CENTRO UNIVERSITÁRIO FADERGS
CURSO DE DIREITO

EDUARDO SALEH RABELLO MOREIRA

OS CRIMES DE INFORMÁTICA E A APLICAÇÃO DA LEI BRASILEIRA

PORTO ALEGRE
Dezembro de 2023

FADERGS
CENTRO UNIVERSITÁRIO

CENTRO UNIVERSITÁRIO FADERGS
CURSO DE DIREITO

EDUARDO SALEH RABELLO MOREIRA

OS CRIMES DE INFORMÁTICA E A APLICAÇÃO DA LEI BRASILEIRA

Artigo científico de pesquisa apresentado para a avaliação da disciplina de Trabalho de Curso, com posterior apresentação à Banca Examinadora, requisitos para a obtenção do diploma de Bacharel em Direito.

Orientadora: Profa. CRISTINA DI GESU

PORTO ALEGRE
Dezembro de 2023

FADERGS
CENTRO UNIVERSITÁRIO

Bacharelado em Direito

Trabalho de Curso

ATA DE APROVAÇÃO EM BANCA EXAMINADORA

O aluno **EDUARDO SALEH RABELLO MOREIRA** defendeu o artigo científico intitulado: **OS CRIMES DE INFORMÁTICA E A APLICAÇÃO DA LEI BRASILEIRA,** apresentado e aprovado pela Banca Examinadora, ao qual foi atribuído o grau final 10.

Porto Alegre, 14 de dezembro de 2023.

Os Crimes de Informática e a Aplicação da Lei Brasileira

Computer crimes and the application of Brazilian Law

Resumo

O surgimento dos crimes de informática trouxe mudanças para o direito e dificuldade de aplicação da legislação brasileira as suas espécies. O aumento da criminalidade utilizando a *internet*, em busca de dados privados que se encontram na rede, que antes eram guardados fisicamente em nossas casas despertou o interesse dos criminosos. Conceitos de crimes de informática, suas espécies e seus tipos. Crimes cometidos no ciberespaço, como a pornografia infantil, a divulgação de conteúdo pornográfico sem consentimento e extorsão proveniente do mesmo, estelionato e o recente crime de perseguição (*stalking*) como exemplos de crimes de informática. Leis que alteraram o Código Penal e a Convenção sobre o Crime Cibernético, recentemente incorporada ao arcabouço legislativo pátrio, com a sua respectiva promulgação. Competência dos crimes de informática e jurisprudências de nossos Tribunais Superiores, em relação aos diversos conflitos de competência instaurados diariamente acerca dos crimes de informática. A transnacionalidade da informação, importante requisito para se definir a competência de um crime de informática. A legislação brasileira sobre os crimes de informática e dispositivos que influenciam a sua aplicação. Dificuldades de aplicação da Lei Brasileira às diversas espécies de crimes de informática.

Palavras – chave: Direito Digital. Crimes de Informática. Internet. Crime cibernético.

Abstract

The emergence of computer crimes has brought changes to the law and difficulty in applying Brazilian legislation to its species. The increase in crime using the internet, in search of private data that is on the network, which was previously physically stored in our homes, has aroused the interest of criminals. Concepts of computer crimes, their species and types. Crimes committed in cyberspace, such as child pornography, the dissemination of pornographic content without consent and extortion from it, embezzlement and the recent crime of stalking as examples of computer crimes. Laws that amended the Penal Code and the

Convention on Cybercrime, recently incorporated into the national legislative framework, with their respective enactment. Competence of computer crimes and jurisprudence of our Superior Courts, in relation to the various conflicts of jurisdiction established daily regarding computer crimes. The transnationality of information, an important requirement for defining the competence of a computer crime. The Brazilian legislation on computer crimes and devices that influence their application. Difficulties in the application of the Brazilian Law to the various types of computer crimes.

Keywords: Digital Law. Computer Crimes. Internet. Cybercrime.

1.Introdução

O presente artigo abordará questões acerca do surgimento dos crimes de informática, suas consequentes mudanças trazidas para o direito e a dificuldade de aplicação da legislação brasileira as suas espécies.

No segundo capítulo, serão realizadas considerações sobre o surgimento da *internet* e as suas consequências para o Direito. Serão sublinhados, ainda nesse capítulo, o aumento da criminalidade através da *internet,* - onde será feito um breve histórico sobre a origem dos crimes de informática, a sua definição geral e aspectos relacionados a quantidade de pessoas que utilizam a rede mundial de computadores. Além disto, serão citados quais os dados privados que se encontram na rede, que antes eram guardados fisicamente em nossas casas.

No terceiro capítulo, será assinalado que o surgimento dos crimes de informática modificou os conceitos de território e local do crime, abordando o ciberespaço.

Ao adentramos ao quarto capítulo, serão citados conceitos de crimes de informática, suas espécies, seus tipos e serão analisados alguns dos principais crimes cometidos no ciberespaço, como a pornografia infantil, a divulgação de conteúdo pornográfico sem consentimento e extorsão proveniente do mesmo, estelionato e o recente crime de perseguição (*stalking*).

Serão abordadas Leis que alteraram o Código Penal e citada a Convenção sobre o Crime Cibernético, recentemente incorporada ao arcabouço legislativo pátrio, com a sua respectiva promulgação.

Ainda nesse capítulo, serão realizadas considerações sobre a competência dos crimes de informática, onde serão trazidas algumas jurisprudências de nossos Tribunais Superiores, mostrando como eles tem se posicionado em relação aos diversos conflitos de competência instaurados diariamente acerca dos crimes de informática.

Será mostrada a questão da transnacionalidade da informação, importante requisito para se definir a competência de um crime de informática.

No quinto capítulo, será trazida à baila a legislação brasileira sobre os crimes de informática, assim como citados alguns dispositivos que influenciam a sua aplicação. Poderá haver dificuldades de aplicação da Lei Brasileira às diversas espécies de crimes de informática.

Por fim, no capítulo 6, serão feitas as Considerações Finais sobre o trabalho ora apresentado.

Após esta breve introdução, passo a abordar o surgimento da *internet* e o incremento da criminalidade utilizando a rede mundial de computadores.

2. O surgimento da *internet* e o incremento da criminalidade utilizando a rede mundial de computadores

Inicialmente, neste primeiro capítulo, convém abordar aspectos relacionados ao surgimento da *internet,* antes de efetivamente adentrarmos às questões relativas ao aumento da criminalidade no âmbito da rede mundial de computadores.

2.1 O surgimento da *internet*

Notório é o fato de que a vida dos cidadãos dos diversos países do mundo tem sido afetadas pelo surgimento da *internet*. Esta se tornou um meio indispensável ao desenvolvimento da atividade humana, nas mais diversas áreas do conhecimento.

Segundo CONTE (2008):

> O surgimento de novas tecnologias, notadamente da informática, como consequência de um ainda contemporâneo processo de globalização, acarretou mudanças consideráveis na sociedade, tanto que poderíamos comparar o impacto causado pelo surgimento da *Internet* ao sofrido com o considerado "avanço técnico" promovido durante a Revolução Industrial no século XVIII.

Desta forma, com este estrondoso surgimento, o Direito não ficou incólume, uma vez que passou a ter de enfrentar questões jurídicas advindas desta nova realidade.

Surge, então, um novo Direito: o Direito da *Internet* e da Sociedade da Informação (CONTE, 2008). A esta nova área jurídica foi atribuída a nobre missão de compor os diversos conflitos causados pelo incontrolável uso da rede mundial de computadores.

Por outro lado, embora a evolução tecnológica tenha trazido benefícios indiscutíveis para o desenvolvimento humano, ela proporcionou que se iniciasse a prática de atos ilícitos, cometidos neste novo ambiente. Conduta, esta, que passou a ser denominada como cibercrime. (JÚNIOR, 2019).

Após estas considerações acerca do surgimento da rede mundial de computadores, passo a sublinhar o aumento da criminalidade ao se utilizar a *internet.*

2.2 . Aumento da criminalidade utilizando a *internet*

Os crimes de informática tiveram sua origem há poucas décadas atrás. O mundo foi pego de surpresa ao criar a rede mundial de computadores, o que trouxe à humanidade um avalanche de possibilidades de desenvolvimento nas mais diversas áreas do conhecimento humano. Porém, com isto, abriu-se a possibilidade de cometimento de delitos cibernéticos através da rede mundial de computadores.

Segundo JESUS (2016):

> A doutrina diverge acerca do primeiro delito informático cometido. Para alguns, o primeiro delito informático teria ocorrido no âmbito do MIT (*Massachusetts Institute of Technology*), no ano de 1964, onde um aluno de 18 anos teria cometido um ato classificado com cibercrime, tendo sido advertido pelos superiores. Outros ainda referenciam o primeiro caso de que se tem notícia sobre *hacking* no ano de 1978, na Universidade de Oxford, onde um estudante copiou de uma rede de computadores uma prova. Uma invasão seguida de uma cópia. Até essa data não existia lei sobre crimes informáticos nos Estados Unidos. A Flórida, no mesmo ano, foi o primeiro Estado americano a formular leis sobre informática.

O surgimento desses crimes causou diversas mudanças para o Direito, surgindo o Direito Digital.

Importante frizar que não há uma padronização sobre a nomenclatura do tipo penal relacionado à tecnologia, mais precisamente com o uso da *internet*. Segundo Antônio Chaves, cibernética é a "ciência geral dos sistemas informantes e, em particular, dos sistemas de informação" (CHAVES, Antônio apud SILVA, Rita de Cássia Lopes).

Através do conceito analítico finalista de crime, pode-se chegar à conclusão de que os crimes cibernéticos são todas as condutas típicas, antijurídicas e culpáveis praticadas contra ou com a utilização dos sistemas da informática (TORMEN, 2018).

Ou ainda, conforme disciplina ROSSINI (2004):

> O conceito de delito informático poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele, e que ofenda, direta ou indiretamente, a segurança informática, que tem por elementos a integridade, a disponibilidade e a confidencialidade.

Possuindo diversos conceitos e tendo como base o número de pessoas que utilizam a rede mundial de computadores, os crimes de informática aumentaram a sua quantidade. Dentre algumas razões para este aumento, pode-se destacar o fato de que a fronteira física dos Estados não se constitui em uma barreira física para conter a prática de delitos desta natureza.

Ademais, a *internet* conecta pessoas de diferentes partes do globo terrestre em questões de segundos, transpassando a fronteira de países, constituindo-se, deste modo, em crimes de difícil investigação.

A criminalidade informática oferta características semelhantes às da informatização global. Possui as seguintes características: a transnacionalidade, uma vez que a maioria dos países fazem uso da internet, não importando seu estágio econômico, cultural ou social; a universalidade, pois as pessoas tem acesso aos produtos informatizados; e por fim, a ubiquidade, devido ao fato de a informatização estar presente em todos os setores públicos e privados do planeta (COSTA, 2004).

Essas peculiaridades fazem com que estes crimes se tornem mais comuns e cada vez mais numerosos, funcionando a rede como uma verdadeira cortina de fumaça para os criminosos agirem.

Nesse sentido, muitos cibercriminosos permanecem impunes, tornando a *internet* um faroeste digital onde a vontade dos criminosos prevalece sobre os direitos e opiniões alheias, frente à facilidade de acesso a *internet* livremente, com a intenção de causar danos pessoais ou patrimoniais (VIEIRA,2023).

Nesse contexto, afirma VIEIRA (2023):

> Sob essa óptica, os crimes cibernéticos têm um impacto econômico significativo, com perdas estimadas em trilhões de dólares anualmente. Eles afetam empresas de todos os setores e governos. Além disso, o uso crescente de criptomoedas, como o *Bitcoin,* tem facilitado a realização de transações financeiras ilegais na *internet.* Essas moedas digitais são usadas por criminosos para realizar atividades ilegais, como lavagem de dinheiro, compra e venda de drogas e armas e financiamento do terrorismo.

Ademais, assevera COURI (2009) que o maior estímulo aos crimes virtuais é dado pela crença de que o meio digital é um ambiente à margem do mundo real. Essa postura existe porque a sociedade não crê na vigilância e na adequada punição aos ilícitos praticados no mundo virtual.

Ainda segundo COSTA (2004), aspecto relevante para o criminólogo é o perfil dos sujeitos no crime cibernético, pois ele, seja de direito público ou privado, via de regra é pessoa jurídica de grande poder econômico, que não comunica o ato de que foi vítima, alimentando, assim, o sistema de impunidade e o crescimento do comportamento ilícito.

O sujeito ativo do crime pode ser, também, pessoas que detém conhecimentos avançados em computação, geralmente novos, e seu perfil acusa pouco temor em relação à norma, indiferença à sanção penal, motivado por dinheiro, autopromoção ou vingança (COURI, 2009).

O aumento de crimes cometidos por essas pessoas, assim, é preocupação de todos os países que utilizam a rede mundial de computadores. Mas como, no Brasil e no mundo, se precaver destes crimes, ou ao menos tentar frear este aumento?

Inicialmente, é preciso, segundo CRESPO (2011):

> É preciso, ademais, convidar instituições educativas, indústrias fabricantes de hardware e de software para incorporar planos de estudo e cursos sobre aspectos legais e éticos da informática, objetivando prevenir abusos informáticos e criar normas comportamentais relacionando a ética e as novas tecnologias. Isso, como dito, com vistas a diminuir a exclusão digital. É preciso, ainda, fomentar mecanismos para educar vítimas potenciais, evitando que pessoas mais simples, com menos conhecimentos técnicos, venham a ser vitimadas de forma frequente. A promoção da cooperação da vítima, com ela obtendo dados sobre o ocorrido, é, portanto, outra ação salutar.

Para que menos pessoas humildes, sem conhecimento técnico, sejam alvo de crimes de informática, necessário se torna que o Estado realize investimentos na área da educação, trazendo computadores para o ensino público, além de professores capazes de ensinar àqueles hipossuficientes a utilização segura da *internet.*

Ao se trazer estas pessoas para o mundo digital, diminuirá, assim, a exclusão digital.

Segundo LOURENÇO (2023):

> No primeiro semestre de 2021, em uma pesquisa divulgada pelo CUPONATION foi apontado que “existem cerca de 4,66 bilhões de usuários ativos na internet em todo o mundo, o que equivale a 59,5% da população mundial” (CUPONATION, 2021), o que quer dizer que mais da metade da população mundial tem acesso ao universo virtual, o fácil acesso a este meio permite cada vez mais consulta a informações, comunicação, atividades que não precisam de se locomover para que sejam realizadas como compras, serviços bancários, e trabalho remoto com grande satisfação, tornando o mundo virtual um ambiente cada vez mais propício à prática de crimes cibernéticos.

Por outro lado, há a necessidade de se fomentar uma cooperação internacional entre as polícias dos Estados e demais órgãos de fiscalização e controle de sistemas de dados, se conduzidos com agilidade e eficiência, agregariam um salutar intercâmbio, para a investigação dos crimes de informática, mormente se caracterizada a sua transnacionalidade (COURI,2009).

E, nesse período, o mundo conheceu a pandemia do coronavírus, período no qual as pessoas em todo o mundo foram confinadas em suas casas, não podendo sair para realizar compras e outras atividades de seu cotidiano.

As pessoas passaram a utilizar a *internet* para realizar compras, transferências bancárias e inúmeros serviços, aumentando o número de crimes cibernéticos, uma vez que os criminosos tiveram de buscar o que não estava mais nas ruas, mas dentro da rede mundial de computadores.

É o que sublinha MOURA (2021), ao afirmar que os computadores pessoais, *tablets, smartwatch, smartphones* e outros objetos armazenam dados mais privados do que aqueles que estão em nossa própria residência, uma vez que o que era materializado, agora, tornou-se virtualizado.

Dados estes que são bem sublinhados por ARAS (2015):

> A atuação do Direito Penal será imprescindível em alguns casos, por conta da natureza dos bens jurídicos em jogo. Pois, pela web e no ciberespaço circulam valores, informações sensíveis, dados confidenciais, elementos que são objeto de delitos ou que propiciam a prática de crimes de variadas espécies. Nas vias telemáticas, transitam nomes próprios, endereços e números de telefone, números de cartões de crédito, números de cédulas de identidade, informações bancárias, placas de veículos, fotografias, arquivos de voz, preferências sexuais e gostos pessoais, opiniões e ideias sensíveis, dados escolares, registros médicos e informes policiais, dados sobre o local de trabalho, os nomes dos amigos e familiares, o número do IP — *Internet Protocol*, o nome do provedor de acesso, a versão do navegador de *Internet (browser),* o tipo e versão do sistema operacional instalado no computador.

Pelo acima exposto, conclui-se que os crimes de informática são delitos novos, a partir dos quais surgiu o Direito Digital.

Ademais, não há padronização sobre a nomenclatura do tipo penal, cuja quantidade vem aumentando.

Para a prática dos mais variados crimes de informática, os criminosos utilizam a rede como uma cortina de fumaça, o que dificulta a sua detecção.

A pandemia do corona vírus alavancou a utilização de serviços *on line*, o que despertou ainda mais o interesse dos criminosos nesse novo espaço.

E, por fim, sublinha-se, principalmente, que os dispositivos eletrônicos hoje em dia armazenam mais dados privados e importantes do que temos fisicamente em nossas residências.

Passo a abordar, em seguida, o novo conceito de território e o local do crime, no que tange aos crimes cibernéticos.

3. Novo conceito de território e o local do crime de informática

Neste capítulo, necessário se torna sublinhar aspectos relacionados ao novo conceito de território, assim como o "novo" local do crime, para os crimes de informática.

3.1 Readequação do conceito de território

Conforme já citado anteriormente, a definição tradicional de território parece não ter lugar quando se trata de crimes de informática.

Segundo CONTE (2008):

> O ciberespaço permite escapar às limitações da vida real. O conceito de território está intimamente relacionado à uma ideia nova, qual seja: a de rede. A rede, como território, se caracteriza pela localização da informação. A informação na rede, portanto, passa a ser elemento identificador do território no ciberespaço. Assim, essas características fazem com que a *Internet* tenha uma maior dificuldade em estabelecer um "centro de comando" tal como na versão tradicional de território físico delimitado.

O ciberespaço nos mostra que é possível uma pessoa estar em um país A, cometer um crime no país B, utilizando um provedor de um país C e trazer consequências para um país D.

Nesse diapasão, VALIN (2000) nos ensina que:

> O grande problema ao se trabalhar com o conceito de jurisdição e territorialidade na *Internet* reside no caráter internacional da rede. Na *Internet* não existem fronteiras e, portanto, algo que nela esteja publicado estará em todo o mundo. Como, então, determinar o juízo competente para analisar um caso referente a um crime ocorrido na rede?

"O ciberespaço não dispõe de fronteiras territoriais, mas de normas ou técnicas, que regulam sistemas de acesso e que não pertencem ao mundo jurídico. Assim, não vigora o conceito de soberania e nem de competência territorial" (MOLES apud CONTE,2008).

Segundo PINHEIRO (2021), *in verbis*:

> No mundo tradicional, a questão da demarcação do território sempre foi definida por dois aspectos: os recursos físicos que esse território contém e o raio de abrangência de determinada cultura. A sociedade digital rompe essas duas barreiras: o mundo virtual constrói um novo território, dificilmente demarcável, no qual a própria riqueza assume um caráter diferente, baseada na informação, que, como vimos, é inesgotável e pode ser duplicada infinitamente.

O ciberespaço é, por conseguinte, um "país" sem fronteiras, tornando-se um conceito diferente de um território físico.

Portanto, cristalino é o fato de que o conceito de território tradicional não pode ser aplicado aos crimes cibernéticos, por ter de sofrer uma readequação em seu significado, quando se trata de delitos informáticos.

Passo, a seguir, a abordar o que seria, então, o novo local do crime.

3.2 O novo local do crime

Com o surgimento do ciberespaço, vale trazer a reflexão do que o Código Penal versa, em seu art. 6°, no que tange ao local do crime:

> Art. 6º: 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.

Como aplicar a lei penal brasileira, então, quando observamos o que leciona MONTEIRO (2017):

> Ciberespaço é definido como um mundo virtual porque está em presente potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, outra realidade. O ciberespaço existe em um local indefinido, desconhecido, cheio de devires e possibilidades.
>
> Não podemos, sequer, afirmar que o ciberespaço esta presente em nossos computadores, tampouco nas redes, afinal onde fica o ciberespaço? Para onde vai todo esse "mundo" quando desligamos nossos computadores? É esse caráter fluido do ciberespaço que o torna virtual.

Por conseguinte, há um saliente desafio à aplicação da lei penal brasileira, quando os crimes de informática tem o Brasil como o local de início, de meio ou de destino (resultado) dos crimes praticados.

Deste modo, faz parte de nossa vida diária esse novo local do crime, virtual e indefinido, que atravessa fronteiras de países em segundos, e que nos impõe a necessidade de cooperarmos internacionalmente para a criação de normas que possam tratar estes crimes adequadamente, evitando que eles não sejam julgados, ou ainda, que haja uma duplicidade de julgamentos.

Portanto, sublinha-se aqui a modificação do que se entende por local do crime quando se fala em delitos informáticos.

A seguir, passo a descrever as espécies de crimes de informática e a tecer algumas considerações sobre a sua competência.

4 As espécies de crimes de informática e considerações sobre competência

Neste capítulo, abordarei especies de crimes de informática, segundo alguns autores, e destacarei aspectos sobre a competência para processar e julgar os crimes cibernéticos.

4.1 Espécies de crimes de informática

Antes de adentrarmos nas espécies de crimes de informática, é necessário definir o que são, então, crimes de informática.

Segundo ARAS (2015), não há consenso para definir o nome jurídico do crime de informática, que pode ser delito computacional, crime de informática, crime de computador,

crime eletrônico, crime telemático, crime informacional, ciberdelito, cibercrimes, crimes cibernéticos, entre outros.

Sendo assim, poderei utilizar qualquer destas denominações quando me referir a estes delitos.

Segundo TAVARES (2014):

> Crime de informática é aquele praticado com auxilio do sistema de informática ou contra, podendo ser compreendido aqueles crimes praticados contra o computador e também seus acessórios e os perpetrados através do computador. Sendo assim podendo incluir neste contexto os crimes praticados através da *Internet*, pois a ferramenta para acessar a rede é o computador.

Os crimes de informática podem ser divididos em duas espécies. A primeira espécie consiste em uma nova maneira de se cometer delitos já existentes (antigos), nos quais o computador e a *Internet* são utilizados como simplesmente ferramentas para a prática do delito. A outra modalidade reúne condutas inéditas, ou seja, aquelas que nasceram com a era digital. No primeiro grupo, deve-se aplicar a lei vigente, haja vista que a *Internet* é utilizada como uma forma para cometer delitos antigos, ou já preexistentes ao surgimento da *Internet*, ex: ameaça via e-mail. Já quanto aos novos crimes, o a questão de como se deve punir se instala, tendo em vista que a legislação penal vigente no Código Penal data de 1940 (CASTRO, 2007).

Segundo COSTA (2004), pode-se classificar os crimes de informática em puros e impuros, próprios ou impróprios. O autor afirma que os verdadeiros crimes cibernéticos são os puros ou próprios, pois os impuros ou impróprios são os crimes comuns, só que praticados pelo computador.

Um exemplo de crime impuro é a conduta típica prevista no diploma legal penal, mais precisamente no Art. 139, que prevê: “ Difamar alguém, imputando-lhe fato ofensivo à reputação - Detenção, três meses a 1 (um) ano e multa”.

Percebe-se que neste tipo de crime é facilmente aplicável a lei penal, sendo o ordenamento penal vigente a legislação apta a realizar tal enquadramento.

Diferente, porém, da outra espécie de crime, na qual não há previsão legal da conduta, causando, deste modo, uma grande dificuldade de aplicação de uma lei penal adequada.

Como exemplo desses crimes virtuais puros (segunda espécie de crimes de informática), pode-se citar as condutas delituosas que atingem bancos de dados, sites, e que espalham vírus causadores de danos às redes de computadores.

Há ainda autores que seguem a classificação dos crimes digitais de maneira diversa, como por exemplo o fato de classificá-los em crimes digitais próprios e impróprios.

Segundo CRESPO (2011), esta divisão parece ser a melhor das classificações, uma vez que é mais ampla e permite que se discorra acerca de suas práticas. Leciona o autor que os crimes digitais próprios são aqueles nos quais o bem jurídico atingido são primordialmente os sistemas informatizados, de telecomunicações ou dados.

Ainda segundo CRESPO (2011), os crimes digitais impróprios são aqueles já tipificados no ordenamento, mas praticados com auxílio de modernas tecnologias. Isso leva-o afirmar que são os mesmos crimes, mas cometidos agora com um novo modo de execução.

Segundo DOS SANTOS (2023), estes delitos são os praticados com maior frequência na *internet.*

Após estas considerações doutrinárias acerca das espécies de crimes de informática, passo a ilustrar alguns exemplos de crimes cibernéticos.

4.2. Exemplos de crimes de informática

Após esta breve abordagem sobre as espécies de crimes de informática, passo a abordar, dentre os mais variados crimes existentes, alguns dos principais delitos informáticos, como a pornografia infantil, a divulgação de conteúdo pornográfico sem consentimento e extorsão proveniente do mesmo, estelionato e o recente crime de perseguição (*stalking*).

Segundo FUCHS (2021), o crime de pornografia infantil existe há muitas décadas, sendo que anteriormente eram gravadas em fitas, fotografias, DVD e em computadores sem conexão com a rede mundial de computadores. Porém, hoje, circula pelo ciberespaço em sites adultos, disfarçados ou habilitados apenas para quem fizer uma assinatura e pagar pelo conteúdo.

Nesse diapasão, o Estatuto da Criança e do Adolescente (Lei n°8.069 de 13 de julho de 1990) prevê do art.241-A ao art. 241-C, em parágrafos e incisos, o seguinte:

> Art. 241-A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008) Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa. (Incluído pela Lei nº 11.829, de 2008).
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia,
> vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente: (Incluído pela Lei nº 11.829, de 2008) Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Incluído pela Lei nº 11.829, de 2008).
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual: (Incluído pela Lei nº 11.829, de 2008).

Mesmo sem abordar os parágrafos e incisos respectivos dos três artigos acima, pode-se comprovar que a lei prevê sanções penais aos tipos penais destacados.

No que tange à divulgação de conteúdo pornográfico sem consentimento e extorsão proveniente do mesmo, FUCHS (2021), aborda ser muito comum as pessoas serem vítimas desse tipo penal, sendo que esta conduta é apelidada nas redes sociais de o "golpe do *nudes*". A pessoa se passa, na maioria das vezes, por uma menina menor de idade, se envolvendo com homens de 25 a 50 anos. Após isso, FUCHS assevera que fotos são enviadas retiradas da rede, e em um pequeno espaço de tempo, a vítima era chamada por outro perfil, na qual o criminoso agora se passa pelo pai ou mãe da menina, alegando que caso não seja realizado um depósito em dinheiro, a vítima seria denunciada à polícia por ter cometido pedofilia.

Por fim, o estelionato, um crime anteriormente praticado pelo telefone, hoje é amplamente praticado nas redes sociais como *whatsapp* e *facebook*, por ser de fácil acesso e gratuito (FUCHS, 2021).

Como exemplo desta conduta, pode-se citar o uso de cartões de crédito na *internet*. Segundo RAMOS (2007):

> A informação que se tem é que qualquer pessoa responsável por um provedor de acesso tem condições de utilizar as informações dos cartões, podendo utilizá-las ilicitamente. O problema reside no fato de que não só o responsável pelo provedor tem acesso, mas qualquer pessoa munida de ferramentas adequadas pode interceptar as informações digitadas no site. Ressalta-se que as empresas de cartão de crédito tem trabalhado bastante para o desenvolvimento de uma melhor tecnologia para segurança nas transações, afinal o comércio eletrônico só tende a crescer cada dia que se passa.

Em 2021, a Lei 14.132 de 31 de março acrescentou no Código Penal o Art. 147-A a previsão do crime de perseguição, tendo revogado o Art.65 da Lei n° 3.688, de 3 de outubro de 1941 (Lei das Contravenções Penais), a saber:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. § 1º A pena é aumentada de metade se o crime é cometido:I – contra criança, adolescente ou idoso; II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código; III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma. § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência. § 3º Somente se procede mediante representação.

O Art.65 que foi revogado pela Lei 14.132 de 31 de março de 2021, abordava a perturbação da tranquilidade e previa:

> Molestar alguém ou perturbar lhe a tranquilidade, por acinte ou por motivo reprovável: Pena - prisão simples, de quinze dias a dois meses, ou multa, de duzentos mil réis a dois contos de réis.

> (https://www.migalhas.com.br/depeso/343235/breve-analise-do-artigo-147-a-do-codigo-penal).

Vários já são os julgados de nosso Egrégio Superior Tribunal de Justiça acerca do crime de perseguição digital; como exemplo, cita-se o HC n° 839293 - MG (2023/0250587-2), cuja Relatora foi a Ministra MARIA THEREZA DE ASSIS MOURA, publicado em 24/07/2023.

No caso em tela, houve pedido de liminar impetrado em favor de L.X.T., sendo a autoridade coator o Tribunal de Justiça do Estado de Minas Gerais.

O paciente, no caso, se encontrava preso preventivamente desde 3/5/2023 pela suposta prática dos delitos previstos nos artigos 147-A e 147, ambos do Código Penal, e 24-A, da Lei n° 11.340/06 (por descumprir decisão judicial que deferiu medidas protetivas de urgência) por três vezes, e artigo 12 da Lei n. 10.826/03 (posse irregular de arma de fogo de uso permitido).

Na decisão, a Ministra Relatora indeferiu a liminar, por sustentar que a prisão preventiva do paciente encontrou arrimo nas circunstâncias dos delitos, que não se limitaram ao crime de descumprimento de medidas protetivas, mas também envolveram o crime de ameaça e de *stalking* **(**perseguição**),** diante das inúmeras ameaças via *whatsapp* proferidas pelo paciente, inclusive de morte, não apenas contra a suposta vítima, mas contra seus familiares, além de destacar sua extensa ficha criminal, com anotações por delitos da mesma natureza.

Sublinha-se aqui a utilização da ferramenta digital (*whatsapp*) para o cometimento de delitos de ameaça e perseguição contra a suposta vítima.

Ainda nesse ano, a Lei 14.155 de 27 de maio também alterou o Código Penal, no sentido de tornar mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica ou pela *internet.* Alterou também o Código de Processo Penal para definir a competência em modalidades de estelionato.

Após isso, em 2023, o Decreto n° 11.491 de 12 de abril promulgou a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

Portanto, diversos são os crimes cometidos no ciberespaço. A seguir, adentrarei nas considerações sobre competência dos crimes de informática, questão muito importante deste trabalho.

4.3 Considerações sobre competência

Atualmente, o maior desafio para os aplicadores do Direito no trato dos crimes de informáticas é, indubitavelmente, a questão da competência para julgar delitos desta natureza.

Segundo CONTE (2008), ao se cometer um crime que atinja a honra de alguém, utilizando-se da *internet* como um meio, verifica-se que a ofensa à honra desta pessoa pode ser conhecida através de vários países, ficando clara a problemática que envolve a análise de qual foro competente deverá julgar a conduta em epígrafe.

Deverá ser levado em consideração o local de onde partiu a ofensa ou a localização do provedor por meio do qual se veiculou a mesma?

Para se responder a essa pergunta, faremos uso do que prevê o artigo 70, *caput*, do Código de Processo Penal, a saber:

> Art. 70: 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.

SANTOMAURO (2010) explica que essa questão é ainda mais preocupante quando envolve jovens de idades entre 15 e 29 anos, pois durante a adolescência os efeitos provocados por esse tipo de violência se intensificam. O *cyberbullying* (termo em inglês para "assédio *online*") tem repercussões ainda maiores que o praticado nas escolas, pois dura vinte e quatro horas por dia e é capaz de alcançar o jovem onde ele estiver.

Ainda segundo CONTE (2008), quando se trata de crimes de informática que produzem resultados em diversos locais dentro do território brasileiro ou, até mesmo, em outros países, a regulamentação se dá pelos parágrafos do Art.70 do Código de Processo Penal, a saber:

> § 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.
> § 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.
> § 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.

Afirma CONTE (2008) que alguns autores defendem que é viável solucionar a fixação de competência dos crimes de informática utilizando o artigo somado à previsão do disposto no Art. 88 do Código de Processo Penal, cujo extrato segue abaixo:

> Art. 88 - No processo por crimes praticados fora do território brasileiro, será competente o juízo da Capital do Estado onde houver por último residido o acusado. Se este nunca tiver residido no Brasil, será competente o juízo da Capital da República.

Há ainda que se avaliar se o crime de informática é de natureza formal ou material.

Os crimes informáticos, em sua maioria, são delitos formais, ou seja, consumando-se no local onde foi realizada a ação, uma vez que nestes, o sujeito ativo, ao realizar a ação, buscava um objetivo, entretanto, mesmo se não conseguir efetivá-lo, restará consumado o delito (INELLAS, 2004).

Por fim, a competência de crimes de informática deverá ser da Justiça Federal, haja vista o que doutrina VIANNA (2000):

> Quando o crime for praticado pela *Internet*, julgamos que a competência deverá ser da Justiça Federal, já que o interesse da União em ter a *Internet* resguardada dentro dos limites brasileiros é evidente. Além do mais, este é um crime em que o resultado nem sempre se produz no lugar da ação, podendo até ocorrer em países diversos (crimes à distância), com repercussões internacionais que nos fazem crer ser prudente deixar a competência para a Justiça Federal.

Nesse sentido, é importante trazer para este trabalho algumas decisões de nosso Egrégio Superior Tribunal de Justiça, no que tange a conflitos de competência, a saber:

O Processo n° 198957 (Conflito de Competência), cujo Relator foi o Ministro REYNALDO SOARES DA FONSECA, foi publicado em 11/09/2023, no DF – (2023/0272721-0).

Cuidou-se de conflito negativo de competência suscitado pelo **Juízo Federal da 15ª Vara da Seção Judiciária do Distrito Federal** em face de decisão do **Juízo de Direito da 3ª Vara Criminal da Comarca de Brasília/DF** que se reputou incompetente para conduzir o inquérito policial instaurado para apurar o cometimento do delito capitulado no art. 171 do Código Penal (estelionato).

No caso concreto, o relato é de que no dia 28/4/2022, no período de 19h12 a 20h28, pessoas não identificadas, mediante quatro operações eletrônicas fraudulentas, subtraíram, para si e para outrem, a quantia total de R$ 38.175,25 da conta bancária de L. R.R., no Banco X, por intermédio de compras fraudulentas debitadas em seu cartão de crédito, em favor da empresa Q.T.V, com sede fora do Brasil e sem filial no país.

Na decisão, o conflito foi conhecido, pelo fato de os juízos que suscitaram a incompetência estarem vinculados a Tribunais diversos, o que atraiu a competência originária do Superior Tribunal de Justiça, consoante o disposto no art.105, inciso I, alínea "d", da Constituição Federal.

Indagou-se nos autos, se a prática de debitar fraudulentamente valores em cartão de crédito de pessoa física vinculado à conta corrente de Banco dentro do país, mas em favorecimento de empresa estrangeira, por meio de operações eletrônicas via *internet*, corresponde a crime que atrairia a competência da Justiça Federal.

Conforme a disposição do inciso V do art. 109 da Constituição da República, quando se tratar de infrações previstas em tratados ou convenções internacionais, quando presentes indícios de transnacionalidade do delito, tem-se que a competência é da Justiça Federal.

Aponta o dispositivo legal:

> Art. 109. Aos juízes federais compete processar e julgar:(...) 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.

Nesse sentido, a jurisprudência do STJ assevera que em se tratando de crime previsto em tratado ou convenção internacional, a competência da Justiça Federal é firmada quando iniciada a execução do crime no País, o seu resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente ou se for praticado em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, nos termos do inciso IV, do mesmo artigo citado.

Ademais, alinhando-se à jurisprudência do Supremo Tribunal sobre o tema, a Terceira Seção do STJ vem afirmando, também, que, "à luz do preconizado no art. 109, V, da CF, a competência para processamento e julgamento de crime será da Justiça Federal quando preenchidos 03 (três) requisitos essenciais e cumulativos, quais sejam, que:

a) o fato esteja previsto como crime no Brasil e no estrangeiro;

b) o Brasil seja signatário de convenção ou tratado internacional por meio do qual assume o compromisso de reprimir criminalmente aquela espécie delitiva; e

c) a conduta tenha ao menos se iniciado no Brasil e o resultado tenha ocorrido, ou devesse ter ocorrido no exterior, ou reciprocamente. (RE n. 628624, Relator Ministro MARCO AURÉLIO, Relator p/ Acórdão Ministro EDSON FACHIN, TRIBUNAL PLENO, julgado em 29/10/2015, DJe 5/4/2016)" (CC n. 168.775/DF, Relatora Ministra LAURITA VAZ, Terceira Seção, julgado em 28/10/2020, DJe de 12/11/2020).”

Ao se analisar outro processo em que figurou conflito de competência, pode-se citar o Processo n° 191336 (Conflito de Competência), cujo Relator foi o Ministro Antonio Saldanha Palheiro, e que foi publicado em 02/12/2022, em GO – (2022/0275776-1).

O referido conflito de competência foi estabelecido entre o **JUÍZO DE DIREITO DA 4ª VARA CRIMINAL DE GOIÂNIA - GO** e o **JUÍZO FEDERAL DA 5ª VARA DE GOIÂNIA - SJ/GO** em autos em que se apuram delitos de transmissão de pornografia infantil (arts. 241-A e 241-B da Lei n. 8.069/1990).

Neste caso, foi declinada a competência pelo Juízo Federal em razão da ausência de prova da transnacionalidade da conduta.

No caso concreto, o acusado foi denunciado após ser flagrado armazenando em vários dispositivos de informática fotografias e vídeos contendo cenas de sexo explícito envolvendo crianças e adolescentes.

Na decisão, o conflito foi conhecido. Foi dito pelo Magistrado que o Supremo Tribunal Federal, ao decidir sobre a competência para processar e julgar o crime previsto no art. 241-A do ECA (divulgação e publicação de conteúdo pedófilo-pornográfico), em repercussão geral, firmou o entendimento de que a potencialidade da transnacionalidade da conduta atrai a competência do Juízo Federal, conforme elucida a respectiva ementa a seguir transcrita:

RECURSO EXTRAORDINÁRIO. REPERCUSSÃO GERAL RECONHECIDA. PENAL. PROCESSO PENAL. CRIME PREVISTO NO ARTIGO 241-A DA LEI 8.069/90 (ESTATUTO DA CRIANÇA E DO ADOLESCENTE). COMPETÊNCIA. DIVULGAÇÃO E PUBLICAÇÃO DE IMAGENS COM CONTEÚDO PORNOGRÁFICO ENVOLVENDO CRIANÇA OU ADOLESCENTE. CONVENÇÃO SOBRE DIREITOS DA CRIANÇA. DELITO COMETIDO POR MEIO DA REDE MUNDIAL DE COMPUTADORES (INTERNET). INTERNACIONALIDADE. ARTIGO 109, V, DA CONSTITUIÇÃO FEDERAL. COMPETÊNCIA DA JUSTIÇA FEDERAL RECONHECIDA. RECURSO DESPROVIDO.

Na visão do Ministro, o exame das razões veiculadas pelos juízos que integram o presente incidente deixaram clara a transnacionalidade da conduta criminosa.

Ele considerou na decisão que, como o acusado utilizava em seu computador programas de extensão de arquivos que funcionam com o protocolo de transferência *Peer to Peer*, que servem para transferência de arquivos entre usuários, qualquer pessoa no mundo ao se conectar à *internet*, poderia ter acesso às imagens compartilhadas.

Restou configurada, desta maneira, a transnacionalidade exigida para atrair a competência da Justiça Federal.

Por conseguinte, o Magistrado entendeu que a competência deveria ser da Justiça Federal para processar e julgar a ação, nos termos do art. 109, V, da Constituição Federal.

Nesse sentido, ainda, pode-se citar o entendimento do Supremo Tribunal Federal, em sede de repercussão geral, nos autos do RE 628.624/SP, cujo Relator para acórdão foi o Ministro Edson Fachin, *in verbis*:

> Compete à Justiça Federal processar e julgar os crimes consistentes em disponibilizar ou adquirir material pornográfico envolvendo criança ou adolescente (arts. 241, 241-A e 241-B da Lei nº 8.069/1990) quando praticados por meio da rede mundial de computadores.

Portanto, a competência dos crimes de informática que transcendem fronteiras físicas nacionais costuma ser da Justiça Federal, desde que sejam atendidos os requisitos neste capítulo elencados.

Após isto, passo a abordar um breve histórico sobre a legislação brasileira sobre os crimes cibernéticos, a saber:

5. A legislação brasileira sobre os crimes de informática

A Lei Federal n° 12.737/2012 trata dos crimes de *internet*, tendo sido apelidada de Lei Carolina Dieckmann. O referido dispositivo legal provocou algumas alterações no Código Penal, incluindo os Art.154-A e 154-B, os parágrafos primeiro e segundo do Art. 266 e único do Art. 298.

Segundo TAVARES (2014) tratou-se de um grande avanço, porquanto havia uma grande dificuldade em criminalizar as condutas de quem clonava cartões e obtinha dados, uma vez que só era possível incriminar o suposto autor no momento em que realizava a fraude.

O artigo 154-A versa sobre o crime de invasão de dispositivo informático, no qual o bem protegido é a inviolabilidade dos segredos, ou seja, os dados e informações armazenados no computador, podendo ser de pessoas físicas como de pessoas jurídicas de direito privado (empresas) e de direito público (estado, órgãos e entidades) (BRASIL, 1940).

Prevê o Art. 266, do CP:

> Interromper ou perturbar serviço telegráfico, radiotelegráfico, ou telefônico, impedir-lhe ou dificultar-lhe o restabelecimento. Pena – detenção, de um a três anos, e multa. § 1° Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. § 2° Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.

No que tange ao Art.298 do CP, que trata sobre a falsificação de documento particular, o parágrafo único que foi incluído pela Lei n° 12.737, de 2012 assegurou que equipara-se a documento particular o cartão de crédito ou débito.

Ainda em 2014, entrou em vigor a Lei n°12.965, de 23 de abril de 2014, a qual estabeleceu princípios, garantias, direitos e deveres para o uso da *internet* no Brasil e determinou as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Esta Lei é considerada o primeiro passo do Direito Digital no Brasil, uma vez que permitiu que o meio cibernético pudesse, então, ser regulamentado.

Segundo JESUS (2014), uma das funções do Marco Civil Brasileiro é gerar segurança jurídica, oferecendo base legal ao Poder Judiciário quando se deparar com questões envolvendo internet e tecnologia da informação, evitando-se decisões contraditórias sobre temas idênticos, o que era muito comum.

Segundo ele, questões que eram submetidas ao Judiciário comumente apresentavam decisões contraditórias e eram julgadas com base na aplicação do Código Civil Brasileiro, Código de Defesa do Consumidor e outras legislações existentes.

Após, entrou em vigor a Lei 13.709, de 14 de agosto de 2018, a Lei Geral de Proteção de Dados Pessoais que, embora atualmente não trate de questões criminais e não seja objeto deste trabalho, trouxe, em seu Art. 1°, a seguinte previsão:

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

Segundo LOURENÇO (2023), esta Lei visa garantir a proteção dos dados das empresas e de seus clientes, evitando prejuízos e garantindo credibilidade e busca assegurar que as empresas lidem com as informações de seus clientes com seriedade, segurança e transparência, deixando claro o objetivo para sua coleta, armazenamento e processamento de dados.

Embora esta Lei não trate especificamente dos delitos de informática, a proteção, transferência e empréstimo de dados é alvo de Acórdão de Repercussão Geral no Supremo Tribunal Federal, no Tema 1148 – Recurso Extraordinário n° 1301250.

No sentido de ilustrar o citado Tema, a questão que foi submetida a julgamento foi um Recurso Extraordinário em que se discute, à luz da Constituição Federal, artigos 5º, X e XII, e 93, IX, a constitucionalidade de decreto judicial genérico de quebra de sigilo de dados telemáticos, para efeito de divulgação de informações pessoais de usuários indeterminados, sem a respectiva identificação, considerada a proteção constitucional da intimidade e da vida privada.

Como outro exemplo de choque entre direitos, pode-se citar um hipotético caso em que figurem os direitos à privacidade e à intimidade em detrimento ao direito à liberdade de expressão, inseridos em um ambiente digital.

Este caso seria, segundo FIORILLO (2016), uma situação em que um *site* coleta e manipula dados dos usuários, sem autorização destes ou, até mesmo, no que tange ao envio indiscriminado de *spam* ou pela utilização dos chamados *cookies*, que são programas que armazenam dados dos usuários.

Nesse prisma, sublinha PINHEIRO (2023):

> Desse modo, verifica-se a importância de se harmonizar, de um lado, a proteção da liberdade de expressão, mas de outro garantir que esta não seja abusiva, que não venha a ferir direitos tão importantes como da privacidade, da reputação, da propriedade intelectual.

Recentemente, o Decreto n° 11.491, de 12 de abril de 2023 promulgou a Convenção sobre o Crime Cibernético, firmada pela República Federativa do Brasil, em Budapeste, em 23 de novembro de 2001.

A Convenção em tela estabeleceu medidas a serem adotadas nas jurisdições nacionais, tanto de Direito Penal (seção 1) quanto de Direito Processual Penal (seção 2). Na seção 3, são abordadas questões de jurisdição.

Há, ainda, no Capítulo 3 da Norma, a previsão da Cooperação Internacional, em que aborda a possibilidade de extradição, assistência mútua, entre outras previsões.

Sobre a adesão do Brasil á Convenção, assegura VIEIRA (2023):

> Esta ação fortalece a cooperação do Brasil com parceiros estratégicos na luta contra os crimes cibernéticos, sendo um avanço estratégico que pode aumentar a eficácia da resposta brasileira aos desafios da cibercriminalidade. Portanto, mesmo que esta adesão não resolva todos os desafios que o Brasil enfrenta na luta contra a cibercriminalidade, ela representa um passo significativo em direção a uma abordagem mais robusta, abrangente e atualizada sobre o problema.

Em que pese a existência de leis que disciplinam condutas cibernéticas no Brasil, segundo LOURENÇO (2023), os cibercriminosos não praticam somente as condutas já tipificadas, pois existem condutas que ocorrem somente no meio virtual e as mesmas não se encontram tipificadas e estão cada dia mais evoluídas.

Não há como não nos perguntarmos, no que tange aos crimes cibernéticos, se realmente as nossas Leis estão atualizadas de acordo com o modo de operação dos criminosos virtuais.

Por essa razão, mister se faz que o nosso legislador estude com profundidade e a todo instante este modo de operação, de modo a estabelecer Leis que realmente freiem estes crimes, prevendo aos infratores penas adequadas.

Nesse sentido, assegura PEREIRA (2022):

> Não obstante, mesmo com o estabelecimento de inúmeras normas para limitar ações maliciosas no mundo virtual, nota-se várias lacunas que ainda devem ser preenchidas pelo legislativo, pois em um mundo que se pode conseguir recursos imensuráveis e ferramentas infinitas, é imprescindível que tal ordenamento esteja apto para lidar com situações em que, por exemplo, o sujeito possa desaparecer no ciberespaço, pois assim, seria muito fácil um usuário criar uma conta falsa e logo em seguida, denegrir a imagem de uma pessoa, e posteriormente, após toda a repercussão, excluir a conta.

Como visto acima, a legislação brasileira tipificou diversas condutas de maneira a conter o aumento da criminalidade que utiliza a rede mundial de computadores, porém, não há dúvidas de que há dificuldade de aplicação dessa legislação às diversas espécies de crimes de informática.

Ainda mais se levarmos em consideração o que afirma SPINELLO (1999):

> A *Internet* é uma tecnologia global sem fronteiras e sem donos, sendo quase impossível para qualquer nação garantir a execução de leis ou restrições que se busque impor no ciberespaço. Se os Estados Unidos, o México ou o Brasil decidirem proibir a pornografia *online*, esses países podem fiscalizar o cumprimento de tal proibição apenas entre os provedores e usuários em seus territórios. Infratores localizados na Europa ou na Ásia não estarão proibidos de disponibilizar material pornográfico na rede, acessível a qualquer pessoa, em qualquer parte.

Diante dessa temática, os criminosos continuam a criar novos delitos informáticos, devido ao crescente e ininterrupto desenvolvimento tecnológico.

Nesse ambiente, aponta VIEIRA (2023):

> A falta de uma legislação específica e abrangente para regulamentar o cibercrime e punir ações prejudiciais pode resultar em uma lacuna legal. Em tal situação, há ações que, apesar de causarem danos irreparáveis às vítimas, podem não se enquadrar em nenhuma categoria de crime previamente definida pelo Código Penal ou outras leis correlatas. Por isso, são consideradas atípicas e não podem ser punidas de acordo com o princípio da legalidade, também conhecido como reserva legal. Este princípio é uma característica fundamental do sistema jurídico brasileiro, especialmente em matéria penal, e estabelece que ninguém pode ser punido por uma ação que não seja explicitamente considerada um crime por lei.

À luz do acima exposto, pode-se verificar que não há uma legislação única que aborde todos os crimes cibernéticos, além de existirem lacunas legais, de delitos que não existem previsão em nosso ordenamento penal.

Seria extremamente salutar que nossa legislação pudesse reunir todos os crimes de informática em um único dispositivo legal. Afinal de contas, o Direito Digital chegou, e foi para ficar.

Após estas considerações acerca da legislação brasileira sobre os crimes cometidos na rede, passo às considerações finais deste trabalho.

6. Considerações Finais

O presente artigo trouxe questões acerca do surgimento dos crimes de informática, suas consequentes mudanças trazidas para o direito e a dificuldade de aplicação da legislação brasileira as suas espécies.

No capítulo 2, foram realizadas considerações sobre o surgimento da *internet* e as suas consequências para o Direito.

Abordou-se o aumento da criminalidade utilizando a *internet* e breve histórico sobre a origem dos crimes de informática, a sua definição geral e aspectos relacionados a quantidade de pessoas que utilizam a rede mundial de computadores.

Para a prática dos mais variados crimes de informática, foi apontado que os criminosos utilizam a rede como uma cortina de fumaça, dificultando, assim a sua detecção, fazendo-os permanecer, na maioria das vezes, no anonimato.

Foram exemplificados os dados privados que se encontram na rede, que antes eram guardados fisicamente em nossas casas.

Nessa ocasião, foi frizada a ideia de que hoje em dia, os aparelhos eletrônicos que possuímos guardam mais dados importantes do que possuímos em nossas próprias casas, em meio físico.

Foi debatido como o surgimento dos crimes de informática modificou os conceitos de território e local do crime (ciberespaço).

Definidos os crimes de informática, passou-se as suas espécies e seus tipos, segundo alguns autores. Após, foram analisados alguns dos principais crimes cometidos no ciberespaço, como a pornografia infantil, a divulgação de conteúdo pornográfico sem consentimento e extorsão proveniente do mesmo, estelionato e o recente crime de perseguição (*stalking*).

A exemplo do crime de perseguição, que foi inserido no Código Penal pela Lei 14.132 de 31 de março de 2021 sob a forma do art. 147-A, percebe-se que na redação de seu *caput,* a tipificação da conduta foi criada de modo a contemplar a possibilidade de se cometer o delito com o uso da *internet*.

Será que seria essa a melhor maneira de se positivar os delitos de informática? Ou deveríamos criar o "Código Penal Digital"?

Citadas as Leis que alteraram o Código Penal e a Convenção sobre o Crime Cibernético, foi abordada a questão da competência dos crimes de informática, tendo sido trazidas algumas jurisprudências de nossos Tribunais Superiores, mostrando como eles tem se posicionado em relação aos diversos conflitos de competência instaurados diariamente acerca dos crimes de informática.

Sublinhada a transnacionalidade da informação, importante requisito para se definir a competência de um crime de informática, foi trazida, então, a legislação brasileira sobre os crimes de informática, assim como citados alguns dispositivos que influenciam a sua aplicação.

Constatou-se, a partir daí, uma grande dificuldade de aplicação da Lei Brasileira às diversas espécies de crimes de informática, uma vez que mesmo tipificando-se as condutas criadas a todos os instantes pelos criminosos da rede, o acesso às informações, realizado em qualquer dispositivo eletrônico de qualquer parte do globo, continua sendo um desafio para os legisladores de todos os países que utilizam a rede mundial de computadores.

Restou clara a necessidade de se firmar a cooperação internacional entre polícias dos Estados, além de órgãos de fiscalização e de controle de sistemas de dados, com a finalidade de facilitar a investigação dos delitos de informática.

Em face do acima exposto, conclui-se que há grandes dificuldades de aplicação da Lei Brasileira às diversas espécies de crimes de informática, pelos motivos ao longo do trabalho expostos.

Referências

ARAS, VLADIMIR. Crimes de informática. Uma nova criminalidade, 2015. Disponível em <https://www.informatica-juridica.com/trabajos/crimes-de-informatica-umanovacriminalidade/#_ftn18> Acesso em : 05nov2023.

BRASIL. Planalto. Decreto-Lei 2.848, de 07 de dezembro de 1940. Código Penal. Diário Oficial da União, Rio de Janeiro, 31 dez. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/Del2848compilado.htm> Acesso em : 05nov2023.

BRASIL. Planalto. Decreto-Lei 3.688, de 03 de outubro de 1941. Lei das Contravenções Penais. Disponível em: < https://www.planalto.gov.br/ccivil_03/decreto-lei/del3688.htm > Acesso em : 05nov2023.

BRASIL. Planalto. Lei n° 12.737, de 30 de novembro de 2012. Disponível em: <https://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm > Acesso em : 30out2023.

BRASIL. Planalto. Lei n° 13.709, de 14 de agosto de 2018. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/l13709.htm> Acesso em : 25set2023.

BRASIL. Planalto. Lei n° 14.132, de 31 de março de 2021. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14132.htm> Acesso em : 30out2023.

BRASIL. Planalto. Lei n° 14.155, de 27 de maio de 2021. Disponível em: < https://www.planalto.gov.br/ccivil_03/_ato2019-2022/2021/lei/l14155.htm> Acesso em : 05nov2023.

BRASIL. Planalto. Decreto n° 11.491, de 12 de abril de 2023. Disponível em: <https://www.planalto.gov.br/ccivil_03/_Ato2023-2026/2023/Decreto/D11491.htm > Acesso em : 05nov2023.

CASTRO, CARLA RODRIGUES ARAÚJO. Impunidade na *Internet*. Direitonet. Disponível em <http://www.direitonet.com.br/doutrina/artigos/x/44/44/444/> Crimes de Informática e seus Aspectos Processuais. 2 ed. Rio de Janeiro, Ed. Lumen Juris, 2003.

CHAVES, ANTÔNIO apud SILVA, RITA DE CÁSSIA LOPES. Direito Penal e Sistema Informático. Disponível em <http://schmidtadvogados.com/v/artigo5> Acessado em 02/06/2017.

CONTE, CHRISTIANY PEGORARI, 2008. Disponível em https://www.migalhas.com.br/depeso/52372/desafios-do-direito-penal-no-mundo-globalizado--a-aplicacao-da-lei-penal-no-espaco Acesso em 30.11.2021.

COSTA, ALVARO MAYRINK, CRIME INFORMÁTICO: REVISTA DA EMERJ, V.7, N.28, 2004, P. 24/40.

COURI, GUSTAVO FUSCALDO, Crimes pela Internet. Escola da Magistratura do Estado do Rio de Janeiro, 2009.

CRESPO, MARCELO XAVIER DE F. Crimes digitais: Editora Saraiva, 2011. E-book. ISBN 9788502136663. Disponível em < https://integrada.minhabiblioteca.com.br/#/books/9788502136663/> Acesso em: 02 nov. 2023.

DOS SANTOS, CAROLINY ESTEFANE PIRES. O aumento dos crimes cibernéticos durante a pandemia da covid 19 e as dificuldades para combatê-las. LIBERTAS DIREITO, Belo Horizonte, v.4, n.1,jan. / jul. 2023.

FIORILLO, CELSO ANTONIO P.; CONTE, CHRISTIANY PEGORARI. Crimes no meio ambiente digital : Editora Saraiva, 2016. E-book. ISBN 9788547204198. Disponível em <https://integrada.minhabiblioteca.com.br/#/books/9788547204198/.> Acesso em: 02 nov. 2023.

FUCHS, PEDRO HENRIQUE CAMARGO, 2021. Acadêmico de direito pela Universidade do Oeste de Santa Catarina – UNOESC, campus São Miguel do Oeste. Email: pedrohenriquefuchs@gmail.com.

INELLAS, GABRIEL CÉSAR ZACARIA DE. Crimes na Internet. São Paulo: Juarez de Oliveira, 2004, p. 84.

JESUS, D.; MILAGRE, J. A. Manual de crimes informáticos . Editora Saraiva, 2016. E-book. ISBN 9788502627246. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502627246/. Acesso em: 02 nov. 2023.

JESUS, D.E.; OLIVEIRA, J.A.M.M.. Marco Civil da Internet : comentários à Lei n. 12.965, de 23 de abril de 2014, 1ª Edição, Editora Saraiva, 2014. E-book. ISBN 9788502203200. Disponível em <https://integrada.minhabiblioteca.com.br/#/books/9788502203200/.>Acesso em: 02 nov. 2023.

JÚNIOR, VICENTE CELESTE DE OLIVEIRA, Cibercrime: Um Estudo Acerca do Conceito de Crimes Informáticos. ISSN 1983-4225 – v.14, n.1, jun. 2019.

LOURENÇO, AMANDA CAROLINA GOMES. O aumento dos crimes cibernéticos durante a pandemia da covid 19 e as dificuldades para combatê-las. LIBERTAS DIREITO, Belo Horizonte, v.4, n.1,jan. / jul. 2023.

MOLES, RAMÓN J. Territorio, tiempo y estructura del ciberespacio, p.25-26

MIGALHAS, 8 de abril de 2021. disponível em <https://www.migalhas.com.br/depeso/343235/breve-analise-do-artigo-147-a-do-codigo-penal.> Acesso em : 03 nov 2023.

MONTEIRO, SILVANA DRUMOND. O ciberespaço: termo, a definição e o conceito. Revista da Ciência da Informação, v 8 n 3 jun/2017.

MOURA, GRÉGORE MOREIRA DE. Curso de Direito Penal Informático. Ed. D'Plácido. Minas Gerais. 2021.

PEREIRA, M.A.C.; OLIVEIRA, T.R.A. Crimes Cibernéticos e os Desafios ao Direito Brasileiro, 2022.

PINHEIRO, PATRÍCIA P. Direito Digital. Editora Saraiva, 2021. E-book. ISBN 9786555598438. Disponível em https://integrada.minhabiblioteca.com.br/#/books/9786555598438/. Acesso em: 02 nov. 2023.

ROSSINI, AUGUSTO EDUARDO DE SOUZA. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

SANTOMAURO, BEATRIZ. Cyberbulling: a violência virtual. Publicado em 2010. Disponível em <https://novaescola.org.br/conteudo/1530/cyberbullying-a-violencia-virtual>

SPINELLO, RICHARD A. Cyberethics: *morality and law in cyberspace*. Londres: Jones and Bartlett, 1999.

TAVARES, ADRIANO LOPES. Revista Jurídica, Ano XIV, n. 23, 2014, v2, Jan. – jun., Anápolis/GO, UniEVANGÉLICA.

TORMEN, CHALIDAN ADONAI CALLEGARI. Crimes cibernéticos: (IM) possibilidades de coerção. Erechim-RS: Monografia, 2018.

VALIN, CELSO. A questão da jurisdição e da territorialidade nos crimes praticados pela *Internet*. In Direito, sociedade e informática: limites e perspectivas da vida digital. Florianópolis: Fundação Boiteux, 2000, p. 115.

VIANNA, TÚLIO LIMA. Dos Crimes pela *internet*. Revista do CAAP, Belo Horizonte, a.5, v.9, 2000, p. 19.

VIEIRA, MARIA EDUARDA PEREIRA. A adesão do Brasil à Convenção de Budapeste e a correção das deficiências legislativas quanto aos crimes cibernéticos, Florianópolis, SC, 2023.

CAMPUS CENTRO:

• Sede Riachulo: Rua Riachuelo, 1257
• Sede General Vitorino: Rua General Vitorino, 25
• Sede Andradas: Rua Uruguai, 330

CAMPUS CIDADE BAIXA

• Sede Luiz Afonso: Rua Luiz Afonso, 84
• Sede João Pessoa: Avenida João Pessoa, 1105

CAMPUS ZONA NORTE

• Sede Sertório: Avenida Sertório, 5310

www.fadergs.edu.br | fadergs@fadergs.edu.br | Fone: (51) 3251 1111