UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE DE DIREITO

OS EFEITOS DOS CONFLITOS DE JURISDIÇÃO SOBRE OS LITÍGIOS TRANSFRONTEIRIÇOS NA INTERNET

CHRISTIAN CARDOSO SOARES

Rio de Janeiro

2023

UNIVERSIDADE FEDERAL DO RIO DE JANEIRO

CENTRO DE CIÊNCIAS JURÍDICAS E ECONÔMICAS

FACULDADE DE DIREITO

CHRISTIAN CARDOSO SOARES

OS EFEITOS DOS CONFLITOS DE JURISDIÇÃO SOBRE OS LITÍGIOS TRANSFRONTEIRIÇOS NA INTERNET

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Caio Cézar Ovelheiro Menna Barreto

Rio de Janeiro

2023

CHRISTIAN CARDOSO SOARES

OS EFEITOS DOS CONFLITOS DE JURISDIÇÃO SOBRE OS LITÍGIOS TRANSFRONTEIRIÇOS NA INTERNET

Monografia de final de curso, elaborada no âmbito da graduação em Direito da Universidade Federal do Rio de Janeiro, como pré-requisito para obtenção do grau de bacharel em Direito, sob a orientação do Professor Caio Cézar Ovelheiro Menna Barreto

Data da Aprovação: 03/07/2023.

Banca Examinadora:

_____

Professor Caio Cézar Ovelheiro Menna Barreto - Orientador

_____

Professor Luis Claudio Martins de Araujo - Membro da Banca

_____

Membro da Banca

Rio de Janeiro

2023

AGRADECIMENTOS

Agradeço primeiramente a Deus, que me deu forças e me sustentou em todos os momentos.

Agradeço também a minha companheira Juliana e nossa filhota canina Amora, por caminharem sempre ao meu lado e me fazerem melhor a cada dia.

Agradeço aos meus familiares, em especial a minha mãe Leila, ao meu pai André, a minha vó Niceia, ao meu avô Bebeco e aos meus tios. Por nunca deixarem nada faltar para mim e por buscarem sempre – em suas visões – a minha melhor versão.

Agradeço aos meus amigos, em especial ao João Henrique e ao Márcio, por sempre apresentarem-se como escape nos momentos de estresse.

Agradeço aos meus amigos de faculdade, em especial a Mariana Aimée, que me ajudou com tantos cadernos e orientações durante o curso, além da companhia por todo o trajeto Barra de Guaratiba – Centro.

Agradeço aos amigos do FutFND, aos quais levarei por muito tempo, seja nos campos e resenhas, seja nas histórias que para sempre serão lembradas.

Por fim, mas não menos importante, agradeço ao Professor Caio Ovelheiro por aceitar esse desafio, por toda atenção durante o trabalho e por todos os ensinamentos.

RESUMO

Esta monografia aborda a influência da tecnologia da informação nas organizações e os riscos potenciais que os Estados precisam enfrentar. Considerando que a informação é um ativo valioso para as organizações, surge a necessidade de proteger a confidencialidade, a integridade e a disponibilidade dessas informações. Porém, no contexto globalizado e mutável, o judiciário enfrenta desafios na execução de sentenças de crimes cibernéticos praticados em território estrangeiro. O objetivo central deste estudo é analisar os tipos principais de crimes cibernéticos, a dificuldade na execução de sentenças além das fronteiras nacionais e como o judiciário brasileiro aborda essa questão. A metodologia utilizada é dedutiva, com abordagem qualitativa e natureza descritiva. Os capítulos abordam tópicos como jurisdição, legislação cibernética, principais crimes cibernéticos, a dicotomia entre territorialidade e internet, e a possibilidade de execução de sentenças pelo judiciário brasileiro em outros países. Conclui-se que, devido à falta de harmonização das leis entre diferentes nações, ocorrem conflitos de jurisdição na internet. Isso resulta em decisões contraditórias e incerteza jurídica. Por fim, o estudo destaca a importância de enfrentar os problemas da criminalidade cibernética, investigar e punir os crimes, enquanto o Estado busca acompanhar a evolução global e virtual.

Palavras- chave: Jurisdição. Internet. Cibersegurança. Sociedade.

ABSTRACT

This monograph addresses the influence of information technology on organizations and the potential risks that States need to face. Considering that information is a valuable asset for organizations, there is a need to protect the confidentiality, integrity and availability of this information. However, in the globalized and changing context, the judiciary faces challenges in the execution of sentences for cyber crimes committed in foreign territory. The main objective of this study is to analyze the main types of cyber crimes, the difficulty in executing sentences across national borders and how the Brazilian judiciary addresses this issue. The methodology used is deductive, with a qualitative approach and descriptive nature. The chapters address topics such as jurisdiction, cyber legislation, major cyber crimes, the dichotomy between territoriality and the internet, and the possibility of enforcement of sentences by the Brazilian judiciary in other countries. It is concluded that, due to the lack of harmonization of laws between different nations, conflicts of jurisdiction occur on the internet. This results in conflicting decisions and legal uncertainty. Finally, the study highlights the importance of facing the problems of cybercrime, investigating and punishing crimes, while the State seeks to keep up with global and virtual evolution.

Keywords: Jurisdiction. Internet. Cybersecurity. Society.

SUMÁRIO

1 INTRODUÇÃO

Com a implementação de tecnologias e tecnologia da informação, as organizações alcançaram outro nível de efetividade ao oferecer serviços e produtos para atender às necessidades de seus clientes e usuários, em termos de organizações governamentais. No entanto, a obtenção desse novo nível de eficácia trouxe implicitamente riscos potenciais que os Estados passaram a enfrentar. As mudanças que tiveram que enfrentar foram inúmeras. Desde a educação e a formação nessas áreas até a implementação de tecnologias, tudo teve um custo, seja para a iniciativa privada, para os Estados e para a sociedade.

Os riscos do computador estavam aparecendo e evoluindo em sintonia com os mesmos avanços tecnológicos e computacionais. E nessa lacuna, as mentes criminosas agiram para adaptar os avanços tecnológicos e o vazio legislativo sobre o tema aos seus anseios criminosos. As soluções e ferramentas para combater esses crimes ainda estão criadas, recomendadas e implementadas pelas instituições.

Em contraponto, como a informação hoje é um dos ativos mais importantes das organizações, há uma necessidade fundamental crescente de buscar os diferentes métodos, estratégias e tecnologias para proteger tais informações, com o objetivo de garantir e preservar a confidencialidade, a integridade e a disponibilidade como eixo fundamental.

Ocorre que, nesse cenário globalizado e completamente mutável, surge um novo desafio a cada instante. Com a crescente prática de crimes se utilizando da internet, novas provocações são feitas ao judiciário a todo instante. É o que pretende se esclarecer neste trabalho. Em especial a dificuldade do judiciário em executar sentenças dos crimes praticados na internet em solo estrangeiro e como o tema vem sendo tratado.

O objetivo central deste trabalho é analisar o contexto dos crimes cibernéticos, seus principais tipos e a dificuldade na execução da sentença destes crimes quando transcendem as

territorialidades nacionais. Restará demonstrado os principais delitos ocorridos na internet, a dificuldade em executar sentenças de crimes praticados na internet em território estrangeiro e a forma com que o judiciário brasileiro vem tratando a questão. A metodologia utilizada neste artigo é de cunho dedutivo, sua natureza é descritiva e sua abordagem qualitativa.

2 DA JURISDIÇÃO

2.1 CONCEITO DE JURISDIÇÃO

O ordenamento jurídico brasileiro constitui-se sobre alguns pilares fundamentais. A jurisdição é inevitavelmente um deles.

O conceito de jurisdição é para Dinamarco[1]:

> Ao mesmo tempo, poder, função e atividade. Como poder, é a manifestação do poder estatal, conceituado como capacidade de decidir imperativamente e impor decisões. Como função, expressa o encargo que têm os órgãos estatais de promover a pacificação de conflitos interindividuais, mediante a realização do direito justo e através do processo. E como atividade ela é o complexo de atos do juiz no processo, exercendo o poder e cumprindo a função que a lei lhe comete.

Já para Chiovenda[2], jurisdição é:

> Função do Estado que tem por escopo a atuação da vontade concreta da lei por meio de substituição, pela atividade de órgãos públicos, da atividade de particulares ou de outros órgãos públicos, já no afirmar a existência da vontade concreta da lei, já no torná-la, praticamente, efetiva.

[1] CINTRA, Antonio Carlos Araújo; GRINOVER, Ada Pelegrini; DINAMARCO, Cândido Rangel. Teoria Geral do Processo. 28ª Ed. São Paulo: Malheiros, 2011. p. 155
[2] CHIOVENDA, Giuseppe. Tradução do original italiano – 2a edição, por Paolo Capitanio. Instituições de Direito Processual Civil. Campinas: Bookseller, volume 2, 1998, p. 8

Ocorre que a jurisdição é, no dizer de Moacyr Amaral Santos[3],

> Função do Estado desde o momento em que, proibida a autotutela dos interesses individuais em conflito, por comprometedora da paz jurídica, se reconheceu que nenhum outro poder se encontra em melhores condições de dirimir os litígios do que o Estado, não só pela força de que dispõe, como por nele presumir-se interesse em assegurar a ordem jurídica estabelecida.

Com isso, podemos definir a jurisdição como uma das formas de expressão da soberania dos Estados. Trata-se da atividade, tomada com exclusividade pelo Estado Moderno, de fazer atuar o Direito no âmbito do território estatal.

No âmbito internacional a jurisdição não encontra limites territoriais. Portanto, tese, demonstra-se ilimitada e indivisível[4]. Entretanto, o reconhecimento da existência de outros Estados soberanos, igualmente dotados de jurisdição, implica a necessária fixação pelo próprio Estado das causas que sejam de seu interesse julgar. Desse modo, o princípio da efetividade torna a ação jurisdicional limitada à possibilidade de lograr seu objetivo.

2.2 LIMITES DA JURISDIÇÃO NACIONAL

De início, cabe traçarmos algumas premissas fundamentais sobre jurisdição, especialmente no que tange à jurisdição brasileira, os seus limites e conceitos.

---

[3] Cf. Primeiras Linhas de Direito Processual Civil. São Paulo: Saraiva, 14ª ed., 1º volume, pág. 67

[4] Sobre tais características, sustentando ainda que soberania é o poder originário, incondicionado, exclusivo e coativo, ver dentre outros, DALLARI, Dalmo de Abreu. Elementos da Teoria Geral do Estado, 16ed. São Paulo: Saraiva, 1991, p.69; PAUPÉRIO, Arthur Machado. Teoria Democrática da Soberania. v.2. 3ed. Rio de Janeiro: Forense Universitária, 1997, p. 15-17.

Partindo diretamente do Código de Processo Civil, tais disposições se encontram no livro II, título II, em seu capítulo I, denominado “Dos Limites da Jurisdição Nacional”.

Logo em seu primeiro artigo, o 21, o legislador se preocupa em fixar alguns parâmetros básicos de jurisdicionalidade a que competiria a justiça brasileira, utilizando-se de três critérios: o domicílio do réu; a territorialidade do cumprimento da obrigação e a territorialidade do fato ou do ato que seja fundamento da ação.

> Art. 21. Compete à autoridade judiciária brasileira processar e julgar as ações em que:
> I - o réu, qualquer que seja a sua nacionalidade, estiver domiciliado no Brasil;
> II - no Brasil tiver de ser cumprida a obrigação;
> III - o fundamento seja fato ocorrido ou ato praticado no Brasil.
> Parágrafo único. Para o fim do disposto no inciso I, considera-se domiciliada no Brasil a pessoa jurídica estrangeira que nele tiver agência, filial ou sucursal.

Seguindo mais adiante, o nosso Código de Processo Civil também preceitua mais três situações especificamente em que o litígio deverá considerar como jurisdição a autoridade judicial brasileira. São eles: na demanda de alimentos, quando o credor tiver domicílio ou residência no Brasil ou quando o réu mantiver vínculos em território nacional que possam garantir o cumprimento da prestação alimentícia; em relações de consumo, quando o consumidor tiver domicílio ou residência no Brasil ou ainda quando as partes - expressa ou tacitamente - submeterem-se a jurisdição nacional.

> Art. 22. Compete, ainda, à autoridade judiciária brasileira processar e julgar as ações:
>
> I - de alimentos, quando:
>
> a) o credor tiver domicílio ou residência no Brasil;
>
> b) o réu mantiver vínculos no Brasil, tais como posse ou propriedade de bens, recebimento de renda ou obtenção de benefícios econômicos;
>
> II - decorrentes de relações de consumo, quando o consumidor tiver domicílio ou residência no Brasil;

Há ainda, neste mesmo capítulo, o artigo 23 que estabelece – em sua forma taxativa – a competência exclusiva da jurisdição brasileira. Isto ocorre nos casos em que

as ações versam sobre imóveis situados no Brasil, sobre partilha de bens situados no Brasil no caso de sucessão hereditária, bem como via divórcio, separação judicial ou dissolução de união estável.

> Art. 23. Compete à autoridade judiciária brasileira, com exclusão de qualquer outra:
>
> I - conhecer de ações relativas a imóveis situados no Brasil;
>
> II - em matéria de sucessão hereditária, proceder à confirmação de testamento particular e ao inventário e à partilha de bens situados no Brasil, ainda que o autor da herança seja de nacionalidade estrangeira ou tenha domicílio fora do território nacional;III - em divórcio, separação judicial ou dissolução de união estável, proceder à partilha de bens situados no Brasil, ainda que o titular seja de nacionalidade estrangeira ou tenha domicílio fora do território nacional.

Isto posto, nota-se a preocupação do legislador em exemplificar parâmetros básicos de jurisdicionalidade. Observamos que grande parte dos limites jurisdicionais versam sobre critérios de territorialidade, interesse das partes ou até facilidade na garantia da execução. Deixando claro a incessante busca por soluções que garantam às partes envolvidas em litígios transnacionais o mesmo grau de proteção em termos de acesso à justiça, economia processual, duração razoável do processo e efetividade em uma sociedade cada vez mais global.

Destaca-se também a divisão entre jurisdição concorrente e jurisdição exclusiva. A primeira se refere às matérias em que se admite atuação tanto da jurisdição brasileira como da jurisdição de outros Estados. Isso significa que o processo pode correr tanto no Brasil como no exterior, mas sendo a jurisdição internacional excepcional, para a sentença ter validade no território brasileiro, ela deve ser homologada pelo Superior Tribunal de Justiça.

De acordo com MORELLI, a expressão ‘competência exclusiva’ é passível de críticas, haja vista que sendo uma norma unilateral, não pode o Brasil estabelecer o que é ou não da alçada das jurisdições estrangeiras conhecer[5]. Cada Estado é livre para

[5] MORELLI, Gaetano. Derecho procesal civil internacional. Trad. de Santiago Melendo, Buenos Aires, Ediciones Jurídicas Europa-América, 1953, pp. 86

estabelecer suas regras de competência, não sendo possível afirmar que a competência do Brasil é exclusiva sobre qualquer caso.

Assim, ao invés de 'excluir' as demais justiças para as situações ali elencadas, seria mais plausível afirmar que a sentença estrangeira que tratar de matéria constante deste dispositivo não será, pelo nosso Judiciário, reconhecida.

No tocante das hipóteses de jurisdição exclusivas, o legislador se preocupou com que a competência do judiciário brasileiro se estendesse expressamente não apenas para inventário e partilha de bens *causa mortis*, mas também enquanto *intervivos*, em caso de divórcio ou separação de casais.

Entretanto, não resta dúvidas de que a grande novidade do novo Código foi a expressa admissão da eleição de foro, dos efeitos positivos e negativos da eleição de foro no plano internacional. Então, quando as partes, num contrato internacional, elegem o Judiciário brasileiro como competente para conhecer de uma demanda, então o art. 22, III traz essa hipótese como de competência concorrente do nosso Judiciário.

E contrariamente, ainda que seja uma hipótese de competência concorrente, quando as partes elegem um Judiciário estrangeiro como competente para decidir aquela causa, o Judiciário brasileiro deverá se abster de julgar a questão, conforme previsão do art. 25 do novo Código de Processo Civil:

> "Art. 25. Não compete à autoridade judiciária brasileira o processamento e o julgamento da ação quando houver cláusula de eleição de foro exclusivo estrangeiro em contrato internacional, arguida pelo réu na contestação."

2.3 DIFERENÇA ENTRE JURISDIÇÃO E LEI APLICÁVEL

No Brasil, historicamente a competência judiciária baseou-se na territorialidade, sem distinção entre nacionais e estrangeiros. Aos poucos foram surgindo normas que dispunham sobre a noção de jurisdição internacional e a inseria em nosso ordenamento jurídico.

Atualmente, com o contexto da globalização e a consequente diminuição das distâncias, aumentou-se a incidência de relações plurilocalizadas, assim como os próprios litígios dessa natureza. Com isso, a questão dos limites da jurisdição dos Estados se torna de suma importância, já que será o fator que determinará o alcance judiciário daquele Estado no plano internacional.

Conforme Irineu Strenger,

> "o Direito Internacional Privado no Brasil é um conjunto de princípios que cuida da legislação aplicável às relações jurídicas privadas envolvidas em mais de uma esfera de soberania".[6]

Já segundo dizeres de Jacob Dolinger,

> "o Direito Internacional Privado entra em ação quando não há direito uniforme, quando ocorrem os conflitos entre normas legais de sistemas jurídicos diversos".[7]

Com efeito, ressalta-se que competência internacional não se confunde com a jurisdição. A competência internacional diz respeito ao exercício do poder jurisdicional de um Estado em relação a um conflito que tenha, de qualquer modo, como parte, um elemento estrangeiro. Jurisdição se refere ao poder que o Direito Internacional concerne ao Estado de administrar, legislar e julgar. O Direito Internacional Privado e suas fontes definem as normas a serem aplicadas em determinados conflito de acordo com o objeto

---

[6] STRENGER, Irineu. Direito Internacional Privado: Parte Geral, Direito Civil Internacional, Direito Comercial Internacional. 5. Ed. São Paulo: LTR, 2003

[7] DOLINGER, Jacob. Direito Internacional Privado: (parte geral). 4. Ed. Atualizada. Rio de Janeiro, Renovar, 1997.

de conexão, não diferindo da competência interna no ponto que ambas são fragmentações da jurisdição.

Nesse contexto, primeiro soluciona-se o conflito de jurisdição para o julgamento de determinada ação – segundo os critérios dos artigos 21 a 25 do NCPC. Considerando-se competente, o próximo passo do juiz é identificar se deve ser aplicável ao problema multifacetado a lei estrangeira ou a lei brasileira.

Portanto podemos depreender que mesmo após fixada a jurisdição brasileira para processar e julgar a ação, não significa que a lei brasileira irá necessariamente reger o mérito da controvérsia. Isto porque os critérios para determinação da lei aplicável são elementos de conexão da LINDB, sendo essas normas instrumentais, ou seja, que apenas indicam dentre os sistemas jurídicos ligados à hipótese, qual deles deve ser aplicado, não sendo este necessariamente o brasileiro.

2.4 A ESCOLHA DA LEI NO ESTRANGEIRO

Na Europa, os países integrantes da chamada Comunidade Europeia já discutiam, desde a da Convenção de Bruxelas, a uniformização das regras relativas aos contratos internacionais, especialmente sobre lei aplicável e jurisdição, a fim de evitar casos do chamado *forum shopping* e conferir mais segurança jurídica às relações comerciais entre os países.

Dessa forma, em 1980, foi assinada a Convenção sobre a Lei Aplicável às Obrigações Contratuais, mais conhecida como Convenção de Roma.

Destaca-se na Convenção de Roma o estabelecimento da liberdade das partes como a principal forma de determinar a lei aplicável ao contrato, consagrando de uma vez por todas a autonomia da vontade. Ao mesmo tempo em que fora um importante

exemplo de uniformização do Direito Internacional Privado pois, dentre os países signatários, há representantes tanto do sistema de direito anglo-saxão como de direito romano-germânico, além de servir de exemplo para diversas tentativas de harmonização de regras de conflitos regionais.

Em 2008, a Convenção de Roma foi substituída pelo Regulamento da Comunidade Europeia sobre a Lei Aplicável para obrigações contratuais 593, que passou a vigorar no final de 2009. No que diz respeito à autonomia da vontade, as regras da Convenção de Roma foram preservadas no Regulamento 593.

A partir de 2010, o Conselho da Conferência da Haia estabeleceu um Grupo de Trabalho para elaborar princípios sobre a lei aplicável aos contratos internacionais.

Diversos doutrinadores defendem a necessidade urgente de atualização do Direito Internacional Privado brasileiro. A imutabilidade de sua principal fonte normativa (a LINDB) resulta em sua inadequação à complexidade e à diversidade do momento atual e na ausência de soluções para os novos rumos da disciplina.

João Grandino Rodas insiste que somente com a atualização das normas de Direito Internacional Privado do Brasil será possível "exorcizar o primitivismo e a inadequação de nossas regras"[8]. Segundo o autor, o tratamento adotado pelo Brasil pela não recepção da autonomia privada nos contratos internacionais é incompatível com a posição do país dentre as dez maiores economias do mundo (à época).

[8] RODAS, João Grandino. Elementos de Conexão do Direito Internacional Privado. In João Grandino (Coord.) Contratos Internacionais. 3. Ed. São Paulo: Revista dos Tribunais, 2002, p. 64

3 LEGISLAÇÃO CIBERNÉTICA

3.1 SURGIMENTO DOS CRIMES CIBERNÉTICOS

O surgimento dos crimes cibernéticos está diretamente ligado ao avanço da tecnologia e à expansão da internet. Com o crescente uso da internet em diferentes aspectos da vida cotidiana, surgiu também uma nova forma de criminalidade que aproveita as vulnerabilidades digitais para cometer delitos. A internet possibilita o anonimato e isso aumenta a sensação de impunidade entre as pessoas, permitindo assim, que usuários com menos conhecimento de informática possam cometer um crime virtual.

Esse fenômeno pode ser atribuído a diferentes fatores. Um deles é a facilidade de acesso à tecnologia e à internet, que permite que uma ampla gama de pessoas possa se envolver em atividades criminosas online. Além disso, a natureza global e descentralizada da internet torna mais desafiador para as autoridades rastrearem e investigarem os criminosos.

A gigantesca quantidade de usuários e o intenso fluxo de informações produziram consequências e riscos maiores em todo mundo. Hoje, milhares de pessoas passam mais tempo navegando na internet do que vivendo o mundo real. A rede mundial de computadores possibilitou ao indivíduo resolver diversos assuntos e se relacionar com diversas pessoas sem sair de casa, mas isto trouxe um aumento da exposição de dados pessoais, como também a necessidade de a legislação evoluir para conter os diversos crimes que são aplicados diariamente.

3.2 CRIMES CIBERNÉTICOS

Embora existam as divergências doutrinárias quanto a conceituar os crimes praticados em meio eletrônico, há uma grande leva de doutrinadores que os denomina como crimes cibernéticos. Entretanto, estes também possuem outras nomenclaturas, como por exemplo, crimes digitais, informáticos, telemáticos, de alta tecnologia, crimes por computador, fraude informática, crimes virtuais, crimes transnacionais, dentre outras.

De acordo com Sérgio Marcos Roque, o conceito de crime cibernético é “toda conduta definida em lei como crime, em que o computador tiver sido utilizado como instrumento de sua perpetração ou consistir em seu objeto material (ROQUE, 2007).”

Esses crimes são condutas ilegais praticadas por pessoas que se utilizam desses meios para aplicarem golpes como fraudes, estelionatos e vazamento de informações. Com o avanço tecnológico, grande parte de informações pessoais ficam acessíveis a milhares de pessoas que possuem acesso à internet. Atualmente, essa facilidade traz novas formas de violação de bens jurídicos protegidos pelo ordenamento, os quais passaram a ser realizados não só no plano físico, mas também no plano virtual, através de usuários que cometem crimes na rede.

Para Augusto Rossini:

> O conceito de “delito informático” poderia ser talhado como aquela conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva omissiva, praticada por pessoa física ou jurídica, com o uso a 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 a confidencialidade (ROSSINI, 2004, p.123).

Rossini sugere que esses crimes não alcançam somente aquelas condutas praticadas no âmbito da internet, mas toda e qualquer conduta em que haja relação com sistemas informáticos, de modo que essa denominação abrangeria, inclusive, delitos em que o computador seria uma mera ferramenta, sem a imprescindível conexão à rede mundial de computadores, ou a qualquer outro ambiente telemático. Ou seja, uma fraude em que o computador é usado como instrumento do crime, fora da internet, também seria alcançada pelo que se denominou delitos informáticos.

De acordo com Guilherme Guimarães Feliciano existe um conceito bem amplo de criminalidade informática.

> Conheço por criminalidade informática o recente fenômeno histórico-sociocultural caracterizado pela elevada incidência de ilícitos penais (delitos, crimes e contravenções) que têm por objeto material ou meio de execução o objeto tecnológico informático (hardware, software, redes etc.) (FELICIANO, 2000, p. 42).

Cabe ao Direito a difícil tarefa de trazer soluções para todos os litígios que possam ocorrer dentro deste ambiente virtual. Sendo este a solução prática para planejar estratégias que resolvam todas as demandas que surgem através da rápida transformação digital que vem acontecendo na sociedade.

Para Vicente Greco Filho existe a seguinte divisão: condutas perpetradas contra um sistema informático e condutas perpetradas contra outros bens jurídicos:

> Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação, praticados por meio da Internet e crimes ou ações que merecem incriminação, praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou (GRECO FILHO, 2000, p. 26.)

Para sintetizar: os crimes próprios são condutas perpetradas contra um sistema informático, sejam quais forem as motivações do agente; já os crimes impróprios são condutas perpetradas contra outros bens jurídicos, por meio de um sistema informático.

A classificação da doutrina majoritária em relação aos delitos se divide em delitos próprios e delitos impróprios. Segundo o Professor Damásio Evangelista de Jesus[9]: delitos próprios aqueles praticados não só por computador, mas também por qualquer meio eletrônico, na qual a informática é o objeto jurídico tutelado; já os delitos impróprios são aqueles em que o agente se vale do computador como meio para produzir resultado naturalístico, que ofenda o mundo físico ou o espaço real, ameaçando ou lesando outros bens diversos da informática.

[9] Em: ALMEIDA, Maria Paula Castro. A evolução no combate aos crimes digitais. 2015. Disponível em: http://tiny.cc/fothoz. Acesso em: 10 de junho de 2023; CARNEIRO, Adeneele Garcia. Crimes virtuais: elementos para uma reflexão sobre o problema na tipificação. Disponível em: https://ambitojuridico.com.br/edicoes/revista-99/crimes-virtuais-elementos-parauma-reflexao-sobre-o-problema-na-tipificacao/. 2012. Acesso em: 10 de junho de 2023; e NASCIMENTO, Talles Leandro Ramos. Crimes cibernéticos. 2018. Disponível em: https://conteudojuridico.com.br/consulta/Artigos/52512/crimescibernetico s. Acesso em: 10 de junho de 2023.

Não é uma tarefa fácil a constatação de um crime digital e a sua consequente classificação, visto que ainda existem poucas conclusões a respeito e a tecnologia evolui a passos largos. Sendo assim é necessário que a opinião dos doutrinadores também mude conforme a evolução tecnológica. Consequentemente é difícil determinar o crime cibernéticos, tendo em vista que existem muitas situações complexas no ambiente virtual.

As denominações quanto aos crimes praticados em ambiente virtual são diversas. Não há um consenso sobre a melhor denominação para os delitos que se relacionam com a tecnologia.

Esses crimes na internet são praticados pelos chamados *crackers*. Já os *hackers* são aqueles que tem um conhecimento avançado em computação e usam todo esse conhecimento em favor da justiça trabalhando junto com a polícia para combater essa rede de criminosos virtuais. Os repórteres de emissoras de televisão ou jornais noticiam esses fatos de forma equivocada, falando para a população que o *hacker* é o causador do dano, dessa forma ele fica apontado como se ele fosse o vilão, quando na verdade é o *cracker* quem comete o delito.

Como podemos ver os chamados crimes cibernéticos englobam os mais diversos tipos de crimes. A seguir, veremos como a legislação trata o tema.

3.2.1 Ameaça

O crime de ameaça na internet, também conhecido como ciberameaça, refere-se a qualquer ação ilegal ou comportamento ameaçador realizado online. Isso pode incluir a utilização de meios eletrônicos, como e-mails, mensagens instantâneas, redes sociais, fóruns, entre outros, para ameaçar, intimidar ou assediar uma pessoa.

As ameaças na internet podem assumir diversas formas, como enviar mensagens ameaçadoras, divulgar informações privadas, disseminar boatos difamatórios, espalhar

conteúdo ofensivo ou violento, praticar o ciberbullying, extorsão online, entre outros comportamentos prejudiciais. Essas ações podem ter sérias consequências emocionais, psicológicas e até mesmo físicas para as vítimas.

O crime de ameaça está previsto no artigo 147 do Código Penal. Nos casos de crimes virtuais, refere-se a ameaçar alguém, utilizando-se de Internet, principalmente das redes sociais para a prática deste crime.

> Art. 147 - 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.
> Parágrafo único - Somente se procede mediante representação (BRASIL, 1940).

3.2.2 Racismo (e outras formas de preconceitos)

Na Lei 7.716 de 1989, no seu artigo 20 está previsto o crime de racismo, alterada também pela Lei 9.459 de 1997, referindo-se a prática, induzimento ou incitação à discriminação ou preconceito racial ou etnológico, podendo ser realizado por alguém através da Internet por meio de divulgação em página eletrônica, correios eletrônicos, bate papos, entre outros.

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional. (Redação dada pela Lei nº 9.459, de 15/05/97)
> Pena: reclusão de um a três anos e multa. (Redação dada pela Lei nº 9.459, de 15/05/97)
> § 1º Fabricar, comercializar, distribuir ou veicular símbolos, emblemas, ornamentos, distintivos ou propaganda que utilizem a cruz suástica ou gamada, para fins de divulgação do nazismo. (Redação dada pela Lei nº 9.459, de 15/05/97)
>
> Pena: reclusão de dois a cinco anos e multa. (Incluído pela Lei nº 9.459, de 15/05/97)
> § 2º Se qualquer dos crimes previstos no caput é cometido por intermédio dos meios de comunicação social ou publicação de qualquer natureza: (Redação dada pela Lei nº 9.459, de 15/05/97)
> Pena: reclusão de dois a cinco anos e multa. (Incluído pela Lei nº 9.459, de 15/05/97)
>
> § 3º No caso do parágrafo anterior, o juiz poderá determinar, ouvido o Ministério Público ou a pedido deste, ainda antes do inquérito policial, sob pena de desobediência: (Redação dada pela Lei nº 9.459, de 15/05/97)
>
> I o recolhimento imediato ou a busca e apreensão dos exemplares do material respectivo;(Incluído pela Lei nº 9.459, de 15/05/97)
> II - A cessação das respectivas transmissões radiofônicas ou televisivas. (Incluído pela Lei nº 9.459, de 15/05/97)

> II a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio; (Redação dada pela Lei nº 12.735, de 2012)
> III a interdição das respectivas mensagens ou páginas de informação na rede mundial de computadores. (Incluído pela Lei nº 12.288, de 2010)
> § 4º Na hipótese do § 2º, constitui efeito da condenação, após o trânsito em julgado da decisão, a destruição do material apreendido. (Incluído pela Lei nº 9.459, de 15/05/97).

O racismo na internet é uma forma de discriminação racial que ocorre por meio de plataformas online, como redes sociais, blog e fóruns. Infelizmente, a internet tem proporcionado um ambiente onde algumas pessoas se sentem mais confortáveis em expressar suas opiniões preconceituosas e propagar discurso de ódio racial.

O racismo na internet pode assumir diversas formas, desde comentários racistas diretos e insultos até a disseminação de estereótipos prejudiciais e imagens ofensivas. Seus efeitos tendem a ser extremamente danosos para as vítimas, causando trauma emocional, isolamento social e afetando sua autoestima. Além disso, contribui para a perpetuação de estereótipos negativos e reforça a desigualdade racial.

É fundamental combater o racismo na internet e criar um ambiente online seguro e inclusivo para todos.

3.2.3 Pornografia infantil

Inicialmente, o crime de pornografia infantil somente tinha sua previsão no artigo 234 do código penal, referindo-se a prática de fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno, estando intimamente ligado à busca de sentimentos eróticos através do uso da criança ou adolescente, denominado de pedofilia, tendo como ferramenta o próprio uso da informática para possibilitar esta disseminação, ocorrendo por meio de páginas eróticas e incentivadoras da pedofilia, como também por envio de imagens e ilustrações eróticas de crianças e adolescentes através de redes sociais, e outro.

Quanto à sua prática na internet, recebeu maior proteção por meio da alteração dos artigos 240 e 241, e da inserção dos artigos 241-A a 241-E da Lei 8.069 de 1990, que disciplina o Estatuto da Criança e do Adolescente, referindo-se dentre outros, ao oferecimento, troca, disponibilização, transmissão, distribuição, publicação ou divulgação por qualquer meio,

inclusive de informática ou telemático, fotográfico, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfico envolvendo criança ou adolescente.

> Art. 234 - Fazer, importar, exportar, adquirir ou ter sob sua guarda, para fim de comércio, de distribuição ou de exposição pública, escrito, desenho, pintura, estampa ou qualquer objeto obsceno:
> Pena - detenção, de seis meses a dois anos, ou multa. § 1º. Incorre na mesma pena quem:
> I vende, distribui ou expõe à venda ou ao público qualquer dos objetos referidos neste artigo;
> II realiza, em lugar público ou acessível ao público, representação teatral, ou exibição cinematográfica de caráter obsceno, ou qualquer outro espetáculo, que tenha o mesmo caráter;
> III- realiza, em lugar público ou acessível ao público, ou pelo rádio, audição ou recitação de caráter obsceno (BRASIL, 1940).

Já a Lei nº 13.718/2018 alterou o artigo 218 do Código Penal, tipificando como crime a produção, venda, divulgação e armazenamento de material pornográfico envolvendo crianças e adolescentes.

> Art. 218-C. Oferecer, trocar, disponibilizar, transmitir, vender ou expor à venda, distribuir, publicar ou divulgar, por qualquer meio - inclusive por meio de comunicação de massa ou sistema de informática ou telemática -, fotografia, vídeo ou outro registro audiovisual que contenha cena de estupro ou de estupro de vulnerável ou que faça apologia ou induza a sua prática, ou, sem o consentimento da vítima, cena de sexo, nudez ou pornografia
>
> Pena - reclusão, de 1 (um) a 5 (cinco) anos, se o fato não constitui crime mais grave. (BRASIL, 1940). ~

A disseminação da pornografia infantil na internet é facilitada pela ampla disponibilidade de tecnologias digitais e pela facilidade de compartilhamento de conteúdo online. Os criminosos se utilizam de redes e fóruns especializados, sites obscuros e até mesmo redes sociais para compartilhar, trocar e comercializar imagens e vídeos de exploração sexual de crianças.

É importante ressaltar que a luta contra a pornografia infantil na internet exige o envolvimento de toda a sociedade para garantir a proteção das crianças e adolescentes, a punição dos criminosos e a construção de um ambiente seguro e saudável na internet.

3.2.4 Estelionato

O crime de estelionato está no artigo 171 do Código Penal, e pode acontecer na Internet, por exemplo, através de criação de páginas falsas, no intuito de obter vantagem patrimonial ilícita da vítima enganada, outra forma, é o envio de correio eletrônico falso, passando a impressão de ter sido enviado por entidade de confiança da vítima, no intuito de obter desta pessoa ganho ilícito sobre o seu patrimônio (SILVA, 2017).

> 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.
>
> § 1º - Se o criminoso é primário, e é de pequeno valor o prejuízo, o juiz pode aplicar a pena conforme o disposto no art. 155, § 2°.
>
> § 2º - Nas mesmas penas incorre quem: Disposição de coisa alheia como própria
>
> I - Vende, permuta, dá em pagamento, em locação ou em garantia coisa alheia como própria;
>
> Alienação ou oneração fraudulenta de coisa própria
>
> II- Vende, permuta, dá em pagamento ou em garantia coisa própria inalienável, gravada de ônus ou litigiosa, ou imóvel que prometeu vender a terceiro, mediante pagamento em prestações, silenciando sobre qualquer dessas circunstâncias;
>
> Defraudação de penhor
>
> III - defrauda, mediante alienação não consentida pelo credor ou por outro modo, a garantia pignoratícia, quando tem a posse do objeto empenhado;
>
> Fraude na entrega de coisa
>
> IV - Defrauda substância, qualidade ou quantidade de coisa que deve entregar a alguém;
>
> Fraude para recebimento de indenização ou valor de seguro
>
> V - Destrói, total ou parcialmente, ou oculta coisa própria, ou lesa o próprio corpo ou a saúde, ou agrava as consequências da lesão ou doença, com o intuito de haver indenização ou valor de seguro;
>
> Fraude no pagamento por meio de cheque
>
> VI - Emite cheque, sem suficiente provisão de fundos em poder do sacado, ou lhe frustra o pagamento
>
> § 3º - A pena aumenta-se de um terço, se o crime for cometido em detrimento de entidade de direito público ou de instituto de economia popular, assistência social ou beneficência.
>
> Estelionato contra idoso
>
> § 4o Aplica-se a pena em dobro se o crime for cometido contra idoso. (Incluído pela Lei nº 13.228, de 2015) (BRASIL, 2015).

Existem diversas formas de estelionato na internet. Uma delas é a criação de páginas falsas, que imitam sites legítimos de empresas ou instituições financeiras, com o intuito de coletar informações pessoais, como senhas e números de cartão de crédito, dos usuários desavisados. Esses golpes, conhecidos como *phishing*, são geralmente realizados por meio de e-mails ou links maliciosos enviados aos usuários, que são induzidos a fornecer suas informações confidenciais.

Outra forma comum de estelionato na internet é a venda de produtos ou serviços falsos. Os golpistas criam anúncios atraentes em sites de comércio eletrônico ou em redes sociais, oferecendo produtos com preços muito abaixo do mercado. No entanto, após o pagamento, o comprador descobre que o produto não existe ou não é entregue conforme o combinado.

3.2.5 Falsa identidade e falsidade ideológica

No crime de falsa identidade, um indivíduo se passa por outro, utilizando dados e até mesmo senhas, em proveito próprio ou alheio, podendo causar dano. As credenciais de acesso a uma rede social, por exemplo, quando usadas por outra pessoa que não o seu titular, com o fim de obter vantagem ou causar dano, pode ser integrado ao crime do art. 307 do Código Penal (falsa identidade).

Existe um projeto de lei de autoria do Deputado Nelson Marchezan Junior que pretende alterar o crime do art. 307 sob o argumento de que “a lei 12.737, de 2012, que dispôs sobre a tipificação penal de delitos informáticos, não tratou especificamente dessa conduta, tendo se baseado na invasão de dispositivo informático, na interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou na informação de utilidade pública e a falsificação de cartão de crédito ou débito” de modo que “faz-se necessário complementar a legislação penal, tipificando o uso de falsa identidade através da rede mundial de computadores” o que foi algo muito equivocado.

Observe a redação do art. 307 do Código Penal:

> 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).

O projeto de lei 7758/2014[10] prevê o seguinte:

> Art. 1° Esta lei tipifica penalmente o uso de falsa identidade na rede mundial de computadores.
>
> Art. 2° O art. 307 do Decreto-Lei no 2.848, de 7 de dezembro de 1940, passa a vigorar acrescido do seguinte parágrafo único:
>
> Art. 307. Atribuir-se ou atribuir a terceiro, falsa identidade, inclusive por meio da rede mundial de computadores ou qualquer outro meio eletrônico, com o objetivo de prejudicar, intimidar, ameaçar, obter vantagem ou causar dano a outrem, em proveito próprio ou alheio:
>
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave

O delito de falsa identidade comumente se confunde com o de falsidade ideológica. Entretanto deve-se atentar para suas significativas diferenças: Enquanto o primeiro encontra-se tipificado no artigo 309 do Código Penal e, para sua consumação é necessário que o perfil falso seja criado com base em uma pessoa real e que esteja manifestada vontade em obter vantagens, entretanto não há necessidade da configuração do dano.

Já o crime de falsidade ideológica está previsto no art. 299 do Código Penal. Nesse crime há inserção de dados falsos ou omissão de algo que deveria constar, em documentos públicos ou particulares, com intenção de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante. Isto seria o mesmo que mentir em um documento, ou alterar seu conteúdo, para modificar o direito de alguém (alterando um direito ou uma obrigação) para obter algum tipo de vantagem.

Vejamos o art. 299 do Código Penal:

> 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

---

[10] (BRASIL. Câmara dos Deputados. Projeto de Lei nº 7.758, de 02 de julho de 2014. Modifica o disposto no art. 307 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal. Brasília: Câmara dos Deputados, 2013. Disponível em: https://www.camara.leg.br/proposiçõesWeb/fichadetramitacao?idProposicao=619448. Acesso em: 11 jun. 2023).

> 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, de quinhentos mil réis a cinco contos de réis, se o documento é particular (BRASIL, 1940).

Diante de todo o exposto, verifica-se que há necessidade de analisar o caso concreto para que se possa compreender e enquadrar a prática delitiva praticada pelo fake de acordo com seus atos efetivamente praticados e danos ou prejuízos causados para os cidadãos que tiveram sua identidade ou imagem utilizada de forma criminosa.

Já o delito de dano está previsto no artigo 163 do Código Penal, referindo-se à destruição, inutilização ou deterioração de coisa alheia, crime este que vem aumentando a cada dia na internet, sendo observado através da disseminação de vírus por computadores, vírus estes que são pequenos programas capazes de provocar prejuízo às informações armazenadas em um computador, sendo normalmente a vítima, qualquer usuário que venha a recebê-lo pela Internet.

O Código de Defesa do Consumidor, no Título II - Das Infrações Penais da Lei 8.078 de 1990, trata dos crimes contra o consumidor. Entre eles, estão os artigos 67 e 68, que se referem a crimes contra o consumidor praticado através da Internet. O artigo 67 refere-se ao ato de fazer ou promover publicidade que sabe ou deveria saber ser enganosa ou abusiva, tendo o artigo o objetivo de buscar uma punição de maneira geral (SILVA, 2017).

Já o artigo 68, refere-se ao ato de fazer ou promover publicidade que sabe ou deveria saber ser capaz de induzir o consumidor a se comportar de forma prejudicial ou perigosa a sua saúde ou segurança, assim o artigo traz um alcance de maior gravidade e consequentemente uma necessidade punitiva mais eficaz. Para este tipo de crime contra o consumidor, o criminoso na forma virtual utiliza página eletrônica ou envio de mensagens por correio eletrônico a pessoas ou grupos, sem prévia determinação pessoal, expondo imagens e textos, do qual se promove uma publicidade enganosa ou abusiva.

Em plena era digital é extremamente complicado legislar sobre a matéria de crime cibernético. Diante dessa situação, alguns deputados formulam projetos de leis para deter a ação dos criminosos, sem muito sucesso, visto que é lento seu processo de aprovação.

A falta de leis específicas demonstra a vulnerabilidade do Brasil, tornando-o um verdadeiro paraíso para todo o tipo de invasão e manipulação ilícita de dados. No entanto, a falta de legislação específica para lidar com os crimes cibernéticos, continua sendo o grande trunfo dos crackers. Sendo assim, se os projetos e decretos de leis fossem aprovados com mais rapidez, seria mais fácil de legislar sobre esses crimes.

Ainda que seja possível realizar o registro da ocorrência pela internet, são poucas as unidades e pessoas qualificadas e preparadas para proceder na investigação desses crimes. Um dos maiores problemas jurídicos dos crimes cibernéticos é a falta de denúncias. Entre outros problemas, faltam delegacias especializadas, compartilhamento de informações, recursos humanos e financeiros. De posse de um maior número de dados e informações, os órgãos competentes poderiam lançar ações preventivas de combates a esses crimes.

3.3 LEGISLAÇÃO BRASILEIRA

A Constituição Federal versa em seu art. 5º, XXXIX que “não há crime sem lei anterior que o defina, nem pena sem previa cominação legal”, sendo assim para que se venha a punir os crimes que são praticados no meio digital, é primordial que o tipo penal venha a se ajustar nas normas já existentes, e as lacunas que eventualmente ainda existam, devem ser preenchidas, sendo que hoje é extremamente essencial a incorporação dos conceitos de informática à legislação vigente.

Até 2012, não existiam leis capazes de punir os crimes cibernéticos próprios, existindo somente legislação acerca dos crimes cibernéticos impróprios. Porém, em decorrência de alguns episódios, como os DDoS - *Distributed Denial of Service* (ataques distribuídos de negação de serviço) a sites do governo e a divulgação de fotos íntimas da atriz Carolina Dieckmann, duas leis foram sancionadas com maior urgência, corrigindo algumas das várias eficiências existentes no ordenamento em relação a essa matéria. São elas, a Lei 12.735/2012, conhecida popularmente como “Lei Azeredo”, e a Lei 12.737/2012, conhecida como “Lei Carolina Dieckmann”.

No ano de 2014, a Lei 12.965/2014, oficialmente chamada de Marco Civil da Internet, foi sancionada pela ex-presidente Dilma Rousseff. Essa lei regula e estabelece princípios, garantias, direitos e deveres para o seu uso, para os usuários e para o próprio Estado.

3.3.1. Lei Azeredo

A Lei n.º 12.735/2012 conhecida como Lei Azeredo, tipifica as condutas realizadas mediante uso de sistema eletrônico, digital ou semelhante, que sejam praticadas contra sistemas informatizados e similares. É um verdadeiro reforço para as demais legislações que venham a ser aprovadas no ordenamento brasileiro, pois traz em seu artigo 4º a determinação de que "os órgãos da polícia judiciária devem criar setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado" (BRASIL, 2012), tudo de acordo como define o regulamento específico de cada órgão policial.

Com esta determinação legal, todos os setores da polícia judiciária brasileira estão providenciando setores especializados em crimes cometidos na esfera virtual, criando no sistema jurídico brasileiro ao auxílio necessário para a edição de legislações dedicadas ao assunto.

3.3.2 Lei Carolina Dieckmann

Em maio de 2012, o Brasil acompanhou um dos casos mais emblemáticos de crime cibernético cometidos no país: o roubo e a divulgação de mais de 30 fotos íntimas da atriz Carolina Dieckmann. Crackers do interior de Minas Gerais e de São Paulo invadiram o e-mail da artista e a chantagearam, por meio de mensagens anônimas, pedindo R$ 10 mil para apagar as imagens. O caso foi parar no Congresso Nacional, que aprovou e colocou em vigor a Lei nº 12.737 apelidada de Lei Carolina Dieckmann, tipificando delitos cometidos em meios eletrônicos e na internet.

Na Lei n.º 12.737/2012 conhecida como Lei Carolina Dieckmann, o legislador foi além, editando a tipificação criminal dos principais delitos informáticos, associados com a invasão de dispositivos informáticos e a publicação indevida de dados computacionais.

O artigo 2°, da Lei 12.737/2012 (Lei Carolina Dieckmann), trouxe alteração ao Código Penal Brasileiro, transformando o seu artigo 154, que trata da invasão de dispositivos informáticos alheios. O Brasil ocupa lugar de destaque no cenário global de cibercrimes. No ano de 2016, 42,4 milhões de brasileiros foram vítimas de crimes cibernéticos. Houve um aumento de 10% no número de ataques digitais em comparação com o ano de 2015. Segundo dados da Norton[11], provedora global de soluções de segurança cibernética, o prejuízo total da prática para o país foi de R$ 10,3 bilhões.

Ainda em seu artigo 2º, alterou o Código Penal Brasileiro, incluindo os artigos 154-A e 154- B ao diploma legal referido. Estes artigos dispõem sobre as maneiras combatidas na esfera virtual, a correspondente sanção legal a ser aplicada aos futuros infratores e a forma de procedimento da devida ação penal (SILVA, 2017).

O artigo 154-A inclui no ordenamento o crime de invasão de dispositivo informático, punindo "quem invadir dispositivo informático, mediante violação dos mecanismos de segurança, visando a obtenção, alteração ou destruição de dados computacionais sem a devida autorização de seu proprietário, ou ainda para instalar vulnerabilidades nos dispositivos a fim de obter vantagem ilícita".

O artigo 154-B estabelece que as ações penais que versem sobre delitos informáticos só poderão ser processadas mediante representação, exceto se o crime for cometido contra a administração direta ou indireta federal, estadual, distrital ou municipal, ou, ainda, contra empresas concessionárias de serviços públicos.

Ainda sobre a Lei n.º 12.737/2012, seu artigo 3º acrescentou parágrafos aos artigos 266 e 298 do Código Penal Brasileiro.

O artigo 266 tipifica o crime de perturbação ou interrupção de serviços ligados à comunicação, e ao incluir os parágrafos, o ordenamento amplia o alcance da norma para os

[11] Investir em sistemas antifraudes não é luxo, é necessidade. Security Report, 2017. Disponível em: < https://www.securityreport.com.br/investir-em-sistemas-antifraudes-nao-e-luxo-e-necessidade/ >.Acesso em: 10 de junho de 2023.

serviços telemáticos ou de utilidade pública, incorporando assim, os ilícitos praticados não só contra o interesse público, mas também, contra dados informáticos (SILVA, 2017).

Já o parágrafo incorporado no artigo 298, que tipifica o crime de falsificação de documento particular, acrescenta os efeitos da norma aos cartões de crédito e de débito, os quais adquiriram do legislador a qualidade de documento particular devidamente reconhecido e protegido pelo ordenamento.

Em suma, essa lei contribui para a proteção dos direitos digitais dos cidadãos, reforça a necessidade de respeito à privacidade e intimidade das pessoas na esfera digital e também busca adequar a legislação brasileira às demandas e desafios do mundo virtual.

Além disso, a Lei Carolina Dieckmann também teve um impacto significativo na conscientização sobre segurança cibernética e na necessidade de cuidados ao lidar com informações pessoais online, destacando a importância da educação digital e do uso responsável da tecnologia.

3.3.3. Marco Civil da Internet

O Marco Civil da Internet, no que lhe concerne, derivou-se do combate ao polêmico projeto de lei 84/99, consequentemente, teve grande participação popular. No decorrer de sua elaboração, foram realizadas consultas públicas, que se dividiram em duas fases: uma com vasta variedade de opiniões, inserindo a sociedade civil e as mais variadas empresas, nacionais e internacionais, do ramo digital, e outra, também com participação popular, mas debatendo cada dispositivo proposto na primeira fase.

Um dos propósitos do Marco Civil da Internet era apontar um documento que se enquadrasse como base para regular os princípios gerais do Marco Civil. O mencionado documento-base foi o publicado pelo CGI.br - Comitê Gestor da Internet no Brasil, chamado “Princípios para a Governança e Uso da Internet no Brasil”. Da mesma forma que a Lei 12.735 e a Lei Dieckmann, o Marco Civil é insuficiente, por mais que pareça ser eficaz ao tratar dos direitos do usuário.

O ato de inserir ferramentas judiciais do mundo físico - como a aquisição de ordem judicial - no mundo virtual é contra produtivo, uma vez que as velocidades entre os dois mundos são inconciliáveis. Ao mesmo tempo que o primeiro é mais moroso, o segundo necessita cada vez mais celeridade. Desta forma, exige-se com ainda mais urgência renovações jurídicas na legislação brasileira, no que refere aos crimes cibernéticos e segurança cibernética nacional.

4 DA DICOTOMIA ENTRE TERRITORIALIDADE E INTERNET

4.1 O ALINHAMENTO ENTRE ESTADO E CIBERESPAÇO

> Um dos temas mais sensíveis do ciberespaço, mesmo após décadas de sua internacionalização, continua a ser o da convivência de diferentes atores, culturas, interesses e demandas no mesmo ambiente. Embora interações que ultrapassem fronteiras político-geográficas não sejam necessariamente uma novidade promovida pela internet, por ela certamente foram impactadas a frequência, a profundidade e a variedade das demandas internacionais. Nesse contexto, o exercício de poder estatal, por meio de um sistema normativo ou do sistema de coerção, é cada vez mais desafiado.

> Em razão de sua natureza global, a internet desafia especialmente as normas que são baseadas na territorialidade. A territorialidade é o critério básico pelo qual os estados, ainda no século XVII, dividiram o alcance de sua soberania, sobre determinado povo situado em determinado limite geográfico. Dessa forma, foram construídos elementos de aplicação de leis, competência de tribunais para resolver os conflitos sociais e mecanismos de observância das ordens estatais. Eles são encontrados, por exemplo, nas disposições legais sobre lei aplicável - no caso do Brasil reunidas principalmente na Lei de Introdução às Normas do Direito Brasileiro (LINDB) - que determinam que a um imóvel deve seguir a lei do país onde se situa ou de competência de um tribunal - que podem ser encontradas no Código de Processo Civil - do lugar em que o réu do processo reside. Esses são apenas alguns exemplos que estão não apenas em leis, mas também em tratados internacionais, regionais e legislações de outros países. Em comum, é possível

perceber as recorrentes expressões relativas ao “local”, “lugar”, “residência” e “localização”, que manifestam a base territorial de exercício do poder estatal.

Por sua vez, sendo a internet um espaço por natureza sem fronteiras e tendo como uma de suas principais características a acessibilidade às mesmas coisas em diferentes lugares do mundo, esses conceitos e a forma de exercício da jurisdição, bem como de suas dimensões, demandam reflexões sobre sua adequação e modernização. É necessário que esses exercícios sejam realizados para que os invariantes da internet, assim como quaisquer decisões regulamentadoras relativas à internet, sejam coerentes com os princípios que regem a Governança da internet e reflitam a proteção aos direitos humanos construída a partir da segunda metade do século XX.

Repensar a jurisdição, o papel dos Estados e da necessidade de coordenação e cooperação no ambiente da internet são pautas importantes das primeiras décadas do século XXI. As questões a serem enfrentadas são as mais diversas: vão desde a segurança para que os diferentes atores possam operar na internet, definições de critérios regulatórios, desenvolvimento de meios de cooperação, até distribuição de nomes de domínio, entre outros.

Observa-se que no artigo 109 da CF não há nenhum inciso ou parágrafo que menciona crimes de informática, concluindo-se que a competência, a princípio, não poderia ser federal, a não ser que o crime seja praticado contra a União, suas autarquias ou empresas públicas. Mas o presente trabalho preocupou-se mais com os crimes cometidos entre particulares, pois estes são mais comuns. Porém, o caráter internacional desses crimes traria problemas para a justiça estadual, pois compete a essa justiça, segundo Tourinho Filho: “[…] julgar as causas da competência dentro das Circunscrições Territoriais em que está dividido o Brasil: Estados – Membros e Distrito Federal”.[12] A solução a este problema é dada pelos Princípios da Territorialidade e Extraterritorialidade.

[12] TOURINHO FILHO, Fernando da Costa. Processo Penal. Vol.II. 24.ed. ver. e atual. São Paulo: Saraiva, 2002, p.82.

4.2 O ALINHAMENTO NO ESPECTRO PENAL

A lei penal vigora dentro dos limites em que o Estado exerce a sua soberania. É o denominado princípio da territorialidade que, inclusive, é aplicado no território brasileiro quando o crime é cometido nele, não importando a nacionalidade do autor e da vítima do delito. O Código Penal adotou os princípios da territorialidade, da proteção, da justiça universal, da nacionalidade ativa e da representação.

O artigo 6° do Código Penal nada mais é que a teoria da ubiquidade, que afirma que o lugar do crime é aquele em que se realizou qualquer dos momentos do *iter criminis*. Acontece que o *iter criminis* dos crimes informáticos, via de regra, ocorre em lugares diferentes.

O estudo do artigo 7° do Código Penal é muito importante, pois ele trata dos casos especiais de extraterritorialidade através da aplicação de Princípios como o da proteção, nacionalidade, justiça universal e da representação. O STF já decidiu que cabe à Justiça Estadual o julgamento de crime cometido por brasileiro no exterior, salvo se for em detrimento da União, suas autarquias ou empresas públicas.

O art. 69 do Código de Processo Penal em seu primeiro inciso dispõe que a regra de fixação de competência será o da consumação da infração. Se não for possível descobrir o local de consumação da infração, parte-se para a segunda regra, qual seja a do domicílio do réu ou sua residência; em seguida passa-se para a natureza da infração.

Segundo Francesco Carnelutti: “A determinação da competência territorial de primeiro grau funda-se, pois, no lugar em que foi cometido o delito; ele é chamado de local do delito”.[13]

Já existem alguns informativos sobre o tema no STJ. Analisadas pode se concluir que o tema não é tão pacífico como parece ser, e ao contrário, bastante divergente:

> As vítimas foram constrangidas mediante mensagens eletrônicas ameaçadoras enviadas pela internet, segundo as quais se pretendia infligir-lhes mal injusto se não providenciassem valores, o que levou as vítimas a ofertar a notícia-crime ao Ministério Público. Assim, não há como entender existir mera tentativa punível, pois o crime se consumou no local em que os ofendidos receberam os e-mails e deles tomaram conhecimento, local em que se fixa a competência, mostrando-se sem influência o de onde foram enviadas as mensagens.[14]

> A Turma, por maioria, decidiu que é da competência da Justiça Federal o crime previsto no art. 218 do CP quando o paciente fotografou, filmou e publicou, na rede internacional de computadores, imagens de menor, retratando a prática de atos libidinosos, inclusive sexo explícito.[15]

Os crimes que acontecem pelo uso da internet são crimes interfronteiriços, ou seja, sem fronteiras que os separam de um local ou de outro. São crimes que acontecem em toda rede.

Tendo em mente que o crime acontece em toda a rede e que esta é transnacional, poderia dizer que os crimes de informática são considerados crimes à distância. Mas surge um problema, qual seja, o fato de que os crimes à distância só se dão em países diferentes e, sabe-se que o cibercrime se dá, inclusive, no ambiente nacional. Então, por ser um conceito mais amplo, acredita-se ser mais conveniente, definir os crimes virtuais como crimes plurilocais. O fato de considerar o crime informático como crime plurilocal, não quer dizer que ele só ocorra no âmbito nacional, mas sim que, em um conflito de

---

[13] CARNELUTTI, Francesco. Lições sobre o Processo Penal. Vol.II. Campinas: Bookseler, 2004, p.306.
[14] CC 40.569-SP, Rel. Min. José Arnaldo da Fonseca, julgado em 10/3/2004.
[15] HC 24.858-GO, Rel. originário Min. Paulo Medina, Rel. para acórdão Min. Fontes de Alencar, julgado em 18/11/2003.

conceitos, por analogia, considerar os cibercrimes como sendo crimes plurilocais seria mais sensato, por estes serem mais amplos do que os crimes à distância.

Sendo assim, o estudo vai muito além das respostas que já foram dadas em linhas anteriores. A internet é um meio que facilita a ofensa e o cometimento de crimes, até mesmo por conta do anonimato.

O professor Carlos Eduardo A. Japiassú[16] classifica como delinquencia internacional por contaminação essa atual modalidade de crime, que se manifesta quase que simultaneamente em diversos lugares dada a facilidade das comunicações e do mundo global

> Denomina-se delinquência por contaminação ou difusão ao conjunto daqueles crimes, convencionais ou não, que se manifestam mais ou menos ao mesmo tempo em lugares diversos, com as mesmas características, passando de um Estado a outro, por assim dizer, epidemicamente, graças à rapidez dos meios de transporte, à instantaneidade das comunicações e à atividade dos *mass media*. Este último aspecto transformou o crime na notícia por excelência e, com isso, o potencializou.

Para José Cretella Neto: "[…] por analogia, cabe aos crimes informáticos, a aplicação do artigo 42 da lei de imprensa".[17]

> Art. 42. Lugar do delito, para a determinação da competência territorial, será aquele e, que for impresso o jornal ou periódico, e o do local do estúdio do permissionário ou concessionário do serviço de radiodifusão, bem como o da administração principal da agência noticiosa.

Segundo Démocrito Ramos Reinaldo Filho: "O STJ possui uma tendência a aplicar a lei de imprensa para regular delitos na internet. […] Ademais, a Internet é um

[16] JAPIASSÚ, Carlos Eduardo A. O direito penal internacional e os crimes internacionais. Disponível em: <https://revistas.faa.edu.br/FDV/article/download/505/383/751>. Acesso em: 10 de junho de 2023 p.13
[17] CRETELA NETO, José. Comentários à Lei de Imprensa: Lei n° 5.250, de 09.02.1967. Rio de Janeiro: Forense, 2004, p. 220.

veículo de publicação e divulgação de informações que satisfaz o caráter de periodicidade".[18]

Acredita-se que, através do conceito da Lei de Imprensa não seria demais incluir a Internet nesse mesmo conceito. Demócrito Ramos Reinaldo Filho cita em sua obra que: "Em nosso país, uma decisão da oitava Câmara Criminal do Tribunal de Justiça do Rio de Janeiro, tomada por maioria de votos, reconheceu a possibilidade de configuração como crimes de imprensa a ofensa cometida em página da Internet."[19]

O mesmo autor afirma que: "As novas formas de comunicação eletrônica levantam uma discussão em torno de problemas de jurisdição."[20] Este também sugere a criação de novos parâmetros para se decidir a competência para esses crimes, pois não existe fronteiras que separe a competência.

Assim sendo, é óbvio que a nível nacional os Estados devem reajustar suas políticas legislativas, mas no que condiz num nível internacional necessita-se estabelecer mecanismos de cooperação como forma de ampliação do combate a esses crimes, como tratados que unifique e oriente os procedimentos na condução das investigações e da própria fase judicial em cada Estado.

Ficaria difícil falar em aplicação da lei quando crimes acontecerem fora do território nacional, até mesmo porque as comunicações eletrônicas deixam registros em diferentes jurisdições territoriais.

---

[18] REINALDO FILHO, Demócrito Ramos. Responsabilidades por Publicações na Internet. Rio de Janeiro: Forense, 2005, p.100.
[19] REINALDO FILHO, Demócrito Ramos. Responsabilidades por Publicações na Internet. Rio de Janeiro: Forense, 2005, p.103.
[20] REINALDO FILHO, Demócrito Ramos. Responsabilidades por Publicações na Internet. Rio de Janeiro: Forense, 2005, p.151.

Para a corrente que afirma caber o artigo 42 da Lei 5.250/1967, as provedoras de acesso seriam equiparadas a empresas jornalísticas, considerando-se, como local da infração penal, aquele onde tiver hospedado o Site com o conteúdo criminoso.

Dessa forma, se o crime é praticado no Brasil por brasileiro ou estrangeiro, através de um site hospedado no Brasil, a competência seria do Brasil, pois utilizar-se-ia o Princípio da Territorialidade. Nesse caso seria, estadual, ou seja, do Estado onde se encontra situado a sede do Site no Brasil. Porém, supondo que o resultado do crime tenha se dado no exterior, aplicar-se-ia o artigo 42 da lei de imprensa, porém, para punir o infrator deve-se utilizar as regras estabelecidas pelo artigo 7° do Código Penal Brasileiro.

Com a aplicação dos Princípios da Extraterritorialidade, a competência territorial estadual será sempre aplicada, exceto nos casos em que o crime for cometido contra a União

5 DA POSSIBILIDADE DE EXECUÇÃO DE SENTENÇA DO PODER JUDICIÁRIO BRASILEIRO SOBRE CONDUTA PRATICADA EM OUTROS PAÍSES

5.1 CASO DO INQUÉRITO DAS FAKE NEWS (INQUÉRITO Nº 4.781/DF)

É tema recorrente nas graduações o instituto do cumprimento de sentença estrangeira em solo brasileiro. É imprescindível o conhecimento sobre a possibilidade de sua execução de acordo com os procedimentos e as regras do STJ. Entretanto, tema que também trata de território estrangeiro e procedimentos dos tribunais superiores vem inquietando a sociedade jurídica acerca de sua legitimidade. Trata-se da possibilidade de execução de sentença do poder judiciário brasileiro sobre conduta praticada em outros países.

O Inquérito Nº 4.781/DF, popularmente conhecido como Inquérito das Fake News, trata-se se um procedimento instaurado pelo Supremo Tribunal Federal para investigar a divulgação de notícias falsas com objetivos eleitorais e tem como relator o Ministro Alexandre de Moraes.

Diversas polêmicas versam sobre o referido inquérito, sobretudo de cunho político. Entretanto, estas não serão tema do nosso estudo, tendo em vista que já foram questionadas e respondidas em âmbitos recursais.

Destarte insta transpor parte a decisão do Exmo. Ministro Alexandre de Moraes acerca do tema:

> Como qualquer entidade privada que exerça sua atividade econômica no território nacional, a rede social Facebook deve respeitar e cumprir, de forma efetiva, comandos diretos emitidos pelo Poder Judiciário relativos a fatos ocorridos ou com seus efeitos perenes dentro do território nacional; cabendo-lhe, se entender necessário, demonstrar seu inconformismo mediante os recursos permitidos pela legislação brasileira.
>
> A liberdade de expressão é consagrada constitucionalmente e balizada pelo binômio "LIBERDADE E RESPONSABILIDADE", ou seja, o exercício desse direito não pode ser utilizado como verdadeiro escudo protetivo para a prática de atividades ilícitas. Não se confunde LIBERDADE DE EXPRESSÃO com IMPUNIDADE PARA AGRESSÃO.
>
> Dessa maneira, uma vez desvirtuado criminosamente o exercício da liberdade de expressão, a Constituição Federal e a legislação autorizam medidas repressivas civis e penais, tanto de natureza cautelar quanto definitivas.
>
> A presente medida não configura qualquer censura prévia, vedada constitucionalmente – mesmo porque não há qualquer proibição dos investigados em manifestarem-se em redes sociais ou fora delas, como vários continuam fazendo, não raras vezes repetindo as mesmas condutas criminosas –, mas pretende, com natureza cautelar, fazer cessar lesão ou ameaça de lesão a direito (art. 5º, XXXV, CF) já praticadas pelos investigados, visando interromper a divulgação de discursos com conteúdo de ódio, subversão da ordem e incentivo à quebra da normalidade institucional e democrática, concretizados por meio da divulgação de notícias e fatos falsos e fraudulentos.
>
> Os bloqueios das contas de redes sociais determinados nestes autos, portanto, se fundam na necessidade de fazer cessar a continuidade da divulgação de manifestações criminosas, que, em concreto, materializam as infrações penais apuradas neste inquérito e, que continuam a ter seus efeitos ilícitos dentro do território nacional, inclusive pela utilização de subterfúgios permitidos pela rede social Facebook.
>
> A suspensão parcial das contas e perfis, utilizados aqui como meio para o cometimento dos crimes em apuração, por limitar seus efeitos práticos a postagens feitas em contas registradas no território nacional, caracteriza descumprimento da ordem judicial, tendo em conta seu objetivo, pois permite plena manutenção de divulgação e acesso das mensagens criminosas em todo o território nacional, perpetuando-se verdadeira imunidade para a manutenção da divulgação de ilícitos penais já perpetrados.
>
> A suspensão – repita-se, em relação a fatos pretéritos – deve ser total e absoluta, configurando-se descumprimento a permissão dada pelo provedor implicado para a continuidade de divulgação das contas bloqueadas no Brasil, a partir de acessos em outros países.
>
> Não se discute a questão de jurisdição nacional sobre o que é postado e visualizado no exterior, mas sim a divulgação de fatos criminosos no território nacional, por meio de notícias e comentários por contas que se determinou o bloqueio

> judicial. Ou seja, em momento algum se determinou o bloqueio de divulgação no exterior, mas o efetivo bloqueio de contas e divulgação de suas mensagens ilícitas no território nacional, não importando o local de origem da postagem.
>
> O descumprimento doloso pelos provedores implicados indica, de forma objetiva, a concordância com a continuidade do cometimento dos crimes em apuração, e a negativa ao atendimento da ordem judicial verdadeira colaboração indireta para a continuidade da atividade criminosa, por meio de mecanismo fraudulento.[21]

A decisão do Ministro, na medida em que ele deixa claro que seus efeitos incidem para usuários com acesso à internet por IPs localizados no país, se mostra como um balizador dos efeitos transnacionais da decisão, visto que os sistemas e tecnologia utilizados pelas empresas são aptos a fazer esse corte.

Ainda que os IPs relacionados à prática delituosa estejam em outros países, o crime tem seus efeitos produzidos no Brasil. Com isso, a decisão não extrapola os limites da jurisdição nacional, tendo em vista a salvaguarda dos interesses das vítimas e do sistema eleitoral brasileiro, que fora posto em cheque.

Entretanto, ainda que observados os limites da jurisdição nacional, é preciso registrar que, em se tratando de internet, qualquer reforço a limites territoriais torna-se um desafio. A amplitude de alcance da internet e a dificuldade em seu controle de uma forma centralizada podem e tendem a sofrer alterações, tendo em vista o obstáculo para que se imponha decisões de sistemas jurídicos diante de toda complexidade envolvida.

Contudo, a despeito da execução da decisão, a autodeterminação e a soberania fazem com que o poder jurisdicional, exclusivo e supremo, esteja definido pelos limites territoriais. Com isso, quando necessária a execução de uma decisão extraterritorial, é necessário que o Estado reconheça a decisão prolatada pelo outro Estado e se disponha a executá-la. Nesse sentido, cada Estado possui suas próprias regras de reconhecimento de decisão estrangeira. Por isso a complexidade do tema.

De certo o Exmo. Ministro Alexandre de Moraes estava ciente do seu papel e da complexidade da sua decisão, que embora recheada de polêmicas, larga na frente no sentido de direcionar, não só o Brasil, como outros Estados, no caminho de haver um procedimento

---

[21] Inq. 4.781/DF, Min. Alexandre de Moraes, decisão do dia 30/07/2020, disponível em: https://www.migalhas.com.br/arquivos/2020/7/C276DD20C52256_Despacho-Facebook.pdf

uniformizado no trato dos limites transnacionais em litígios que transcendem barreiras territoriais dada a fluidez das relações modernas. Traça-se um rumo para que acordos entre Estados sejam celebrados no sentido da colaboração, homogeneização e regulamentação dos processos.

5.2 CASO DO REsp 1745657/SP

Vejamos também o caso do REsp 1745657/SP, que consiste em determinar a competência da Poder Judiciário Brasileiro para a determinação do fornecimento de registros de acesso de endereço de e-mail, localizado em nome de domínio genérico ".com".

O entendimento foi estabelecido pela Terceira Turma do Superior Tribunal de Justiça (STJ), sob relatoria da Exma. Ministra Nancy Andrighi ao manter acórdão do Tribunal de Justiça de São Paulo (TJSP) que determinou o prosseguimento da execução de multa de R$ 310 mil contra a Microsoft, por descumprimento de ordem judicial para fornecer informações de um usuário de e-mail que teria lançado ameaças contra uma pessoa e uma empresa. Observemos o acórdão, que logo se transformou em jurisprudência da mesma corte:

> Em conflitos transfronteiriços na internet, a autoridade responsável deve atuar de forma prudente, cautelosa e autorrestritiva, reconhecendo que a territorialidade da jurisdição permanece sendo a regra, cuja exceção somente pode ser admitida quando atendidos, cumulativamente, os seguintes critérios: (i) fortes razões jurídicas de mérito, baseadas no direito local e internacional; (ii) proporcionalidade entre a medida e o fim almejado; e (iii) observância dos procedimentos previstos nas leis locais e internacionais.
>
> Quando a alegada atividade ilícita tiver sido praticada pela internet, independentemente de foro previsto no contrato de prestação de serviço, ainda que no exterior, é competente a autoridade judiciária brasileira caso acionada para dirimir o conflito, pois aqui tem domicílio a autora e é o local onde houve acesso ao sítio eletrônico onde a informação foi veiculada, interpretando-se como ato praticado no Brasil. Precedente.
>
> É um equívoco imaginar que qualquer aplicação hospedada fora do Brasil não possa ser alcançada pela jurisdição nacional ou que as leis brasileiras não sejam aplicáveis às suas atividades.
>
> Tem-se a aplicação da lei brasileira sempre que qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet ocorra em território nacional, mesmo que apenas um dos dispositivos da comunicação esteja no Brasil e mesmo que as atividades sejam feitas por empresa com sede no estrangeiro[22].

[22] REsp 1.745.657-SP, Rel. Min. Nancy Andrighi, Terceira Turma, por unanimidade, julgado em 03/11/2020, Disponível em: https://processo.stj.jus.br/jurisprudencia/externo/informativo/?aplicacao=informativo&acao=pesquisar&livre=@cnot=017938

Ao manter o acórdão do Tribunal de Justiça de São Paulo, a Exma. Ministra Nancy Andrighi afirmou que o Marco Civil da Internet previu expressamente em seu artigo 11 a aplicabilidade a legislação brasileira a operações de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet, mesmo que apenas um dos dispositivos da comunicação esteja no Brasil e que as atividades sejam feitas por empresa com sede em território estrangeiro.

Com o advento do Marco Civil da Internet e com as, cada vez mais recorrentes, provocações ao judiciário nacional, é de se esperar a aplicação cada vez mais corriqueira da legislação brasileira a atos que ocorram com usuários brasileiros.

Com essa decisão, ficou definido que o Poder Judiciário brasileiro é competente para determinar a quebra do sigilo de dados, sempre que o ato ilícito praticado na internet atingir pessoas residentes no Brasil, independentemente de onde os dados estejam hospedados, não podendo servir a hospedagem de dados em países estrangeiros de subterfúgios para a prática de atos considerados ilícitos em nosso ordenamento jurídico.

Aos poucos, dada a característica mutacional, inerente às tecnologias e à internet, o Estado vai se moldando aos novos desafios dos usuários. Novos litígios, novos crimes e novas provocações são observadas diariamente, e assim será por muitos anos. Cabe aos legisladores e até aos chefes de Estado organizarem-se a fim de suprir as novas demandas que surgem em âmbito interno e externo. Já podemos observar alguns passos, como o Marco Civil da Internet, mas ainda há muito a ser feito.

6 CONSIDERAÇÕES FINAIS

Na contemporaneidade, com a diminuição das fronteiras globais e, à medida que o uso da internet aumenta, observamos a constante mutação das relações. Sejam elas pessoais, organizacionais, laborais e até criminais. E são estas que mais nos preocupam. Todo período pós revolução é como um quadro em branco, onde qualquer coisa pode surgir.

É nesse sentido que as atividades criminosas também se moldam. E enquanto a criatividade criminosa se expande em progressão geométrica, o Estado, em seu poder legislador e correicional engatinha. É nesse vazio em que as mentes criminosas se destacam.

Diariamente o judiciário brasileiro é provocado para versar sobre temas relacionados ao direito digital e seus efeitos. E dentre as suas maiores dificuldades está a execução de sentença de crime praticado na internet em território estrangeiro. A legislação está surgindo gradativamente, como o Marco Civil da Internet. Entretanto, muitas mutações e complementações ainda se fazem e farão necessárias por muitos anos. Talvez pra sempre, dada a criatividade criminal.

Uma das principais preocupações dos conflitos de jurisdição na internet é a falta de harmonização das leis e regulamentações entre diferentes países. Cada nação tem sua própria legislação e procedimentos jurídicos, o que pode resultar em uma multiplicidade de decisões contraditórias em casos semelhantes. Isso gera incerteza jurídica e dificulta a aplicação consistente da lei em um contexto transnacional.

Além disso, os conflitos de jurisdição podem levar a situações em que as decisões judiciais em um país são ineficazes em outros, principalmente quando há dificuldades práticas em sua implementação. Por exemplo, quando uma plataforma online é sediada em um país, mas suas operações e usuários estão distribuídos globalmente, pode ser desafiador para as autoridades de diferentes jurisdições aplicarem suas leis de forma efetiva.

Por fim, a questão dos conflitos de jurisdição na internet não é um problema que pode ser totalmente resolvido, mas sim um desafio em constante evolução que requer atenção contínua. A busca por um equilíbrio entre os interesses das partes envolvidas, a proteção dos direitos fundamentais e a estabilidade da governança da internet é crucial para garantir um ambiente online seguro, transparente e inclusivo para todos os usuários, independentemente de sua localização geográfica.

Problemas a resolver, crimes a investigar e a punir. Os desafios não param de surgir. Esperamos que, ainda que vagarosamente, as mentes brilhantes sobressaiam-se sobre as criminosas e o Estado consiga acompanhar a evolução global e cibernética. Me mantenho na torcida e disposto a acrescentar no que puder.

7 REFERÊNCIAS

ANGELO. Ana Elisa de; SANCHES, Ademir Gasques. Insuficiência das leis em relação aos crimes cibernéticos no Brasil: . Disponível em: <https://www.mpsc.mp.br/campanhas/sobre-a-pedofilia-na-internet>

ARAUJO, Nadia De. Direito Internacional Privado: Teoria e Prática Brasileira. Porto Alegre: Revolução eBook, 2016.

ARAUJO, Nadia de. O que todo advogado precisa saber sobre o Direito Internacional Privado e nunca teve coragem de perguntar! Revista Advocacia Hj. N. 04, jul/2020.

ARAUJO, N.; DE NARDI, Marcelo. Circulação de sentenças judiciais pelo mundo. Valor Econômico, v. 1, p. 1-5, 2017.

ARAUJO, N.; SPITZ, L.; CRUZ, A. A. S.; DEMIDOFF, A. O.; ALMEIDA, B. R.; SENGÈS, G.A.; GOUVEIA, J. C. B. F.; BRANCO, L. G. B.; VIANNA, N. R.; WEBER, P. M. N.. Cooperação Jurídica Internacional no Superior Tribunal de Justiça: comentários à Resolução nº9/2005. Rio de Janeiro: Renovar, 2010. 159p.

BARBIERE, Carlos. **Governança de Dados: Práticas, conceitos e novos caminhos**. Rio de Janeiro: Alta Books, 2019.

BEM, Geyslan Gregório; ESMERALDO, Guilherme Álvaro Rodrigues Maia. Uma Abordagem para Redução do Tamanho de Shellcodes sem Comprometimento do Comportamento. In: **Anais do XXI Simpósio Brasileiro em Segurança da Informação e de Sistemas Computacionais**. SBC, 2021. p. 192-204.

BLUM, Rita Peixoto Ferreira. **O Direito à Privacidade e à Proteção dos Dados do Consumidor**. Digitaliza Conteúdo, 2019.

BOTELHO, Marcos César. A LGPD e a proteção ao tratamento de dados pessoais de crianças e adolescentes. **Revista Direitos Sociais e Políticas Públicas–Unifafibe**, v. 8, n. 2, 2020.

BRASIL Art. 20 da Lei 2.848 de 07 de dezembro de 1940, alterada pela Lei 9.459 de 13 de maio de 1997. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7716.htm>, <http://www.planalto.gov.br/ccivil_03/LEIS/L9459.htm>

CÂMARA, dos Deputados. Projeto agrava pena para crimes cibernéticos: Disponível em:<https://www2.camara.leg.br/camaranoticias/noticias/SEGURANCA/572711-

CARNELUTTI, Francesco. Limiti della giurisdizione del giudice italiano. Rivista di Diritto Processuale Civile, Cedam, Padova, v. IX, parte I, p. 218-223, 1931, p. 218-219

CARREIRAS, Helena et al. Cibersegurança e ciberdefesa em tempos de pandemia. **IDN Brief**, 2020.

CORDEIRO, Silvério; GOUVEIA, Luís Borges. Regulamento Geral de Proteção de Dados (RGPD): o novo pesadelo das empresas? **Relatórios Internos* TRS**, v. 2018, n. 07/2018, 2018.

CORREIA, Pedro Miguel Alves Ribeiro; DA SILVA SANTOS, Susana Isabel. A ação do Estado em matéria de cibersegurança: Estudo de percepções no caso português. Simbiótica. **Revista Eletrônica**, v. 5, n. 2, p. 01-20, 2018.

COUTO, Joana Catarina Pimenta. Auditoria de Cibersegurança-um caso de estudo. **Engtec,** 2018.

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

DE MORAES, Maria Celina Bodin. LGPD: um novo regime de responsabilização civil dito proativo. **Civilistica. com**, v. 8, n. 3, p. 1-6, 2019.

DE TEFFÉ, Chiara Spadaccini; VIOLA, Mario. Tratamento de dados pessoais na LGPD: estudo sobre as bases legais. **Civilistica. com**, v. 9, n. 1, p. 1-38, 2020.

DICIONÁRIO DIREITO O que são crimes virtuais; disponível em: <https://dicionariodireito.com.br/crimes-virtuais>

DINO. Crimes virtuais afetam 42 milhões de brasileiros, juritec**.** 2020

ECOIT, Segurança digital. Crimes cibernéticos: saiba onde denunciar caso você seja vítima: Disponível em: <https://ecoit.com.br/crimes-ciberneticos/>

FELICIANO, Guilherme Guimarães. Informática e criminalidade. Parte I: lineamentos e definições. Boletim do Instituto Manoel Pedro Pimentel, São Paulo, v. 13, n. 2, p. 35-45, set. 2000. p. 42.

FREITAS, Marcos André dos Santos. **Fundamentos do gerenciamento de serviços de TI**. 2. ed. Rio de Janeiro: Brasport, 2013.

GARCIA, Lara Rocha et al. **Lei Geral de Proteção de Dados (LGPD):** Guia de implantação. Editora Blucher, 2020.

GRECO FILHO, Vicente. Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim. São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

HABERMAS, Jürgen. **O discurso filosófico da modernidade**. Editores Katz, 2008.

Inq 4.781/DF, Rel. ministro Alexandre de Moraes, data da decisão: 28 de jul. 2020.

JESUS, Damásio de; MILAGRE, José Antônio. Manual de Crimes. Informáticos: Crimes informáticos. São Paulo: Saraiva, 2016.

JUSBRASIL. Crimes virtuais: conceito e seus tipos: Disponível em:<https://carmo311.jusbrasil.com.br/artigos/307607071/crimes-virtuais-conceito-e-seus tipos>

KOBS, Anderson Vagner; VIEIRA, Sylvio André Garcia. Cibersegurança: identificação de Keystroke por dispositivo Rubber Ducky. **Disciplinarum Scientia| Naturais e Tecnológicas**, v. 22, n. 1, p. 135-149, 2021.

MACHADO, Rodrigo et al. Vazamentos de Dados: Histórico, Impacto Socioeconômico e as Novas Leis de Proteção de Dados. In: **Anais da XVII Escola Regional de Redes de Computadores**. SBC, 2019. p. 154-159.

MARTINS, José et al. SENSIBILIZAÇÃO E TREINO DE SEGURANÇA DA INFORMAÇÃO E CIBERSEGURANÇA. CASO DE ESTUDO PARA DECISORES. **Órgãos da PROELIUM**, 2021.

MENDES, LAURA SCHERTEL FERREIRA et al. **Privacidade, proteção de dados e defesa do consumidor-Linhas gerais de um novo direito fundamental**. Saraiva Educação SA, 2017.

MINISTÉRIO PÚBLICO. Sobre a pedofilia: Disponível em: <http://www.planalto.gov.br/ccivil_03/_Ato2007-2010/2008/Lei/L11829.htm#art2>

PINTO, Walker Douglas Garcia; MOREIRA, João Padilha; DOS SANTOS SILVA, Anderson. Cibersegurança. **Seminário De Tecnologia Gestão E Educação**, v. 2, n. 2, 2020.

PINTO, Walker Douglas Garcia; MOREIRA, João Padilha; DOS SANTOS SILVA, Anderson. Cibersegurança. **Seminário De Tecnologia Gestão E Educação**, v. 2, n. 2, 2020.

PLANALTO. Art. 147 do CP, Decreto Lei 2.848 de 07 de dezembro de 1940. Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>

PLANALTO. Art. 154-A do CP, Lei 12.737 de 30 de novembro de 2012. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>

PLANALTO. Art. 19 do CP Lei 7.492, de 16 de junho de 1986. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l7492.htm>

PLANALTO. Artigos 138, 139 e 140 do CP, Decreto Lei 2.848 de 07 de dezembro de 1940.Disponível em:<http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>

PLANALTO. Artigos 240, 241, 241-A, 241-B, 241-C, 241-D, 241-E do ECA, Lei 8.089, de 13 de julho de 1990. Disponível em: <http://www.planalto.gov.br/ccivil_03/leis/l8069.htm>

PLANALTO. Artigos 67 e 68 do CP, Decreto Lei 2.848 de 07 de dezembro de 1940. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm>

ROQUE, André. A tutela coletiva dos dados pessoais na lei geral de proteção de dados pessoais (LGPD). **Revista Eletrônica de Direito Processual**, v. 20, n. 2, 2019.

ROQUE, Sérgio Marcos. Criminalidade informática: crimes e criminosos do computador. São Paulo: ADPESP Cultural, 2007. P. 25.

ROSSINI, Augusto Eduardo de Souza. Informática, telemática e direito penal. São Paulo: Memória Jurídica, 2004.

SCHWAITZER, Lenora; NASCIMENTO, Natália; DE SOUZA COSTA, Alexandre. Reflexões sobre a contribuição da gestão de documentos para programas de adequação à Lei Geral de Proteção de Dados Pessoais (LGPD). **Acervo,** v. 34, n. 3, p. 1-17, 2021.

SILVA, Ângelo Roberto Ilha da. Crimes Cibernéticos - 2ª Ed. Porto Alegre: Liv. do Advogado Ed., 2017.

TERESO, Marco; PRATAS, António. Cibersegurança e teletrabalho: um mundo de oportunidades de risco. **Atas do VII Encontro Científico da UI&D (ecUI&D 21)**, p. 119.

TERESO, Marco; PRATAS, António. Cibersegurança e teletrabalho: um mundo de oportunidades de risco. **Atas do VII Encontro Científico da UI&D (ecUI&D 21)**, p. 119..

VECTRA, Consultoria e serviços. Conheça os 6 principais tipos de crime na internet: Disponível em:<https://blog.vectracs.com.br/conheca-os-6-principais-tipos-de-crime-na-internet/>

WENDT, Emerson; Jorge, Higor Vinícius Nogueira. Crimes Cibernéticos: Ameaças e procedimentos de investigação. Rio de Janeiro: Brasport, 2013.

YARSHELL, Flávio Luiz; CAMARGO GOMES, Adriano. Internet e Limites da Jurisdição: uma breve análise à luz do Direito Processual Civil. In: WOLKART, Erik Navarro et. al. Direito, Processo e Tecnologia. São Paulo: Thomson Reuters Brasil. 2020.