consequentemente tais mudanças que ocorreram na sociedade, alteram também, as relações jurídicas, e assim, demonstram a importância deste trabalho que tem como objetivo geral expor novas perspectivas sobre crimes já conhecidos pelo ordenamento jurídico e também discorrer sobre aqueles que até então não existiam; trazendo o uso dos dispositivos informáticos, o âmbito digital e a internet como meio exclusivo para prática destes novos atos ilícitos.

No tocante a metodologia utilizada foi pretendida a exposição dos crimes virtuais considerando a sua tipificação por meio do Código Penal Brasileiro e alteração na sua respectiva sanção, se houver; o mesmo ocorreu sobre os procedimentos pertinentes aos crimes

virtuais relativos à sua aplicação territorial, jurisdição e competência e a influência da internet nos respectivos temas. Por fim, foi demonstrada uma breve explicação sobre a nomenclatura dos dados e como a Lei Geral de Proteção de Dados os classifica além da importância de seu rigoroso tratamento.

Ainda acerca da metodologia, utilizou-se o método bibliográfico por meio de livros, artigos e publicações os quais pudessem embasar o tema de forma crítica e analítica concomitantemente com o que o ordenamento jurídico elucida.

Em síntese, o trabalho discorre sobre os crimes virtuais da seguinte forma: contextualização sobre o que é a sociedade da informação e a sua origem, a tipificação dos crimes virtuais dentro do Código Penal Brasileiro, os procedimentos pertinentes aos crimes virtuais no que diz respeito à competência e jurisdição e por fim a classificação dos dados segundo Lei Geral de proteção de Dados.

1 SOCIEDADE DA INFORMAÇÃO E A DISSEMINAÇÃO DA TECNOLOGIA

A sociedade da informação teve início na década de 90, na qual após a revolução industrial começou uma mudança nos valores e princípios da sociedade, em que a valorização dos bens materiais é perdida e o foco é direcionado aos bens imateriais; acompanhando a evolução da tecnologia cada vez mais o mundo se tornava digital.

A partir da década de 90 desenvolve-se a sociedade da informação onde é dada importância significativa aos bens imateriais, como no caso da propriedade intelectual, segredo industrial e depósitos de dinheiro, dentre outros. Isto se dá por conta da convergência entre informática e telecomunicações, da popularização da internet (CRESPO, 2011, p.32).

Acompanhando a evolução tecnológica a sociedade também se transforma – ocorrendo mudanças em sua composição, relações sociais e sua organização – uma mudança estrutural que acarretaria na sociedade como a conhecemos hoje.

Esta nova sociedade, da qual se vive nos dias de hoje, traz consigo, por conta dos mais profundos avanços tecnológicos, um novo conceito de vida e organização em sociedade, refletindo nas mais diversas relações sociais como, por exemplo: a produção, uso da informação, mercado, geração de conhecimento, dentre outras (FIORILLO; CONTE, 2016, p.18).

Esta nova sociedade foi denominada sociedade da informação, pois com o início desta, a manipulação, o acesso e a integração da informação têm papel essencial em sua estrutura e formação acarretando benefícios culturais, econômicos e principalmente na comunicação.

A internet e as tecnologias da informação passam a ter papel fundamental na Sociedade da Informação, pois refletem diretamente na realidade jurídica, trazendo uma nova forma de apreciar os velhos direitos como à informação, à comunicação, à liberdade de expressão e à privacidade (FIORILLO; CONTE, 2016, p.16).

Difícil imaginar a vida nos tempos atuais sem toda essa tecnologia tão presente em nosso dia a dia. Assim, conforme nos adaptamos em sociedade, o Direito também deve acompanhar essas mudanças e se adaptar a esta nova realidade, de novas tecnologias, novas formas de comunicação e interação.

Como consequência do desenvolvimento tecnológico, a Globalização também surge como fator de grande influência na Sociedade da Informação por conta da evolução social apresentada e traz uma nova interpretação para espaço, não sendo este mais limitado fisicamente, ou seja, o progresso tecnológico reduz o planeta a uma aldeia, onde qualquer um estabelece comunicação com o outro, passando o mundo a ficar interligado (CRESPO, 2011, p.36).

À luz da globalização em que a interação social não se limita mais ao espaço físico, acarretando em uma aproximação e uma maior eficácia na comunicação surgem também novas maneiras de infringir a lei e surgem também novas condutas consideradas antiéticas tanto quanto condutas ilícitas.

Em contrapartida, como ônus da evolução da internet e dos dispositivos tecnológicos, uma vez que estes passam a ter interferência direta nas relações sociais pacíficas, também possibilitam algumas práticas socialmente desagradáveis e indesejadas, colocando em risco inclusive bens que outrora não tinham relevância para o direito (FIORILLO; CONTE, 2016, p.16).

Logo, o avanço tecnológico traz consigo, o acompanhamento das condutas criminosas que passam a ser realizadas por meio de dispositivos tecnológicos, ou seja, formas de impor e controlar futuras ações humanas, o que pode influenciar direta ou indiretamente também na prática de condutas criminosas (CRESPO, 2011, p.32).

Surgem os crimes virtuais como espécies do ônus gerados por conta dos avanços tecnológicos, ou ainda como parte dos riscos da modernização e de dimensão social principalmente, uma vez que o uso indevido da tecnologia cotidiana pode trazer sérias ameaças, dentre elas a delinquência informática como um fenômeno social (CRESPO, 2011, p.36).

Diante de tal cenário, novos bens jurídicos necessitam de tutela; outras já existentes precisam de novas adequações para os enquadrarem nas novas formas de interação digital e

por isso, a necessidade de o Direito acompanhar todas essas mudanças e se adequar a esta nova realidade.

A globalização e os avanços tecnológicos, assim como exigem das pessoas e da sociedade a alfabetização tecnológica, também exigem que o pensamento jurídico acompanhe tal evolução de modo que se possa a aplicar as normas de acordo com os contextos impostos (PINHEIRO, 2013).

2 CRIMES VIRTUAIS - NOMENCLATURA E CONCEITO

Juntamente com o avanço tecnológico, a sociedade alterou-se em sua forma, estrutura e na sua maneira de se comunicar e interagir. Com essas recentes mudanças, originaram-se complexidades e desdobramentos resultando em novas formas dos atos ilícitos serem cometidos, além de novos atos ilícitos surgirem para tutelar essa nova realidade. O sistema jurídico passou por mudanças e precisou adaptar-se.

Neste cenário foram criados os crimes virtuais, que conforme Damásio de Jesus e José Antonio Milagre (2016, P. 49) conceituaram crime virtual da seguinte maneira:

> (...) o fato típico e antijurídico cometido por meio da ou contra a tecnologia da informação. Decorre, pois, do direito informático, que é o conjunto de princípios, normas e entendimentos jurídicos oriundos da atividade informática. Assim, é um ato típico e antijurídico, cometido através da informática em geral, ou contra um sistema, dispositivo informático ou rede de computadores. Em verdade, pode-se afirmar que, no crime informático, a informática ou é o bem ofendido ou o meio para a ofensa a bens já protegidos pelo direito penal.

No mesmo sentido, Emerson Wendt e Higor Vinicius Nogueira Jorge (2012, p. 18) dispõem que: "Os crimes virtuais são os delitos praticados contra ou por intermédio de computadores, ou seja, são condutas indevidas praticadas por um computador".

Após a conceituação do que é o crime virtual propriamente dito, há a necessidade de discorrer sobre a sua classificação, podendo ocorrer na sua forma própria ou imprópria.

2.1 CRIMES VIRTUAIS IMPRÓPRIOS

Os crimes virtuais próprios são aqueles que possuem condutas já reconhecidas e tuteladas pelo direito penal no ordenamento jurídico e o meio digital apenas mais uma forma de sua prática Jesus e Milagre (2016) conceituam crimes virtuais da seguinte maneira:

> (…) a tecnologia da informação é o meio utilizado para a agressão a bens jurídicos já protegidos pelo Código Penal brasileiro. Para estes delitos, a legislação criminal é suficiente, pois grande parte das condutas realizadas encontra correspondência em algum dos tipos penais.

Para tanto, o Código Penal será suficiente para proteger o bem jurídico e o uso da tecnologia poderá ser um novo agravante ou condição, o crime é o mesmo, entretanto a forma de realizá-lo o torna "novo", apresentando-se assim, um novo modus operandi. Com objetivo de complementar a conceituação previamente mencionada, Wendt e Jorge (2012, p. 19) afirmam que "o computador é apenas o meio para a prática do crime, que também poderia ser cometido sem o uso dele".

A seguir, serão mencionados os principais crimes virtuais impróprios, sua caracterização penal e o novo modus operandi que os meios tecnológicos trouxeram a tal prática.

2.1.1 Ameaça

A ameaça encontra-se tipificada no Código Penal Brasileiro em seu artigo 147 que diz: "Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave: Pena - detenção, de um a seis meses, ou multa" (BRASIL, 1940).

Para Nucci (2011, p. 705) "ameaçar significa procurar intimidar alguém, anunciando-lhe a ocorrência de mal futuro, ainda que próximo".

Um dos crimes mais comuns nos dias atuais, e que, conforme Wendt e Jorge afirmam, o conhecimento de como lidar com uma situação de ameaça é de conhecimento da sociedade, mesmo que leiga no viés Jurídico. É válido afirmar que a ameaça, fere direito individual, portanto, deverá ser direcionada a pessoa específica.

Este tipo de crime é muito comum e normalmente a vítima procura a delegacia de polícia para comunicar o recebimento da ameaça por e-mail, redes sociais, mensagens de comunicadores instantâneos ou telefonemas (WENDT;JORGE, 2012, p.105).

2.1.2 Participação em suicídio

No ordenamento jurídico brasileiro o suicídio não encontra tipificação penal, entretanto, quem ajuda, induz ou de certa forma motiva tal ato encontra sua conduta em correspondência com o artigo 122 do Código Penal Brasileiro que diz: "Art. 122 - Induzir ou instigar alguém a suicidar-se ou prestar-lhe auxílio para que o faça: Pena - reclusão, de dois a

seis anos, se o suicídio se consuma; ou reclusão, de um a três anos, se da tentativa de suicídio resulta lesão corporal de natureza grave" (BRASIL, 1940).

Sobre seu novo modus operandi Crespo afirma que: "este tipo de crime também pode ser cometido pela internet, porém é necessário que se tenha eficácia e que seja contra determinada pessoa" (CRESPO, 2011, p.88).

Isto é, o crime só terá correspondência jurídica se for cometido contra pessoa determinada, a instigação, motivação ou auxílio deverá ser direcionada para que ocorra o crime por meio tecnológico.

2.1.3 Incitação e Apologia ao Crime ou a Criminoso

A incitação e a apologia estão, respectivamente, disciplinadas no código penal brasileiro nos artigos 286 e 287 que diz:

> Artigo 286- incitar, publicamente, a prática de crime: Pena - detenção, de três a seis meses, ou multa
> (...)
> Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime:
> Pena - detenção, de três a seis meses, ou multa (BRASIL, 1940).

Ambas as condutas não possuem agravante por seu cometimento por via tecnológica ou digital, somente um novo modus operandi, um novo meio de realização.

2.1.4 Falsidade Ideológica e Falsa Identidade

Os crimes de falsidade ideológica e falsa identidade são 2 dos mais comuns crimes que ocorrem no âmbito digital, estão disciplinados nos artigos 299 e 307 do Código Penal Brasileiro, respectivamente:

> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
> Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, se o documento é particular.
> (...)
> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, 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 constitui elemento de crime mais grave (BRASIL, 1940).

Para Nucci (2011, p. 989), o crime de falsidade ideológica conceitua-se da seguinte forma:

> O crime de falsidade ideológica é o ato de omitir, ou seja, deixar de inserir ou não mencionar, em documento público ou particular, declaração dissociada da realidade que neste documento deveria constar, ou ainda inserir ou fazer inserir falsa ou diversa declaração que deveria ser escrita, com o objetivo de 54 prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante.

Sobre o novo modus operandi, Crespo afirma que grande parte dos casos que ocorrem nos meios tecnológicos são de pessoas que se passam por pessoas com o intuito de obter vantagem para si ou outrem, ou até mesmo prejudicar terceiros.

Neste tipo de crime por meio de dispositivos tecnológicos, os casos mais comuns são de pessoas que se passam por outras pessoas para obter vantagem própria ou a terceiro, ou ainda para causar dano a outrem (CRESPO, 2011. p. 89).

Crespo ainda afirma que a categoria mais comum destes crimes são os Fakes, termo esse que significa uma pessoa se passando por outra por meio de um perfil em rede social.

Os exemplos atuais desta modalidade são os fakes, que são pessoas que se passam por outras em redes sociais através da criação de perfis falsos em redes sociais (CRESPO, 2011. p. 89).

2.1.5 Violação de Direitos Autorais, uso indevido de marcas, pirataria de software, concorrência desleal e espionagem eletrônica/industrial

Os direitos autorais são tutelados pela constituição federal em seu artigo 5o inciso XXVII que doutrina: "(...) aos autores pertence o direito exclusivo de utilização, publicação ou reprodução de 55 suas obras, transmissível aos herdeiros pelo tempo que a lei fixar" (BRASIL, 1988).

Sendo assim, como grande parte desta publicação e/ou reprodução é feito por meio digital atualmente a proteção a esse direito estende-se também aos meios digitais.

A violação deste direito encontra-se no artigo 184 do Código Penal Brasileiro que disciplina: "violar direitos de autor e os que lhe são conexos" prevendo "pena de detenção, de 3 (três) meses a 1 (um) ano, ou multa" (BRASIL, 1940).

Ao decorrer do avanço tecnológico, os direitos autorais foram estendidos aos softwares (programa de computadores) na lei 9609/98, neste sentido Crespo (2011, p. 89) afirma que:

> Com relação à violação de direito autoral de software, crime no qual visa-se proteger o bem jurídico também os direitos do autor, denominada popularmente como pirataria de software, a Lei 9609/98 aborda o tema de forma a tratar como crime a violação de direitos de autor de programa de computador e atividades comerciais produzidas tendo como objeto o software violado.

2.1.6 Pornografia Infantil

Tal prática encontra-se tipificada no Código Penal Brasileiro nos artigos 240 a 241, que compreende em qualquer ato ou participação do ato desde a produção até o armazenamento ou distribuição/comercialização desses vídeos ou filmes consistem em crime, sendo a internet apenas um novo meio para a possível prática destes atos. Para Wendt e Jorge (2012, p. 98), a ponografia infantil na internet é uma das maiores preocupações como é possível notar em: "uma forma ilegal de pornografia que se caracteriza pela utilização de imagens de cunho erótico de crianças e adolescentes e representa uma das maiores preocupações na internet".

Para Crespo (2011, p. 90), em forma de afirmar os caputs dos artigos mencionados, diz:

> Ocorre que a lei brasileira pune diversas formas situações envolvendo a exposição da sexualidade infantil em fotos, imagens, filmagens e interpretações teatrais, como, por exemplo, a produção, reprodução, filmagem e o registro de cenas de sexo explícito envolvendo situações de pornografia com crianças e adolescentes.

2.1.7 Crimes contra a Honra

Sobre a honra, Ishida (2009, p. 256) traz boas exemplificações sobre a caracterização do conceito de honra, afirmando que a honra seria um "conjunto de atributos morais, intelectuais e físicos de uma pessoa, que lhe conferem consideração social e estima própria".

Ainda sobre a honra:

> (…) a mesma pode ser dividida em dois tipos, sendo estes a honra subjetiva que é o sentimento de cada um perante seus atributos físicos, intelectuais, sociais e morais, e a honra objetiva que trata-se do juízo que a comunidade faz do indivíduo (ISHIDA; 2009, p.256).

As condutas típicas dos crimes contra a honra são encontradas nos artigos 138,139 e 140 do código penal brasileiro, e tratam respectivamente sobre a calúnia, difamação e a injúria:

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa (BRASIL, 1940).

Para Gatto, o uso dos meios tecnológicos facilita a disseminação de tais atos, pois, com novas tecnologias, as formas de manifestar nossas opiniões foram criadas além de novos lugares digitais em que essa livre expressão ocorre:

> Esses crimes que se alastram com extrema facilidade com o uso da internet se tornaram ainda mais evidente com o advento das novas tecnologias, se expressar e manifestar uma opinião, com ilustrações como vídeo, foto, mensagens com áudio etc.
> Com a criação de blogs, sites de relacionamento dentre outras maneiras ofender e ser ofendido, seja direta ou indiretamente acabou se tornando rotina na vida de quem acessa a grande rede.- grave (GATTO, 2011).

2.1.8 Cyberbullying

O cyberbullying é o termo que caracteriza uma forma do bullying por meios tecnológicos, a tipificação do ato encontra-se na lei 13.185/2015 no seu artigo 2o:

> Art. 2º Caracteriza-se a intimidação sistemática (bullying) quando há violência física ou psicológica em atos de intimidação, humilhação ou discriminação e, ainda:
> I - ataques físicos;
> II - insultos pessoais;
> III - comentários sistemáticos e apelidos pejorativos;
> IV - ameaças por quaisquer meios;
> V - grafites depreciativos;
> VI - expressões preconceituosas;
> VII - isolamento social consciente e premeditado;
> VIII - pilhérias.
> Parágrafo único. Há intimidação sistemática na rede mundial de computadores (cyberbullying), quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial (BRASIL, 2015).

É notório que o bullying praticado por meios tecnológicos é uma preocupação do legislador, pois em seu parágrafo único determinou qual seria a caracterização do cyberbullying.

2.1.9 Fraudes Virtuais (Furto, Estelionato e Fraudes)

As fraudes virtuais podem ser conceituadas como uma estratégia ou esquema com o objetivo de obter vantagem ilícita sob outrem. O bem jurídico a ser tutelado nesse tipo de crime é a moralidade do setor comercial e das relações mercantis.

Para Wendt e Jorge (2012, p. 75), os meios tecnológicos ampliaram as oportunidades para a prática desses atos: “a fraude pode ocorrer em vários ambientes, entretanto com o surgimento de dispositivos tecnológicos e da internet ficou potencializada a disseminação e o uso de fraudes virtuais”.

Neste mesmo sentido, pode-se afirmar que a fraude virtual consiste em uma mensagem por meio eletrônico com o objetivo de induzir quem recebe a referida mensagem a dispor de informações pessoais e/ou comerciais para que quem enviou a mesma possa usar estas informações a fim de obter vantagem ilícita.

São diversas as possibilidades em que se pode cometer fraude virtual, porém, as mais comuns são o estelionato e a fraude no comércio, tipificadas no código penal brasileiro nos artigos 171 e 175, respectivamente, que dizem:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
> Art. 175 - Enganar, no exercício de atividade comercial, o adquirente ou consumidor:
> I - vendendo, como verdadeira ou perfeita, mercadoria falsificada ou deteriorada;
> II - entregando uma mercadoria por outra:
> Pena - detenção, de seis meses a dois anos, ou multa. (BRASIL, 1940).

2.1.10 Tráfico de Drogas

A tipificação do tráfico de drogas encontra-se na lei nº 11.343/2006 comumente conhecida como lei de drogas, no artigo 33 encontra-se o seguinte texto:

> Art. 33. Importar, exportar, remeter, preparar, produzir, fabricar, adquirir, vender, expor à venda, oferecer, ter em depósito, transportar, trazer consigo, guardar, prescrever, ministrar, entregar a consumo ou fornecer drogas, ainda que gratuitamente, sem autorização ou em desacordo com determinação legal ou regulamentar:
> Pena - reclusão de 5 (cinco) a 15 (quinze) anos e pagamento de 500 (quinhentos) a 1.500 (mil e quinhentos) dias-multa. (BRASIL, 2006)

Sendo assim, como expõe o caput do artigo supramencionado, expor a venda drogas constitui ato ilícito tipificado em lei específica e esta prática cometida por meio tecnológico mesmo que não tão corriqueira ou simples, ainda assim é crime.

2.1.11 Atentado a Serviço de Utilidade Pública

O atentado a serviço de utilidade pública encontra sua tipificação no artigo 265 do Código Penal Brasileiro: “Art. 265 - Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública: Pena - reclusão, de um a cinco anos, e multa” (BRASIL, 1940).

Sendo assim, os serviços que possuem versão digital serão considerados também incluindo serviços de utilidade pública como exemplifica Wendt e Jorge (2012, p. 28): “os serviços disponibilizados na internet são considerados também como serviços de utilidade pública, ou seja, tem o mesmo objetivo de servir a população”.

Pelo motivo de servirem a população, caracterizam-se como serviços de utilidade pública e abarcados pelo artigo 265, portanto, apenas um novo modus operandi para um crime já existente.

2.2 CRIMES VIRTUAIS PRÓPRIOS

Com o advento das novas tecnologias, novos bens jurídicos também surgiram e destas formam novos crimes que precisam ser tutelados pelo ordenamento jurídico brasileiro. Tais crimes, pelo motivo de apenas serem possíveis por meios tecnológicos, receberam a classificação de crimes virtuais próprios. Wendt e Jorge afirmam que:

“eles somente podem ser praticados com a utilização de computadores ou de outros recursos tecnológicos que permitem o acesso à internet” Wendt e Jorge (2012, p. 19).

Com objetivo de complementar tal conceituação, Crespo (2011, p. 57) diz que: “neste diapasão, pode-se complementar que são crimes que violam inicialmente a informação ou a privacidade como bem jurídico principal, e que de forma secundária atingem os dados ou sistemas”.

A seguir, alguns dos principais crimes virtuais próprios e suas respectivas tipificações.

2.2.1 Acesso Não autorizado (Invasão)

O acesso não autorizado é atualmente previsto pela lei 12.737/2012 que alterou o Código Penal Brasileiro e doutrina que:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou

> tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa (BRASIL, 2012).

Sobre tal crime, Crespo (2011, p. 64) discorre que:

> O acesso não autorizado, também conhecido como invasão ou ainda como hacking, é a conduta de acessar indevidamente um sistema informático, seja para obter prestígio perante aos seus pares ou ainda para que se obtenha algum tipo de vantagem ou manipulação de dados.

2.2.2 Obtenção de dados e transferência ilegal de dados

A obtenção de dados e transferência ilegal de dados encontra sua tipificação no §3o e 4o do artigo 154-A da lei 12.737 de 2012 que diz:

> (...) § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º , aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidas (BRASIL, 2012).

Sendo assim, entende-se que após a invasão do dispositivo tecnológico, seja fisicamente ou por método remoto, obter informações consideradas sigilosas ou particulares incidirá no parágrafo 3o e no caso de haver transferência ou comercialização desses dados coletados ilegalmente sofreu majoração da pena do crime cometido.

Sobre as formas em que é realizado as invasões, Crespo (2011, p. 70) dispõe que:

> A obtenção de dados e a transferência ilegal de dados, são condutas que podem ser dadas em diversas formas, entretanto algumas são mais comuns no cotidiano da sociedade atual. A principal delas é por meio de spywares ou espiões que são programas que rastreiam informações contidas no dispositivo tecnológico.

Estes espiões que Crespo apresenta são softwares (programas de computadores como um aplicativo de celular por exemplo) que possuem a finalidade da invasão do dispositivo ou do roubo de dados da vítima em questão, estes programas normalmente são camuflados com aparência de outro programa ou alguma oportunidade de negócio que parece interessante. Sobre a criação dos spywares, Bittencourt (2013) afirma que:

> Sobre os spywares ou espiões, estes programas foram criados com o objetivo de serem utilizados por empresas para que estas pudessem identificar os hábitos de possíveis clientes em potencial e consequentemente usar as informações capturadas afim de direcionar estratégias de publicidade e propaganda, porém, com o passar do tempo, estes programas passaram a ser utilizados ilicitamente.

Após o fato típico da obtenção de dados, a transferência desses arquivos ou informações para outros dispositivos com ou sem a finalidade de obtenção de lucro configura o parágrafo 4º do dispositivo supramencionado com majoração da pena de um terço a dois terços.

2.2.3 Divulgação ou utilização indevida de informações

A divulgação ou utilização indevida de informações encontra sua correspondência no ordenamento jurídico por meio de dois artigos, a combinação do artigo 154 do Código Penal com o parágrafo 4º do artigo 154-A da lei 12.737 de 2012 já mencionado anteriormente neste artigo.

Vale ressaltar aqui que não importa, nesta conduta, se houve invasão ou não de dispositivo tecnológico, pois o objeto em questão é a divulgação ou utilização indevida da informação. Sobre a sua prática no mundo real, Crespo (2011, p. 80) afirma que:

> Chama-se atenção para uma das formas de realização da divulgação ou utilização de informações, que são os casos em que usuários fazem seus cadastros em sites, seja para compras ou qualquer ação interativa junto à internet, em que insira os seus dados pessoais e que estes sejam manipulados ou abusados, oriundos de acesso não autorizado ou não.

O artigo 154 do Código Penal dispõe que:

> Art. 154 - Revelar alguém, sem justa causa, segredo, de que tem ciência em razão de função, ministério, ofício ou profissão, e cuja revelação possa produzir dano a outrem: Pena - detenção, de três meses a um ano, ou multa. (BRASIL, 1940).

Sendo assim, a conduta deste artigo leva em consideração uma posição social, em que a pessoa proveito de sua posição em que determinadas informações consideradas sigilosas ou com potencial prejudicial a outrem e apodera-se dessas informações e as divulga sem a devida permissão.

É válido mencionar que a conduta de divulgação ou utilização indevida de informações fere o direito à privacidade encontrado no inciso X do artigo 5º da Constituição Federal que diz: “são invioláveis a intimidade, a vida privada, a honra e a imagem das

pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (BRASIL, 1988).

2.2.4 Engenharia Social e Phishing

Engenharia social é um conjunto de técnicas de manipulação praticadas por potenciais criminosos com o intuito de induzir ao erro vítimas desavisadas, tal erro consiste no envio de dados em sites não confiáveis ou download de programas maliciosos como os spywares já mencionados neste no decorrer deste trabalho.

Sobre a engenharia social Wendt e Jorge (2012, p. 20) dispõe que:

> A engenharia social é a utilização do artifício intelectual e de um conjunto de técnicas empregadas em um método que mascara a realidade, para fazer com que o a vítima acredite nas informações e envie dados pessoais aos criminosos para que estes possam, a partir destes dados, executar as ações desejadas.

No mesmo sentido, em relação a quem age e de que forma complementam que:

> Os engenheiros sociais, como são chamadas pessoas que incorrem nesta conduta, usam técnicas a partir da emoção de seus alvos, usando dentre outras formas emotivas, o medo, a ganância, a simpatia e a curiosidade. Criada a motivação, o usuário presta assim as informações necessárias (WENDT; JORGE, 2012, p.23).

Em suma, o engenheiro social dispõe de técnicas que se camuflam com a verdade, estimula determinada emoção na vítima a fim de desestabilizá-la e torná-la mais suscetível ao seu golpe com o intuito de obter informações sigilosas e privadas ou vantagem econômica.

Já acerca do phishing, tal técnica pode ser considerada um tipo de engenharia social, em que o criminoso, golpista, se perfaz como alguém confiável, seja essa uma pessoa ou uma empresa querendo prestar serviços ou vender algo, o phishing normalmente é direcionado a vítimas especificas, pois necessitam de determinadas características que validem a sua falsa autenticidade. O golpe comumente acontece por meio de mensagens eletrônicas, por exemplo, e-mail, sms, ou mensagens em redes sociais.

Sobre o que fora aqui exposto, Crespo (2011, p. 83) afirma que:

> Já o phishing, na tradução específica para este caso significa pescar, pode ser considerado uma modalidade da engenharia social, uma vez que parte do mesmo princípio de realização da fraude virtual, ludibriando a vítima para obtenção de dados pessoais importantes, ou seja, a "pesca dos dados", entretanto a sua particularidade é o meio por onde se age é especificamente através do envio de mensagens eletrônicas.

Neste sentido, é possível afirmar que por se tratar de uma forma de engenharia social, o phishing busca chamar a atenção de uma empresa ou pessoa de forma atrativa por meio de uma mensagem eletrônica, Wendt e Jorge (2012, p. 39) conceituam phishing como "(...) a conduta das pessoas que encaminham mensagens com a finalidade de induzir a vítima a preencher formulários com seus dados privados ou instalar códigos maliciosos, capazes de transmitir para o criminoso cibernético as informações desejadas".

Em ambos os casos, a técnica mais comumente utilizada é o email. Sobre tal fato, Crespo (2011, p. 82) afirma que:

> Os casos mais comuns que ocorrem tanto de engenharia social quanto de phishing, ou seja, por meio de sites falsos; e-mails que contenham links para acesso a sites falsos; e-mails que encaminham o usuário para o acesso a um site falso contendo programas que são instalados automaticamente no dispositivo do usuário, são os casos de captura de informações bancárias, de cartões de crédito, senhas em geral; e por fim, atualmente casos em mensagens postadas em redes sociais com falsos links.

Sobre a tipicidade destas práticas, ambas encontram sua correspondência no mesmo artigo, o artigo 171 do Código Penal Brasileiro, que diz:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis (BRASIL, 1940).

Para Crespo (2011, p.85) "(...) é estelionato pelo fato de que o autor visa vantagem econômica".

Sendo assim, pelo fato do objetivo ser a vantagem econômica incide na conduta do ato típico estelionato. Não há agravante pela prática do estelionato ocorrer em dispositivo tecnológico, entretanto é válido ressaltar que a prática de engenharia social e phishing somente podem ocorrer pela internet mesmo que sua tipificação ocorra em ato típico ilícito já conhecido pelo ordenamento jurídico brasileiro.

O artigo 171 do Código Penal Brasileiro faz menção ao crime estelionato, prevendo que a pessoa que obtenha para si ou outrem vantagem de forma ilícita mediante a algum tipo de fraude será punido com a reclusão de um a cinco anos e mais multa prevista conforme lei. Entretanto, no caso do envio de e-mail encaminhando a instalação de programas maléficos que facilitam a invasão ao dispositivo e permitem o acesso indevido e a captura de dados ou

informações para cometimento de fraude, o enquadramento cabe também no art. 154-A do Código Penal Brasileiro:

> Art. 154-A - Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita. Pena – detenção, de 3 (três) meses a 1 (um) ano, e multa) (BRASIL, 1940).

Logo, este tipo de conduta por meio de dispositivo tecnológico pode ser tipificado pela combinação dos artigos 171 que é a previsão do crime normalmente utilizada, com o artigo 154-A que prevê a invasão ao dispositivo, neste caso para a obtenção dos dados e informações a serem usadas para o estelionato.

3 PROCEDIMENTOS DOS CRIMES VIRTUAIS

Após abordagem dos crimes virtuais próprios e impróprios, suas conceituações e peculiaridades, há de se falar dos seus procedimentos, mais especificamente, sobre a competência, jurisdição e a aplicação territorial para valência da lei ao caso concreto e, por fim, sua investigação, como será feita e como serão produzidas as provas.

3.1 APLICAÇÃO TERRITORIAL

Com o advento do mundo virtual, as perspectivas de tempo e espaço tomam novas formas, expandindo-se e transcendendo os limites territoriais a época em que a doutrina foi escrita. Sendo assim, algumas aplicações nas formas em que a lei era utilizada tornam-se um pouco mais complexas com novos fatores a serem considerados e adaptados a esta nova realidade.

Sobre tal fato, Crespo (2011, p. 117) afirma que:

> O surgimento do mundo virtual apresenta novas concepções de tempo e espaço, gerando empecilhos à aplicação de leis tradicionais e apresentando um novo entendimento a território, uma vez que rompem-se as barreiras de limites territoriais físicos.

Em tom complementar, Fiorillo e Conte (2016, p. 203) sobre a aplicação territorial discorrem que "com a internet e o ambiente virtual, não existem barreiras ou limites de

separação física, pois a concepção de território passa a ser qualquer um dos pontos interligados a rede e que tenha acesso às informações".

Apresentando-se assim uma das dificuldades encontrada com o cometimento de crimes no âmbito digital: Qual será o ponto territorial de cometimento do crime:

Onde o crime foi cometido afetará a competência e jurisdição de quem julgar tal fato.

Para Wendt e Jorge (2012, p. 181):

> Os recursos tecnológicos passam a permitir inclusive que os criminosos ajam em parcerias organizadas, mesmo em locais diferentes, distantes e muitas vezes sem ao menos se conhecerem, para que possam cometer o crime.

Isto é, a ambivalência, consistente na era digital em que vivemos, propicia grandes facilidades e agilidades na vida cotidiana. Entretanto, tal facilidade também viabiliza novos crimes e novas formas de cometimento de crimes já conhecidos, além de que facilita as conhecidas parcerias organizadas em que os indivíduos não precisam se encontrar fisicamente para organizarem e planejarem suas práticas ilícitas.

Para Pinheiro (2013), esta ambivalência não é decorrente exclusivamente do mundo digital e da internet, é consequência da globalização e da contemporaneidade globalizada em que vivemos:

> O problema não está apenas no âmbito da Internet, mas em toda sociedade globalizada e convergente, na qual muitas vezes não é possível determinar qual o território em que aconteceram as relações jurídicas, os fatos e seus efeitos, sendo difícil determinar que norma aplicar utilizando os parâmetros tradicionais.

Sendo assim, fica claro que a delimitação de onde ocorre o fato típico é crucial para determinação de sua jurisdição e competência, e por consequência qual norma será aplicada; mesmo que via de regra, o código penal brasileiro possui aplicação em todo território nacional. Sobre tal apontamento Fiorillo e Conte (2016, p. 207) afirmam que:

> Em que se pesem todas as dificuldades para a definição territorial, a lei penal brasileira, no tocante a sua aplicação, tem como regra a aplicação dentro de seu limite territorial, salvo os casos de tratados ou convenções internacionais nos quais também é permitido a aplicação de lei estrangeira, ou seja, a combinação destas aplicações dá origem a denominada territorialidade temperada.

Sendo assim, a possibilidade de utilização de tratados internacionais e/ou convenções determinam uso do princípio da territorialidade temperada, que consiste na aplicação da lei penal brasileira em regra e em casos excepcionais a lei estrangeira, por meio dos tratados e

convenções, poderá ser aplicada em sua totalidade ou parcialmente ao caso concreto. Sobre tal afirmação, a Lei diz em seu 5º artigo do Código Penal Brasileiro que: “Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional” (BRASIL, 1940).

Sobre o local do cometimento do fato típico Crespo (2011, p. 117) afirma que:

> Com relação ao lugar do crime, a teoria aplicada aos crimes cometidos, determinando o local do crime, é a teoria da ubiquidade a qual apresenta a combinação de outras duas teorias, considerando uma ou outra, sejam elas a teoria da atividade que entende como local do crime o local da ação onde foi cometido e a teoria do resultado que prevê como local do crime o local aonde se deu o resultado da ação cometida.

Apresenta-se então o conceito da teoria da ubiquidade, que consiste na combinação de outras duas teorias e suas respectivas aplicações sendo estas a teoria da atividade e a teoria do resultado. Na primeira, o local do crime e onde foi de fato cometido o fato típico, enquanto na teoria do resultado o local do crime seria onde o resultado do fato típico ocorreu.

A correspondência dentro do ordenamento jurídico a esta teoria encontra-se no artigo 6º do Código Penal Brasileiro que diz: “considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado” (BRASIL, 1940).

É valido mencionar que para Jesus (2008, p.127): “basta que a porção da conduta criminosa tenha ocorrido em nosso território para que ser aplicada a nossa lei”,

Sendo assim, para que a lei penal seja aplicada é necessário que pelo menos parte do crime tenha sido realizado em território nacional.

Para Crespo (2011, p. 117):

> O ambiente virtual não é um território propriamente, sendo assim, ganha importância o local da informação, pois é que este que indica minimamente o lugar do crime. Ganha destaque neste caso crimes que são cometidos de forma parcial em diversos países.

Portanto, como não há território no âmbito digital, o local será definido pela localidade da informação, possibilitando também o cometimento parcial de crimes em países diferentes. Nesta mesma linha de raciocínio, os crimes virtuais cometidos fora do território nacional possuem, também, tipicidade e são abarcados pelo p. 7º do Código penal Brasileiro que abrange o princípio da extraterritorialidade e doutrina que:

> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: (Redação dada pela Lei nº 7.209, de 1984)
> I - os crimes: (Redação dada pela Lei nº 7.209, de 11.7.1984)
> a) contra a vida ou a liberdade do Presidente da República; (Incluído pela Lei nº 7.209, de 1984)
> b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público; (Incluído pela Lei nº 7.209, de 1984)
> c) contra a administração pública, por quem está a seu serviço; (Incluído pela Lei nº 7.209, de 1984)
> d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil; (BRASIL, 1940).

No 2º parágrafo do artigo supramencionado, encontra-se o respaldo para aplicação da lei nacional do código penal brasileiro para os crimes que forem cometidos no estrangeiro. Porém, o Brasil, por ser signatário de convenção ou tratado, obrigou-se a cumprir, até mesmo, crimes cometidos por brasileiros em solo estrangeiro, a bordo de aeronaves ou embarcações brasileiras em território estrangeiro:

> (...) II - os crimes: (Redação dada pela Lei nº 7.209, de 11.7.1984)
> a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;(Incluído pela Lei nº 7.209, de 1984)
> b) praticados por brasileiro; (Incluído pela Lei nº 7.209, de 1984)
> c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados. (Incluído pela Lei nº 7.209, de 1984) (BRASIL, 1940).

Ainda na mesma linha de raciocínio de análise do artigo 7º do Código Penal Brasileiro, em seu parágrafo primeiro doutrina que nos casos que possuem correspondência com o inciso primeiro, o agente deverá ser punido com as leis brasileiras mesmo que absolvido no exterior: "(...) § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro. (Incluído pela Lei nº 7.209, de 1984) (BRASIL, 1940)".

No segundo parágrafo, encontra-se condições concorrentes para os crimes terem aplicabilidade da lei brasileira:

> (...) § 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições: (Incluído pela Lei nº 7.209, de 1984)
> a) entrar o agente no território nacional; (Incluído pela Lei nº 7.209, de 1984)
> b) ser o fato punível também no país em que foi praticado; (Incluído pela Lei nº 7.209, de 1984)
> c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição; (Incluído pela Lei nº 7.209, de 1984)
> d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena; (Incluído pela Lei nº 7.209, de 1984)

> e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável. (Incluído pela Lei nº 7.209, de 1984) (BRASIL, 1940).

Na sequência, em seu 3º parágrafo o artigo 7º afirma que os crimes cometidos contra brasileiro por estrangeiro no exterior serão acobertados pela lei brasileira, se reunirem as condições do parágrafo 2o:

> § 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior: (Incluído pela Lei nº 7.209, de 1984)
> a) não foi pedida ou foi negada a extradição; (Incluído pela Lei nº 7.209, de 1984)
> b) houve requisição do Ministro da Justiça. (Incluído pela Lei nº 7.209, de 1984) (BRASIL, 1940).

Para Jesus (2008,p. 129):

> A lei penal brasileira, no tocante a sua aplicação, tem como regra a aplicação dentro de seu limite territorial, porém, para casos de tratados ou convenções internacionais permite também a aplicação de lei estrangeira para os crimes praticados total ou parcialmente em território nacional, adotando ao princípio da territorialidade temperada.

Sendo assim, reafirma sobre o que foi exposto do artigo 7o do Código Penal Brasileiro sobre a competência da lei nacional para crimes em que o Brasil, por ser signatário de tratado ou convenção, compromete-se a punir com lei estrangeira, empregando assim o princípio da territorialidade temperada.

Sobre tal fato, Fiorillo e Conte (2016, p. 321) afirmam que: “é inegável a necessidade de cooperação internacional entre os Estados, independente de qual será o responsável pela aplicação da legislação”.

Isto é, a aplicação da territorialidade se mostra necessária e fundamental, ainda mais, quando o assunto é crimes digitais. Para tanto vale mencionar o tratado que ocorreu na Hungria em 2001, chamado de Convenção de Budapeste. Até o presente momento, 66 países são signatários deste tratado que visa celebrar normas internacionais para prevenção e repreensão dos crimes digitais. Foi aprovada a adesão do Brasil recentemente, em junho de 2021, considerado um grande passo no avanço ao combate a crimes digitais e cibernéticos.

Comentado [SS1]: Quem é signatário?

Comentado [GF2R1]: resolvido

Em tom de desfecho deste tópico, é possível concluir que com o advento das tecnologias e do mundo digital a determinação do local do crime se torna bem mais complexo. Adaptações são necessárias à doutrina para que essa seja aplicada ao caso concreto. Ressalta-se que quando os crimes forem cometidos por estrangeiro ou brasileiros no

exterior são fatores que complicam, ainda mais, a competência e jurisdição devendo cada caso ser estudado em sua individualidade com suas peculiaridades e objetivando a melhor e mais correta forma de aplicação da lei para tal.

3.2 JURISDIÇÃO E COMPETÊNCIA

Ao falarmos de jurisdição no âmbito dos procedimentos, podemos defini-la como a função do Estado em aplicar a teoria ao caso concreto. Isto é, o Estado, por meio do Poder Judiciário, aplicar as normas teóricas da legislação aos casos em que houver sua tipicidade e a necessidade de intervenção.

Para Capez (2015, p. 257):

> (...) jurisdição é uma função do Estado, que representado pelo Poder Judiciário, aplica as normas da ordem em casos concretos de forma imparcial para a solução pacífica de litígios entre partes conflitantes, de forma a firmar a autoridade da ordem jurídica e a verticalidade na relação Estado particular.

Já a competência para Nicolitt (2009, p. 168): “entende-se por competência como a organização sistemática do exercício da jurisdição, ou seja, uma parcela da jurisdição que é entregue para cada órgão jurisdicional, fixando limites da atividade jurisdicional dentro do Poder Judiciário”.

Capez (2015, p. 259) em tom de caracterização discorre que competência:

> (...) é a delimitação do poder de jurisdicional (fixa os limites dentro dos quais o juiz pode prestar jurisdição), sendo a fixação em razão de especialidades, sendo estas: de acordo com o a natureza do crime praticado, de acordo com a qualidade da pessoa incriminada ou ainda de acordo com o local que foi praticado o crime, local que foi consumado o crime ou o local da residência do autor.

Isto é, entende-se que a competência nada mais é que o conjunto de condições como por exemplo fato típico, local ou até mesmo agentes e vítima que somados indicaram quem deverá julgar o caso concreto. No entanto, quando falamos de crimes virtuais, o tema se torna mais complexo com determinadas peculiaridades, por exemplo, qual seria o local de cometimento do crime; como já abordado anteriormente, sendo este o de residência da vítima, do ator ou do provedor do site que está hospedado tais informações. Além disso, há as circunstâncias de que os autores não possuem residência em território brasileiro como esclarece Pinheiro (2016):

Comentado [SS3]: Ficou confuso

Comentado [GF4R3]: resolvido

> O tema fica complexo a partir do momento que ocorre no ambiente virtual, ou seja, pela internet onde há extrema dificuldade na determinação territorial uma vez que o crime é cometido normalmente à distância, podendo ser inclusive pessoas de outros países e de outras culturas.

Sobre a competência, o artigo 70 do Código de Processo Penal Brasileiro legisla que: “a competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução” (BRASIL, 1940).

Em Consonância com o artigo supramencionado, Orrigo e Filgueira (2016, p. 6) afirmam que: "tem-se como regra que os crimes serão julgados onde foram consumados, ou seja, onde o bem jurídico foi afetado".

Entretanto, para os crimes virtuais nem sempre é possível tal determinação ou, até mesmo, por ocorrerem resultados em diversas localidades em que bens jurídicos foram afetados, em plurilocais, incluindo territórios não nacionais. O parágrafo 1o do artigo 70 do Código de Processo Penal Brasileiro aborda tal circunstância em: “§ 1o Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução” (BRASIL, 1940).

Sendo assim, caso o fato típico tenha se iniciado em território nacional, porém, consumado fora deste, a competência será fixada pelo local do último ato executivo do fato típico.

Todavia, nos casos em que o último ato executivo também for praticado fora do território nacional, terá competência para julgar o ato o juiz em que o crime devesse, mesmo que parcialmente, produzir resultado como pode ser observado no 2º parágrafo do mesmo artigo: “§ 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado” (BRASIL, 1940).

Enfim, o 3º parágrafo do artigo 70 do Código de Processo Penal disciplina sobre os casos em que for incerta a jurisdição, pela localidade, estar entre dois limites territoriais ou quando tal limite for incerto, determinar-se-á a competência pela prevenção:

> §3o Quando incerto o limite territorial entre duas ou mais jurisdições, ou quando incerta a jurisdição por ter sido a infração consumada ou tentada nas divisas de duas ou mais jurisdições, a competência firmar-se-á pela prevenção (BRASIL, 1940).

Isto é, aquele juízo que antecipar-se processualmente ou reconhecer competência para julgar o ato primeiramente será o juiz competente para o caso assim como determina o artigo 83 do Código de Processo Penal:

> Art. 83. Verificar-se-á a competência por prevenção toda vez que, concorrendo dois ou mais juízes igualmente competentes ou com jurisdição cumulativa, um deles tiver antecedido aos outros na prática de algum ato do processo ou de medida a este relativa, ainda que anterior ao oferecimento da denúncia ou da queixa (BRASIL, 1940).

O Superior Tribunal de Justiça possui jurisprudência firmada sobre tais aplicações do fora exposto neste assunto:

> CC 136700 / SP
> CONFLITO DE COMPETENCIA
> 2014/0274368-9
> RELATOR
> Ministro ROGERIO SCHIETTI CRUZ (1158)
> DATA DO JULGAMENTO
> 23/09/2015
> EMENTA
> CONFLITO DE COMPETÊNCIA. CRIMES CONTRA HONRA PRATICADOS PELA INTERNET. COMPETÊNCIA. VEICULAÇÃO DO CONTEÚDO OFENSIVO. FIXAÇÃO NO LOCAL DO TITULAR DO PRÓPRIO DOMÍNIO E QUE CRIOU A HOME PAGE ONDE É ABASTECIDO SEU CONTEÚDO.
> 1. Tratando-se de crimes contra a honra praticados pela internet, a competência deve ser firmar de acordo com a regra do art. 70 do Código de Processo Penal, segundo o qual "A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução". Isso porque constituem-se crimes formais e, portanto, consumam-se no momento de sua prática, independentemente da ocorrência de resultado naturalístico. Assim, a simples divulgação do conteúdo supostamente ofensivo na internet já é suficiente para delimitação da competência.
> 2. Esse local deve ser aquele de onde efetivamente partiu a publicação do conteúdo, o que ocorre no próprio local do domínio em que se encontra a home page, porquanto é ali que o titular do domínio alimenta o seu conteúdo, independentemente do local onde se hospeda o sitio eletrônico (provedor).
> 3. No caso, a veiculação da reportagem que deu ensejo ao inquérito policial partiu de sítio eletrônico cujo domínio era de empresa situada no Mato Grosso, razão pela qual a competência é do Juízo Federal da 5ª Vara da Seção Judiciária do Estado do Mato Grosso **(BRASIL, 2015)**.

Neste acórdão, observa-se que a regra do artigo 70, em que a competência será designada onde fora pratica o último ato executivo, por tratar-se de veiculação de conteúdo ofensivo em sites, a simples hospedagem de tal conteúdo já caracteriza o fato típico e consequentemente determina sua competência, sendo assim, o domicílio do réu de onde partiu tais publicações será o foro competente para julgar tal caso.

> HC 591218 / SC

HABEAS CORPUS
2020/0150284-6
09/02/2021
RELATOR
Ministro JOEL ILAN PACIORNIK (1183)

HABEAS CORPUS SUBSTITUTIVO DE RECURSO PRÓPRIO. CRIME CONTRA A HONRA PRATICADO POR MEIO DA INTERNET. NATUREZA FORMAL. CONSUMAÇÃO NO LOCAL DA PUBLICAÇÃO DO CONTEÚDO OFENSIVO. TODAVIA QUANDO ESSE LUGAR É DESCONHECIDO, INCIDÊNCIA DA REGRA SUBSIDIÁRIA DO ART. 72 DO CÓDIGO DE PROCESSO PENAL - CPP. COMPETÊNCIA DO LOCAL DE DOMICÍLIO OU RESIDÊNCIA DA QUERELADA. EXCEÇÃO DE INCOMPETÊNCIA OPOSTA NO PRAZO DA DEFESA. OBSERV NCIA DO ART. 108 DO CPP. PRECLUSÃO CONSUMATIVA NÃO CONFIGURADA. ORDEM CONCEDIDA DE OFÍCIO. ACÓRDÃO IMPUGNADO CASSADO.

RESTABELECIDA A DECISÃO DE PRIMEIRO GRAU QUE DEU PROVIMENTO À EXCEÇÃO DE INCOMPETÊNCIA.

1. Diante da hipótese de habeas corpus substitutivo de recurso próprio, a impetração sequer deveria ser conhecida segundo orientação jurisprudencial do Supremo Tribunal Federal - STF e do próprio Superior Tribunal de Justiça - STJ. Contudo, razoável o processamento do feito para verificar a existência de eventual constrangimento ilegal.

2. "Crimes contra a honra praticados pela internet são formais, consumando-se no momento da disponibilização do conteúdo ofensivo no espaço virtual, por força da imediata potencialidade de visualização por terceiros" (CC 173.458/SC, Rel. Ministro JOÃO OTÁVIO DE NORONHA, TERCEIRA SEÇÃO, DJe 27/11/2020).

3. Na hipótese dos autos é incontroverso que não se identificou o local de onde partiram as supostas ofensas. Tal indefinição é apontada desde a inicial acusatória e também mencionada nas decisões prolatadas na instância ordinária. Destarte, torna-se impossível a aplicação da regra descrita no art. 70 do CPP, a qual determina a fixação da competência no local da consumação. Diante disso, deve incidir na espécie a regra subsidiária descrita no art. 72 do CPP que fixa a competência do juízo do local da residência ou domicílio do réu.

4. A apresentação da exceção de incompetência, mediante peça autônoma, na mesma oportunidade em que apresentada a defesa prévia, atende perfeitamente à determinação do art. 108 do CPP, segundo o qual "a exceção de incompetência do juízo poderá ser oposta, verbalmente ou por escrito, no prazo da defesa". No caso dos autos, as manifestações da querelada anteriormente à apresentação da defesa prévia, quais sejam, pedido de adiamento de audiência conciliatória e discordância do pedido de justiça gratuita, em nada anteciparam as teses defensivas, as quais foram efetivamente apresentadas de forma plena, no momento oportuno da defesa prévia, em concomitância com a peça em que oposta a exceção de incompetência relativa.

5. A incompetência relativa, como é o caso da competência territorial, se não arguida no momento oportuno, prorroga a competência do juízo. Entretanto, no caso em análise, o acórdão impugnado praticou flagrante ilegalidade ao afirmar que teria havido preclusão consumativa, porquanto o defensor da querelada apresentou a exceção de incompetência territorial concomitantemente à defesa prévia, ou seja, no prazo da defesa como determina o art. 108 do CPP.

6. De acordo com o artigo 43, do Código de Processo Civil - CPC, aplicado subsidiariamente no caso concreto por força do artigo 3º, do CPP, "determina-se a competência no momento do registro ou da distribuição da petição inicial, sendo irrelevantes as modificações do estado de fato ou de direito ocorridas posteriormente, salvo quando suprimirem órgão judiciário ou alterarem a competência absoluta".

7. Está configurada flagrante ilegalidade no acórdão impugnado que apontou extemporaneidade por preclusão consumativa inexistente na espécie, bem como fixou competência do juízo do local da residência da querelante, no caso de crime contra a honra praticado pela internet, em total desconformidade com a jurisprudência desta Corte Superior e com as regras insculpidas no art. 70 e seguintes do CPP.

> 8. Ordem concedida de ofício tão somente para cassar o acórdão proferido pelo Tribunal de Justiça do Estado de Santa Catarina no julgamento do recurso em sentido estrito e restabelecer integralmente a decisão do Juízo da 3ª Vara Criminal de Comarca de Florianópolis que julgou procedente a exceção de incompetência oposta pela paciente determinando a remessa dos autos à Comarca de Chapecó/SC **(BRASIL, 2021)**.

Neste 2º acórdão, vemos uma exceção à regra do artigo 70 do Código de Processo Penal Brasileiro, o crime fora concretizado no momento da veiculação do conteúdo, entretanto, como foi desconhecido o local de onde partiu tais publicações, desde a fase instrutória até o presente momento, não podia assim aplicar o dispostos no caput do artigo 70 e seus parágrafos, aplicando-se então a regra subsidiária do artigo 72 do Código Penal Brasileiro que diz: "Art. 72 - não sendo conhecido o lugar da infração, a competência regular-se-á pelo domicílio ou residência do réu" (BRASIL, 1940).

3.3 INVESTIGAÇÃO E PROVAS

No quesito de investigação e produção de provas para os crimes virtuais deve-se primeiramente averiguar quem poderá realizá-la, preliminarmente, analisa-se a Constituição Federal que em seu artigo 144, caput, e parágrafo 4º, disciplina que:

> Art. 144. A segurança pública, dever do Estado, direito e responsabilidade de todos, é exercida para a preservação da ordem pública e da incolumidade das pessoas e do patrimônio, através dos seguintes órgãos:
> § 4º Às polícias civis, dirigidas por delegados de polícia de carreira, incumbem, ressalvada a competência da União, as funções de polícia judiciária e a apuração de infrações penais, exceto as militares (BRASIL, 1940).

Ainda, sobre a competência possui jurisprudência consolidada na súmula 234 do Superior Tribunal de Justiça que diz: "Súmula 234 - A participação de membro do Ministério Público na fase investigatória criminal não acarreta o seu impedimento ou suspeição para o oferecimento da denúncia." (BRASIL, 1999)

Sendo assim, conclui-se que a competência e poder de investigação para os crimes virtuais é conferido ao Ministério Público e a Polícia Civil.

Sobre tal tema, Wendt e Jorge (2012, p. 52) afirma que:

> No tocante a investigação criminal nos casos de crimes virtuais, esta é de extrema complexidade e possui peculiaridades, como uma fase técnica inicialmente para que somente após seja realizada a investigação policial propriamente dita, ou seja, pode-se dizer que a investigação para estes casos é dividida em fase técnica e fase de campo.

Ainda sobre a investigação, Wendt e Jorge (2012, p. 52) concluem que um dos principais pontos de partida dessas investigações é a identificação e localização do dispositivo tecnológico que fora utilizado para a prática do ato: "na fase técnica da investigação de crimes virtuais são executadas e analisadas tarefas e informações com o objetivo de localizar o dispositivo tecnológico que foi utilizado para a ação criminosa".

Em validação, Cavalcante (2013) afirma que:

> Um dos principais fatores para a investigação é tomar conhecimento da prática e identificar qual meio foi utilizado para a prática do crime. De acordo com o meio, as técnicas para apuração das informações são diferentes, principalmente no que tange a localização do dispositivo.

Ainda sobre o processo de investigação Wendt e Jorge (2012, p. 52) listam diversas etapas a serem seguidas com o intuito de constatar os fatos:

> (...) é possível elencar uma série de tarefas a serem realizadas na fase técnica para apurar as informações como: análise do relato da vítima com o intuito de preservar o material comprobatório e compreensão dos fatos; orientação a vítima para preservação do material comprobatório; coleta inicial de provas no ambiente virtual; registro de um boletim de ocorrências formalizando o fato; investigação inicial referente aos dados do autor; formalização de relatório ou certidão das provas coletadas preliminarmente; representação perante ao Poder Judiciário para que se obtenha quebra de dados, conexão ou acesso e que se possa solicitar dados cadastrais para o provedores de conteúdo; e análise das informações prestadas pelos provedores de conteúdo.

Tais fatos só podem ser constatados e averiguados por meio da coleta de informações comumente chamadas de evidências digitais que Pinheiro (2013) conceitua como:

> (...) evidência digital é toda informação ou assunto de criação ou intervenção humana ou não, que pode ser extraído de um compilado ou depositário eletrônico. E essa evidência deve estar em um formato de entendimento humano

Isto é, as evidências digitais são as informações que se traduzem em arquivos digitais, dados rastreáveis, informações veiculadas e até mesmo fotos, e, portanto, possuem certo intricamento pois tais dados podem ser perdidos, alterados ou até mesmo apagados e além disso, comumente estão situados em locais que possuem uma infinidade de informações similares dificultando ainda mais a identificação para seguir com os procedimentos investigativos.

Para alcançar tais dados e/ou informações são necessários a identificação e rastreio dos Logs e do chamado IP.

Os logs para Cavalcante (2013):

> (...) são os registros gerados das ações do operador na internet e do caminho que as informações percorrem, não permitindo que haja um anonimato total na internet, pois cada página da internet acessada pelo usuário é registrada, sendo assim possível identificar o local onde houve o acesso e inúmeros outros dados.

O IP, segundo o site oficial do Kaspersky (2023) empresa especializada em proteção contra vírus e malwares conceitua IP como:

> Endereço IP é um endereço exclusivo que identifica um dispositivo na Internet ou em uma rede local. IP vem do inglês "Internet Protocol" (protocolo de rede) que consiste em um conjunto de regras que regem o formato de dados enviados pela Internet ou por uma rede local.
> Basicamente, o endereço IP é o identificador que permite que as informações sejam enviadas entre dispositivos em uma rede: ele contém as informações de localização e torna o dispositivo acessível para comunicação. A Internet precisa de um meio de distinguir diferentes computadores, roteadores e sites. O endereço IP providencia isso, além de ser uma parte essencial do funcionamento da Internet.

Ainda no que diz respeito às investigações de crimes virtuais, além dos IPs e LOGs há o chamado domínio, importante para as investigações acerca de e-mails eletrônicos, redes sociais e principalmente na investigação de sites.

Sobre tal afirmação Cavalcante (2013) afirma que:

> Quando se trata de investigação a sites envolvidos em crimes, as informações principais, principalmente o detentor do domínio, o IP e os LOGS de operações realizadas no site, podem ser fornecidas pelo órgão gestor dos registros de domínios de cada país.

O registro do domínio propicia uma facilidade no rastreio nos casos em que algum site possui informações consideradas ilícitas facilitando as investigações e identificação do detentor responsável por tais dados e/ou informações.

No Brasil o órgão responsável é Registro.br, o qual disponibiliza por meio do endereço www.registro.br uma ferramenta para consulta da pessoa detentora do endereço do site, também denominado como domínio. Para consulta de domínios de sites de fora do Brasil o órgão a ser consultado é o IANA (Internet Assigned Numbers Authority), por meio da ferramenta disponibilizada através do endereço www.iana.org/domains/root/db (CAVALCANTE, 2013).

Seguindo o mesmo raciocínio, nos crimes cometidos por e-mail a investigação não se conduzirá apenas ao conteúdo da mensagem fruto da investigação e denuncia, será investigado também o remetente, o domínio usado, data e o endereço IP. Todos esses dados

corroboram para identificação e rastreio do usuário que enviou a mensagem e a sua respectiva localização.

Já para os casos das redes sociais, Cavalcante (2013) discorre que:

> No caso das redes sociais, quando ocorrido fato criminoso no ambiente de alguma rede social, a investigação deverá solicitar, amparada por ordem judicial, a pessoa jurídica responsável por tal rede ou site para que forneça informações que possam levar ao autor, como logs de acesso, dados dos perfis de usuários e se necessário inclusive interceptação telemática do fluxo de dados.

Isto é, por meio de ordem judicial a pessoa jurídica responsável por tal rede social deverá colaborar com as informações necessárias que podem identificar o usuário desta rede que praticou os crimes possibilitando também sua identificação e localização.

Validando e complementando o supramencionado por Cavalcante, Wendt e Jorge (2012, p. 177) afirmam que:

> O Poder Judiciário pode ainda determinar ao administrador de rede de determinado local para que preste as informações técnicas específicas de forma que possam auxiliar na identificação do local do dispositivo tecnológico ou do autor. Isto ocorre principalmente em redes corporativas, as quais devem obter as informações referentes aos acessos.

Após prestadas tais informações pelo provedor ou responsável legal da rede social passa-se a etapa mais incisiva em que há mobilidade de força policial para cumprir as diligências necessárias à investigação.

> Identificado e localizado o dispositivo tecnológico que foi utilizado como meio para o crime, passa-se para a fase de campo na qual há o deslocamento de policiais e a realização das diligências com o objetivo de realizar o reconhecimento operacional de forma discreta, mas amparado pelo Poder Judiciário, principalmente no que toca ao mandado de busca e apreensão (WENDT; JORGE, 2012, p.53).

Findo esta análise procedimental conclui-se que as investigações somente serão executadas por autoridades competentes, com ajuda de agentes técnicos especializados em colaboração com os agentes responsáveis que detenham as informações ou estejam sob seu domínio para que assim materialize-se uma investigação de crime virtual eficiente, célere, objetiva e precisa.

4 DOS DADOS NO AMBIENTE VIRTUAL

Ao que se refere aos dados necessários às investigações acerca dos crimes virtuais, a lei 12965/2014 comumente chamada de Marco Civil da Internet em seu artigo 15º afirma que:

> Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento (BRASIL, 2014).

Em suma, os detentores de tais dados, deverão por força de lei armazená-los em ambiente seguro e controlado e caso haja necessidade disporem de tais dados para colaborarem com as investigações.

Ainda sobre os dados, a lei 13709 dispõe sobre a classificação destes que podem ser divididos em 4 categorias:

Dados Pessoais, aqueles em que permitem a identificação da pessoa natural que disponibilizou tal informação, são exemplos de dados pessoais: Nomes e sobrenomes, local de nascimento, Registro Geral e Cadastro de Pessoa Física, e-mail, endereço e dados de localização como GPS do celular e endereço IP.

Há também os chamados dados sensíveis que apesar de serem dados pessoais possuem certo cuidado e necessitam atenção maior pois podem pertencer a uma criança ou adolescente ou terem origem étnico-racial, religiosa, orientação política ou questões genéticas, biométricas ou até mesmo da saúde da pessoa que forneceu tal informação.

No tocante a dados de menores de idade há sempre a necessidade de consentimento de um dos pais ou responsável legal, entretanto, existe uma exceção para essa regra quando a coleta de dados é necessária para contatar os pais ou responsável legal do menor de idade em questão, nesses casos só é permitido o uso desses dados uma única vez e é vedado seu armazenamento.

Há também os chamados dados públicos, e seu tratamento deve ser considerado pela métrica da finalidade, do interesse público e da boa-fé. Com o advento da LGPD é possível o tratamento de dados que foram disponibilizados como dados públicos sem um novo consentimento. Entretanto, no caso dessa mesma organização considerar necessário compartilhar tais dados com outras organizações deverá, necessariamente, de um novo consentimento para a nova finalidade. É válido mencionar que a LGPD atua juntamente com a Lei de Acesso à informação e em consonância com os princípios constitucionais, como por exemplo o inciso XXXIII do artigo 5º da Constituição Federal que diz:

> XXXIII - todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo ou geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado (BRASIL, 1988).

Por fim, há os dados anonimizados que serão aqueles dados que passaram pela técnica de processamento de dados de anonimização, que consiste na remoção ou alteração de informações que possam de qualquer forma identificar o detentor daquele dado o que garantirá sua desvinculação. O dado somente será considerado anonimizado se por nenhum meio possa ser reconstruída a identificação do detentor daquele dado.

Ainda sobre os dados e a Lei Geral de Proteção de Dados é válido conceituar o que é tratamento de dados, porém, para tanto deve se considerar que o tratamento só poderá ser feito por dois agentes, chamados agentes de tratamento. Sobre tal fato o Tribunal de Justiça de São Paulo (2023) conceitua o controlador como:

> O controlador é definido pela Lei como a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais.
> Na Administração Pública, o controlador será a pessoa jurídica do órgão ou entidade pública sujeita à Lei, representada pela autoridade imbuída de adotar as decisões acerca do tratamento de tais dados.

Sendo assim, o controlador será pessoa natural ou jurídica, de direito público ou privado designado ao tratamento de dados pessoais.

Já o operador, o 2º e último agente de tratamento que foi precisado pelo Tribunal de Justiça de São Paulo (2023) como:

> O operador é a pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador, aí incluídos agentes públicos no sentido amplo que exerçam tal função, bem como pessoas jurídicas diversas daquela representada pelo controlador, que exerçam atividade de tratamento no âmbito de contrato ou instrumento congênere.

Em desfecho, o tratamento de dados significará qualquer atividade que se utiliza de um dado pessoal em determinada operação ou consumação de ato. O TJSP cita alguns exemplos como:

> (...) coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração. (Tribunal de Justica de Sao Paulo, 2023).

Por fim, conclui-se que os dados possuem categorias distintas em que seu tratamento deverá ser compatível com sua classificação específica realizada por seus agentes de tratamento. O devido tratamento destes dados por seus detentores possibilita um processo investigativo mais célere e eficiente.

CONSIDERAÇÕES FINAIS

Ao abordar tal tema era esperado uma exposição e compreensão sucinta porém efetiva dos crimes virtuais e como estes estão intimamente ligados às mudanças que ocorrem na sociedade. Foram analisados tanto os crimes próprios como impróprios no que diz respeito a sua tipificação, seu modus operandi que concretizam tais crimes, suas sanções e as aplicações das referidas leis além de apresentar os princípios e parâmetros que regem os procedimentos que regem um inquérito policial acerca dos crimes virtuais, podendo assim elucidar o leitor sobre novas mudanças e assegurar conhecimento sobre os crimes dentro do âmbito digital.

Para tanto foi apontado os principais crimes virtuais, tanto os próprios como impróprios, a sua tipificação legal, isto é, como estes se enquadram no cotidiano da sociedade brasileira que sofre mudanças constantemente devido às inovações tecnológicas e como se adequam as lacunas que o ordenamento jurídico brasileiro ainda possui sobre este tema devido ao fato de não poder nivelar a velocidade que tais mudanças ocorrem. Conclui-se que apesar de grandes avanços ocorreram no últimos 5 anos dentro do viés jurídico no que diz respeito às garantias constitucionais e a proteção dos direitos dentro do mundo digital a lei ainda se mostra defasada no que tange a proteção e o controle judicial no âmbito digital por mostrar-se pouco explorada, deixando lacunas e espaço para melhorias e avanços, como por exemplo adequação e elaboração de novas doutrinas acerca das mudanças e como implicam no Código Penal Brasileiro, recomenda-se neste ponto cursos de atualização tanto para o magistrado quanto para legisladores no que diz respeito às novas tecnologias, a internet e suas atualidades além de inovações tecnológicas que impactam as relações sociais de qualquer forma pois tais fatores influenciam também o âmbito jurídico e por meio desta espera-se que ao longo do tempo construa-se uma sólida e eficaz justiça de forma que se estabeleça segurança jurídica para a sociedade brasileira.

Tal análise só foi possível por meio de um estudo do referencial bibliográfico, a letra da lei, artigos de renomados operadores do Direito especializados no assunto e publicações em fóruns de debate acerca da ciência jurídica que norteia este tema. Os livros utilizados possibilitaram uma maior compreensão sobre a tipificação dos crimes e como está se

relaciona aos atos da vida de forma descomplicada, a interpretação dos autores e sua explanação acerca dos principais crime e os procedimentos necessários a adequação da lei ao caso concreto para que sejam preenchidas as lacunas no caso destas existirem se mostrou acessível e descomplicada e este sentimento que foi adquirido ao longo do desenvolvimento deste trabalho é o impacto esperado sobre o leitor, de tornar conhecimento técnico e complexo em informação relevante no cotidiano e acessível, de fácil compreensão.

A pesquisa jurisprudencial e o estudo da legislação possibilitaram o enquadramento e correspondência do que fora exposto pelos autores acerca do Código e suas interpretações perante os crimes virtuais com o que foi encontrado positivado em nosso ordenamento jurídico como por exemplo o Código Penal Brasileiro, a Lei Carolina Dieckmann e a Lei Geral de Proteção de Dados. Por fim os artigos científicos e publicações de fóruns disponibilizaram informações acerca dos dados a importância de seu correto tratamento segundo a Lei Geral de Proteção de dados e como este tratamento correto facilitariam a identificação, rastreio e persecução de contraventores assegurando uma maior celeridade e eficiência no Inquérito Policial.

A completude do referencial bibliográfico criara respaldo para fornecer conhecimento técnico de forma descomplicada e acessível ao leitor acerca dos crimes virtuais e seus procedimentos na aplicação da teoria ao caso concreto e as adaptações necessárias, sobre os dados e como as leis complementares os compreendem e os classificam além da necessidade do tratamento de forma complacente com a referida lei independentemente de quem esteja na posse de tais dados. É possível também embasar a afirmação de que o ordenamento jurídico brasileiro atual necessita acompanhar as mudanças que ocorrem na sociedade e implicam nas relações jurídicas veementemente. Conforme ocorrem estas mudanças sociais o Direito deve necessariamente avançar nivelando e almejando uma maior proteção e efetivo controle e consequentemente estabelecer segurança jurídica para aqueles que estão sob sua égide.

REFERÊNCIAS

BITTENCOURT, Thiago. **Saiba o que são spywares, vírus, e outros malwares; veja como se proteger**. TechTudo. 2013. Disponível em: https://www.techtudo.com.br/noticias/2013/06/entenda-o-que-sao-virus-spywares-trojans-worms-e-saiba-como-se-proteger.ghtml. Acesso em: 6 mai. 2023.

BRASIL. Acesso à Informação. 2021. Disponível em: https://www.gov.br/cidadania/pt-br/acesso-a-informacao/lgpd/classificacao-dos-dados. Acesso em: 6 mai. 2023.

BRASIL. Constituição Federal, de 04 de outubro de 1988. **Diário Oficial da União**, Brasília, 05 de outubro de 1988, ano 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 26 abr. 2023.

BRASIL. Código Penal. Lei n. 2.848, de 06 de dezembro de 1940. **Diário Oficial da União**, Rio de Janeiro, 31 de dezembro de 1940, ano 1940. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm. Acesso em: 7 abr. 2023.

BRASIL. Decreto, de 02 de outubro de 1941. Código de Processo Penal. **Diário Oficial da União**, 24 de outubro de 1941, ano 1941. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm. Acesso em: 2 mar. 2023.

BRASIL. Lei n. 12.965, de 22 de abril de 2014. **Diário Oficial da União**, Brasília, 25 de abril de 2014, ano 2014. Disponível em: https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm. Acesso em: 6 mai. 2023.

BRASIL. **Súmula nº 234**. Superior Tribunal de Justiça. 1999. Disponível em: https://www.stj.jus.br/docs_internet/revista/eletronica/stj-revista-sumulas-2011_17_capSumula234.pdf. Acesso em: 6 mai. 2023.

BRASIL. Superior Tribunal de Justiça. Quinta Turma. Habeas Corpus n. 591218 / SC (2020/0150284-6). Relator: Min. Joel Ilan Paciornik. Julgamento em 09 de fevereiro de 2021. Diário Judicial Eletrônico. Brasília, 12 de fevereiro de 2021. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?tipoPesquisa=tipoPesquisaNumeroRegistro&termo=202001502846&totalRegistrosPorPagina=40&aplicacao=processos.ea. Acesso em: 11 maio de 2023

BRASIL. Superior Tribunal de Justiça. Conflito de Competência n. 136.700 - SP (2014/0274368-9). Relator: Min. Rogerio Schietti Cruz. Julgamento em 23 de setembro de 2015. Diário Judicial Eletrônico. Brasília, 01 de outubro de 2015. Disponível em: https://processo.stj.jus.br/processo/pesquisa/?termo=2014%2F0274368-9&aplicacao=processos.ea&tipoPesquisa=tipoPesquisaGenerica&chkordem=DESC&chkMorto=MORTO. Acesso em 11 maio de 2023

CAPEZ, Fernando. **Curso de Direito Penal**: Parte Geral. 8 ed. São Paulo: Saraiva, v. 1, 2005.

CAVALCANTE, Waldek Fachinelli. **Crimes Cibernéticos**: noções básicas de investigação e ameaças na internet. 2013. Disponível em: https://jus.com.br/artigos/25743/crimes-ciberneticos. Acesso em: 6 mai. 2023.

CAVALCANTE, Waldek Fachinelli. **Provas Processuais Penais**: Interceptação telefônica e telemática na legislação brasileira e jurisprudência atual do Supremo Tribunal Federal. 2014. Disponível em: https://jus.com.br/artigos/30444/provas-processuais-penais. Acesso em: 6 mai. 2023.

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

FIORILLO, Celso Antonio Pacheco; CONTE, Christiany Pegorari. **Crimes no meio ambiente digital**: e a sociedade da informação. 2 ed. São Paulo: Saraiva, 2016.

GATTO, Victor Henrique Gouveia. **Tipicidade penal dos crimes cometidos na internet**. 2012. Disponível em: https://egov.ufsc.br/portal/conteudo/tipicidade-penal-dos-crimes-cometidos-na-internet. Acesso em: 6 mai. 2023.

ISHIDA, Válter Kenji. **Estatuto da criança e do adolescente**: doutrina e jurisprudência. 10 ed. São Paulo: Atlas, 2009.

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

JESUS, Damasio E. **Direito Penal**. 29 ed. São Paulo: Saraiva, 2008.

KASPERSKY. **O que é endereço IP**: definição e explicação. 2023. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address. Acesso em: 6 mai. 2023.

NICOLITT, André. **Manual de Processo Penal**. Rio de Janeiro: Elsevier, 2009.

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

ORRIGO, Gabriel Marcos Archanjo; FILGUEIRA, Matheus Henrique Balego. **Crimes Cibernéticos**: uma Abordagem Jurídica sobre os Crimes Realizados no Âmbito Virtual. Encontro de Inicação Científica. 2016. Disponível em: https://egov.ufsc.br/portal/conteudo/crimes-cibern%C3%A9ticos-uma-abordagem-jur%C3%ADdica-sobre-os-crimes-realizados-no-%C3%A2mbito-virtual. Acesso em: 6 mai. 2023.

TRIBUNAL DE JUSTIÇA DE SÃO PAULO. **Lei Geral de Proteção de Dados**. 2023. Disponível em: https://www.tjsp.jus.br/LGPD/LGPD/ALGPD. Acesso em: 6 mai. 2023.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos**: Ameaças e Procedimentos de Investigação. Rio de Janeiro: Brasport, 2012.

Universidade Presbiteriana Mackenzie | Faculdade de Direito

TERMO DE AUTENTICIDADE DO TRABALHO DE CONCLUSÃO DE CURSO

Eu, GIOVANNI PERCIDO FERRI

discente regularmente matriculado(a) na disciplina TCC II, da 10ª etapa do curso de Direito, matrícula nº (inserir TIA), período (inserir período), turma (inserir turma), tendo realizado o TCC com o título: CRIMES VIRTUAIS 41728576, MATUTINO, 10A

sob a orientação do(a) Professor(a) CARLOS EDUARDO NICOLETTI CAMILLO

declaro para os devidos fins que tenho pleno conhecimento das regras metodológicas para confecção do Trabalho de Conclusão de Curso (TCC), informando que o realizei sem plágio de obras literárias ou a utilização de qualquer meio irregular.

Declaro ainda que, estou ciente que caso sejam detectadas irregularidades referentes às citações das fontes e/ou desrespeito às normas técnicas próprias relativas aos direitos autorais de obras utilizadas na confecção do trabalho, serão aplicáveis as sanções legais de natureza civil, penal e administrativa, além da reprovação automática, impedindo a conclusão do curso.

São Paulo, 11 de 05 de 2023

Assinatura do discente