CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A INFOMARÉ EM ALTA: UMA ANÁLISE DA COMPETÊNCIA NOS CRIMES INFORMÁTICOS IMPRÓPRIOS

Gabriel Videira da Silva

Presidente Prudente/SP

2018

CENTRO UNIVERSITÁRIO ANTÔNIO EUFRÁSIO DE TOLEDO DE PRESIDENTE PRUDENTE

CURSO DE DIREITO

A INFOMARÉ EM ALTA: UMA ANÁLISE DA COMPETÊNCIA NOS CRIMES INFORMÁTICOS IMPRÓPRIOS

Gabriel Videira da Silva

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação do Prof. Mário Coimbra.

Presidente Prudente/SP

2018

A INFOMARÉ EM ALTA: UMA ANÁLISE DA COMPETÊNCIA NOS CRIMES INFORMÁTICOS IMPRÓPRIOS

Monografia apresentada como requisito parcial de Conclusão de Curso para obtenção do grau de Bacharel em Direito, sob orientação do Prof. Mário Coimbra.

Prof. Mário Coimbra

Claudio José Palma Sanchez

Wilton Boigues Corbalan Tebar

Presidente Prudente, 26 de novembro de 2018

Às vezes a vida te bate com um tijolo na cabeça. Não perca a fé. Estou convencido de que a única coisa que me fez continuar foi que eu amava o que eu fazia. Você precisa encontrar o que você ama. E isso vale para o seu trabalho e para seus amores. Seu trabalho irá tomar uma grande parte da sua vida e o único meio de ficar satisfeito é fazer o que você acredita ser um grande trabalho. E o único meio de se fazer um grande trabalho é amando o que você faz. Caso você ainda não tenha encontrado o que gosta de fazer, continue procurando. Não pare. Do mesmo modo como todos os problemas do coração, você saberá quando encontrar. E, como em qualquer relacionamento longo, só fica melhor e melhor ao longo dos anos. Por isso, continue procurando até encontrar, não pare.

Steve Jobs.

Dedico este trabalho às bases da minha vida, meus pais, Sergio e Izilda e ao meu irmão, Matheus.

AGRADECIMENTOS

Em primeiro lugar, a Deus por todo incentivo, companhia e força para continuar, tudo que sou é graças ao Pai, por isso meus sinceros agradecimentos.

Às minhas bases, meus pais, Izilda e Sérgio, e meu irmão, Matheus, pessoas essenciais, que movem o mundo para ver o meu melhor, fica a minha gratidão e minha promessa de buscar ao máximo retribuir todo carinho, cuidado e incentivo recebido.

Aos meus amigos, por me aturarem (principalmente nessa época de monografia), alegrarem, incentivarem e fazerem eu crescer como pessoa nesses últimos anos, fica a minha gratidão! Dentre essas pessoas, deixo meu agradecimento especial para: Odaysa, Karine, Micaele, Eliel, Gustavo (Peixe), Leonardo (Leo), Daniel, Fernando, Larissa, Gabriel Samorano, Allan, José Luiz (Zizo), Rômulo, Beatriz Dias, e Izabela Costa.

Aos amigos e companheiros que o estágio no Ministério Público Federal me deu, em especial, ao Dr. Luís Roberto Gomes, Eliane (Ly), Elza, Francisco, Giovana, Paulo, Verônica e Aline Borba. Fica minha gratidão pela convivência, apoio, paciência e incentivos recebidos todos os dias.

Agradeço ao meu orientador, Dr. Mário Coimbra, exemplo de profissional e pessoa, que me acompanhou e incentivou desde a escolha do tema até a parte final da escrita, sou muito grato pela força, apoio, paciência e compreensão.

Também agradeço ao meu professor, amigo e examinador, Wilton Boigues Corbalan Tebar, exemplo de pessoa e profissional. Sou muito grato pelos ensinamentos, incentivo, por comprar as minhas ideias malucas de artigos, companhia nos eventos e, principalmente, pela amizade.

Por fim, mas não menos especial, deixo meu agradecimento ao professor Cláudio José Palma Sanchez, primeiro professor que tive contato no curso de Direito, talvez o grande responsável pela paixão que nutro por essa ciência. Fica a minha gratidão por todos ensinamentos, confiança e incentivo dados desde o início da minha carreira acadêmica.

RESUMO

Trata-se de monografia criada com o escopo de analisar a competência nos crimes informáticos impróprios. De início tece considerações e explicações sobre era da informação, apresentando considerações históricas acerca da computação e internet, tanto no cenário internacional, quanto no brasileiro, indo da síntese da concepção de número à ascensão da era digital, com a invenção dos meios eletrônicos de cálculo e a internet, objetivando destacar um dos principais atributos da era digital, a velocidade, evidenciando as mudanças provocadas pelo advento dessa nova era, e a dificuldade do Direito se adequar a essas rápidas e constantes evoluções. No segundo momento a pesquisa se dedica à compreensão dos crimes informáticos, tecendo considerações acerca do bem jurídico, classificações (com enfoque especial na que divide os crimes em próprios e impróprios), conceito, "nomen juris", sujeição ativa e passiva, e principalmente, demonstrando as principais peculiaridades do meio informático, que diferenciam esse meio de qualquer outro existente, iniciando a ideia de necessidade de normas específicas aos crimes informáticos, dado que esse meio acaba trazendo inúmeros problemas, como a dificuldade de determinação de competência nesses crimes. Com escopo de avançar na última ideia trabalhada, a monografia traz o cenário normativo dos crimes informáticos no Brasil, destacando especialmente as Leis 12.735/12 e 12.737/12 como as primeiras normas darem tratamento específico aos crimes informáticos, traçando uma evolução normativa, de forma a evidenciar o atraso normativo do direito brasileiro, e o pautando como um dos principais motivos para problemas tanto de ordem penal objetiva, como no direito processual tendo, como exemplo principal a dificuldade de atribuição de competência nos crimes informáticos. Na última parte a monografia trata do objeto principal, a análise de competência dos crimes informáticos, tecendo primeiro considerações gerais acerca da competência, com conceito e destaque às principais regras e critérios, e depois adentrando de fato no objetivo, separando a análise em critérios para determinação da competência de justiça, nesse caso destacando a residualidade da justiça estadual e destacando as hipóteses de competência federal, e na segunda na análise, a competência de foro, a fim de determinar o juízo localidade será competente para julgar esses crimes, trazendo regras de caráter geral e destacando casos específicos em que a jurisprudência deu uma maior atenção, como no caso dos crimes contra à honra, racismo, ameaça, crimes contra a criança e adolescente, e patrimônio. Ao final traça como as grandes dificuldades a adoção da teoria do resultado e não a teoria da ubiquidade pelo Código de Processo Penal, e, acima de tudo, o atraso normativo, salientando que as peculiaridades do meio informático impõe a necessidade de criação de normas específicas ainda que sejam crimes informáticos impróprios, pois só com atualização do ordenamento a análise da problemas como a análise de competência serão definitivamente solucionados.

,

Palavras-chave: Crime informático. Competência. Era da Informação. Computação. Digital.

ABSTRACT

It is about a monograph that was created with the scope of analyzing the competence of the improper computer crimes. At the start, it makes considerations and explanations about the information age,.presenting historical considerations about computing and internet, as much in the international scene as in the Brazilian scenario, from the synthesis of number, to the rise of the digital age, with the invention of electronic media of calculation and the internet, seeking to highlight one of the main attributes of the digital age, the speed, showing the chances that was brought by the advent of this new era, and also the difficulty of the law to adapt to these fast and constant evolutions. In a second moment, the research is dedicated to the understanding of cybercrimes, making considerations about the legal interest, classifications (with a special focus on dividing crimes into proper and improper), concept, *nomen juris,* active and passive subjection, and mostly, demonstrating the main peculiarities of the computer environment, which distinguish this one from any other existing one, starting with the idea of the need for specific laws for cybercrimes, once that this causes endless problems, like the difficulty of determining the competence of these crimes. With the objective to advance in the last worked idea, the monograph brings the normative scenario of cybercrimes in Brazil, contrasting, especially, the Laws 12.735/12 and 12.737/12, as the first rules to give specific treatment to cybercrimes, tracing a normative evolution, which brings the normative backwardness of Brazilian law, that show the main problems, as much criminal as procedural, having as biggest example the difficulty of assigning competence in cybercrimes. In the last part of the monograph, it deals with the main object, the competence analysis of cybercrimes, bringing general considerations about the competence, with concept and emphasis to the principal rules and criteria, and then, entering the objective, separating the analysis into criteria for determination of the jurisdiction competence, in this case, highlighting the residuality of the state justice and contrasting the hypotheses of federal competence. In the second moment, it will brings the analysis about the forum competence,seeking to determinate the locality judgment to judge about those crimes, bringing rules of general character and showing specific cases in which jurisprudence has given greater attention, like it is in the cases of crimes against honor, racism, threat, crimes against the children and teenager, and also patrimony. In the end, show how as one of the biggest difficulties, the adoption of the theory of the result, instead of the theory of the ubiquity, by the Criminal Procedure Code, and, above all, the normative backwardness, emphasizing that the peculiarities of the computer mean, makes the need to create specific rules, even though they may be improper crimes, because only with an update of the law, the analysis of the problems and the analysis about competence will be definitively solved.

Key words: Cybercrime. The Information Era. Computation. Digital.

SUMÁRIO

1 INTRODUÇÃO

A presente monografia utilizou-se predominantemente do método dedutivo a fim de analisar a competência penal nos crimes informáticos impróprios.

Em um primeiro momento, a pesquisa realizou uma análise histórica acerca da era da computação e internet, de forma a evidenciar os principais aspectos da chamada “era da informação” e seu principal atributo, a velocidade, dado que o advento das tecnologias computacionais revolucionou a sociedade em vários aspectos, tanto no que diz respeito à velocidade e facilitação do acesso à informação, quanto em um aspecto temporal e evolutivo, pois, nos primórdios da humanidade o homem sempre esteve acostumado com evoluções que se pautavam em décadas e séculos, com o advento dessa nova era, a evolução é exponencial e constante, o período de um ano, um prazo considerado irrisório, pode marcar a obsolescência de várias tecnologias, e aí entra o papel do Direito, levantando a questão da dificuldade dessa ciência se amoldar as evoluções tão rápidas dessa era.

No histórico da computação, observou que o advento da computação sempre esteve atrelado à dilemas matemáticos, para isso traçou uma linha evolucional, partindo dos primórdios da humanidade, quando o homem dissociou os números de objetos, passando pelos primeiros instrumentos mecânicos de cálculo até chegar no advento da era da computação, onde o cálculo passa a ser feito por meios eletrônicos, o que revoluciona o modo inicia a tão famigerada “era da informação”. Após a evolução mundial, foi demonstrada ainda a evolução no aspecto nacional, demonstrando os dispositivos informáticos que marcaram o início dessa era no Brasil.

Em uma segunda parte do histórico, foram feitas considerações sobre a internet e seu advento tanto global, quanto no Brasil, dado que essa é uma das inovações mais importantes para a era da informação, pois, possibilitou que o mundo inteiro se conecta-se, fomentando ainda mais o atributo da velocidade, facilitando a comunicação, o acesso às informações, e até fomentando as práticas criminosas a partir desse meio, já que a tecnologia tem uma neutralidade, podendo ser utilizada tanto ao bem quanto ao mal.

Superadas as considerações históricas e conceituais atinentes a era da informação, a monografia buscou demonstrar a realidade dos crimes informáticos,

uma realidade que nasce com essa nova era e vem tendo grandes impactos ao redor do mundo e no Brasil, que já figura como uma das nações que mais sofrem com esse tipo de crime.

Para compreensão das bases dos crimes informático, iniciou analisando a objetividade jurídica, passou pelas classificações evidenciando que existem delitos que dependem exclusivamente do meio informático, lesionando o bem jurídico especifico, o sigilo e a integridade de dados, os chamados crimes informáticos próprios, e, existem crimes comuns que se utilizam dos meio informático e suas facilidades, os crimes informáticos impróprios, chegando ao conceito de que o crimes informáticos são todas as práticas que se utilizam dos aparatos tecnológicos para agredir o sigilo e a integridade de dados.

Analisado o conceito, ainda foram explanadas considerações acerca do nomen juris, justificando a adoção da nomenclatura “crimes informáticos”.

Após, foi feita uma análise da sujeição ativa e passiva, destacando que vem se alterando o estigma de que o criminoso informático necessita de conhecimentos específicos, e demonstrando os principais tipos de criminosos informáticos. Do ponto de vista da sujeição passiva foram feitas observações a fim de destacar o papel ativo da vítima para tais crimes, de modo que a apresentar a prevenção como melhor remédio para essa criminalidade.

Ao final da segunda parte, foram realizadas considerações acerca das peculiaridades do meio informático como internacionalidade, a velocidade, o anonimato, a intangibilidade, a pluralidade e a ubiquidade, que tornam esse ambiente diferente de qualquer outro. De forma a evidenciar os problemas gerados como a dificuldade de determinação da competência, e iniciar a ideia da necessidade da criação de normas específicas, tendo em vista essas peculiaridades.

Avançando, a monografia teceu considerações acerca da disciplina legal dos crimes informáticos no Brasil, dividindo em antes e depois das Leis 12.735/12 e 12.737/12, as primeiras normas a tratar de forma mais específica a matéria de crimes informáticos no Brasil, a fim de evidenciar o atraso normativo brasileiro, e o papel desse como fator determinante para problemas como o da determinação da competência nos crimes informáticos.

Por fim, a monografia entrou na questão principal, a discussão da competência nos crimes informáticos impróprios. Para isso, primeiro teceu considerações gerais de competência, de forma a estabelecer as bases para

análise, conceituando competência, traçando os passos de sua atribuição, e explicitando os três principais critérios de atribuição, a competência em razão da matéria, da pessoa e o critério territorial, nessa última dando especial atenção a adoção da teoria do resultado pelo artigo 70 do Código de Processo Penal para fins de determinação da competência de foro, em contraposição à teoria da ubiquidade adotada pelo Código Penal.

Após a análise geral, foi feita a análise da competência dos crimes informáticos propriamente dita, evidenciando as dificuldades e a problemática de estabelecimento da competência nesses crimes. Para isso dividiu a análise em competência de justiça, e de foro, na de justiça objetivou principalmente evidenciar em quais hipóteses os crimes informáticos serão julgados pela Justiça Federal, já na competência de Foro, buscou observar o foro de qual território será competente para julgar os crimes informáticos, destacando tanto hipóteses de aplicação das regras gerais, quanto também casos específicos da jurisprudência, como nos crimes contra a honra, racismo, ameaça e patrimônio.

Feita a análise, finalizou concluindo pela necessidade da criação de normas específicas para a solução das dificuldades de atribuição de competência nos crimes informáticos, tendo em vista que, mesmo na modalidade imprópria desses crimes, a legislação existente não consegue se adequar de forma plena ao meio informático, dadas suas peculiaridades, causando assim um cenário de total insegurança jurídica.

2 DO ÁBACO AO SMARTPHONE: O ADVENTO DA ERA DIGITAL E SUA IMPORTÂNCIA

Tablet, smartphone, aplicativos, comunicação à distância em tempo real e com alta velocidade, questões comuns da atualidade, mas que em um passado recente seriam tidas como uma grande utopia. Uma realidade inimaginável e inalcançável, que em menos de um século se materializou e hoje ocupa parcela essencial da vida cotidiana, essa é a chamada “Era Digital”, nesse sentido, John Palfrey coloca:

> Este foi o mais rápido período de transformação tecnológica que ocorreu, pelo menos no que se refere à informação. Os chineses inventaram a imprensa vários séculos antes de Gutenberg desenvolver a imprensa europeia e produzir suas primeiras Bíblias. Poucas pessoas puderam se permitir comprar os livros impressos possibilitados pelas prensas por vários séculos. Em contraste, a invenção e a adoção das tecnologias digitais por mais de um bilhão de pessoas no mundo todo ocorreu no período de poucas décadas. Apesar da saturação de tecnologias digitais em muitas culturas, nenhuma geração ainda viveu toda uma vida na era digital.[1]

Uma das mais marcantes características dessa nova era, é a velocidade, tanto no ponto de vista da sua evolução, a qual será analisada a diante com o histórico, quanto, e principalmente, na comunicação e acesso à informação, nesse sentido, Patrícia Peck Pinheiro ao mencionar Alvin Tofler[2], traz a ideia de que a sociedade atual seria regida por “dois relógios”, um analógico que simboliza o tempo padrão de 24 horas, e um digital, onde o tempo virtual facilmente extrapolaria o tempo físico, fazendo o ser humano exercer um grande número de atividades de forma simultânea e cada vez mais rápida.

Essa era é tão marcada pelo volume, quantidade e velocidade na propagação de informações que costuma ser designada como "Era da Informação", caracterizada essencialmente por uma ligação umbilical entre a informação e os meios tecnológicos, nesse sentido, válidos sãos os dizeres de Karen Kohn e Cláudia Herte de Moraes sobre essa era:

> A Sociedade da Informação estrutura-se, em primeiro lugar, a partir de um contexto de aceitação global, na qual o desenvolvimento tecnológico

[1]PALFREY, John. **Nascidos na era digital**: entendendo a primeira geração de nativos digitais / John Palfrey, Urs Gasser; tradução: Magda França Lopes; revisão técnica: Paulo Gileno Cysneiros: Dados eletrônicos. Porto Alegre: Artmed, 2011, p.13.
[2]TOFLER. AIVIN, apud, PINHEIRO, Patricia Peck. **Direito Digital,** 6.ed. São Paulo: Saraiva, 2016, p.51.

> reconfigurou o modo de ser, agir, se relacionar e existir dos indivíduos e, principalmente, propôs os modelos comunicacionais vigentes. Não se pode separar a informação da tecnologia, algo que vem sendo remodelado e institucionalizado com os avanços na área do conhecimento e das técnicas.[3]

Toda essa evolução tecnológica trouxe vantagens como a facilitação do acesso à informação, a comunicação mais rápida, e a possibilidade de novas descobertas no campo da ciência, do outro lado, também trouxe desvantagens, o stress de uma vida mais acelerada, mudanças na forma das pessoas se relacionarem, e, em um plano concreto, os crimes informáticos, ou seja, aqueles cometidos por meio do aparato tecnológico através desse novo universo.

Feita a presente introdução quanto a Era Digital, é importante analisar os aspectos históricos da informática e internet, com a finalidade de compreender melhor seu funcionamento, importância, modos e, principalmente a velocidade de expansão, fator determinante nas lacunas jurídicas dos crimes informáticos, já que o Direito acaba tendo dificuldade para acompanhar as rápidas evoluções dessa nova realidade.

2.1 Conceito e os Primórdios da Informática

Compreender a história da computação, bem como a da internet, torna-se fundamental para a compreensão da era digital, também é importante, para entender como o conceito de tempo se alterou ao longo do desenvolvimento tecnológico, já que tudo passa a funcionar de forma rápida, dinâmica, onde um intervalo de 10 anos que pode não parecer muito tempo, passa a ser comparado com séculos na era da informação, essa sensação ocorre em razão do grande número de evoluções em frações temporais irrisórias.

Definir computação não é tarefa das mais fáceis, é uma ciência muito técnica e ampla, nesse sentido, brilhante é o conceito trazido por Cléuzio Fonseca Filho:

> A computação é um corpo de conhecimentos formado por uma infraestrutura conceitual e um edifício tecnológico onde se materializam o

[3] KOHN, Karen; MORAES, Cláudia Herte de. **O impacto das novas tecnologias na sociedade:** conceitos e características da Sociedade da Informação e da Sociedade Digital, artigo científico, Santos: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, XXX Congresso Brasileiro de Ciências da Comunicação. Disponível em: < https://bit.ly/2Kxm4SF> Acesso em: 08/03/2018 às 20h02min. p. 2-3.

> hardware e o software. A primeira fundamenta a segunda e a precedeu. A teoria da computação tem seu desenvolvimento próprio e independente, em boa parte, da tecnologia. Essa teoria baseia-se na definição e construção de máquinas abstratas, e no estudo do poder dessas máquinas na solução de problemas.[4]

Para compreender a história da informática e toda evolução digital que nos circunda, é essencial a noção de que a matemática foi imprescindível para tais desdobramentos.

A humanidade ao longo de seu processo evolucional sempre se deparou com dilemas essenciais a sua sobrevivência e a melhora na qualidade de vida, o primeiro destaque vai para os egípcios, tal civilização se destacou pela utilização de métodos para a contagem de animais, demarcação de áreas para plantio em razão das cheias do Nilo, e noções de geometria para a construção das suntuosas e exuberantes pirâmides. Perceba, questões do cotidiano que foram resolvidas graças ao uso da matemática, por mais arcaica que fosse.

Nos primórdios da humanidade, como coloca Cléuzio Fonseca Filho[5], não havia a noção de números independentes, a matemática rudimentar se dava a partir de associações, como por exemplo, entre objetos e animais.

De acordo com o referido autor[6], foi de grande importância para a evolução da matemática o fenômeno da dissociação dos números das coisas, tornando-os independentes de objetos, ou seja, o homem passa a ter a noção da possibilidade de sistematizar seus dilemas em uma relação paralela ao mundo fático, através de símbolos, os chamados "números", surgindo assim os sistemas numéricos essenciais para evolução e compreensão das operações matemáticas.

Em uma rápida passada pelos sistemas numéricos, os primeiros a surgirem[7], se baseavam em símbolos para expressar quantidades, posteriormente vem o chamado "sistema de algarismos romanos". Uma observação interessante, é que conforme salienta Cléuzio Fonseca Filho[8], havia uma dificuldade muito grande dessas sociedades compreenderem a existência do número zero, ou seja, do "nada", isso acabava por dificultar as representações matemáticas limitando os cálculos possíveis.

---

[4]FONSECA FILHO, Cléuzio. **História da computação:** O Caminho do Pensamento e da Tecnologia, 1. ed, Porto Alegre: EDIPUCRS, 2007, p. 13.
[5] FONSECA FILHO, 2007, **loc.cit.,** p. 35.
[6] FONSECA FILHO, 2007, **loc.cit.,** p. 35.
[7] FONSECA FILHO, 2007, **loc.cit.,** p. 13-15.
[8] FONSECA FILHO, 2007, **loc.cit.,** p. 13.

As limitações dos sistemas numéricos antigos só foram superadas quando o mundo passou a adotar o sistema numérico e de cálculos “hindu-árabe”, os numéricos da atualidade. Não há uma data precisa para a criação desse sistema, já que é fruto de modificações e mutações pelas mãos de muitos povos, fato é que esse existe a séculos e tem suma importância para o crescimento da matemática, nesse sentido Cléuzio Fonseca Filho coloca:

> O advento do que nós chamamos de sistema numérico hindu-arábico, com seu rígido esquema de valores e posições, juntamente com o zero (que era usado para representar um espaço em branco), foi uma das grandes invenções da humanidade, e possibilitou o desenvolvimento dos métodos matemáticos e aritméticos, que a partir disso evoluíram muito mais do que qualquer coisa que se conhecia até então*.[9]

Apesar de antigo, tal sistema numérico levou um tempo para adentrar no continente europeu e se espalhar pelo mundo, o principal empecilho foi a questão da comunicação, pois, para compreender a língua árabe era necessário se deslocar até um país de tal origem, pois, existiam muitas peculiaridades no idioma árabe, fator que acabava por dificultar o processo de tradução das obras que retratavam os conhecimentos árabes, inclusive com relação ao sistema matemático.[10]

A difusão do sistema numérico hindu-árabe ao redor do globo, se deu principalmente em face de conflitos e guerras, como as cruzadas, que acabaram provocando o contato do europeu com o árabe, culminando no surgimento de algumas obras e traduções dos ensinamentos árabes, nesse sentido Cléuzio Fonseca Filho[11] destaca três obras, a primeira “Liber Abaci” de Fibonacci no ano 1202, essa pelo rigor técnico não teve tanto prestígio, e duas outras principais “Carmen de Algorismo” de Alexander De Villa Dei, por volta do ano 1220, e o “Algorismus Vulgaris” de John de Halifax, em meados dos anos 1250.

2.1.1 O início da mecanização do cálculo

Com o advento da matemática, tanto os problemas do homem, como os cálculos, vão se tornando cada vez mais complexos, surgindo assim a necessidade de instrumentos para o auxílio e agilização desse processo, surge

[9] FONSECA FILHO, 2007, **op.cit.,** p. 13.
[10] FONSECA FILHO, 2007, **op.cit.,** p. 30-35.
[11] FONSECA FILHO, 2007, **op.cit.,** p.32-34.

então a chamada “mecanização do cálculo”, o primeiro passo para uma evolução que em seu ápice culmina na invenção do computador, abrindo as portas para era digital e toda alteração no modo de vida da humanidade.

Um dos primeiros e mais conhecidos instrumentos que marcaram o início do processo de mecanização do cálculo foi o ábaco, há estimativas da existência desse dispositivo há cerca de 3000 mil anos na Babilônia[12], segundo Patrícia Peck Pinheiro[13], tal instrumento era composto de pequenas pedras ordenadas em sequência específica que auxiliavam os matemáticos em várias tarefas, uma delas, a contabilidade.

Avançando um pouco na história, em meados dos anos 1600, 1650, outro instrumento de suma importância acaba por ser concebido, surge a régua de cálculo, invenção, que como pontuado por Clézio Fonseca Filho[14], foi criado pelas mãos do matemático Willian Ougtred. A régua de cálculo foi um dos frutos da teoria dos logaritmos elaborada por John Napier, e tal instrumento foi utilizado até os tempos recentes, nesse sentido Álvaro Doménech Pujol coloca:

> Durante el año 2014 se cumplió el cuarto centenario de la publicación de Mirifici Logarithmorum Canonis Descriptio (1614), el texto donde John Napier of Merchiston enunció la teoría de los logaritmos y su utilidad y publicó las primeras tablas. La poca relevancia de esta efeméride se debe a que la calculadora electrónica de bolsillo le quitó la utilidad. Pero en los estudios de bachillerato, hasta los años 70 del siglo xx, los alumnos aprendían el uso de las tablas de logaritmos y los estudiantes y profesionales de ciencias e ingeniería tenían que ser diestros con la regla de cálculo, un dispositivo manual que aprovecha sus propiedades. Las escuelas disponían de modelos a gran escala de las reglas de cálculo para que los instructores enseñaran su uso.[15]

Quanto ao funcionamento, Álvaro Doménech Pujol[16], diz que a régua de cálculo era composta por 3 peças, uma régua fixa, uma régua paralela móvel e

---

[12] FONSECA FILHO, 2007, **op. cit.,** p.85.
[13] PINHEIRO, 2016, **op. cit.,** p.60.
[14] FONSECA FILHO, 2007, **op. cit.,** p.86.
[15] PRIETO, Xavier Molero. **Un viaje a la história de la informática**, 1.ed. Valência: Editorial Universitat Politècnica de València, 2016, p. 4. Tradução livre: Durante 2014 foi completado o quarto centenário da publicação de Mirifici Logarithmorum Canonis Descriptio (1614), o texto onde John Napier de Merchiston enunciou a teoria dos logaritmos e sua utilidade e publicou as primeiras tabelas. A pouca relevância deste evento se deve ao fato de que a calculadora de bolso eletrônica retirou o utilitário. Mas nos estudos de bacharelado, até os anos 70 do século XX, os estudantes aprenderam o uso de tabelas logarítmicas e estudantes e profissionais em ciência e engenharia tinham que ser destros com a régua de cálculo, um dispositivo manual que aproveita propriedades. As escolas tinham modelos em larga escala das regras de cálculo para os instrutores ensinarem seu uso.
[16] PRIETO, 2016, **loc. cit.,** p. 4-5.

uma espécie de cursor, permitindo ao matemático a realização de cálculos com números reais aproximados.

O desenvolvimento da teoria dos logaritmos e da régua de cálculo para Clézio Fonseca Filho[17], foram divisores de águas para o desenvolvimento de uma mecanização do cálculo propriamente dita, onde vários pesquisadores passaram a se dedicar a criação de instrumentos de ampliação da capacidade e dos limites do cálculo.

Ainda no século XVII, no levante de criação de instrumentos mecânicos para realização do cálculo, surge a primeira versão de um instrumento importante até os dias atuais, a calculadora, que em seu início, assim como os outros instrumentos, baseava-se em engrenagens e tração, já que não existiam os circuitos eletrônicos e todas linguagens digitais da atualidade.[18]

Segundo Miquel Barceló Garciá[19], há certa discussão quanto a quem de fato inventou a máquina de calcular, o mais comum é a atribuição de tal feito a Blaise Pascal, que projetou no ano de 1642 os desenhos da chamada “máquina aritmética”, que era composta por uma série de engrenagens com 10 dígitos, que permitia a priori somar e subtrair, invenção que fora aprimorada por Gottfried Wilhelm Leibniz, com a invenção de uma máquina capaz de realizar multiplicação, no entanto, aparentemente segundo o autor, a primeira calculadora surgiu pelas mãos de Wilhelm Schickard, em 1623, que projetou um dispositivo composto por dois conjuntos de seis engrenagens onde era capaz de realizar multiplicações.

Outro pensador essencial à evolução dos instrumentos mecânicos de cálculo foi Charles Babbage, um Inglês muito à frente de seu tempo, que concebeu em 1830 a chamada *“Analitical Engine”*[20], esse projeto se aproximou muito do que vem a se tornar no século XX o computador.

Babbage, já nutria a ideia de que seria possível manipular informações através de uma máquina[21], e concebeu pela primeira vez a ideia de um dispositivo programável, capaz de realizar múltiplos cálculos, rompendo com o estigma da época de uma máquina para cada operação específica[22], infelizmente, por limitações

---

[17] FONSECA FILHO**,** 2007, **op. cit**., p. 86.
[18] GARCIÁ, Miquel Barceló. **Una história de la informática**, 1.ed. Barcelona: Editorial UOC, 2008, p. 32.
[19] GARCIÁ, 2008, **loc. cit.,** 32.
[20] FONSECA FILHO, 2007, **op. cit.,** p.88.
[21] FONSECA FILHO, 2007, **op. cit.,** 87-89.
[22] FONSECA FILHO, 2007, **op. cit.,** 87-89.

tecnológicas, não foi possível a concretização de sua invenção. Válidas são as colocações de Xavier Molero Prieto, quanto a máquina de Babbage, suas bases e sua importância para a computação:

> La primera concepción de un ordenador universal es obra del matemático británico Charles Babbage, un pionero del cálculo automático atraído por la exactitud y obsesionado con la idea de eliminar los errores de las tablas matemáticas utilizadas para ayudar al cálculo en disciplinas como la estadística, la economía o la navegación (...) La máquina incorporaba todos los elementos que podemos encontrar hoy en día en un ordenador: una memoria (store, almacén) para almacenar hasta unos mil números de cinco cifras, una unidad de procesamiento (mill, molino) encargada de hacer las operaciones aritméticas, una unidad de control (control) (...) Sin embargo, desde un punto de vista arquitectónico, la estructura de la Máquina Analítica es equivalente a la de las grandes máquinas de calcular que precedieron la invención del ordenador moderno, en las que los programas se iban introduciendo desde el exterior. Lamentablemente, las dificultades tecnológicas —engranajes, vapor como fuerza motora— y financieras, amén de otros factores como el perfeccionismo desmesurado de Babbage y los continuos retoques del diseño, impidieron que la máquina viera la luz.[23]

Dessa forma, em que pese a não concretização da Máquina Analítica, os estudos de Babbage o tornam um dos precursores dos computadores, influenciando na evolução tecnológica. Válido ressaltar a contribuição de Ada Augusta Byron[24] nos conceitos de programação, mecanismo esse, que se tornou essencial na atualidade para o uso e aperfeiçoamento dos computadores e seus softwares.

Outro grande marco para a história da computação, foram as ideias do matemático inglês Georges Boole, que trouxe em 1847 a ideia de que estabelecendo certos padrões seria possível traduzir cálculos e informações em sistemas não numéricos[25], através de um sistema de duas premissas, “universo” e “nada”, e a partir daí realizar diversas operações, nascendo o “sistema booleano”, a

---

[23] PRIETO, 2016, **op. cit.,** p. 16-17. Tradução livre: A primeira concepção de um computador universal é o trabalho do matemático britânico Charles Babbage, um pioneiro do cálculo automático atraído pela precisão e obcecado com a ideia de eliminar erros de tabelas matemáticas utilizadas para ajudar o cálculo em disciplinas como a estatística, economia ou a navegação (...) A máquina incorporou todos os elementos que podemos encontrar hoje em um computador: uma memória (loja, armazém) para armazenar até mil números de cinco dígitos, uma unidade de processamento (moinho, moinho) responsável para fazer operações aritméticas, uma unidade de controlo (controlo) (...) no entanto, de um ponto de vista arquitetônico, a estrutura da máquina analítica é equivalente ao de grandes máquinas de computação que precederam a invenção de computador moderno, em que os programas foram introduzidos a partir do estrangeiro. Infelizmente, as dificuldades tecnológicas - engrenagem, vapor como força motriz - e dificuldades financeiras, além de outros fatores como o excessivo perfeccionismo de Babbage e o contínuo retoque do design, impediram a máquina de ver a luz.

[24] FONSECA FILHO, 2007, **op. cit**., p. 90-91.

[25] FONSECA FILHO, 2007, **op. cit**., p. 57.

famosa “linguagem binária”, que foi e ainda é essencial para o funcionamento dos computadores, pois, a maioria dessas máquinas realizam operações convertendo todas premissas em “0” e “1”. Nesse sentido, sábios os dizeres de Clézio Fonseca Filho:

> Ele percebeu que poderia ser construída uma álgebra de objetos que não fossem números, no sentido vulgar, e que tal álgebra, sob a forma de um cálculo abstrato, seria capaz de ter várias interpretações [Kne68] (...) De especial interesse para a Computação, sua idéia de um sistema matemático baseado em duas quantidades, o ‘Universo’ e o ‘Nada’, representados por ‘1’ e ‘0’, o levou a inventar um sistema de dois estados para a quantificação lógica. Mais tarde os construtores do primeiro computador entenderam que um sistema com somente dois valores pode compor mecanismos para perfazer cálculos†.[26]

Fica nítido que no século XIX foram construídas as principais bases e alicerces da computação, onde o processo de mecanização do cálculo passa a ganhar ares de processo de digitalização do cálculo, com as primeiras concepções de “dispositivos digitais” e linguagens do que vem a se tornar a computação.

Ao final do século XIX, em 1889[27], Herman Holerrith desenvolve uma máquina baseada em conceitos de programação trazidos por Charles Babbage, tendo suas informações de trabalho inseridas através de cartões perfurados, a invenção teve por finalidade realizar o senso americano, realizando tal feito com a metade do tempo do sistema manual.

Esse foi o ponta pé para as criações de Holerrith, que no ano de 1896 funda a “International Bussines Machine” (IBM), empresa que no futuro acaba se tornando uma das mais importantes do ramo da computação, tendo papel essencial na popularização do “Personal Computer”, os computadores domésticos.[28]

2.1.2 O advento da computação e o início da digitalização do cálculo

Com o advento do século XX, as evoluções até então relatadas, somadas a duas guerras mundiais, confluíram finalmente na chamada era da computação, ou seja, o cálculo passa a ser realizado de forma digital em uma

---

[26] FONSECA FILHO, 2007, **op. cit**., p.57.
[27] MARÇULA, Marcelo. **Informática:** Conceitos e Aplicações / Marcelo Marçula, Pio Armando Benini Filho**.** 4. ed. São Paulo: Érica, 2013, p. 34.
[28] PINHEIRO, 2012, **op. cit**., p. 60.

velocidade e quantidade nunca antes vista, provocando mudanças profundas no modo de vida da sociedade, criando a “Era da Informação” na qual vivemos.

Antes que o mundo pudesse conceber a ideia de um dispositivo automático de cálculo totalmente eletrônico, pode se dizer, que existiram máquinas imediatamente antecessoras, “híbridas”, que por ainda contarem com alguns segmentos mecânicos, não foram consideradas o primeiro computador propriamente dito.

Segundo Miquel Barceló Garciá[29], para considerar o primeiro computador eletrônico e consequentemente distinguir dos dispositivos que ainda possuíam partes mecânicas, dois elementos foram essenciais, o uso da válvula de vácuo e da chamada “arquitetura da Von Neuman”, vejamos as considerações do autor:

> Cuándo se habla de un “primer ordenador electrónico” nos referimos al uso, por primera vez en el cálculo, de la tecnología “electrónica” de los tubos electrónicos de vacío y, también, a la estructura funcional de un sistema de cálculo versátil con un “programa almacenado en memoria” que conocemos hoy como arquitectura von Neumann, que define lo que hoy se considera um “ordenador”.[30]

As válvulas, segundo Marcelo Marçula[31], foram criadas em 1904 por J. Ambrose Fleming, esses foram os primeiros componentes, que através de eletrodos, traduziam o sistema binário de “0” e “1”, possibilitando assim a independência dos componentes mecânicos e a criação dos primeiros circuitos eletrônicos a partir do agrupamento de inúmeras válvulas e de outros componentes que foram surgindo, esses circuitos permitiram um aumento exponencial na velocidade de cálculo, e a materialização de ideias, como as de Charles Babbage e Boole, ou seja, a criação de máquinas universais e a tradução de inúmeras relações para o sistema binário.

Já a chamada “Arquitetura de von Neumann”, vem das ideias do Alemão Max Neumann, de que o ideal seria a armazenagem dos programas no interior das máquinas, possibilitando reiniciar a operação a qualquer momento, sem

---

[29] GARCIÁ, 2008, **op. cit**., p. 61.
[30] GARCIÁ, 2008, **op. cit.**, p. 61. Tradução livre: Quando falamos de um "primeiro computador eletrônico" nos referimos ao uso, pela primeira vez no cálculo, da tecnologia "eletrônica" de tubos eletrônicos a vácuo e, também, à estrutura funcional de um sistema de cálculo versátil com um "Programa armazenado na memória" que conhecemos hoje como arquitetura von Neumann, que define o que hoje é considerado um "computador”.
[31] MARÇULA, 2013, **op. cit**., p. 34.

necessidade de reprogramar o dispositivo, economizando tempo e também facilitando a programação da máquina, nesse sentido, Miquel Barceló Garciá coloca:

> En un calculador tradicional, el operador introduce los datos en secuencia com la operación que quiere que se ejecute entre ellos. Para realizar la misma operación con otros datos, hay que volver a introducir más datos y, otra vez, repetir la introducción de las instrucciones u operaciones. En lo que hoy llamamos ordenador, la novedad radical reside en el hecho que el programa, es decir, la secuencia de operaciones que hay que realizar, está previamente almacenado en la memoria. Esto se ha denominado precisamente arquitectura von Neumann.[32]

O período intermediário que precede as máquinas de cálculo eletrônicas foi composto pelos chamados “computadores eletromecânicos"[33], máquinas que possuíam alguns componentes eletrônicos, mas que ainda dependiam de elementos mecânicos como rodas, engrenagens, chaves rotatórias[34]. Merecem destaque duas invenções, os computadores eletromecânicos do alemão Konrad Zuse, em especial o chamado "Z3", e a máquina de Howard H. Aiken em parceria com a IBM e Harvard, a chamada "Mark 1".

A primeira versão totalmente funcional do computador eletromecânico de Konrad Zuse, foi o Z3, criado em 1941, segundo Miquel Barceló Garciá[35], teve sua importância, sendo a primeira máquina de calcular que utilizava o código binário para operar, realizando multiplicações entre dois números em um tempo de 4 segundos. No que pese a utilização de relês, dispositivos eletromecânicos utilizados para traduzir as relações de "0" e "1" do sistema binário, segundo coloca Cléuzio Fonseca Filho[36], a máquina não era 100% digital, pois ainda dependia de alguns componentes mecânicos como “fitas de películas de cinema” para realizar as movimentações da máquina.

O Mark 1 ficou pronto em 1944, também chamado de " IBM - Automatic Sequence Controlled Calculator", nasceu das mãos de Howard H. Aiken em conjunto

---

[32] GARCIÁ, 2008, **op. cit**., p. 53. Tradução livre: Em uma calculadora tradicional, o operador insere os dados em sequência com a operação que deseja executar entre eles. Para executar a mesma operação com outros dados, você deve inserir novamente mais dados e, novamente, repetir a introdução de instruções ou operações. No que hoje chamamos de computador, a novidade radical está no fato de que o programa, isto é, a sequência de operações que devem ser realizadas, é anteriormente armazenada na memória. Isso foi chamado precisamente de arquitetura von Neumann.
[33] MARÇULA, 2013, **op. cit.,** p. 35.
[34] MARÇULA, 2013, **op. cit.,** p. 34.
[35] GARCIÁ, 2008, **op. cit**., p. 48.
[36] FONSECA FILHO, 2007, **op. cit**., p. 102.

com engenheiros da IMB e de Harvard[37], tinha potência parecida com o Z3 e chamava atenção pelo tamanho, medindo aproximadamente 15 metros de largura por 2,60m de altura.

Um dispositivo gigantesco que ainda utilizava algumas partes mecânicas. Sua programação, por exemplo, segundo Miquel Barceló Garciá[38] era feita de forma manual, através de cartões perfurados, e teve como inovação a utilização de memórias mais avançadas com núcleo de ferrite, tal invento marcou novamente a importância da IBM na era da computação, sendo tal máquina utilizada pela Marinha dos EUA.

Chegando ao momento do surgimento das primeiras máquinas de cálculo automáticas e totalmente eletrônicas, ou seja, os primeiros "computadores" de fato, existe certa discussão sobre qual invenção pode ser considerada como o primeiro computador, o mais comum tem sido considerar o ENIAC (Eletronic Numeric Integrator and Computer), criado em 1946, por John Presper Eckert Jr e John Mauchly, na Universidade da Pensilvânia[39], no entanto, há quem defenda, e parece fazer sentido, atribuir tal feito à criação inglesa de Allan Turing, chamada “Colossus”, desenvolvida em 1943 com o objetivo de decifrar a criptografia nazista.

O referido raciocínio de atribuir a Colossus o título de primeiro computado e não ao ENIAC, se dá pelo fato de que antes do advento desse, a Colossus já possuía estrutura muito parecida, utilizando válvulas num total de 1800 válvulas e a arquitetura de “von Neumann”, isso praticamente 3 anos antes do início do funcionamento do ENIAC, nesse sentido, são válidas as colocações de Miquel Barceló Garciá:

> Como se ha dicho, si hay que hablar propiamente de ordenadores con programa almacenado (lo que hoy denominamos arquitectura von Neumann), el ENIAC no llega a serlo por completo, y este mérito corresponde al EDSAC, el ordenador europeo que Maurice Wilkes completó en Cambridge (Inglaterra). Pero, de hecho, el ENIAC tampoco fue la primera máquina de cálculo electrónica programable de propósito general. Lo precedió la serie de los Colossus en Inglaterra, poco conocidos durante muchos años por el secreto militar asociado a su nacimiento y su utilización en tareas de espionaje.[40]

---

[37] FONSECA FILHO, 2007, **op. cit**., p. 102-103.
[38] GARCIÁ, 2008, **op. cit.,** p. 48-49.
[39] MARÇULA, 2013, **op. cit.,** p. 35.
[40] GARCIA, 2008, **op. cit.,** p. 57. Tradução livre: Como já foi dito, se tivermos que falar corretamente de computadores com programas armazenados (o que hoje chamamos de arquitetura von Neumann), o ENIAC não se torna completamente, e esse mérito corresponde ao EDSAC, o computador europeu que Maurice Wilkes completou em Cambridge. (Inglaterra). Mas, na verdade, o ENIAC também não

Um fator em comum tanto para os computadores eletromecânicos, como, principalmente, para o surgimento dos computadores eletrônicos, foi que os principais motivadores para tais equipamentos foram os interesses militares, ou seja, auxilio no cálculo de trajetórias de misseis, estratégias, elaboração de armamentos, desvendar criptografias, dentre outras necessidades.[41]

A “Colossus” não fugiu da regra estabelecida acima, tal máquina foi projetada da necessidade de desvendar as comunicações nazistas que eram criptografadas por uma complexa máquina chamada “Enigma”, o governo inglês, com a necessidade de prever ataques e conseguir avançar na guerra, financiou o projeto de construção de um dispositivo capaz de quebrar essa criptografia, para isso vários estudiosos foram recrutados, dentre eles, Alan Turing, e Janós Louis von Neumann.[42]

Segundo Clézio Fonseca Filho[43], Turing quando projetou a Colossus já tinha status de grande importância para ciência da computação, pois, havia elaborado inúmeros conceitos, ideias e máquinas hipotéticas que foram essenciais ao avanço da ciência.

Em 1943, depois de inúmeros projetos, a Colossus é produzida, seus principais diferenciais eram o fato de ser projetada inteiramente com circuitos eletrônicos, possuindo cerca de 1800 válvulas[44], além disso, como já colocado, ela utilizava “a arquitetura de Von Neumann”, tendo seus programas armazenados em uma memória interna, podendo ser considerada o primeiro computador[45], só não é assim tão reconhecido em virtude do segredo do projeto, pois, era extremamente sigiloso, nesse sentido Xavier Molero Prieto coloca:

> El gobierno inglés, por ejemplo, invirtió grandes esfuerzos en la construcción de uma serie de máquinas electrónicas para descifrar los mensajes que la marina alemana codificaba mediante la conocida máquina Enigma. Interceptar e interpretar correctamente los mensajes que contenían las órdenes de destrucción a los submarinos alemanes desplegados en el océano Atlántico se convirtió en un objetivo crucial. En esta tarea,

era a primeira máquina de cálculo eletrônico programável de uso geral. Ele foi precedido pela série Colossus, na Inglaterra, pouco conhecida há muitos anos pelo segredo militar associado ao seu nascimento e seu uso em tarefas de espionagem.

[41] FONSECA FILHO, 2007, **op. cit.,** p. 103.
[42] FONSECA FILHO, 2007 **op. cit.,** p. 105.
[43] FONSECA FILHO, 2007 **op. cit.**, p.102.
[44] FONSECA FILHO, 2007 **op. cit.** p. 78.
[45] GARCIÁ, 2008, **op. cit.,** p. 57-58.

> desarrollada en Betchley Park, al noroeste de Londres, participaron matemáticos de la talla de Alan Turing i Max Newman. Sabemos poco de estas máquinas, denominadas Colossus y construidas bajo la dirección del ingeniero Thomas H. Flowers a partir de 1943, por el secretismo militar ligado a todas estas tareas de espionaje y porque, finalizada la guerra, se dio orden de destruirlas junto con toda la información relevante.[46]

O ENIAC, como dito, foi desenvolvido por John Presper Eckert Jr e John Mauchly na Universidade da Pensilvânia, no ano de 1946[47], sendo considerado por muitos o primeiro computador eletrônico, não só pelo motivo de desconhecimento da máquina Colossus de Alan Turing, mas também pelo fato dessa máquina ter tido mais funções e usos que a Colossus, cujo objetivo exclusivo, era decodificação das mensagens nazistas.

O objetivo principal para a construção do ENIAC, como colocado por Xavier Molero Prieto[48], foi o cálculo de trajetórias balísticas e a elaboração de táticas de guerra. O ENIAC[49] era uma máquina de grandes proporções, ocupando uma área de aproximadamente 94 metros quadrados, possuindo cerca de 18 mil válvulas e 1500 relês, em comparação com os computadores eletromecânicos, como Z3 e Mark 1, a velocidade do ENIAC foi algo impressionante para época, conseguindo realizar mais de 5 mil somas por segundo, o que provocou uma verdadeira revolução no desenvolvimento da sociedade[50].

Em que pese o ENIAC atender os preceitos tidos como essenciais para uma máquina eletrônica, sendo programável e contendo circuitos eletrônicos, parte das informações ainda eram inseridas por meio de cartões perfurados, o que tornava sua programação algo demorado e complicado, até por essas questões, Miquel Barceló Garciá[51] diz que esse dispositivo usava parcialmente a "arquitetura da Von Neumann", já que ainda dependia dessa inserção de informações por via dos cartões.

---

[46] PRIETO, 2016, **op. cit.,** p.17-18. Tradução livre: O governo inglês, por exemplo, investiu grandes esforços na construção de uma série de máquinas eletrônicas para decifrar as mensagens que a Marinha alemã codificava através da conhecida máquina Enigma. Para interceptar corretamente e interpretar as mensagens que continham as ordens de destruição para os submarinos alemães implantados no Oceano Atlântico tornou-se um objetivo crucial. Nesta tarefa, desenvolvida em Betchley Park, a noroeste de Londres, envolveu matemáticos da estatura de Alan Turing e Max Newman. Sabemos pouco sobre essas máquinas, chamadas Colossus e construídas sob a direção do engenheiro Thomas H. Flowers, de 1943, pelo sigilo militar ligado a todas essas tarefas de espionagem e porque, após a guerra, eles foram ordenados a destruí-los juntos com todos as informações relevantes.
[47] MARÇULA, 2013, **op. cit.,** p. 35.
[48] PRIETO, 2016, **op. cit.,** p. 18.
[49] MARÇULA, 2013, **op. cit.,** p. 35.
[50] PRIETO, 2016, **op. cit.,** p. 20.
[51] GARCIÁ, 2008, **op. cit.**, p. 55-56.

As dificuldades enfrentadas no ENIAC, principalmente no que concerne a lentidão na programação, só vão ser sanadas com o desenvolvimento do EDVAC (Electronic Discrete Variable Automatic Computer) em 1945, entrando em operação em 1952, produzido da parceria entre John Presper Eckert Jr, John Mauchly e Janós Louis von Neumann, possuindo a arquitetura de Neumann, com o conceito de programa armazenado[52]. Desse ponto em diante a evolução da computação ganha vida e dinamismo, surgindo inúmeros dispositivos em um curto espaço de tempo, sempre sucedendo com evolução considerável.[53]

Outro marco para a história da computação foi o UNIVAC-1 (Universal Automatic Calculator), surgiu em 1951 e foi o primeiro computador comercial, ou seja, pela primeira vez essa invenção se desliga da finalidade militar e inicia a trajetória de satisfação de outros interesses da sociedade.[54]

De 1956 até o início da década de 60 tem-se a chamada “segunda geração de computadores eletrônicos”, tal geração, conforme colocado por Miquel Barceló Garciá[55], teve máquinas com potência 10 vezes maior que a geração anterior, e foi marcada principalmente pelo advento das linguagens de programação e a invenção do transistor, nesse sentido Cléuzio Fonseca Filho, faz as seguintes considerações:

> A segunda geração (1956 - 1963) foi impulsionada pela invenção do *transistor* (1948) e em 1956 já se produziam computadores com esta tecnologia. Apareceram também os modernos dispositivos, tais como as impressoras, as fitas magnéticas, os discos para armazenamento, etc. Os computadores passaram a ter um desenvolvimento rápido, impulsionados principalmente por dois fatores essenciais: os sistemas operacionais e as linguagens de programação.[56]

A evolução da informática não parou, e ganhou ainda mais força a partir de 1964, com o maior desenvolvimento dos sistemas operacionais, e principalmente pelo surgimento dos primeiros circuitos integrados, tal tecnologia possibilitou uma redução significativa no tamanho dos circuitos, já que era possível aglutinar inúmeros componentes menores e conseguir uma potência muito maior, a respeito dessa observação, Miquel Barceló Garciá coloca:

---

[52] GARCIÁ, 2008, **op. cit**., p. 53-55.
[53] GARCIÁ, 2008, **op. cit**., p. 53-55.
[54] MARÇULA, 2013, **op. cit**., p. 36.
[55] GARCIÁ, 2008, **op. cit.**, p. 76.
[56] FONSECA FILHO, 2007, **op. cit.,** p.123.

> La *tercera generación* se suele situar hacia la mitad de la década de los sessenta y está basada en la tecnología de estado sólido y los *circuitos integrados* (módulos de semiconductores integrados en pastillas que, descubiertos en el año 1957, se empezarán a conocer genéricamente como *chips*). El ejemplo más conocido de la tercera generación es posiblemente el IBM 360 que se empezó a construir en 1961 y se comercializó a partir de 1964, y se convirtió en una de las líneas de productos fundamentales en la historia de la informática. En una primera etapa, con la *integración a pequeña escala* (SMI), se llegan a poner de 1 a 16 componentes por circuito con la tecnología TRL, más o menos entre 1959 y 1964. Eso permite multiplicar por mil la potencia de cálculo por unidad de volumen en relación, por ejemplo, con la del ENIAC.[57]

Com a chegada da década de 70, o processo de integração de circuitos é ampliado, culminando na criação do microprocessador, um chip capaz de reunir e gerenciar múltiplas funções e cálculos, tecnologia que certamente revolucionou a computação abrindo espaço à modernidade, inaugurando assim, a chamada "quarta geração de computadores", nesse sentido merece destaque a criação do INTEL 4004 em 1970, o primeiro microprocessador disponível comercialmente[58].

Da quarta geração em diante, apesar de autores como Miquel Barceló,[59] mencionarem a possível existência de uma quinta, torna-se muito complicado e complexa a separação da informática por gerações, dado que a evolução passa ocorrer de forma muito rápida e simultânea, inexistindo uma forma cronológica ideal de classificação.

Já encerrando o esboço histórico da computação, alguns pontos merecem destaque, o primeiro é a criação do microcomputador, sendo o primeiro chamado de Altair 8800[60], criado em 1975. O segundo ponto é o advento da Microsoft, empresa criada por Paul Allen e Bill Gates, grande responsável pela evolução dos sistemas operacionais como o MS-DOS, sistema que equipava os

---

[57] GARCIÁ, 2008, **op. cit**., p. 76-77. Tradução livre: A terceira geração é geralmente localizada no meio da década de 70 e é baseada em tecnologia de estado sólido e circuitos integrados (módulos semicondutores integrados em chips que, descobertos em 1957, começarão a ser conhecidos genericamente como chips). O exemplo mais conhecido da terceira geração é possivelmente o IBM 360, que começou a ser construído em 1961 e foi comercializado a partir de 1964, e se tornou uma das linhas de produtos fundamentais da história da computação. Numa primeira fase, com integração de pequena escala (SMI), conseguem colocar de 1 a 16 componentes por circuito com tecnologia TRL, mais ou menos entre 1959 e 1964. Isso permite multiplicar por mil a potência de cálculo por unidade. de volume em relação, por exemplo, com a do ENIAC.

[58] MARÇULA**,** 2013, **op. cit**., p. 38.

[59] GARCIÁ, 2008, **op. cit.,** p. 154.

[60] MARÇULA, 2013, **op. cit.,** p. 38.

primeiros computadores pessoais da IBM, os IBM-PCs[61] e posteriormente com o Windows, o sistema operacional mais utilizado na atualidade[62], sendo, nas palavras de Cléuzio Fonseca Filho “uma das mais bem-sucedidas empresas de software”[63].

Por fim, a APPLE, empresa criada no ano de 1986 por Steve Jobs e Stephen Wozniak, teve especial destaque ao produzir o primeiro computador pessoal de sucesso, o APPLE 1, em 1976[64], mantendo sucesso com o APPLE 2. A Apple teve e tem ainda grande importância para a era da informática, inovou com o streaming de músicas na criação do IPOD, e foi uma das precursoras dos celulares inteligentes, os chamados “smartphones”, com a invenção do IPHONE[65].

Dessa forma, as tecnologias foram avançando de forma rápida até chegar a atualidade, com os tablets, smartphones, e o foco na realidade virtual. Fato é, que a tecnologia cresce em velocidade exponencial, tanto do ponto de vista material, ou seja, no número de dispositivos, como na sua importância para a sociedade, dado que essa acaba por se tornar cada vez mais integrada e dependente das tecnologias computacionais.

2.2 Pela Internet

Após tecer considerações a respeito do advento da informática, resta um ponto para finalizar a compreensão básica da era digital, a internet, hoje talvez seja a essência dessa nova era de informação, já que constitui elo principal de interligação de todos aparatos informáticos criados, movimentando a comunicação, armazenamento de dados, notícias, pesquisas, entretenimento, dentre várias outras utilidades.

Antes de adentrar em uma breve síntese histórica da internet, história essa, que assim como toda informática, se resume a um conjunto de atos evolutivos que ocorreram e ocorrem em um curto espaço de tempo, pelo menos, se considerar o “tempo comum” e não o da era da informação, faz-se necessário uma breve conceituação; nesse sentido, Fernando José da Costa a define como “uma rede

---

[61] MARÇULA, 2013, **op. cit.,** p. 38-39.
[62] MARÇULA, 2013, **op. cit.,** p. 40.
[63] FONSECA FILHO, 2007, **op. cit**., p. 130.
[64] FONSECA FILHO, 2007, **op. cit**., p. 130.
[65] MARÇULA, 2013, **op. cit.,** p. 41.

mundial de usuários que simultaneamente trocam informações. Trata-se da maior e mais célere rede de comunicação do planeta. ”[66].

Segundo Miquel Barceló Garciá[67], na segunda metade da década de 1960 as empresas de informática se dedicaram a criar os primeiros sistemas de comunicação entre computadores, a princípio eram sistemas separados, privativos de cada empresa, que tinham por característica principal a ligação direta entre esses equipamentos.

A internet, assim como os computadores, tem seu nascimento atribuído a uma necessidade militar, tendo sua origem do projeto ARPANET, uma rede criada em 1969 para o exército americano, desenvolvida por Larry Roberts que se utilizou da ideia de um estudante do MIT, Leonard Kleinrock, de que as informações podiam ser fragmentadas em conjuntos, chamados de “pacotes”, e serem transmitidas por ondas de rádio e satélite[68].

Em 1973, surge o chamado “Protocolo TCP/IP”, esse conforme a explicação de Lilian Minardi Paesani[69], é uma espécie de algoritmo que permitiu que sistemas distintos pudessem se comunicar entre si, abrindo a barreira daqueles primeiros sistemas paralelos criados pelas empresas na década de 60, tal protocolo é utilizado até os dias atuais.

Com o passar do tempo, outras redes de computadores similares a ARPANET foram surgindo, segundo Fernando José da Costa[70], um acontecimento de grande importância ao surgimento da internet, foi a ligação de duas grandes redes de computadores, a ARPANET com a National Science Foundation Network (NSFNET), que possibilitou uma aglomeração muito maior de pessoas na rede, a essas grandes ligações de computadores e cabeamentos, o referido autor dá o nome de “backbones”, aos poucos outros backbones foram surgindo, como o ANSNET, e os backbones europeus[71].

Outro grande marco foi a criação da World Wide Web (www), protocolo que possibilitou a abertura da internet para o mundo, possibilitando uma

---

[66] COSTA, Fernando José da. **Locus delicti nos crimes informáticos.** 2011. Tese (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: https://bit.ly/2A83hXr > Acesso em: 11/03/2018 às 20h59min, p. 19.
[67] GARCIÁ, 2008, **op. cit**., p. 101-102.
[68] PRIETO**,** 2016, **op. cit**., p. 72.
[69]PAESANI, Liliana Minardi. **Direito e Internet:** liberdade de informação, privacidade e responsabilidade civil / Liliana Minardi Paesani. 7. ed. São Paulo: Atlas, 2014, p.10.
[70] COSTA, 2008, **op. cit.** p. 23.
[71] COSTA, 2008, **op. cit.** p. 23.

universalização do acesso e a criação dos primeiros “provedores”, empresas capazes de permitir o acesso ao mundo virtual, nesse sentido, válidas são as palavras de Andrés Marzal Varó, María José Castro Bleda e Pablo Aibar Ausina:

> En la segunda mitad de los años 90 asistimos a otro cambio radical con la apertura de Internet al gran público y al comercio, que se hizo accesible a todos gracias, especialmente, a la World Wide Web. Lo que hasta entonces era una red que unía a universidades y algunas administraciones, se abrió a la sociedad y la transformó hasta el punto de que hoy cuesta recordar que hubo un tiempo sin Internet. En la última mitad de los años 90 surgieron empresas que pretendían cubrir nichos de intermediación en Internet, o portales de acceso a Internet, o buscadores...[72]

Assim nasceu a internet para o mundo, essa se encontra em constante evolução, não só no que concerne as velocidades, como nos dispositivos de acesso, que antes se restringiam apenas aos computadores, mas que hoje até os eletrodomésticos são capazes de conectar-se.

2.3 A “Infomaré” Brasileira

O desenvolvimento da informática e da internet no Brasil sem dúvidas é muito pouco comentado, a maior razão talvez seja que grande parte da tecnologia computacional utilizada no Brasil foi proveniente de importações, ou seja, tecnologias trazidas de países mais desenvolvidos na área, no entanto, tal fator não significa que tal história é inexistente, sendo válido observar os principais pontos dessa história no âmbito nacional.

Segundo Marilza de Lurdes Cardi[73], o governo do Presidente Juscelino Kubistchek de Oliveira teve grande importância para o início do desenvolvimento da informática no país, criando várias políticas de incentivo a compra de computadores, bem como de capacitação para uma futura produção de máquinas nacionais.

---

[72] PRIETO, 2016, **op. cit.,** p. 83. Tradução livre: Na segunda metade dos anos 90 assistimos a uma outra mudança radical com a abertura da Internet ao público em geral e ao comércio, que ficou acessível a todos graças, especialmente, à World Wide Web. O que até então era uma rede que unia universidades e algumas administrações, foi aberto à sociedade e transformou-a ao ponto de que hoje é difícil lembrar que houve um tempo sem Internet. Na última metade dos anos 90, surgiram empresas que buscavam cobrir a intermediação de nicho na Internet, portais de acesso à Internet ou mecanismos de busca ...

[73] CARDI, Marilza de Lourdes. **Evolução da computação no Brasil e sua relação com fatos internacionais.** 2002. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Santa Catarina, Santa Catarina, 2002. Disponível em: <https://bit.ly/2yA9BVKl> Acesso em: 12/03/2018 às 18h39min, p. 53-54.

O primeiro computador a de fato ser utilizado no Brasil, foi um Burroughs Datatron 205, uma máquina da primeira geração de computadores eletrônicos com recursos bem básicos e ausência de programa interno “arquitetura de Von Neumann”, que foi instalado em 1960, posteriormente vieram outras máquinas por via de importação, como o IBM-360, primeiro computador da terceira geração utilizado no pais, a partir de então, inúmeras outras máquinas foram adentrando no território ao longo dos anos e ficando cada vez mais comuns.[74]

Quanto a produção interna de computadores, em que pese Marilza de Lurdes Cardi[75], citar como primeiro computador brasileiro o IME, uma máquina hibrida desenvolvida entre 1958 e 1961, por um grupo de alunos do ITA (Instituto de Tecnologia e Aeronáutica), o mais comum é atribuir tal feito ao chamado “Patinho Feio”, um computador desenvolvido na Universidade de São Paulo, no ano de 1972[76].

Após o Patinho Feio, o Brasil desenvolveu um segundo computador em 1975, foi o chamado G-10, máquina um pouco mais avançada, fruto de uma parceria entre a Universidade de São Paulo e a Pontifícia Universidade Católica do Rio de Janeiro, tal projeto foi interessante, pois teve uma finalidade comercial, sendo o projeto continuado pela empresa “Cobra”, que utilizou parte dos conceitos e tecnologias como base para os futuros computadores da marca[77].

Quanto a Internet no Brasil, segundo Fernando José da Costa[78], chegou em 1988, através da RPN (Rede Nacional de Pesquisa), porém o primeiro “backbone”, ou seja, a primeira grande rede nacional conectável a internet, só foi instalada em 1992, e era restrita a alguns centros de pesquisa e universidades do país[79].

O ano de 1995, segundo Marilza de Lurdes Cardi[80], marca o início do uso comercial da internet no Brasil, surgindo ao longo do ano as regulamentações básicas sobre o uso e difusão da internet no país, assim iniciando a difusão da rede que não para de obter novos conectados, nesse sentido, Fernando José da Costa diz:

---

[74] CARDI, 2002, **loc. cit.**, p. 55-58.
[75] CARDI, 2002, **loc. cit.**, p. 54.
[76] MARÇULA**,** 2013, **op. cit.**, p.41.
[77] CARDI, 2002, **op. cit.**, p. 61-62.
[78] COSTA, 2011, **op. cit**. p. 24.
[79] COSTA, 2011, **op. cit**. p. 24.
[80] CARDI, 2002, **op. cit.,** p. 64.

> O Brasil já conta com aproximadamente 36,4 milhões de internautas40, com previsão de expandir ainda mais este expressivo número, vez que o comércio e os serviços migram a cada dia para este terreno abstrato que é a internet, razão pela qual tem demonstrado preocupação no que diz respeito ao regramento jurídico do tema.[81]

Dessa forma, encerasse a breve análise da computação e internet no território tupiniquim, realidade que se encontra em amplo desenvolvimento, com a entrada de cada vez mais nacionais na era digital, a Fundação Getúlio Vargas revelou ao Estadão esse ano que o número de smartphones no Brasil superou o número de habitantes, de tão grande e crescente está a inclusão digital, e que com o passar dos anos tende a se tornar cada vez maior.[82]

[81] COSTA, 2011, **op. cit.** p. 24.
[82] LIMA, Mariana. **Brasil já tem mais de um smartphone ativo por habitante, diz estudo da FGV,** São Paulo: O Estado de São Paulo, 2018. Disponível em: < https://bit.ly/2JZALdf> Acesso em 30/07/2018 às 22h12min, s/p.

3 DOS CRIMES INFORMÁTICOS

Como mencionado no tópico anterior, o advento da computação e informática ocasionou profundas mudanças na sociedade, inaugurando a chamada "era da informação", esse conjunto de mudanças, como visto, trouxe inúmeras vantagens, principalmente no que concerne a velocidade de comunicação e acesso à informação, que passou a circular em uma velocidade jamais observada.

Não só de vantagens é marcada a revolução computacional, nesse sentido, válidas são as colocações de Garry Kasparov[83], que traz a ideia de "dualidade" da tecnologia, que pode ser utilizada tanto para o bem, quanto para o mal:

> No fim das contas, como sempre, é uma questão de valores. A tecnologia em si é agnóstica: tem poder para fazer o bem ou o mal, dependendo de quem a controle. Isso sempre foi assim. Os combustíveis fósseis poluem, os antibióticos levam às superbactérias resistentes e um pode derrubar metade da internet.[84]

No campo da informática, a "utilização para o mal" desses instrumentos tecnológicos se perfaz na figura dos chamados "crimes informáticos". Segundo Damásio de Jesus[85], não se sabe ao certo o ano de origem dessas práticas, porém atribui-se a década de 60, sendo que a partir da década de 70 já existiam menções ao termo hacker, e assim, acompanhando as evoluções tecnológicas, essas práticas foram se difundindo por todo globo.

De acordo com dados da Symantec Corporation,[86] em pesquisa realizada em 20 países no ano de 2017, aproximadamente 980 milhões de pessoas sofreram algum ataque no ambiente informático, isso representa mais da metade da população com acesso à internet nos países pesquisados (1,8 bilhões de pessoas), o que representou um prejuízo econômico na casa dos 172 bilhões de dólares.

---

[83] KASPAROV, Garry. **O poder da tecnologia para o bem ou para o mal depende de quem a controla**. Avast Blog, 2016. Disponível em: <https://blog.avast.com/pt-br/o-poder-da-tecnologia-para-o-bem-ou-para-o-mal-depende-de-quem-a-controla> Acesso em 06/08/2018 às 19h42min, s/p.
[84] KASPAROV, 2016, **loc. cit.,** s/p.
[85] JESUS, Damasio de. **Manual de crimes informáticos,** 1. ed. São Paulo: Saraiva, 2016. (Recurso Eletrônico – "Minha Biblioteca"), p. 22-23.
[86] CORPORATION, Symantec. **Norton Cyber Security Insights Report 2017 Global Results** 2017. Disponível em: <https://symc.ly/2G8VNnU> Acesso em 25/08/2018 às 22h53min, s/p.

O Brasil, ocupou o segundo lugar nos prejuízos sofridos[87] em razão dos ataques informáticos, ficando atrás apenas da China, tendo perdido mais de 20 bilhões de dólares com ataques a mais de 62 milhões de brasileiros. Considerando os dados de 2016, do Instituto Brasileiro de Geografia e Estatística (IBGE)[88], no qual registrou que 64% dos domicílios brasileiros tem acesso à internet, os atingidos pelas práticas criminosas superam a metade dos usuários do país.

Ainda, de acordo com o relatório[89], as práticas criminosas mais comuns são a violação de dados pelo contato de softwares maliciosos, fraudes à cartões bancários, acesso indevido às informações de e-mails e redes sociais, além de fraudes e estelionatos por meio de sites maliciosos de compras.

Outros institutos também trouxeram dados significativos quanto ao cenário dos crimes informáticos, o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil – CERT,[90] recebeu só no ano de 2017 mais de 800 mil notificações de práticas irregulares no ambiente virtual, valor quase 30% superior ao ano anterior, o que demonstra um avanço dos crimes informáticos de forma exponencial, acompanhando de certa forma a velocidade das inovações tecnológicas que surgem a cada instante.

A SaferNet Brasil[91], associação civil de direito privado que desenvolve um trabalho em conjunto com organismos nacionais, como a Polícia Federal e o Ministério Público Federal, apresenta interessantes dados quanto ao cenário nacional dos crimes informáticos. De acordo com a associação, através do projeto da Central Nacional de Denúncias de Crimes Cibernéticos, recebeu só em 2017, quase 34 mil denúncias de páginas suspeitas.

Analisando os dados da associação é possível traçar, ainda que de forma simplória, um perfil dos crimes informáticos no Brasil, aproximadamente um

---

[87] CORPORATION, 2017, **op. cit.**, s/p.
[88] IBGE, Instituto Brasileiro de Geografia e Estatísticas. **PNAD – Pesquisa Nacional por Amostra de Domicílios Contínua - Acesso à Internet e à Televisão e posse de telefone móvel celular para uso pessoal,** 2016. Disponível em: < https://bit.ly/2QOxb8x> Acesso em 22/08/2018 às 14h02min, s/p.
[89] CORPORATION, 2017, **op. cit.**, s/p.
[90] CERT, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas dos Incidentes Reportados ao CERT.br**, 2017. Disponível em: <https://bit.ly/2EWbOMn> Acesso em 13/10/2018 às 15h42min, s/p.
[91] SAFERNET. **Indicadores Safernet,** 2017, Disponível em: <https://bit.ly/1q6AeeW> Acesso em: 29/09/2018 às 19h09min, s/p.

terço das denúncias[92], se referiram a práticas de pornografia infantil, seguidas de racismo, apologia e incitação ao crime.

Fica nítido o quão preocupante é o cenário criado pelos crimes informáticos, pensando nisso, como o direito é uma ciência dinâmica e que deve acompanhar as evoluções sociais, torna-se essencial um aprimoramento na compreensão desses delitos, para assim regular as situações críticas, e frear o avanço dos criminosos digitais.

A seguir será feito um aprofundamento em alguns pontos essenciais desse "mal" da evolução tecnológica, de forma a consolidar as bases para o objeto principal do presente trabalho, qual seja, discutir a competência nos crimes informáticos "impróprios".

3.1 Objetividade Jurídica

[93]Antes de adentrar na terminologia adequada aos crimes informáticos, torna-se essencial tecer considerações quanto a objetividade jurídica desses delitos.

O Direito Penal, especialmente em países de caráter democrático como o Brasil, tem por base essencial a proteção de bens jurídicos, nesse sentido, Cezar Roberto Bitencourt parafraseando Roxin, traz interessante conceito, vejamos:

> Em uma linha similiar, mas sem recorrer expressamente ao método analítico da *filosofia da linguagem*, Roxin defende que: "em um Estado democrático de Direito, que é o modelo de Estado que tenho como base, as normas penais somente podem perseguir a finalidade de assegurar aos cidadãos uma coexistência livre e pacífica garantindo ao mesmo tempo o respeito de todos os direitos humanos. Assim, e na medida em que isso não passa ser alcançado de forma mais grata, o Estado deve garantir penalmente não só as condições individuais necessárias para tal coexistência (como a proteção da vida e da integridade física, da liberdade de atuação, da propriedade etc.), mas também das instituições estatais que sejam imprescindíveis a tal fim (uma Administração da justiça que funcione, sistemas fiscais e monetários intactos, uma Administração sem corrupção etc.). Chamo "bens jurídicos" a todos os objetos que são legitimamente protegidos pelas normas sob essas condições"[34]... Na nossa concepção essa é verdade mais adequada na conceituação de bem jurídico penal. E com essa base defendemos que a exegese do Direito Penal está estritamente vinculada à

[92] SAFERNET, 2017, **op. cit.,** s/p.

[93] Tópico utilizado em resumo expandido intitulado "CONSIDERAÇÕES ACERCA DO "NOMEN JURIS" DOS CRIMES INFORMÁTICOS", do Encontro Toledo de Iniciação Científica "Prof. Dr. Sebastião Jorge Chammé" (ETIC), no ano de 2018, disponível em: <https://bit.ly/2RsVA43> acesso em: 01/10/2018.

> dedução racional daqueles bens essenciais para a coexistência livre e pacífica da sociedade.[94]

Assim, toda disciplina penal é orientada com escopo de proteger um elemento essencial à sociedade, por exemplo, a tipificação do homicídio[95] visa tutelar o bem jurídico vida, a do peculato[96], que tutela a administração pública. E os crimes informáticos, tem por finalidade principal proteger qual, ou quais bens jurídicos?

Em primeiro lugar, conforme Marcelo Xavier de Freitas Crespo[97] sabiamente coloca, a objetividade jurídica dos crimes informáticos pode ser vista através de duas lentes, uma lente que guia a informática como um instrumento para a prática de delitos já conhecidos, como estelionato, calúnia, fraudes bancarias, e, uma lente que leva à visão de crimes que surgiram essencialmente da evolução tecnológica informática, e que portanto, só podem ser praticados por esse meio, um exemplo seriam as invasões de e-mails, propagações de “vírus” e o sequestro de dados e informações digitais, é o que Túlio Viana[98] classifica e divide como “crimes informáticos impróprios”, e “crimes informáticos próprios”, classificação essa que será esmiuçada mais à frente.

Dessa forma, Marcelo Xavier de Freitas[99], traz a ideia de que os crimes informáticos, principalmente na perspectiva imprópria, acabam por assumir um caráter eminentemente pluriofensivo, ou seja, ofendem vários bens jurídicos típicos e já conhecidos, como honra, patrimônio e etc, e mais, por outro lado, analisando a ótica dos crimes informáticos “próprios”, se vislumbram novos bens jurídicos, surgindo uma concepção autonomista desse tipo de delito.

Aí vem a questão, afinal, quais são esses bens jurídicos novos? O que considerar como base para essa nova categoria de crimes? Spencer Toth Sydow[100], traz a ideia de que o bem jurídico desses delitos seria a segurança informática, um bem jurídico de natureza difusa, que assim como o meio ambiente, outro bem

---

[94] ROXIN, Claus, 2007, p. 447. apud, BITENCOURT, Cezar Roberto. **Tratado de direito penal, v.1 parte geral. 21.** São Paulo: Saraiva, 2015, p. 45-46.
[95] Artigo 121 do Código Penal - BRASIL. **Código Penal. Decreto-Lei 2.848, de 07 de dezembro de 1940**, 1940. Disponível em: <https://bit.ly/1dqm1Rx> Acesso em 09/10/2018 às 14h29min. s/p.
[96] BRASIL, 1940, **loc. cit.,** s/p.
[97] CRESPO, Marcelo Xavier de Freitas. **Crimes digitais.** São Paulo: Saraiva, 2011. p. 56-57.
[98] VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013, p.29.
[99] CRESPO, 2011, **loc. cit.,** p. **57**
[100] SYDOW, Spencer Toth. **Col. Saberes monográficos - Crimes informáticos e suas vítimas,** 2. ed. São Paulo: Saraiva, 2015. [Recurso Eletrônico – “Minha Biblioteca”], p. 85.

jurídico difuso, é de suma importância para a vida e desenvolvimento da sociedade, afetando-a direta e indiretamente, sendo por isso, digno de proteção jurídica, nesse sentido o autor expõe:

> Isto posto, condutas que aviltem a rede como um todo merecem o titulo de violadoras de bem jurídico difuso, como a propagação incontrolada de malwares ou o ataque de negação de serviço a um provedor de conteúdo da internet que viola razoável segurança da rede.[101]

Túlio Vianna[102], também acredita na concepção de bens jurídicos novos aos delitos informáticos, porém, em vez de tratar esses como sendo "a segurança informática", o autor busca analisar de forma um pouco mais específica e menos difusa, colocando como bem jurídico desses delitos a "inviolabilidade das informações automatizadas"[103], que no fundo nada mais é que os dados armazenados nos dispositivos e redes informáticos, pois, na concepção do autor[104], tal armazenamento possui peculiaridades em razão de ser fruto de uma conversão totalmente eletrônica, diferente do que se tinha no passado.

Há outros autores, como Marcelo Xavier de Freitas Crespo, que apesar de reconhecer a existência de particularidades e bens jurídicos específicos aos delitos informáticos de natureza imprópria, no fundo acredita que o bem jurídico essencial dessas tipificações é a "informação"[105], pois, o meio informático é composto por uma aglutinação de dados, que nada mais são que informações sujeitas a vulnerabilidades, ataques, destruição, quebra de sigilo.

Postas as considerações, não há, por ora, na doutrina, um caminho seguido por todos autores para a determinação de um bem jurídico informático específico, parecem que as posições colocadas são complementares, ainda que tenham suas diferenças, pois, o meio informático possui de fato uma natureza difusa e se apresenta claramente como um aglomerado de informações.

Parece, entretanto, que em um aspecto prático a ideia de qualificação da informação trazida por Túlio Vianna aparenta ser mais acertada, já que em razão das peculiaridades do meio informático, ter um bem jurídico específico como a "inviolabilidade das informações automatizadas" pode facilitar a compreensão e a

---

[101] SYDOW, 2015, **op. cit.,** p. 88.
[102] VIANNA, 2013, **op. cit.,** p. 21.
[103] VIANNA, 2013, **op. cit.,** p. 21.
[104] VIANNA, 2013, **op. cit.,** p. 21.
[105] CRESPO, 2011, **op. cit.** p. 57-58.

disciplina legal desses crimes, questão essa que ainda engatinha lentamente frente ao avanço da era digital.

3.2 Classificações

Classificar algo em qualquer ciência não é tarefa fácil, pois, as classificações, tanto em outras áreas, quanto no Direito, podem surgir de vários critérios e aspectos, tendo um certo grau de subjetividade de seu classificador, contudo, para fins de obter um conceito sólido, adentrar em algumas classificações torna-se essencial para a compreensão dos delitos informáticos.

Vários doutrinadores se preocuparam em trazer classificações para os crimes virtuais, buscando vários critérios, Rovirá del Canto[106] separou os crimes informáticos em quatro espécies, a primeira abarcando os ilícitos relacionados à intimidade, a segunda aos de caráter econômico, a terceira aos conteúdos de comunicação ou difusão de conteúdos nocivos e na quarta outros delitos que não se enquadravam nessas hipóteses.

Klaus Tiedmann[107] buscou um viés mais econômico, classificando os delitos informáticos em “manipulações”, “espionagem”, “sabotagem”, “furto de tempo”; perceba que diferente da primeira classificação que menciona situações subjetivas como a intimidade, as nomenclaturas da classificação de Tiedmann denotam lesões eminentemente patrimoniais, típicas do aspecto econômico objetivado pelo autor na classificação.

O mais importante critério de classificação, no entanto, parece ser o das classificações que observam que o meio informático pode assumir duas principais posições quanto aos delitos, uma como o ator principal, através de práticas delituosas cuja existência depende do meio informático, ou adotar uma postura de figurante, secundária, sendo o cenário e, ou, instrumento para a prática de um tipo penal independente do universo informático. Dentre os doutrinadores que levaram em conta esse critério, um dos precursores foi Briat, a despeito de sua classificação, válidas são as palavras de Damásio de Jesus, que coloca:

---

[106] CANTO. Rovira del, 2002, p.128, apud JESUS, Damasio de. **Manual de crimes informáticos**, 1. ed. São Paulo: Saraiva, 2016. (Recurso Eletrônico – “Minha Biblioteca”). p. 52.
[107] TIEDMANN. Klaus, 1980, p. 122-129, apud CRESPO, 2011, **op. cit.,** p. 60.

> Em nosso sentir, a classificação mais precisa se assemelha à proposta por Briat (1985), diga-se, a distinção entre crimes informáticos em que a informática é o meio para a prática de velhos crimes ou agressão a bem jurídico protegido pelo Direito Penal, e crimes informáticos em que a informática (inviolabilidade dos dados) é o bem jurídico protegido, propriamente dito.[108]

Uma das classificações mais famosas e de grande importância para o presente trabalho, é a trazida por Túlio Vianna[109], a qual leva em consideração principalmente a objetividade jurídica dos crimes informáticos para situar a posição do meio informático em relação às figuras delituosas. Dessa forma o autor[110] divide os crimes informáticos em 4 classes: a) Crimes Informáticos impróprios; b) Crimes informáticos próprios; c) Crimes informáticos mistos; d) Crimes informáticos mediatos ou indiretos;

A seguir, veremos os principais pontos dessa classificação, tendo em vista que o conceito, principalmente de delitos informáticos impróprios, integra a discussão principal do presente trabalho.

3.2.1 Delitos informáticos próprios, impróprios, mistos e imediatos

Os delitos informáticos impróprios para o autor,[111] são aqueles em que o bem jurídico tutelado não é o bem jurídico típico dos delitos informáticos, ou seja, não é a inviolabilidade de dados, são, como nome sugere, impropriamente chamados de crimes informáticos.

Esses delitos impróprios, são tipos penais comuns e já conhecidos dos ordenamentos, cuja existência independe do meio informático, esse acaba por ser utilizado como ambiente ou ferramenta, arma, para a prática delituosa comum, como nos crimes de estelionato digital, fraude, crimes contra a honra, pornografia, e até, segundo o autor[112], tráfico de drogas e prostituição.

A contrário sensu, os delitos informáticos próprios, são aqueles cuja objetividade jurídica é a “inviolabilidade da informação automatizada (dados)”[113], são delitos umbilicalmente ligados ao meio informático, pois, sem esse, inexistem.

---

[108] BRIAT. Martine, 1985, p. 287, apud JESUS, 2016, **op. cit.**, p.52.
[109] VIANNA, 2013, **op. cit.,** p. 29-36.
[110] VIANNA, 2013, **op. cit.,** p. 29.
[111] VIANNA, 2013, **op. cit.,** p. 30-31.
[112] VIANNA, 2013, **op. cit.,** p. 31.
[113] VIANNA, 2013, **op. cit.,** p. 32.

Dentre os exemplos de crimes informáticos próprios, a invasão de sistemas, também chamado de *hacking*, é um dos mais famosos tipos de delito, segundo Marcelo Xavier de Freitas Crespo[114] essa conduta é caracterizada pela entrada a partir de um meio irregular a um sistema, como um computador, um email, e o que motiva o invasor pode ser tanto mero deleite, como à obtenção de alguma vantagem técnica ou econômica, podendo em muitos casos, a "invasão" ser utilizada como um "delito meio", nesses casos o delito informático recebe o nome de "imediato", "indireto".

Além da invasão a sistemas informáticos, outros exemplos de delitos próprios são: obtenção ou transferência ilegal de dados[115], dano informático[116], propagação de vírus, e o delito de "*phishing"*, "pesca", delito muito comum na atualidade, no qual, a partir do uso de armadilhas como anúncios chamativos, páginas falsas, os criminosos acabam por obter informações e dados pessoais das vítimas, que poderão ser utilizados para outros crimes, como fraude, compras irregulares e etc.[117]

Em relação aos delitos informáticos mistos, segundo Damásio de Jesus,[118] são delitos que além de proteger a inviolabilidade de dados, a lei atribuiu outro bem jurídico específico, Túlio Vianna[119] usa como exemplo de tais delitos, a conduta descrita no art. 72, inciso I, da Lei 9.504/1997, que é o crime de acesso irregular ao sistema de dados utilizado pelo serviço eleitoral a fim da alterar a apuração ou contagem de votos, nesse delito percebe-se além da proteção aos dados, existe uma proteção ao sistema democrático e à integridade das eleições.

Por fim, quanto aos delitos informáticos mediatos, ou indiretos, remonta àquela situação mencionada no crime de "hacking", ou seja, quando um delito informático próprio é utilizado como crime-meio para um crime-fim, nesse sentido Damásio coloca:

> trata-se do delito informático pra- ticado para a ocorrência de um delito não informático consumado ao final. Em Direito informático, comumente um delito informático é cometido como meio para a prática de um delito-fim de ordem patrimonial. Como, por exemplo, no caso do agente que captura

[114] CRESPO, 2011, **op. cit.,** p. 64.
[115] CRESPO, 2011, **op. cit.,** p. 70.
[116] CRESPO, 2011, **op. cit.,** p. 71.
[117] CRESPO, 2011, **op. cit.,** p. 74-86.
[118] JESUS, 2016, **op. cit.,** p. 52.
[119] VIANNA, 2013, **op. cit.,** p. 34-35.

> dados bancários e usa para desfalcar a conta corrente da vítima. Pelo princípio da consunção, o agente só será punido pelo delito-fim (furto)[120]

Calha dizer que os delitos informáticos impróprios integram o objeto principal do presente trabalho, por um simples motivo, enquanto que nas práticas próprias até por força da legalidade, leis específicas vieram e vêm regulando tais delitos, nas práticas impróprias não há uma harmonização legal que adeque totalmente os delitos às peculiaridades do ambiente virtual, criando áreas de discussão e problemas importantes, um deles se dá no âmbito da determinação da competência.

3.3 Conceito e "*Nomen Juris"*

A partir de uma análise conjunta da objetividade jurídica e das classificações dos crimes praticados no âmbito informático, é possível extrair um conceito simplório e adequado acerca do tema. Podendo considerar delitos informáticos como sendo toda prática que se utiliza dos aparatos tecnológicos da atualidade, como computadores, celulares, internet, dentre outros, com a finalidade de agredir o sigilo e a integridade dos dados que compõe o mundo digital.[121]

Ainda, cabe dizer, que apesar das práticas impróprias não lesarem propriamente os bens jurídicos informáticos, essencial agregá-las ao conceito, tendo em vista que se convencionou chamar todos os delitos que utilizam dos meios digitais, de crimes informáticos, embora impreciso, já faz parte dos ensinamentos, logo, deve ser aceita a terminologia; "crimes informáticos impróprios", para designar as práticas que se utilizam dos meios digitais, porém, acabam por visar a tutela de bens jurídicos diversos dos dados e informações armazenadas.

3.3.1 A busca pelo *"nomen juris"*

[122]Uma questão muito divergente no meio doutrinário é no que tange ao "*nomen juris"* dos delitos praticados no meio informático. Em uma breve pesquisa

---

[120] JESUS, 2016, **op. cit.,** p. 53.
[121] VIANNA, 2013, **op. cit.,** p. 29.
[122] Tópico utilizado em resumo expandido intitulado "CONSIDERAÇÕES ACERCA DO "NOMEN JURIS" DOS CRIMES INFORMÁTICOS", do Encontro Toledo de Iniciação Científica "Prof. Dr.

sobre as obras relacionadas ao tema, é perceptível a pluralidade de designações atribuídas, como: crimes virtuais, crimes digitais, cibercrimes, crimes informáticos, crimes de computação, e aí fica a dúvida, existe uma mais adequada?

A doutrina não é pacífica, sendo equivocado condenar plenamente uma ou outra nomenclatura. Dentre as múltiplas expressões utilizadas, serão analisadas as três mais usuais: *cibercrimes*, *crimes digitais* e *crimes informáticos*, o motivo da restrição é que muitos dos nomes acabam sendo sinônimos ou termos muitos vagos, dessa forma a separação busca evitar repetições.

A primeira expressão que merece destaque é muito utilizada, contudo, se destaca por receber críticas quanto sua tecnicidade, é a expressão *"cibercrimes"*. Segundo Fernando José da Costa[123], a cibernética é uma ciência de caráter amplo, que estuda a interação do homem com os sistemas que o circundam, tendo em vista as inúmeras variáveis e fenômenos que compõe essas interações, uma delas é a que se dá com os sistemas computacionais.

Assim, nota-se uma relação de continência entre os sistemas computacionais e a cibernética, objetivando uma diferenciação, Fernando José da Costa coloca:

> no sistema informático, com integração do sistema de informação e do computador, o homem alimenta a máquina com dados, que irão produzir um resultado ocasionado em razão deste comando humano.22 Esse resultado, alcançado pela vontade humana através do cérebro, do sistema nervoso e da máquina, pode ser denominado "cibernética".[124]

Dessa forma fica nítido que a expressão *"cibercrimes"* acaba por não ser adequada em razão do seu caráter genérico, já que a Cibernética como ciência pode representar inúmeros outros sistemas que não necessariamente o virtual, e seu foco não é a prática ou o objeto informático em si, mas sim a análise da interação do organismo humano com outros meios e máquinas. Nesse sentido, Túlio Vianna coloca:

> Muitos autores insistem em inserir o crime informático em uma categoria que eles denominam de crimes cibernéticos. Trata-se, contudo, de uma denominação completamente inadequada, baseada tão somente no uso vulgar que é dado à palavra, relacionando-a a tudo aquilo que está

Sebastião Jorge Chammé" (ETIC), no ano de 2018, disponível em: <https://bit.ly/2RsVA43> Acesso em: 01/10/2018.

[123] COSTA, 2011, **op. cit.,** p. 16-17.

[124] COSTA, 2011, **op. cit.,** p. 18.

> vinculado às modernas tecnologias. O objeto de estudo da Cibernética é extremamente amplo e eminentemente multidisciplinar e não tem qualquer relação com os delitos aqui estudados, extrapolando em muito os limites do presente trabalho. O pouco que há de cibernético na análise ora apresentada se limita ao estudo do controle exercido pelo homem em relação a computadores e pelo ordenamento jurídico em relação àquele homem capaz de controlar tais máquinas. Nada mais.7[125]

Outro termo muito utilizado é a expressão *"crimes digitais"*, essa, em especial, tem caráter bem interessante, pois, como ensina um dos defensores da designação, Marcelo Xavier de Freitas Crespo[126], tal expressão aparenta ser mais adequada justamente por um dos motivos que sofre críticas, sua generalidade, em razão dessa característica ela consegue se amoldar de forma bem eficaz à evolução informática e das consequentes novas formas de praticar esses delitos, já que os sistemas digitais são amplos, podendo ser desde uma calculadora até as interações na internet.

Válido observar, que generalidade não se confunde com a falta de tecnicidade da expressão crimes cibernéticos, pois, essa cita uma ciência com pouquíssima relação com o objeto estudado, diferente da expressão crimes digitais que apesar de sua generalidade, possui relação íntima com o objeto ao qual se refere.

Por fim, a última nomenclatura que merece destaque, é a expressão "delitos informáticos", segundo Túlio Vianna[127], a melhor nomenclatura é aquela capaz de privilegiar o bem jurídico tutelado, no caso, como já pontuado no tópico de objetividade jurídica, a essência desses crimes parece ser a proteção do sigilo e integridade das informações, dados, armazenados no meio informático, logo há conexão direta entre a referida expressão, o meio onde se situam as práticas delituosas e o bem jurídico tutelado.

Diante dessa breve análise, sem desprezar a expressão *"crimes digitais"*, parece mais adequado ao trabalho a designação *"crimes informáticos"*, o motivo é realmente a maior tecnicidade em razão da adequação com o bem jurídico e o meio onde ocorrem tais práticas delituosas.

---

[125] VIANNA, 2013, **op. cit.,** p. 22.
[126] CRESPO, 2011, **op. cit.,** p. 47-51.
[127] VIANNA, 2013, **op. cit.,** p. 21.

3.4 Os Criminosos Digitais

Segundo Damásio[128], por muito tempo a figura do criminoso informático esteve ligada ao sujeito dotado de grande conhecimento técnico sobre as tecnologias computacionais, o crime informático tinha uma natureza especializada, o criminoso se valia de seus saberes e executava invasões e golpes complexos.

Hoje, no entanto, segundo o autor[129], tal pensamento vem se alterando, a grande tendência é que cada vez mais agentes “comuns”, sem tanto conhecimento específico, pratiquem crimes de natureza informática.

Essa mudança de vertente, se dá tanto pela difusão dos saberes informáticos, quanto pelo próprio descuido das vítimas, já que esses novos usuários em massa nem sempre são cuidadosos, contribuindo e facilitando à pratica dos delitos informáticos, um exemplo é o caso das pessoas que clicam em “*links”* suspeitos, ou instalam programas de fontes desconhecidas e consequentemente acabam por se tornar vítimas desses criminosos que se aproveitam do descuido. Assim, hoje é possível afirmar que qualquer pessoa pode ser um possível criminoso digital.

Trazendo a questão da classificação dos crimes informáticos em próprios e impróprios à presente análise, conforme Marcelo Xavier de Freitas Crespo[130] nos ensina, seguindo a lógica de que os crimes informáticos impróprios são práticas delituosas já conhecidas fora do ambiente informático, mas que utilizam das particularidades desse para atingir o resultado pretendido, enquanto que os crimes próprios são às práticas que visam lesar as informações armazenadas nos sistemas informáticos, é possível dizer que, em tese, o sujeito ativo de um crime informático próprio, na maioria das vezes tem a necessidade de um maior conhecimento informático, do que um criminoso informático impróprio, pois, no último a prática delituosa vem de fora do mundo tecnológico, não demandando conhecimentos tão específicos.

Sem adentrar muito nos aspectos criminológicos, válido dizer que no âmbito dos delitos informáticos a “comunidade” de usuários acaba por trazer nomenclaturas para definir os criminosos virtuais, principalmente os que praticam os

---

[128] JESUS, 2016, **op. cit.,** p. 56.
[129] JESUS, 2016, **op. cit.,** p. 56.
[130] CRESPO, 2011, **op. cit.,** p. 94.

delitos impróprios. Tais nomenclaturas levam em conta desde os conhecimentos técnicos, até o tipo de delito praticado.

Um dos termos popularmente utilizados em relação aos criminosos virtuais, é o *"hacker"*, em que pese muitas vezes esse termo ser utilizado para definir um sujeito que pratica crimes virtuais,[131] é importante dizer que a expressão tem caráter genérico, de forma que nem sempre um "hacker" será um criminoso, nesse sentido, Damásio[132] define o hacker como um "profundo conhecedor de informática, podendo ser um profissional de segurança da informação ou pesquisador, que não utiliza seus conhecimentos para fins ilegítimos."

Da definição dada por Damásio acima, se extrai a figura dos chamados *"White hats"*[133], que são considerados "hackers do bem", que muitas vezes trabalham para empresas, ou ajudam de forma gratuita a comunidade virtual, buscando detectar ataques e fragilidades dos sistemas informáticos, de forma a proporcionar maior segurança no ambiente digital.

Adentrando nas outras designações, a maioria dos indivíduos pertencentes ao universo informático, são os que utilizam dos sistemas tecnológicos sem grandes pretensões ou ânimo de cometer práticas delituosas, os chamados *"lusers"*[134].

Existem indivíduos com conhecimento básico de informática, que na prática não representam tanto risco, mas que acreditam ser verdadeiros e perigosos criminosos informáticos, são os chamados *"lammers"*, tais pessoas não são bem vistas na comunidade, e segundo Crespo[135], são comumente insultadas e depreciadas pelos criminosos informáticos experientes. Em um patamar acima desses, estão os chamados *"wannabes"*, que na visão de Marcelo Xavier de Freitas Crespo[136], em razão do grau de conhecimento maior, compreendem melhor sua capacidade lesiva, apresentando mais risco que os *"lammers"*.

Chegando aos verdadeiros criminosos informáticos, representando os mais perigosos, tem-se os *"crackers",* os *"internals"* e os "espiões". Os crackers[137], segundo Crespo, são os invasores, aqueles que quebram sistemas de segurança,

---

131 CRESPO, 2011, **op. cit.,** p. 95.
132 JESUS, 2016, **op. cit.,** p. 58.
133 BRITO, Auriney. **Direito penal informático,** 1ª edição, São Paulo: Saraiva, 2013. (Recurso Eletrônico – "Minha Biblioteca"), p. 83.
134 BRITO, 2013, **op. cit.,** p. 83.
135 CRESPO, 2011, **op. cit.,** p. 97.
136 CRESPO, 2011, **op. cit.,** p. 97.
137 CRESPO, 2011, **op. cit.,** p. 96.

sequestram dados e praticam inúmeras atrocidades e delitos, possuem geralmente um grau de conhecimento mais elevado, dentro dos crackers, mesmo que alguns autores separem dessa categoria, é possível colocar os *"caders"* e os *"phreakers",* pois, ambas categorias representam invasores digitais, sendo contudo, invasores específicos, os *"caders"* no que concerne às práticas bancárias[138], como clonagem de cartões de crédito, e simulação de contas falsas, e os *"phreakers",* sendo os especialistas em telefonia móvel e fixa, interceptando ligações, fraudando pagamentos e etc.[139][140]

Os *"internals"*, no que pese poderem ser *"crackers",* possuem uma característica específica que os tornam diferentes, pois, segundo Túlio Vianna[141], tal categoria é representada por funcionários de empresas que possuem acesso a inúmeros dados e informações, quando saem, ou são demitidos acabam se utilizando desses conhecimentos para atacar a própria empresa.

Por fim, os "espiões", também chamados de "professional criminals",[142] são indivíduos com alto conhecimento informático, treinados por organizações de Inteligência mundial, que quando saem dessas, utilizam de seus conhecimentos para fazer os mais variados tipos de ataques, um exemplo é a espionagem corporativa[143].

Um caso interessante que provavelmente se utilizou de "espiões", é o grande escândalo envolvendo as eleições norte-americanas de 2017, o caso denominado *"Spygate"*[144]*,* trata-se da suspeita do uso de "espiões virtuais" com ligação à Rússia, para obtenção de informações importantes a campanha e eleição do Presidente Donald Trump, se tais denúncias vierem a se confirmar, só evidenciará o quão grande é a importância dos meios informáticos e dos agentes digitais na vida atual, podendo decidir eleições, e alterar estruturas do Estado.

Diante do exposto, é possível compreender em primeiro lugar que nem todo indivíduo que domina a tecnologia informática será um criminoso virtual, e também, no que pese uma parcela importante dos criminosos informáticos deterem

---

138 CRESPO, 2011, **op. cit.,** p. 96.
139 CRESPO, 2011, **op. cit.,** p. 97.
140 VIANNA, 2013, **op. cit.,** p. 42.
141 VIANNA, 2013, **op. cit.,** p. 41.
142 VIANNA, 2013, **op. cit.,** p. 41.
143 VIANNA, 2013, **op. cit.,** p. 41.
144 KESSLER, Glenn. **Trump's 'spygate' claim is latest off-target salvo at Russia probe**, Chiacago: Chicago Tribune, 2018. Disponível em: <https://trib.in/2J2NrTU> Acesso em 25/09/2018 às 16h58min, s/p.

conhecimentos específicos do meio virtual, esses conhecimentos aprofundados não são essenciais para o cometimento de crimes informáticos.

Está havendo uma mudança de prisma, já que muitos criminosos "comuns" observaram nas peculiaridades do ambiente virtual uma grande oportunidade para praticar delitos já conhecidos, como estelionato, pedofilia, fraude e etc, de modo que os crimes informáticos impróprios acabam por ganhar tanta ênfase, quanto os próprios, em razão disso, merecendo um tratamento especial.

3.5 As Vítimas dos Delitos Informáticos

Dos dados já apresentados sobre os impactos dos crimes informáticos, é possível extrair a ideia de que qualquer pessoa está sujeita a ser vítima de um crime virtual.

A conclusão do parágrafo anterior, segundo Fabio R. Kummer,[145] ocorre porque advento tecnológico fez e faz com que a sociedade se integre de maneira maior ao ambiente informático, e dessa maior integração, resulta em aumento no grau de exposição das pessoas ao ambiente virtual, o que acaba por fomentar e favorecer as ações dos criminosos informáticos, tendo em vista que muitos desses usuários acabam por não adotar cuidados básicos de segurança, criando um campo de vulnerabilidade a ser explorado pelos infocriminosos.

Auriney Brito Junior[146] ressalta que muitas vezes nos crimes informáticos a vítima acaba contribuindo de forma determinante para a ação dos criminosos, principalmente por não tomarem cautelas necessárias no mundo informático, adentrando em páginas suspeitas, abrindo e-mails desconhecidos, se expondo de forma exagerada em redes sociais, dentre outros comportamentos.

Um dos exemplos mais claros de atuação positiva da vítima para a ocorrência dos crimes virtuais é na chamada conduta de *"phishing",* "pesca", nessas práticas o criminoso informático cria "armadilhas" com programas, e-mails, sites suspeitos, capaz de induzir o usuário descuidado a interagir com as armadilhas, ao clicar, fazer download ou digitar dados com informações de cartões de crédito e etc, abre caminho para o criminoso informático realizar dezenas de outros ilícitos

---

[145] KUMMER, Fabiano Ratton. **Direito Penal na Sociedade da Informação**. 1.ed. Paraná: Publicação Independente, 2017. (Recurso Eletrônico – "Edição do Kindle"). s/p.
[146] BRITO, 2013, **op. cit.,** p. 86.

derivados, como compras indevidas, sequestro de dados, clonagem de cartões de crédito e etc.[147]

Outro ponto que merece destaque, é a triste situação relacionada ao crescente número de crianças vítimas do meio informático, especialmente em delitos de caráter sexual, onde segundo Fabio R. Kummer[148], criminosos se aproveitam de chats, salas de bate papo, muitas vezes mentindo a própria idade, a fim de convencer o menor a enviar fotografias ou realizar atos libidinosos pelo meio virtual.

O assunto sobre a proteção das crianças e adolescente no meio computacional, ganhou tanta importância, que a Convenção de Budapeste de 2001, tratado internacional destinado ao combate dos crimes informáticos, colocou como uma de suas bases essenciais a proteção do menor e do adolescente, visando coibir principalmente a pornografia infantil.[149]

Ante as breves considerações realizadas, extrai-se em primeiro momento, que a vítima no âmbito informático tem um caráter bem amplo, estando qualquer pessoa vulnerável a um delito desse porte, contudo, existe uma preocupação crescente no cenário relacionado à crianças e adolescentes no ambiente virtual, situação que vem adquirindo inclusive importância internacional.

E por fim, nota-se que nos crimes informáticos, de regra, a vítima acaba contribuindo de alguma forma para o delito, facilitando a ação do criminoso virtual ao se expor e não tomar cuidados no ambiente virtual.

Da conclusão acima, é possível dizer que um importante caminho para o combate dos crimes virtuais está na prevenção, assim como existem campanhas de prevenção a doenças sexualmente transmissíveis, informativas dos perigos da ingestão de bebidas alcóolicas ao dirigir, devem existir campanhas para conscientização dos cuidados a serem tomados no ambiente informático, para assim reduzir as fragilidades do ambiente virtual e consequentemente reduzir o número de crimes informáticos.

---

147 BRITO, 2013, **op. cit.,** p. 87.
148 KUMMER, 2017, **op. cit.,** s/p.
149 BRITO, 2013, **op. cit.,** p. 53.

3.6 Peculiaridades do Ambiente Informático

O ambiente informático é dotado de certas peculiaridades capazes de dar um ar, e características diferenciadas aos delitos, mesmo nos crimes de natureza imprópria, aqui serão tratadas algumas dessas qualidades a fim de evidenciar que todo tipo de delito informático, ainda que não exclusivo do meio, merece um tratamento especial.

A primeira característica que merece destaque, é a internacionalidade do ambiente informático, nesse ponto, o advento da internet e da comunicação em geral teve e tem grande importância, de forma que o mundo atual está todo conectado através dos grandes provedores. Assim essa característica se traduz pelo rompimento das barreiras geográficas e temporais que existiam, um chinês pode acessar um site hospedado em um servidor brasileiro, da mesma forma que um turista americano no Brasil pode obter imagens em tempo real dos acontecimentos em sua residência nos Estados Unidos.[150]

O caráter internacional nos crimes informáticos cria inúmeras discussões, dentre elas a relacionada a dificuldade de detecção do infrator, que pode estar em qualquer lugar do globo, e também de punição efetiva desse, dúvidas de aplicação da lei penal no espaço, e questões relacionadas a extraterritorialidade e à atribuição da competência de julgar.

A evolução tecnológica não só rompeu as barreiras geográficas, como também com a barreira temporal, e aí entra a velocidade, tal elemento recebeu destaque no estudo do histórico da computação, e é marca registrada dessa nova era, pois amplifica a transmissão de informações e dados de maneira nunca antes vista.

Na seara criminal a velocidade é capaz de amplificar os impactos de vários delitos, como da pirataria digital, facilitando a disseminação dos conteúdos replicados[151], outro exemplo é o caso dos crimes contra a honra, já que as ofensas podem se espalhar com grande rapidez, que somada a internacionalidade do ambiente informático, é capaz de causar uma enorme lesão ao ofendido.

---

[150] SYDOW, 2015, **op. cit.,** p. 94.
[151] SYDOW, 2015, **op. cit.,** p. 111-112.

O anonimato, também é uma das marcas do ambiente informático, segundo Spencer Toth Sydow,[152] o mundo virtual se caracteriza por um indivíduo transmitindo comandos a um dispositivo informático, daí nasce o anonimato, pois, no que pese a existência de mecanismos de identificação desse usuário como senhas, nomes, símbolos, é quase impossível afirmar, com certeza, que aquela pessoa de fato é quem estava por detrás daqueles comandos. [153]

Essa característica contribui para muitos delitos no âmbito informático, já que dá ao criminoso uma certa "segurança", de que não será facilmente identificado e punido, o que acaba por desmoralizar os próprios mecanismos de repressão do Estado, dada a dificuldade e a falta de aparatos para investigar esses delitos.

Os dados informáticos são intangíveis, ou seja, não possuem uma concretude, para Spencer Toth Sydow "nada mais são do que bits interpretados por dispositivos"[154], assim, não são palpáveis, ainda, segundo o autor, tal fator é importante, pois "leva a uma forte dificuldade de adaptação das regras que já existem, atinentes a delitos que violam patrimônio e, portanto, geram uma necessidade de legislação especial."[155] Dessa característica decorre outra, chamada pelo autor[156] de "pluralidade", essa nada mais é que a capacidade de replicação dos dados informático, ou seja, é possível criar cópias idênticas de dados e programas.

A "pluralidade" além de ser bastante aproveitada pela pirataria digital, cria algumas discussões, pois, em tese no mundo digital os dados não são "furtados", mas sim replicados, então a coisa muitas vezes não sai propriamente da esfera de cuidado da vítima, mas sim transmuta-se em arquivo idêntico para o agressor, perceba, novamente a intangibilidade dificultando a aplicação da lei penal padrão.

Da intangibilidade se extrai mais um elemento, o fato de que no ambiente informático é possível um indivíduo estar ao mesmo tempo em lugares distintos, é o que Spencer Toth Sydow[157] chama de "ubiquidade do meio informático", isso é possível através da soma de várias das peculiaridades aqui demonstradas, dentre elas as principais são a intangibilidade, a velocidade, e a

[152] SYDOW, 2015, **op. cit.,** p. 109.
[153] SYDOW, 2015, **op. cit.,** p. 111.
[154] SYDOW, 2015, **op. cit.,** p. 100.
[155] SYDOW, 2015, **op. cit.,** p. 102.
[156] SYDOW, 2015, **op. cit.,** p. 105.
[157] SYDOW, 2015, **op. cit.,** p. 106-109.

internacionalidade, isso permite por exemplo, que um criminoso informático direcione inúmeros ataques à regiões distintas do globo, ao mesmo tempo, ou até, em exemplo mais simples e corriqueiro, qualquer pessoa em seu computador pode através das abas de seu “browser”, “navegador de internet”, acessar sites de localidades distintas ao mesmo tempo.

As peculiaridades apresentadas, demonstram que o ambiente informático se diferencia em muito do ambiente físico em que se desenvolveram as relações humanas de até então, não é à toa que como já pontuado na análise histórica, provocou uma revolução no modo de viver e pensar da sociedade.

Nos crimes informáticos, como demonstrado nos pequenos exemplos, o impacto de tais peculiaridades é gigantesco, tanto no ponto de vista do direito penal objetivo em questões como a determinação do “locus delict”, do tempo do crime, consumação e tipificação, quanto no ponto de vista processual.

Atualmente um dos pontos mais debatidos acerca dos crimes informáticos é a determinação da competência de julgar, questão essa, frise-se, será aprofundada posteriormente. Fato é que as peculiaridades desse meio, somadas a falta de evolução normativa, criaram uma celeuma na doutrina e jurisprudência que acaba a cada momento adotando posicionamentos distintos e controversos, dificultando a vida dos aplicadores do direito.

4 DISCIPLINA LEGAL DOS DELITOS INFORMÁTICOS NO DIREITO BRASILEIRO

Após estudar todas estruturas e desvendar as bases dos crimes informáticos, é importante compreender um pouco acerca da disciplina e estruturação legal da matéria no ordenamento jurídico pátrio, que segundo Damásio de Jesus[158] é bem prematura e recente, estando atrasada em relação a vários países do globo. Cumpre destacar, que as considerações a seguir serão feitas com um caráter mais genérico, sem abordar de forma exaustiva os crimes informáticos próprios, de forma a evitar uma fuga do tema.

Observando o ordenamento brasileiro, a primeira percepção que se tem, é de que não existe uma legislação específica que concentra os delitos informáticos, de modo que Damásio[159] acredita ser uma tendência do direito pátrio a busca pela adequação da legislação já existente, criando um sistema marcado por alterações legislativas pontuais que inserem normas tanto no direito penal objetivo, quanto no direito processual.

Dentre as legislações responsáveis por desenhar as bases dos crimes informáticos no direito brasileiro, sem dúvida alguma as leis 12.135 e 12.137 de 2012, podem ser consideradas marcos importantes desse processo, por esse motivo, visando uma sistematização didática, o estudo breve do sistema legal brasileiro, será divido em, antes e depois das referidas normas, com destaque especial para essas legislações.

4.1 O Sistema Legal Brasileiro Antes das Leis 12.135/12 e 12.137/12

Uma das primeiras normas a trazer de forma mais específica no direito brasileiro a matéria dos delitos informáticos, foi a Lei nº 9.296, de 24 de julho de 1996, também conhecida como Lei da Interceptação telefônica, criminalizou em seu artigo 10 a conduta de quebra de sigilo e interceptação indevida de comunicações telefônicas e informáticas[160].

Outras leis que merecem destaque são, a Lei nº 9.609, de 19 de fevereiro de 1998, que dispõe sobre a propriedade intelectual dos programas de computador, e, a Lei nº 9.983, de 14 de julho de 2000, que inseriu os delitos dos

[158] JESUS, 2016, **op. cit.,** p. 68.
[159] JESUS, 2016, **op. cit.,** p. 68.
[160] COSTA, 2011, **op. cit.,** p. 124.

artigos 313-A e 313-B do Código Penal, tipificando as condutas de inserção de dados e modificação de forma não autorizada de sistemas de informações, segundo Damásio, essa norma "mais se destacou pelo "alerta" sobre os crimes eletrônicos do que contribuiu para o chamado "controle de criminalidade"[161].

Antes do advento das leis nº 12.735 e 12.737, de 30 de novembro de 2012, importante alteração ocorreu no Estatuto da Criança e do Adolescente (Lei nº 8.069, de 13 de julho de 1990), através da Lei nº 11.829, de 13 de julho de 2008, que visando aumentar o combate à pornografia infantil alterou substancialmente os artigos 240 e 241, tornando-os mais amplos, além disso, promoveu a tipificação das condutas de distribuição, armazenamento, aliciamento e simulação de cena pornográfica com criança e adolescente nos artigos 241-A, 241-B, 241-C e 241-D.[162]

Todas alterações promovidas, trouxeram elementos diretos ou indiretos da possibilidade de punição no âmbito informático, adequando a questão da pornografia infantil à evolução tecnológica, dado que essas ganharam muita força através do ambiente virtual[163]. Outra questão interessante que se extrai das alterações da Lei nº 11.829, de 25 de novembro de 2008, é a quebra do estigma de que só seriam necessárias alterações para abarcar os crimes informáticos próprios, perceba, pornografia infantil é um crime informático impróprio, mas as alterações legislativas foram de suma importância para adequação e aplicação das normas punitivas.

4.2 O Advento das Leis nº 12.735/12 e 12.737/12

Miguel Reale[164] concebeu a importante "Teoria Tridimensional do Direito", que de forma simplista, sem qualquer aprofundamento, seria a ideia de que um fato pode desencadear a criação de uma norma ao produzir reflexos em valores sociais, nessa ótica, no ano de 2012, uma invasão ao computador da atriz Carolina

---

[161] JESUS, 2016, **op. cit.,** p. 61.

[162] BRASIL. **Lei nº 11.829, de 25 de novembro de 2008.** Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008. Disponível em: <https://bit.ly/2EkYqpN> Acesso em 11/10/2018 às 15h16min, s/p.

[163] FORTES, Carlos José e Silva**. Lei 11.829 de 25 de outubro de 2018 – "Lei da Pornografia Infantil",** Todos Contra a Pedofilia, 2011. Disponível em: <https://bit.ly/2RKLUTf> Acesso em 28/08/2018 às 19h42min, s/p.

[164]REALE, MIGUEL. **Filosofia do Direito,** 20ª ed. São Paulo: Saraiva, 2002. (Recurso Eletrônico - Minha Biblioteca), p.539.

Dieckmann, com a divulgação de fotos íntimas da famosa[165], provocou bastante comoção social, o que desencadeou o advento de duas marcantes normas para o cenário dos crimes informáticos no Brasil, as leis nº 12.735 e 12.737, de 30 de novembro de 2012, essa última apelidada como Lei Carolina Dieckmann.

A respeito da influência dos fatos de grande comoção social e midiática na criação de normas do direito brasileiro, nota-se que esse movimento não é incomum, existindo inúmeros exemplos, como o caso a edição da Lei nº 8072, de 25 de julho de 1990, Lei dos Crimes Hediondos, cuja criação se deu no bojo do sequestro do empresário Abílio Diniz e do publicitário Roberto Medina[166], outro exemplo é o caso da Favela Naval, no ano de 1997, em que policiais foram flagrados torturando e aterrorizando moradores na região de Diadema, São Paulo, desse fato adveio a Lei nº 9.445, de 7 de abril de 1997, Lei de Tortura.

Além desses, existem vários outros exemplos em que o legislador influenciado pelo destaque midiático editou novas normas em um movimento apelidado por Damásio de Jesus como “populismo penal”[167], acerca do tema o autor pede atenção e observa:

> Em uma sociedade de risco, a aprovação de um Projeto de Lei às pressas, sem ampla discussão, pode gerar margens a enquadramentos errôneos e atitudes que violem direitos e garantias dos cidadãos.[168]

Independentemente dessa “concepção às pressas”, fato é que as leis nº 12.735/2012 e 12.737/2012 possuem grande importância, pois, apesar da pouca amplitude, foram as primeiras normas do direito brasileiro a expressar uma abordagem mais direta e concreta dos crimes informáticos.

A lei nº 12.735/2012 não partiu de uma discussão recente à época, mas sim foi produto de uma discussão nascida em 1999, com o projeto de lei nº 84/99, projeto esse que ao longo de suas discussões foi agregando características inovadoras e ganhando uma abrangência enorme, com alterações não só no Código Penal (Decreto-lei nº 2.848, 7 de dezembro de 1940), como no Código Penal Militar

---

165 G1, Globo. **Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'**, São Paulo: G1. Globo, 2012. Disponível em: <http://glo.bo/KXcf5Z> Acesso em 25/08/2018 às 16h51min, s/p.

166 LIMA, Djalba. **Comoções sociais influenciaram punição de crimes hediondos,** Agência Senado, 2010. Disponível em: <https://bit.ly/2vWdpT1> Acesso em 12/09/2018 às 13h02min, s/p.

167 JESUS, 2016, **op. cit.,** p. 72.

168 JESUS, 2016, **op. cit.,** p. 72.

(Decreto-lei nº 1.001/69, de 21 de outubro de 1969), Lei nº 7.716, de 5 de janeiro de 1989, Lei nº 8.069, de 13 de julho de 1990 e Lei nº 10.446, de 8 de maio de 2002.[169]

O projeto inicial previa alterações como a previsão dos crimes de dano informático, estelionato eletrônico, falsificação de dados eletrônicos, também discorria sobre algumas regras de combate à pornografia infantil no âmbito informático, bem como, quanto o dever e a responsabilidade dos servidores e provedores de internet ante os delitos informáticos.[170]

Contudo o projeto aprovado foi totalmente diferente, muito mais restrito, com alterações pontuais que são observadas a seguir, sendo objeto de muitas críticas doutrinárias, pois, o que poderia ser um marco de inovação no combate e disciplina legal dos delitos informáticos, se tornou apenas uma fumaça de alterações pontuais, nesse sentido Spencer Toth Sydow coloca:

> O projeto inicial – que buscava apresentar princípios, dar definições e criminalizar condutas de dano informático, acesso indevido, alteração de dados, obtenção indevida de dados, violação de segredo e produção de malares em 18 artigos que alterariam o Código Penal – foi aprovado com apenas 6 artigos, sendo que apenas um deles modificou o Código Penal, um alterou o Código Penal Militar e um alterou a Lei n. 7.716/89 (lei que define os crimes resultantes de preconceito de raça ou de cor)...Perdeu-se a maior parte dos tipos penais inovadores para se conseguir a aprovação de algum normativo na área de crimes informáticos, desperdiçando-se muitos anos de trabalho...[171]

Dessa forma a norma foi aprovada com 6 artigos, dos quais os artigos 2º e 3º sofreram veto presidencial. O artigo 2º previa uma alteração no artigo 298 do Código Penal, equiparando a falsificação de documento particular a falsificação de cartão de crédito e débito, tal dispositivo foi vetado por uma questão lógica, pois, a Lei nº 12.737/12, trouxe essa mesma disposição em seu rol, de forma que o veto impediu um centauro jurídico, com duas modificações idênticas na mesma norma.

Já o artigo 3º, da Lei nº 12.735/12, previa duas alterações no artigo 356 do Código Penal Militar (Decreto-lei nº 1001/69), que prevê o crime de favor inimigo, tais alterações objetivavam inserir a expressão “dados eletrônicos” nos incisos II, e III do referido artigo, de forma a responsabilizar os militares que de alguma forma frustrassem ou comprometessem operações militares através do manuseio

---

169 SYDOW, 2015, **op. cit.,** p. 279.
170 JESUS, 2016, **op. cit.,** p. 77-82.
171 SYDOW, 2015, **op. cit.,** p. 279-280.

equivocado de dados eletrônicos, a despeito do motivo do veto Damásio de Jesus coloca:

> Tais alterações foram vetadas pela Presidência da República sob o fundamento de que a amplitude do conceito de dado eletrônico como elemento de ação militar torna o tipo penal demasiado abrangente, inviabilizando a determinação exata de incidência da norma proibitiva.[172]

Assim, a lei nº 12.735/12 promoveu apenas 2 alterações fáticas no ordenamento brasileiro, a primeira foi uma determinação para que os órgãos de polícia judiciária criassem grupos e estruturas específicas de combate aos crimes informáticos. A segunda, talvez a única efetiva, foi na Lei nº 7.716/89, em seu artigo 20, §3º, inciso II, trazendo a possibilidade do magistrado determinar em casos de delitos de preconceito a raça, cor, etnia, religião cometidos pelo meio informático, que o servidor, provedor do site, cesse imediatamente a distribuição dos conteúdos preconceituosos, sob pena de incorrer no crime de desobediência.

A Lei nº 12.737/12, apelidada como Lei Carolina Dieckmann, foi deflagrada na mesma data da lei anterior, e como o apelido indica, foi consequência direta do incidente já relatado com a famosa atriz Carolina Dieckmann, essa norma talvez possa ser considerada a mais importante disciplina legal de crimes informáticos no Brasil, tendo em vista que realizou importantes alterações no ordenamento jurídico pátrio.

Dentre as alterações trazidas pela Lei nº 12.737/12, a primeira que merece destaque foi a inserção dos artigos 154-A, e 154-B ao Código Penal. Tais alterações constituem a base de um novo delito, o crime de Invasão de Dispositivo Informático, nesse sentido o tipo descrito pelo artigo 154-A do Código Penal possui a seguinte redação:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. § 1ºNa mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. § 2ºAumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.§ 3ºSe da invasão resultar a obtenção de conteúdo de

[172] JESUS, 2016, **op. cit.,** p. 77.

> comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos. § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: I - Presidente da República, governadores e prefeitos; II - Presidente do Supremo Tribunal Federal; III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal.

Da redação do tipo penal, é possível observar que tal crime objetiva punir o indivíduo que invade sem autorização um dispositivo informático alheio com o especial fim de manipular os dados ali constantes, seja para cópia, alteração ou destruição, sendo qualificado o delito se os dados manipulados forem informações sigilosas ou de acesso controlado.

A primeira crítica feita pela doutrina[173], é a exigência feita pelo tipo, de que o dispositivo informático possua alguma forma de proteção, pois, do contrário, restará atípica a conduta, tal previsão é prejudicial, dado que o cerne da questão não é a quebra do mecanismo de proteção, mas sim a invasão, entrada não autorizada pelo dono do dispositivo, tendo o legislador pecado ao disciplinar essa exigência.[174]

Outra observação conexa a relatada acima, é a presença dos elementos subjetivos “obter, adulterar ou destruir dados ou informações”[175], previsão essa que Auriney Brito Jr.[176] trata como “temerária”, pois, uma prática comum no âmbito dos criminosos informáticos é a invasão como teste, aprendizado, o indivíduo invade um sistema com o objetivo único de aprimorar suas habilidades, nesses casos, o fato poderá ser considerado atípico pela ausência dos elementos subjetivos específicos, o que demonstra uma falha do legislador, pois, a invasão, ainda que despretensiosa, acaba por violar a vontade do titular do direito, já que não há autorização.

Convém mencionar que o §1º do artigo 154-A, traz uma figura equiparada ao *caput*, cujo objetivo é punir aquele que produz um software, um

---

[173] BRITO, 2013, **op. cit.,** p. 70.
[174] BRITO, 2013, **op. cit.,** p. 70.
[175] Código Penal, Artigo 154-A, BRASIL, 1940, **op. cit.,** s/p.
[176] BRITO, 2013, **op. cit.,** p. 70-71.

programa malicioso capaz de explorar as fragilidades dos sistemas informáticos, nesse ponto, Spencer Toth Sidow[177] observa que deve existir cautela na aplicação do dispositivo, pois, nem sempre quem produz um programa tem noção de sua lesividade, outro caso de cuidado é a situação mencionada por Auriney Brito Jr.[178], pois, muitas vezes, algumas empresas e pesquisadores tem a necessidade de criar métodos e programas para explorar as fragilidades de seus produtos, o que para o autor não seria abarcado pelo delito, desde que demonstrado o fim científico ou técnico da aplicação.

O artigo 154-B, trouxe em sua redação às questões processuais acerca delito anterior, prevendo que, em regra, tal delito se procederá mediante ação pública condicionada a representação, com a exceção da situação em que a administração pública, em seu sentido mais amplo, for a vítima do delito.[179]

A segunda importante alteração trazida pela Lei Carolina Dieckmann, se deu no âmbito do artigo 266, do Código Penal, alterando a redação do dispositivo tanto no "nomen juris", como pela inserção do §1º, de forma a punir quem interrompe serviço informático, telefônico, telegráfico ou de informação de utilidade pública[180]. Tal alteração foi muito bem acertada, pois, visa coibir uma das práticas mais comuns no âmbito informático[181], os ataques por DDoS[182] (*Denial Of Service*), prática pela qual o cracker sobrecarrega um site, ou sistema informático afim de torna-lo indisponível por um determinado tempo, tal qual aconteceu em 2011 no Brasil, deixando fora do ar as páginas da Presidência da República e Portal Brasil da Receita[183].

Por fim, a última das alterações previstas por esse tão importante dispositivo ocorreu no artigo 298 do Código Penal, sendo inserido o parágrafo único, equiparando cartão de crédito e débito a documento particular.

Observando a alteração, no entanto, parece que o legislador se precipitou, nesse sentido Damásio de Jesus[184], levanta o fato de que o mundo vive

---

[177] SYDOW, 2015, **op. cit.,** p. 310.
[178] BRITO, 2013, **op. cit.,** p. 72.
[179] JESUS, 2016, **op. cit.,** p. 108.
[180] Código Penal, artigo 266, BRASIL, 1940, **op. cit.,** s/p.
[181] LUCA, Cristina. **Brasil sofreu 264,9 mil ataques DDoS em 2017, 34% gerados no próprio país,** NIC.BR, 2018. Disponível em: <https://bit.ly/2yfA2Ay> Acesso em 17/09/2018 às 14h29min, s/p.
[182] CANALTECH. **O que é DoS e DDosS?,** Canaltech. Dispnível em: <https://bit.ly/2GP6lt8> Acesso em 22/09/2018 às 16h29min, s/p.
[183] G1, Globo. **Ataque hacker foi o maior já sofrido por sites do governo na internet**, São Paulo: G1. Globo, 2011. Disponível em: <http://glo.bo/joEpHt> Acesso em 25/08/2018 às 17h41min, s/p.
[184] JESUS, 2016, **op. cit.,** p. 120-121.

em constante evolução e as formas de pagamento não fogem dessa lógica, existindo meios que não mais se exteriorizam nos conhecidos cartões físicos, como as “e-wallets”, pagamentos via NFC (Near Field Communication)[185], criptomoedas, dentre outros novos métodos, de forma que o tipo penal acabou ficando demasiadamente restrito, Damásio[186] levanta interessante caminho que o legislador poderia ter seguido, qual seja, ter equiparado os documentos digitais aos particulares, dando uma maior abrangência ao tipo e resolvendo a lacuna no que tange a falsificação dos documentos no âmbito digital, evitando assim que a lei ficasse defasada ou inócua.

Conclui-se que as leis 12.735/12 e 12.737/12 tiveram importante papel no Direito Penal Informático nacional, contudo, parece que o legislador na pressa de dar uma resposta à sociedade, acabou por mitigar muitas das alterações necessárias, criando normas pouco abrangentes e muito longe de suprir as lacunas normativas existentes.

4.3 Considerações Finais Acerca do Sistema Jurídico Brasileiro de Crimes Informáticos

Chegando ao fim da análise dos principais pontos da disciplina legal do acerca dos delitos informáticos no âmbito nacional, calha destacar rapidamente a Lei nº 12.965, de 23 de abril de 2014, conhecida como “Marco Civil da Internet”, surgiu para ser considerado como a constituição do “direito informático brasileiro”.

Em que pese a norma não trazer matérias específicas aos delitos informáticos, Spencer Toth Sidow[187] explica que essa norma refletiu no âmbito criminal, pois, buscou definir os objetos e características do ambiente informático, vide como exemplo; a questão de tratar os dados como algo manipulável, e a concepção de que o ambiente digital é eminentemente difuso e universal,[188] de modo a concretizar bens para atuação e proteção penal, preenchendo lacunas e criando caminhos de proteção.

A lei também influenciou no âmbito processual, trazendo algumas previsões como a do artigo 13 da Lei nº 12.965/14, acerca da forma e tempo pelo

---

[185]SEBRAE. Meios de Pagamento Digitais, Brasília, 2012. Disponível em: <https://bit.ly/2z0gq0W > Acesso em 15/09/2018, s/p.
[186] JESUS, 2016, **op. cit.,** p. 120-121.
[187] SYDOW, 2015, **op. cit.,** p. 274-279.
[188] SYDOW, 2015, **op. cit.,** p. 275.

qual os provedores devem armazenar dados e registros informáticos, tal fator é importante no Processo Penal, principalmente para fins probatórios, já que tais informações podem ser importantes para determinação dos atos processuais e materialidade dos delitos.[189] Contudo, Fabiano R. Kummer[190] atenta que o referido dispositivo sofre muitas críticas em razão do prazo curto de armazenamento, o que dificulta tanto a atuação penal, como a civil.

Destacam-se ainda, respectivamente, a alteração promovida pela Lei nº 13.188, de 11 de novembro de 2015, no artigo 143, do Código Penal, que previu que a retratação de calúnia e difamação que se utilizaram de meios de comunicação, como exemplo, páginas da internet, podem ser feitas através do mesmo meio utilizado para ofensa. Outro destaque vai para a alteração do Estatuto da Criança e do Adolescente promovida pela Lei nº 13.441, de 8 de maio de 2017, essa norma, segundo dispõe Fabiano R. Kummer[191], regulou a atuação e infiltração de agentes policiais no meio informático para o combate dos crimes contra a dignidade sexual de crianças e adolescentes.

Por fim, a mais recente novidade no campo informático é a Lei nº 13.709, de 14 de agosto de 2018, que veio como complemento ao Marco Civil da Internet, visando regulamentar a situação da distribuição e difusão de dados pessoais, impondo regras de uso, autorização e inclusive sansões de caráter administrativa.[192][193] Infelizmente a norma foi silente no campo penal, ponto que pode ser classificado novamente como uma falha do legislador, já que as situações trazidas pela lei têm íntima ligação com o bem jurídico nativo dos crimes informáticos, de forma que seria interessante trazer algumas inovações de proteção penal dos dados.

Diante de todas as observações trazidas, fica comprovado que o ordenamento jurídico brasileiro ainda engatinha na matéria de crimes informáticos, o principal motivo para tal cenário é a timidez legislador, que muitas vezes teve a

---

189 KUMMER, 2017, **op. cit.,** s/p.
190 KUMMER, 2017, **op. cit.,** s/p.
191 KUMMER, 2017, **op. cit.,** s/p.
192 BENTO, Beatrice Helena Silveira**. A nova lei de proteção de dados no Brasil e o general data protection regulation da União Europeia**, Migalhas, 2018. Disponível em:< https://bit.ly/2Rd0stE> Acesso em 23/10/2018 às 22h15min, s/p.
193 BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Brasília, 2018. Disponível em < https://bit.ly/2NH4yIF> Acesso em 23/10/2018 às 22h20min, s/p.

possibilidade de realizar alterações mais profundas, mas simplesmente não as promoveu, como foi o caso da Lei nº 12.735/12.

Comparando com outras nações ao redor do globo, fica ainda mais evidente esse "engatinhar", tendo em vista países como França, que cuida da matéria de 1988[194], Itália que iniciou a normatização em 1991, e teve seu ápice em 1993 inserindo tais matérias em seu Código Penal[195], Portugal[196], cuja lei 109 de 1991, já trazia as disposições legais sobre os delitos informáticos. Na América do Sul merecem destaque o Chile, que trata da matéria em Lei Específica desde de 1993, e a Argentina, cujo Código Penal sofreu alterações importantes em 2008, se adequando a realidade de tais delitos.[197]

Outro fator que contribui para o atraso Brasileiro em disciplinar os delitos informáticos, é o fato de não ter assinado a Convenção de Budapeste, esse tratado foi criado no ano de 2001 com o objetivo central de incentivar a positivação de preceitos, bem como uniformizar as normatizações sobre delitos informáticos ao redor do globo, focando principalmente em uma evolução rápida dos meios de detecção e combate desses delitos.[198]

Em que pese o Brasil possua normas em acordo com esse tratado, não o assinou, diferente de países como Estados Unidos, Chile, Argentina. Tal questão deve ser vista de forma negativa, dado que a maioria dos delitos informáticos adota um viés internacional, sendo importante uma uniformização normativa para evitar, por exemplo, conflitos com a jurisdição internacional e dificuldades de aplicação da norma brasileira.[199]

Assim, existem ainda muitas lacunas no Direito Penal Informático brasileiro, causando problemas tanto de natureza penal, como de natureza processual penal.

Na seara do Direito Penal Subjetivo quase não foram mencionadas novidades normativas, e aí nasce um dos mais sérios problemas da atualidade, a dificuldade de determinação da competência nos crimes informáticos impróprios, tal questão é produto das peculiaridades do ambiente informático somadas a ausência

---

194 CRESPO, 2011, **op. cit.,** p. 141-142.
195 JESUS, 2016, **op. cit.,** p. 64.
196 CRESPO, 2011, **op. cit.,** p. 138-139.
197 JESUS, 2016, **op. cit.,** p. 67.
198 BRITO, 2013, **op. cit.,** p. 48-58.
199 EUROPE, **Council of. Chart of signatures and ratifications of Treaty 185,** Council of Europe, 2018. Disponível em: <https://bit.ly/2NYqIKp> Acesso em 13/10/2018 às 11h38min, s/p.

de legislação específica, o que acaba por gerar uma enorme dificuldade e retardo na aplicação do jus puniendi estatal, causando situações de impunidade frente a tais delitos.

5 ANÁLISE DE COMPETÊNCIA NOS CRIMES INFORMÁTICOS IMPRÓPRIOS

Por fim o trabalho chega ao ponto principal, analisar a competência nos crimes informáticos impróprios, tal questão é resultado de uma raiz comum de outras controversas que envolvem esses delitos, sendo uma soma de três principais fatores até então aqui observados: a velocidade de expansão da era da informação, as peculiaridades do meio informático e o atraso legislativo.

Do primeiro fator, como observado no histórico, a sociedade antes da era da informação vivia uma evolução pautada em intervalos temporais de décadas e séculos, a partir do advento da era da informação, com a criação de dispositivos informáticos e da internet, a evolução muda de eixo, o meio informático passa a ter uma evolução de caráter exponencial, onde o intervalo de um ano pode representar a obsolescência de tecnologias e padrões desse meio. A sociedade também passou a ter acesso a informações em segundos, diferente dos dias e meses que levavam antes dessa era, essa velocidade influencia no Direito, pois, em um prisma da teoria tridimensional de Reale, esse deve se amoldar as evoluções sociais, e quanto mais rápida a evolução, mais dificultoso para o Direito alcançar a regulação e evitar conflitos e problemas.[200]

O segundo fator tem ligação direta com o primeiro, conforme já observado anteriormente, o ambiente informático possui inúmeras peculiaridades além da velocidade, como a internacionalidade, anonimato, intangibilidade, pluralidade.

Esses fatores tornam esse ambiente distinto de qualquer outro com o qual o Direito já estava “acostumado” a regular, tornando a legislação que já tem dificuldade de acompanhar a rápida evolução desses meios, defasada desde o advento a era da informação, veja, é muito complexo determinar, por exemplo, o local de um delito informático, pois, a internacionalidade e pluralidade fazem com que o indivíduo possa estar países diferentes, e em mais de um local ao mesmo tempo.

Tais peculiaridades são extremamente prejudiciais para determinação da competência *“ratione loci”* (em razão do lugar) e *“ratione materiae”* (em razão da matéria), pois, um crime praticado no Brasil pode acabar suscitando questões de

[200] REALE, 2002, **op.cit.**, p.539.

extraterritorialidade dentre outras regras relacionadas à aplicação da lei penal no tempo e no espaço.

Por fim, a defasagem da legislação brasileira, por mais que a maioria dos delitos informáticos apresentem a forma imprópria, todas as peculiaridades retratadas evidenciam a necessidade de normas específicas, e como foi observado, ainda que esse ambiente se expanda e evolua rapidamente. O legislador brasileiro teve oportunidades para disciplinar normas adequadas a fim de sanar problemas relativos a esses crimes, mas não o fez, como foi o caso da grande mitigação que ocorreu no processo legislativo da Lei 12.735/12.

Para conseguir determinar a competência nos crimes informáticos impróprios, faz-se necessário antes tecer breves considerações a respeito do que é competência, e quais os principais critérios de determinação, utilizados pelo direito brasileiro.

5.1 Considerações Gerais Acerca da Competência Penal

A compreensão do fenômeno da competência está intimamente ligada ao entendimento de outro instituto essencial à sua existência, a jurisdição. Renato Brasileiro[201] ensina que a vivência gera inúmeros conflitos, que na maioria das vezes acabam sendo solucionados no âmbito interno, contudo, nem todos conflitos se resolvem dessa forma, exatamente aí que entra a figura do Estado, pois, ao vedar a autotutela "justiça com as próprias mãos", acaba tomando para si o poder-dever de resolver esses conflitos e restaurar a paz e a harmonia das relações sociais, para isso se vale do chamado "poder jurisdicional".

Jurisdição vem do latim *"jurisdictio",* que significa ato de dizer o direito, nesse sentido Antônio Heráclito Mossin[202] conceitua jurisdição como sendo "a atividade que o Estado exerce por meio do Poder Judiciário, para compor um litígio, visando dar a cada um aquilo que é seu, mediante a aplicação do Direito Penal, valendo-se para tanto do processo."

Dessa forma, tem-se que a jurisdição é uma atividade estatal que visa a solução de conflitos, no âmbito penal isso é traduzido pela figura da chamada "lide

[201] LIMA, Renato Brasileiro de. **Manual de processo penal:** volume único. 5.ed. rev., ampl. e atual. Salvador: 5. ed. JusPodivm, 2017, p. 329.
[202] MOSSIN, Heráclito Antônio. **Compêndio de Processo Penal:** Curso Completo. Barueri: Manole, 2010. (Recurso Eletrônico – "Minha Biblioteca"), p. 167.

penal", tendo em vista que o *"jus puniendi"* (direito de punir) é de titularidade do Estado, fazendo-se necessário o estabelecimento de um processo para que através do manuseio dos princípios e normas do Direito Penal objetivo, alcance uma futura punição ao agente que cometeu o delito.

O que ocorre, no entanto, é que apesar da doutrina reconhecer a característica da unidade e indivisibilidade do poder jurisdicional[203], seria impossível um único órgão estatal manusear a aplicação da jurisdição a todos os litígios, sendo necessária a distribuição da jurisdição para diferentes órgãos do judiciário, e aí surge a noção de competência, a qual Edilson Mougenout conceitua como:

> A competência é, assim, a medida ou limite em que juízo o julgador exercer o poder de jurisdição. Representa a porção do poder jurisdicional que é conferido a cada órgão investido de jurisdição.
> Dessarte, não obstante todo magistrado seja dotado de poder jurisdi- cional, somente juízo exercê-lo dentro de certos limites fixados em lei, é dizer, dentro de sua esfera de competência.
> Assim, podemos dizer que, enquanto abstratamente todos os órgãos do Poder Judiciário são investidos de jurisdição, as regras de competência é que concretamente atribuem a cada um desses órgãos o efetivo exercício da função jurisdicional1.[204]

Assim, cada órgão jurisdicional será competente para aplicar a jurisdição em determinadas situações, aí vem a importância dos critérios de determinação e atribuição de competência, a esse respeito o artigo 69 do Decreto-lei 3.689/41, Código de Processo Penal[205], traz a seguinte redação: "Determinará a competência jurisdicional: I – o lugar da infração: II – o domicílio ou residência do réu; III – a natureza da infração; IV – a distribuição; V–a conexão ou continência; VI–a prevenção; VII–a prerrogativa de função."

Da redação do artigo supramencionado é possível compreender que a determinação da competência passa por 3 principais critérios, o critério pessoal, chamado pela doutrina de *"ratione personae"*, o critério material, *"ratione materiae"*, e o critério territorial, *"ratione loci"*, critérios esses que serão observados de forma mais específica a frente. Frisa-se, também, como observado da redação do artigo 69, que a competência pode ser atribuída por vias de conexão e continência, matéria que deixará de ser analisada no trabalho, tendo em vista sua especialidade, o que

---

[203] MOUGENOT, Edilson. **Curso de Processo Penal,** 12. ed. São Paulo: Saraiva, 2017. (Recurso Eletrônico – "Minha Biblioteca"), p. 68.
[204] MOUGENOT, 2017, **loc. cit.**, p. 308.
[205] BRASIL**. Código de Processo Penal. decreto lei nº 3.689, de 03 de outubro de 1941.** 1941. Disponível em: <https://bit.ly/2pPI2Uh> Acesso em: 15/082018 às 16h21min, s/p.

poderia provar uma fuga do objeto principal a ser estudado, qual seja a competência no âmbito dos delitos informáticos.

Antes de adentrar nas considerações mais específicas de cada critério de atribuição de competência, mister entender a forma que tais critérios serão manejados para a determinação da competência, a doutrina não é convergente em uma única fórmula, existindo inúmeros "passo a passos" para atingir esse fim.

Em uma busca de determinação da competência penal, o primeiro passo importante é delimitar a chamada "competência de justiça", ou seja, qual das "estruturas jurisdicionais" deverá ser utilizada, a estrutura judiciária brasileira se divide em justiça federal e estadual, a federal, por sua vez, se subdivide em comum e especial, composta pela Justiça do Trabalho, Justiça Militar e Justiça Eleitoral.

Na atribuição dessa competência de justiça, os critérios material e pessoal ganham força, pois, as regras para essa estruturação judiciária levaram em conta que determinadas pessoas e matérias merecem um cuidado mais especializado, até por isso, esses dois critérios são tidos como "matérias de competência absoluta", pois, não são passiveis de "prorrogação", ou seja, não é possível renunciar esse critério, diferente do critério territorial *"ratione loci"*, que como será observado, em algumas situações é possível sua prorrogação.[206]

Determinada qual a justiça competente, parte-se para análise do chamada "competência originária", isso porque, como se sabe, o judiciário brasileiro é dividido em níveis, tendo a justiça de primeiro grau, federal ou estadual, acima, os Tribunais de Justiça e Regionais, e no topo, os Tribunais Superiores, Tribunal Superior de Justiça, Tribunal Superior do Trabalho, Tribunal Superior Militar, Tribunal Superior Eleitoral e para fins constitucionais do Supremo Tribunal Federal.

Em regra, os processos se iniciam na justiça de primeiro grau, contudo, certas pessoas em razão da função exercida acabam por ser processadas em tribunais específicos, ainda que a matéria não seja de competência originária daquela Justiça, aí tem-se a chamada "competência funcional", a exemplo, o Presidente da República é processado no Supremo Tribunal Federal.[207]

Superada essa etapa, parte-se para a análise da "competência de foro", ou seja, saber em qual espaço territorial iniciará aquele processo, qual "a comarca (Justiça Estadual), seção e subseção judiciárias (Justiça Federal),

[206] LIMA, 2017, **op. cit.**, p.337-338.
[207] LIMA, 2017, **op. cit.,** p. 483.

circunscrição judiciária militar (Justiça Militar da União) ou Zona eleitoral (Justiça Eleitoral) competente?"[208]. Aqui reina o critério "ratione loci", que como observado acima, é tido como matéria de "competência relativa", podendo em algumas hipóteses ser prorrogada, alterada.

Por fim, em alguns casos pode ocorrer de em uma comarca ou subsecção judiciária ter mais de um juiz, a respeito dessa situação Norberto Avena coloca:

> Depois de firmada a competência *ratione materiae* (Justiça Federal, Justiça Estadual, Militar etc.) e após definido o foro competente para a apuração segundo os critérios lugar do crime, domicílio e residência do réu e prevenção, é necessário definir o Juiz competente dentro da Comarca a que incumbir o processo e julgamento do feito.
> Sob este último enfoque, estabelece o art. 74 do CPP que devem ser consideradas as normas de organização judiciária. Essas leis é que estabelecerão, por exemplo, dentre os vários juízes criminais de uma determinada Comarca, qual deles detém competência para julgar este ou aquele delito. Essa regulamentação poderá ser determinada a partir da espécie de pena (reclusão, detenção, prisão simples), do tipo de infração (crime ou contravenção), da espécie delituosa (crimes contra o patrimônio, crimes contra a dignidade sexual etc.) e qualquer outro critério.[209]

É a chamada "competência de juízo"[210], na qual será analisado se existe um juiz específico para dispor daquela causa, daquele delito.

De forma simplória, esse é procedimento a ser adotado para determinar o órgão competente para julgar determinado delito. Desenha essa noção, mister observar de forma mais específica cada um dos critérios de atribuição de competência, para assim firmar as bases que serão utilizadas na análise de competência dos crimes informáticos.

5.1.1 Da competência em razão da pessoa *"ratione personae"*

O critério de atribuição de competência em razão da pessoa, "ratione personae", prega que algumas pessoas em razão do cargo ou posição que ocupam, deverão ser julgadas por um órgão e grau jurisdicional distintos da regra comum (que é a ação penal correr a partir do primeiro grau), como é o caso dos deputados federais, governadores, juízes, promotores de justiça dentre outros casos.

---

[208] LIMA, 2017, **op. cit.,** p. 349.
[209] AVENA, Norberto Pâncaro. **Processo Penal/**Norberto Avena, 9.ed. Rio de Janeiro: Método, 2017. (Recurso Eletrônico – "Minha Biblioteca"), p. 660.
[210] LIMA, 2017, **op. cit.,** p.480.

A função ocupada está intimamente ligada a esse critério, logo, se o indivíduo deixar o cargo ou função, acaba perdendo tal privilégio, sendo o processo remetido ao juízo que seria competente de regra.[211]

Tal competência, como anota Norberto Avena[212], predomina perante os critérios de competência em razão da matéria e do local, por esse motivo não será aprofundado tal critério, já que em qualquer infração penal, inclusive nas informáticas, a competência "ratione personae" prevalecerá, inexistindo um conflito a ser resolvido nesse caso.

5.1.2 Competência em razão da matéria *"ratione materiae"*

O artigo 69, inciso III do Código de Processo Penal elenca a possibilidade de estabelecimento da competência através da natureza das infrações, critério também chamado de competência "*ratione materiae"*, como anteriormente falado, junto com o critério *"ratione personae"* tem papel essencial para a determinação da chamada "competência de justiça", trazendo à tona se o delito será apreciado no âmbito das chamadas "justiças especializadas" ou das justiças comuns federal ou estadual.

Desse modo, a análise da competência em relação a matéria, deve adotar uma ótica de princípio da especialidade, devendo as justiças comum federal e estadual serem vistas como "residuais", ou seja, deve analisar se o delito e suas características são abarcados pelas justiças específicas, como a Militar e a Eleitoral, para só depois partir aos moldes das justiças comuns.

Na colocação acima, não foi mencionada a Justiça do Trabalho, a razão para tal, é que o Supremo Tribunal Federal no âmbito do julgamento Ação Direta de Inconstitucionalidade nº 3684, pacificou que a Justiça Trabalhista não possui competência na seara criminal.[213]

As regras de atribuição de competência em razão da matéria estão espalhadas pelo ordenamento jurídico, tanto na Constituição Federal de 1988, quanto em legislações infraconstitucionais, como o Código de Processo Penal, o Código Penal Militar e o Código Eleitoral, sem excluir ainda a vasta jurisprudência

---

211 LIMA, 2017, **op. cit.,** p. 490.
212 AVENA, 2017, **op. cit.,** p. 620.
213 NOTÍCIA. Expresso da. **Justiça do Trabalho não tem competência para julgar ações penais,** JusBrasil, 2006. Disponível em: <https://bit.ly/2CHoqKC> Acesso em 26/08/2018 às 21h48min, s/p.

como a Súmula 53 do STJ que estabeleceu a competência da Justiça Comum Estadual, para processar e julgar civil acusado de prática de crime contra militares estaduais[214], dentre outros julgados.

De todos dispositivos que preveem as regras de competência pela natureza da infração, merecem destaque pela importância futura ao objeto do presente trabalho o artigo 109 incisos, IV, V, V-A, VI, VII, IX e X da Constituição Federal, que estabelecem as regras atinentes à Justiça comum federal.

Acerca da atribuição da competência em razão da matéria; em relação a Justiça Comum Estadual, compete a essa julgar todas as matérias que não forem abarcadas pelas justiças especializadas e/ou pela Justiça Comum Federal, pois, é residual.[215]

Por fim, cabe frisar que o critério "*ratione materiae",* assim como o critério "*ratione personae"*, constitui as chamadas "matérias de competência absoluta", não sendo passíveis de alteração, prorrogação.

5.1.3 Competência territorial *"ratione loci"*

O critério de atribuição de competência territorial também chamado de "competência de foro", conforme já observado constitui uma das últimas análises do ponto de vista da determinação da competência, seu fundamento encontra-se disciplinado nos artigos 69, incisos I e II, e artigo 70 do Código de Processo Penal, nessa o objetivo principal é determinar qual o juízo competente à análise e julgamento do delito.

O artigo 70, caput,[216] do Código de Processo Penal postula a regra de atribuição da competência *"ratione loci"*, que nada mais é do que o local da consumação da infração, ou, no caso do crime tentado o local onde ocorreu o último ato de execução, assim se um indivíduo roubou um banco na cidade de Presidente/SP, o foro competente é a justiça comum estadual dessa cidade.

Como Heráclito Antônio Mossin[217] destaca, a consumação opera-se de forma diferente entres os vários tipos de delito, sendo composto por um resultado

---

[214] STJ, Superior Tribunal de Justiça. **Enunciado de Súmula nº 53,** Brasília: STJ, 1992. Disponível em: <https://bit.ly/2Ejr62E> Acesso em 21/09/2018 às 19h39min, s/p.
[215] AVENA, 2017, **op. cit.,** p. 647.
[216] BRASIL, 1941, **op. cit.,** s/p.
[217] MOSSIN, 2010, **op. cit.,** p. 175.

material apenas os delitos materiais, ocorrendo a consumação dos outros delitos da seguinte forma:

> os formais, com a mera atividade; os permanentes, desde quando configurados seus requisitos, perdurando até que cesse a conduta do agente; os omissivos próprios, no momento do comportamento omissivo do agente; e os omissivos impróprios ou comissivos, por emissão e qualificados pelo resultado na ocasião em que se produz o resultado ou evento.[218]

Assim a regra vai se amoldando aos tipos de consumação, a respeito do estabelecido no artigo 70, caput, Renato Brasileiro[219] observa algo importante, para fins de competência o Código de Processo Penal adotou a teoria do resultado acerca do local da infração, postura distinta da adota no artigo 6º do Código Penal, que abraçou a teoria da ubiquidade, ou seja, considera o local do crime tanto onde ocorreu a ação, quanto o resultado.

Edilson Mougenot[220], acredita que não há conflitos entre Código de Processo Penal e Código Penal em razão dessa divergência de teorias, já que para o autor, o legislador ao adotar a teoria do resultado na legislação processual, optou por estabelecer uma regra baseada em motivos de conveniência e instrumentalidade, pois, normalmente, o local do resultado é onde os vestígios do delito são produzidos e os impactos sociais do rompimento da norma são gerados, sendo oportuno processar o indivíduo nesse local para facilitar a instrução e dar uma resposta estatal à sociedade. Além do mais, o autor ressalta que tanto os parágrafos do artigo 70 do Código de Processo Penal, quanto a própria jurisprudência dosam a regra do “caput”, trazendo à ubiquidade quando necessária[221].

Abrindo um parênteses, com toda vênia a postura doutrinária predominante a favor da compatibilidade dos artigo 6º do Código Penal e artigo 70, caput, do Código de Processo Penal, será observado, que ainda que compatíveis entre si, talvez o legislador não tenha andado tão bem na adoção de uma regra pautada na teoria do resultado, pois, na solução alguns problemas que existem em delitos como os informáticos, cuja determinação do local, mesmo com regras de transnacionalidade e plurilocalidade, é de difícil compreensão, uma regra pautada na ubiquidade parece mais conveniente.

---

[218] MOSSIN, 2010, **op. cit.,** p. 175.
[219] LIMA, 2017, **op. cit.,** p. 524.
[220] MOUGENOT, 2017, **op. cit.,** p. 329.
[221] MOUGENOT, 2017, **op. cit.,** p. 329.

Seguindo com o estudo da competência “ratione loci”, além da regra do local da consumação, existem algumas exceções e regras complementares. A primeira envolve os crimes plurilocais, aqueles que atingem mais de uma localidade dentro do pais, sejam crimes comuns, permanentes ou até em razão de continuidade delitiva, nesses casos aplica-se importante critério, a prevenção, prevista nos artigos 70,§3º, 71, 72 §2º, 78 e 83 do Código de Processo Penal, por essa será competente o primeiro foro dos lugares em que o delito passou que tiver contato com esse, ficará prevento para julgá-lo.

Outra situação a respeito dos crimes plurilocais, são os casos que a conduta ocorre em uma localidade e o resultado propriamente dito opera em outra, nesse sentido Renato Brasileiro[222], prega que apesar da regra geral levar a entender que o foro competente seria o do resultado, a jurisprudência e grande parte da doutrina desenha que o foro competente será da localidade em que se desenvolveram as últimas ações, pois, ali, é o local onde o crime afetou a sociedade e que possui os maiores indícios materiais para a investigação, logo, excepciona a teoria do resultado defendida no artigo 70 do Código de Processo Penal.

Quanto aos delitos praticados no estrangeiro se observam duas situações, a primeira nos chamados “delitos a distância”, em que de alguma forma o delito tocou o Brasil, seja pela execução, seja pelo resultado, nesses casos o artigo 70, §1º e 2º do Código de Processo Penal prega que será competente o local em que foi praticado o último ato de execução ou onde tenha produzido, ainda que parcialmente, o resultado no território nacional, perceba, nesses dispositivos o código adota a teoria da ubiquidade ao invés da do resultado pregada pelo “caput”[223]. A segunda situação é no caso dos crimes totalmente internacionalizados dos quais o artigo 7º do Código Penal prega a aplicação da lei penal brasileira, nesses delitos, prevalece a regra disposta no artigo 88 do Código de Processo Penal[224], ou seja, o foro da capital onde o acusado tenha residido, ou, caso não tenha residido no país, o foro do juízo de Brasília. [225]

Por fim, cabe mencionar ainda a possibilidade de o foro competente ser o local onde o réu reside ou é domiciliado, tal prerrogativa encontra-se nos artigos 69, II, 72 e 73 do Código de Processo Penal, e se baseia na hipótese em que não for

[222] LIMA, 2017, **op. cit.,** p. 527-528.
[223] MOSSIN, 2010, **op. cit.,** p. 176.
[224] Código de Processo Penal, artigo 88, BRASIL, 1941, **op. cit.,** s/p.
[225] LIMA, 2017, **op. cit.,** 529.

possível auferir o local da infração, servindo como um plano secundário para determinar a competência *"ratione loci"*[226].

5.1.4 Demais considerações gerais sobre competência

Percebe-se que foram estabelecidos os principais critérios de determinação da competência criminal, contudo, salienta-se que a intenção não foi exaurir a matéria, existindo outras discussões e critérios não essenciais ao objeto de estudo, e até por isso não foram abordados, como as questões relacionadas a competência por distribuição, conexão e continência, descritas dentre os artigos 75 a 82 do Código de Processo Penal. Também, pela mesma razão, não foram observadas as competências recursais, da execução e o funcionamento dos juizados especiais criminais.

Assim, nota-se que a competência é um mar complexo, cheio de veios e regras importantes, estabelecidas as bases do estudo, agora resta a análise do objeto essencial do presente trabalho, a análise de competência nos crimes informáticos impróprios.

5.2 Da Análise de Competência nos Crimes Informáticos Impróprios

Conforme observado na introdução do presente capítulo, esse problema é fruto das peculiaridades do meio informático aliado a falta de legislação. A discussão acerca da competência será focada em dois principais planos, o da competência de Justiça e a Competência de Foro, tendo em vista que a internacionalidade e a pluralidade dão ao ambiente informático um caráter difuso e ao mesmo tempo, em transnacional, o que acaba por dificultar a compreensão do território em que ele ocorre, e pode suscitar inclusive a aplicação da extraterritorialidade do Direito Penal.

Um exemplo da dificuldade de determinar a competência nos crimes informáticos é imaginar que um indivíduo pode no Brasil inserir materiais de pornografia infantil em um site armazenado em um servidor na Rússia, que será acessado por inúmeras pessoas de diferentes localidades do mundo, e aí vem a questão, qual foro competente para punir esse indivíduo? A partir de agora serão

[226] AVENA, 2017, **op. cit.,** p. 657.

observadas algumas regras específicas, a fim de traçar um rumo para a solução dessa celeuma.

5.2.1 Da competência de justiça

Como já falado, um dos pontos de discussão na determinação da competência nos crimes informáticos, acontece na já estudada “competência de justiça”, ou seja, determinar se compete às justiças especializadas, à justiça federal ou à estadual.

O primeiro ponto que se destaca, é que aqui o plano de discussão se opera no critério “ratione materiae”, pois, como já dito anteriormente, quando envolver situações de competência funcional, “ratione personae”, essa competência vai prevalecer perante as outras, inexistindo discussões sobre qual órgão vai apreciar o delito, pois, será o que tem legitimidade para julgar aquele indivíduo em razão do cargo que ocupa.

Outra questão, é que do ponto de vista das justiças especializadas, acaba por também não existir quase discussões, pois, quando a matéria for de alçada das justiças especializadas militar ou eleitoral, situação pouco comum nos delitos informáticos, a competência será dessas justiças sem muitos debates, como o que ocorre, por exemplo, com o indivíduo que realiza alguma modificação na urna eletrônica para fraudar as eleições, artigo 72, inciso II da Lei 9504/97, esse crime é de natureza eleitoral, logo será de competência da Justiça Eleitoral.

Então fica perceptível que a discussão aqui se concentra entre Justiça Comum Federal, e Justiça Comum Estadual, como a competência dessa última é residual, por exclusão, basta elencar os casos em que os crimes informáticos serão de alçada federal, situação que poderá ocorrer em duas hipóteses que veremos a seguir.

A primeira hipótese é a descrita no artigo 109, IV da Constituição Federal de 1988[227], ou seja, quando o crime informático for praticado lesionando bens, serviços ou interesses da União, autarquias ou empresas públicas, nesse sentido, o Ministério Público Federal traz interessante exemplo em seu roteiro sobre

[227] Artigo 109, da Constituição Federal de 1988. BRASIL**. Constituição da República Federativa do Brasil, de 5 de outubro de 1988.** 1988. Disponível em <https://bit.ly/1dFiRrW> Acesso em: 12/10/2018 às 16h52min, s/p.

crimes cibernéticos[228], qual seja o furto qualificado mediante fraude por saques realizados por via digital contra correntistas da Caixa Econômica Federal, a esse respeito a segunda turma do Egrégio Superior Tribunal de Justiça decidiu:

> CRIMINAL. RHC. FURTO QUALIFICADO. PRISÃO EM FLAGRANTE. IMPRESTABILIDADE DAS PROVAS. IMPROPRIEDADE DO MEIO ELEITO. COMPETÊNCIA DA JUSTIÇA FEDERAL. OFENSA A BENS DA CAIXA ECONÔMICA FEDERAL. LIBERDADE PROVISÓRIA. INDEFERIMENTO. POSSIBILIDADE CONCRETA DE REITERAÇÃO CRIMINOSA. NECESSIDADE DA CUSTÓDIA DEMONSTRADA. RECURSO DESPROVIDO. A via eleita não se presta ao exame das alegações relacionadas à imprestabilidade da prova produzida no auto de prisão em flagrante no inquérito policial, em virtude da necessidade de revolvimento no conjunto fático-probatório. Maiores incursões a respeito da matéria devem ser efetivadas no decorrer da instrução criminal. Impõe-se o processamento da ação penal no âmbito da Justiça Federal, conforme expresso no art. 109, IV, da Constituição, pois, ainda que os saques tenham sido empreendidos de conta de particulares, o crime, em tese, atingiu diretamente bens e interesses da referida empresa pública, tendo em vista que o dinheiro subtraído encontrava-se ainda na posse do ente federal. A hipótese dos autos evidencia a suposta prática de saques em contas-correntes, inclusive via Internet, sendo que em poder do réu foram encontradas senhas de acesso a contas bancárias, cartões magnéticos e numerário. Trata-se de acusado proveniente de uma localidade onde, segundo o Magistrado singular, tal tipo de prática criminosa estaria ocorrendo de forma reiterada, não sabendo o paciente explicar o motivo pelo qual mudou o distrito da culpa. Constata-se, pelas evidências concretas do caso em tela, a real possibilidade de reiteração criminosa, o que é suficiente para fundamentar a segregação do paciente para garantia da ordem pública. Recurso desprovido.[229]

Deve ser ressaltado que é necessária uma situação que coloque de fato em riscos os interesses da União, autarquias ou empresas públicas, pois, caso as lesões ou ameaças figurem apenas no plano particular, a competência não será da Justiça Federal, já que deve ter em mente que o objetivo de tal deslocamento é proteção do interesse público.

A segunda hipótese de competência federal nos crimes informáticos demanda uma análise um pouco mais complexa, é a descrita no artigo 109, inciso V da Constituição Federal que traz a seguinte redação:

> Art. 109. Aos juízes federais compete processar e julgar: V - os crimes previstos em tratado ou convenção internacional, quando, iniciada a

---

[228] MPF. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Roteiro de atuação**: crimes cibernéticos,** 2. ed. Ver, Brasília: MPF/2ªCCR, 2013. Disponível em: <https://bit.ly/2IV5Xu2> Acesso em 28/08/2018 às 18h12min, p. 366.

[229] STJ, Superior Tribunal de Justiça. **RHC 19846 / GO RECURSO ORDINARIO EM HABEAS CORPUS 2006/0153072-3**, Brasília: STJ, 2006. Disponível em: < https://bit.ly/2P3e9hH> Acesso em: 13/10/2018, s/p.

> execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente;[230]

Essa hipótese tem relação com a transnacionalidade, ou seja, quando um delito tem uma parte de sua execução ou resultado no Brasil, e outra parte no estrangeiro, segundo Kummer, para um delito informático desse gênero (transnacional) ser de competência da Justiça Federal, faz-se necessário 3 requisitos cumulativos:

> i. quando se refere a crimes previstos em tratados ou convenções internacionais; ii. que o Brasil seja signatário de compromisso internacional de combate àquela espécie delitiva; iii. que seja constatada uma relação de internacionalidade entre a conduta criminosa praticada e o resultado produzido;[231]

Dentre casos que se amoldam a essa hipótese de competência federal, merecem destaque os crimes dos artigos 241, 241-A, 241-B do Estatuto da Criança e do Adolescente (Lei 8069/1990), que dispõe sobre a venda e difusão de pornografia infantil. Nesses delitos o fator determinante para serem de competência federal vai ser justamente o local da disponibilização, pois, se presente o caráter transnacional, e a publicidade capaz de permitir que pessoas de outras localidades diversas do Brasil acessem o conteúdo pornográfico (para configurar a internacionalidade), todos os requisitos relatados acima estarão preenchidos, dado que o Brasil se compromete na Convenção Sobre os Direitos da Criança da ONU (Decreto nº 99.710/90), no art. 34, alínea “c”,[232] a combater a exploração de crianças em cenas de sexo ou materiais pornográfico, nesse sentido o Supremo Tribunal Federal em caso de repercussão definiu:

> Ementa: 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. 1. À luz do

[230] BRASIL, 1988, **op. cit.** s/p.
[231] KUMMER, 2017, **op. cit.,** s/p.
[232] BRASIL. **Decreto nº 99.710, de novembro de 1990.** Promulga a Convenção sobre os Direitos da Criança, 1990. Disponível em: <https://bit.ly/28TFYGb> Acesso em 10/10/2018 às 15h16min, s/p.

> 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. 2. O Brasil pune a prática de divulgação e publicação de conteúdo pedófilo-pornográfico, conforme art. 241-A do Estatuto da Criança e do Adolescente. 3. Além de signatário da Convenção sobre Direitos da Criança, o Estado Brasileiro ratificou o respectivo Protocolo Facultativo. Em tais acordos internacionais se assentou a proteção à infância e se estabeleceu o compromisso de tipificação penal das condutas relacionadas à pornografia infantil. 4. Para fins de preenchimento do terceiro requisito, é necessário que, do exame entre a conduta praticada e o resultado produzido, ou que deveria ser produzido, se extraia o atributo de internacionalidade dessa relação. 5. Quando a publicação de material contendo pornografia infanto-juvenil ocorre na ambiência virtual de sítios de amplo e fácil acesso a qualquer sujeito, em qualquer parte do planeta, que esteja conectado à internet, a constatação da internacionalidade se infere não apenas do fato de que a postagem se opera em cenário propício ao livre acesso, como também que, ao fazê-lo, o agente comete o delito justamente com o objetivo de atingir o maior número possível de pessoas, inclusive assumindo o risco de que indivíduos localizados no estrangeiro sejam, igualmente, destinatários do material. A potencialidade do dano não se extrai somente do resultado efetivamente produzido, mas também daquele que poderia ocorrer, conforme própria previsão constitucional. 6. Basta à configuração da competência da Justiça Federal que o material pornográfico envolvendo crianças ou adolescentes tenha estado acessível por alguém no estrangeiro, ainda que não haja evidências de que esse acesso realmente ocorreu. 7. A extração da potencial internacionalidade do resultado advém do nível de abrangência próprio de sítios virtuais de amplo acesso, bem como da reconhecida dispersão mundial preconizada no art. 2º, I, da Lei 12.965/14, que instituiu o Marco Civil da Internet no Brasil. 8. Não se constata o caráter de internacionalidade, ainda que potencial, quando o panorama fático envolve apenas a comunicação eletrônica havida entre particulares em canal de comunicação fechado, tal como ocorre na troca de e-mails ou conversas privadas entre pessoas situadas no Brasil. Evidenciado que o conteúdo permaneceu enclausurado entre os participantes da conversa virtual, bem como que os envolvidos se conectaram por meio de computadores instalados em território nacional, não há que se cogitar na internacionalidade do resultado. 9. Tese fixada: "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". 10. Recurso extraordinário desprovido.[233]

É nítido que o Supremo Tribunal Federal no caso acima desenhou as regras já dispostas a acerca da aplicação do artigo 109, V da Constituição Federal aos crimes informáticos, calha dizer que não se restringe aos crimes contra a criança

[233] STF. Supremo Tribunal Federal. **RE 628624, Relator(a): Min. MARCO AURÉLIO, Relator(a) p/ Acórdão: Min. EDSON FACHIN, Tribunal Pleno, julgado em 29/10/2015, ACÓRDÃO ELETRÔNICO REPERCUSSÃO GERAL - MÉRITO DJe-062 DIVULG 05-04-2016 PUBLIC 06-04-2016,** Brasília: STF, 2015. Disponível em: <https://bit.ly/2RL8uLo> Acesso em: 15/09/2018 às 14h25min, s/p.

e adolescente, podendo atingir outros crimes, desde que preenchidos os requisitos apresentados, nesse sentido, outro exemplo muito importante são os crimes relacionados ao preconceito racial, como os descritos na Lei 7.716/1989 e a própria injúria racial descrita no artigo 140, §3º do Código Penal, dado que o Brasil é signatário de inúmeros tratados em prol da igualdade, em especial a Convenção dos Direitos Humanos e na Convenção de Combate ao Racismo e à Discriminação Racial de 1965, que em seu artigo 4º deixa bem claro que o Brasil se compromete a tipificar e punir condutas discriminatórias, dessa forma, desde que tenha o caráter transnacional e minimamente público, serão de Competência Federal.

Por fim, vale frisar em um pensamento até que redundante, que nem todo delito no âmbito virtual, vai se processar no âmbito da competência federal, pois, se faltar proteção por tratado internacional ratificado pelo Brasil, a transnacionalidade, ou esse caráter minimamente público essencial para a caracterização da internacionalidade, não haverá motivos para a competência ser federal, foi o que o Egrégio Superior Tribunal de Justiça entendeu:

> CONFLITO DE COMPETÊNCIA Nº 145.516 - ES (2016/0050531-4) RELATOR : MINISTRO JOEL ILAN PACIORNIK SUSCITANTE : JUÍZO FEDERAL DA 1A VARA CRIMINAL DA SEÇÃO JUDICIÁRIA DO ESTADO DO ESPÍRITO SANTO SUSCITADO : JUÍZO DE DIREITO DA 3A VARA CRIMINAL DE VILA VELHA - ES INTERES. : MINISTÉRIO PÚBLICO DO ESTADO DO ESPÍRITO SANTO INTERES. : JOSÉ AGRIPINO MAIA INTERES. : MARCELO HASTENREITER DORNELAS DECISÃO Cuida-se de conflito de competência instaurado entre o Juízo Federal da 1ª Vara Criminal da Seção Judiciária do Estado do Espírito Santo SJES, o suscitante, e o Juízo de Direito da 3ª Vara Criminal de Vila Velha/ES, o suscitado. Colhe-se dos autos que foi instaurada ação penal privada para apuração da prática de delito descrito nos artigos 138 (calúnia), 139 (difamação) e 140 (injúria) c/c art. 141, III (causa de aumento de pena em razão do meio facilitador da divulgação), todos do Código Penal CP. Conforme queixa-crime, o querelado tem, de forma reiterada, por meio da página do Facebook denominada "Democratas 25", imputando falsamente ao querelante a prática de condutas tipificadas no ordenamento jurídico como crime, bem como fatos inexistentes que atentam contra sua honra objetiva e subjetiva... É o relatório. Decido. O presente conflito de competência deve ser conhecido, por se tratar de incidente instaurado entre juízos vinculados a Tribunais distintos, nos termos do art. 105, inciso I, alínea d da CF. De um lado o Juízo suscitado aduz tratar-se de crime à distância, o que, no seu entendimento, justificaria a competência da Justiça Federal e, de outro lado, o Juízo suscitante alega competência da Justiça Estadual, por não existir tratado ou convenção internacional firmados pelo Brasil sobre crime contra a honra praticado pela Internet, bem como em razão de as supostas ofensas não estarem ligadas ao cargo ocupado pelo querelante. Com razão o suscitante. Primeiramente, o Superior Tribunal de Justiça já entendeu que o fato de o delito ter sido praticado por meio de publicação na página do Facebook, por si só, não configura sua internacionalidade. Nesse sentido: PROCESSO PENAL. AGRAVO REGIMENTAL NO CONFLITO DE COMPETÊNCIA. CRIME DE

> AMEAÇA E CONTRAVENÇÃO DE PERTURBAÇÃO DA TRANQUILIDADE PRATICADOS POR MEIO DA INTERNET. INDÍCIOS DE TRANSNACIONALIDADE. INEXISTÊNCIA. COMPETÊNCIA DA JUSTIÇA ESTADUAL. AGRAVO REGIMENTAL NÃO PROVIDO. 1. Hipótese em o conflito se estabeleceu em virtude de queixa-crime apresentada pelo fato de um suposto hacker enviar ameaças e manipular diversos adolescentes e pais de um mesmo ciclo de amizade e convivência, por meio de e-mails, Orkut, Twitter e Facebook. 2. A jurisprudência desta Corte Superior é no sentido de que, embora se trate de crime praticado por meio da rede mundial de computadores, necessária se faz a existência de indícios mínimos de extraterritorialidade para que seja determinada a competência da Justiça Federal. A mera utilização da internet não basta, por si só, para caracterizar a transnacionalidade do delito. 3. In casu, não há, pelo menos neste momento processual, a presença de qualquer indício de transnacionalidade dos delitos apto a justificar a competência da Justiça Federal. 4. Agravo regimental não provido. (AgRg no CC 118.394/DF, Rel. Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 10/08/2016, DJe 22/08/2016). Ademais, ainda que se considere o Facebook um sítio de relacionamento internacional, conforme sustentou o Juízo suscitado, a internacionalidade não é suficiente para a fixação da competência da Justiça Federal, sendo indispensável o preenchimento de duplo requisito exigido pelo art. 109, V, da CF, qual seja, transnacionalidade e da participação do Brasil em ato internacional objetivando a repressão do crime em questão... I. Hipótese na qual foi requisitada a quebra judicial do sigilo de dados para fins de investigação de crimes de difamação e falsa identidade, cometidos contra menor impúbere e consistentes na divulgação, no Orkut, de perfil da menor como garota de programa, com anúncio de preços e contato. II. O Orkut é um sítio de relacionamento internacional, sendo possível que qualquer pessoa dele integrante acesse os dados constantes da página em qualquer local do mundo. Circunstância suficiente para a caracterização da transnacionalidade necessária à determinação da competência da Justiça Federal. III. Ademais, o Brasil é signatário da Convenção Internacional Sobre os Direitos da Criança, a qual, em seu art. 16, prevê a proteção à honra e à reputação da criança. IV. Conflito conhecido para declarar a competência do Juízo Federal e Juizado Especial Federal de Londrina SJ/PR, o suscitante. (CC 112.616/PR, Rel. Ministro GILSON DIPP, TERCEIRA SEÇÃO, julgado em 13/04/2011, DJe 01/08/2011) Diante disso, em razão de o Brasil não ser signatário de tratado ou convenção internacional que objetive a repressão de crimes cibernéticos e tampouco de crimes contra a honra de pessoa que não se enquadre na definição de criança ou adolescente, não está configurada a hipótese descrita no art. 109, V, da CF. Ademais, da leitura do teor das ofensas dirigidas ao querelante José Agripino Maia, contata-se que não se relacionam ao exercício de funções do cargo Senador da República, mas à sua pessoa física, ou, quando muito, à sua condição de presidente nacional do partido Democratas (DEM). Diante disso, não se identifica violação a interesse da União, razão pela qual compete à Justiça Estadual a apuração do delito, por não estar configurada a hipótese descrita no art. 109, IV, da CF. Ante o exposto, conheço do conflito para declarar competente o Juízo de Direito da 3ª Vara Criminal de Vila Velha/ES, o suscitado. Publique-se. Intimem-se. Brasília, 20 de abril de 2017.[234]

Assim, se os crimes informáticos não se enquadrarem nas hipóteses do artigo 109, inciso IV e V da Constituição, por exclusão será de competência da

[234] STJ, Superior Tribunal de Justiça. **CC: 145516 ES 2016/0050531-4, Relator: Ministro JOEL ILAN PACIORNIK, Data de Publicação: DJ 28/04/2017**, Brasília: STJ, 2017. Disponível em: <https://bit.ly/2RMYNMv> Acesso em 12/10/2018 às 9h06min, s/p.

Justiça Estadual, já que como demonstrado anteriormente, possui caráter residual, “exceção” que em verdade acaba por se tornar a regra, tendo em vista os inúmeros requisitos necessários para assim não ser.

5.2.2 Da competência de foro

Determinada a competência de justiça, passa-se a analisar então o prisma da competência territorial, ou seja, a aplicação do critério “ratione loci” aos crimes informáticos, a fim de determinar o foro de qual localidade será competente para apreciar tais crimes.

Aqui reside às principais discussões acerca da competência dos delitos informáticos impróprios, pois, como já afirmado várias vezes ao longo do presente trabalho, as características do ambiente informático, principalmente a pluralidade (que permite ao indivíduo estar em várias localidades ao mesmo tempo), a internacionalidade (a possibilidade do crime informático facilmente expandir além das barreiras territoriais) e o anonimato (a dificuldade de identificar o indivíduo e até o local de onde partiu o delito), acabam por tornar o local do crime algo difuso, de difícil compreensão, imagine que o indivíduo x, cuja localidade é desconhecida, publicou em uma rede social, cujo servidor está localizado em Berlim, mensagens racistas contra Y, residente em São Paulo, qual local competente? Berlim? São Paulo ou outro local?

A priori a definição da competência territorial nos crimes informáticos deve seguir a velha regra disposta no artigo 70 do Código de Processo Penal, ou seja, o local da consumação ou último ato de execução, contudo para os delitos informáticos, essa teoria do resultado adotada pelo Código de Processo Penal acaba por não ser tão eficaz, veja o caso do exemplo acima, mesmo com uma regra sólida como a do artigo 70, torna-se difícil compreender qual o foro competente, se foi Berlim, São Paulo, ou outra localidade, nesse ponto, segundo Túlio Viana[235] a teoria da ubiquidade disciplinada no artigo 6º do Código Penal acaba por ser muito mais útil, pois, traz mais uma possibilidade de averiguação da competência *“ratione loci”.* Como demonstrado anteriormente, o legislador quando estabeleceu a teoria do resultado, visou principalmente uma questão de conveniência e aplicabilidade legal, cadê a conveniência da aplicação da lei penal nos casos informáticos?

[235] VIANNA, 2013, **op. cit.,** p. 48.

Talvez o ideal fosse manter a equidade do Código Penal como regra principal e permitir que a competência "*ratione loci"* fosse determinada conforme a conveniência de caso, partindo de uma regra mais abrangente que é a ubiquidade, para um critério mais restrito que é a teoria do resultado, além do mais, Vianna elenca importante observação que mesmo em crimes a adoção da teoria do resultado acaba dando alguns problemas:

> Fato é que o critério adotado pelo CPP padece de vícios. Imagine-se a situação de um homicídio em que a vítima é alvejada por disparos de arma de fogo em uma comarca, mas, levada ao hospital da comarca vizinha, vem a falecer neste último local. Pelo critério do CPB (teoria da ubiquidade), o lugar do crime seria tanto o da conduta quanto o do resultado, mas segundo o CPP (teoria do resultado), o foro competente para processo e julgamento do crime seria o do local da consumação, ou seja, a comarca do hospital onde a vítima veio a óbito. Nesse caso, qual seria a utilidade de se fixar a competência na comarca onde se encontra o hospital? Como se percebe, não há lógica nessa definição, já que o conjunto probatório estaria em comarca diversa daquela onde se fixaria o juízo competente.[236]

Feita a crítica à teoria do resultado disciplinada no artigo 70 do Código Penal, resta prosseguir com a análise, então a primeira premissa é, se for possível determinar o local do resultado, ou último local da execução, o foro competente será dessa localidade, assim, no caso de um indivíduo A, residente em Presidente Prudente/SP, adentrar no site da prefeitura de sua cidade colocar frases difamando o sujeito Y, que também reside em Presidente Prudente, o local competente será a referida cidade, tendo em vista que a honra subjetiva do indivíduo foi ofendida no site de servidor localizado nessa cidade.

Contudo, conforme já explanado, nem sempre será possível a aplicação da regra do artigo 70, seja por questões da internacionalidade, seja pela dificuldade de determinação do local das infrações, ou pela dificuldade de auferir a consumação de determinados delitos, para solucionar essas questões existem casos específicos dos quais a doutrina e jurisprudência tratou, como ocorre com parte dos crimes contra a honra, crimes contra o patrimônio, racismo, ameaça e crimes contra a criança e adolescente, casos que serão destacados de forma específica mais à frente, regras genéricas que se estenderão à maioria dos crimes informáticos.

---

[236] VIANNA, 2013, **op. cit.,** p. 48-49.

A primeira regra genérica é que nos casos de não ser possível a aplicação do artigo 70, caput do Código de Processo Penal, e não for caso de internacionalidade ou delito à distância, Patrícia Santos Silva diz que deve se adotar a regra secundária do artigo 72 do referido código, qual seja o domicílio ou residência do réu.[237]

Outro aliado importante para a determinação da competência territorial dos crimes informáticos, será o critério da prevenção, esse será aplicado em três hipóteses, a primeira quando o réu possui mais de um domicílio[238], a segunda hipótese será no caso do crime informático ser plurilocal, acontecer dentro do país, mas não conseguir auferir o território da execução de forma alguma, devido a multiplicidade de locais,[239] e a terceira é quando for totalmente incerto tanto o local da consumação, quanto a residência do réu, aí o primeiro foro que tiver contato com a causa será competente.[240]

Também é aplicável aos crimes informáticos a regra do artigo 70, §1º e 2º do Código Penal, ou seja, quando um delito informático à distância, quando é praticado parte no exterior, parte no Brasil, é possível considerar o foro competente do local no qual o delito tocou no Brasil, ex: sujeito X residente na Itália, consegue desviar uma quantia de dinheiro da agência da Caixa Econômica Federal localizada na cidade de Presidente Prudente, o foro competente será a Justiça Federal de Presidente Prudente, quanto à punição do criminoso, deve-se a atentar às regras de extraterritorialidade disciplinadas no Código Penal, artigo 7º.[241][242]

Ainda existe a possibilidade do crime informático totalmente internacionalizado, ou seja, aquele que se perpetua em sua totalidade no exterior, ex: um brasileiro que vive no exterior e monta um site destinado a difusão de pornografia infantil ao redor do globo, se preenchidos os requisitos do artigo 7º do Código Penal sobre extraterritorialidade, poderá ser aplicado o artigo 88 do Código de Processo Penal, sendo competente o foro dá última residência do Brasileiro, ou, se não houver, o foro de Brasília.

---

[237] SILVA, Patrícia Santos da. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais [recurso eletrônico] / Patrícia Santos da Silva, Matheus Passos Silva (coord.)**. Brasília: Vestnik, 2015. Disponível em: <https://bit.ly/2CcoQHD> Acesso em: 25/08/2018 às 18h22min, p. 80.
[238] Artigo 72, §1º do Código de Processo Penal. BRASIL, 1941, **op. cit.,** s/p.
[239] Artigo 70, §3º do Código de Processo Penal. BRASIL, 1941, **op. cit.,** s/p.
[240] Artigo 72, §2º do Código de Processo Penal. BRASIL, 1941, **op. cit.,** s/p.
[241] BRITO, 2013, **op. cit.,** p. 99.
[242] LIMA, 2017, **op. cit.,** p. 528.

Como foi observado acima, além das considerações gerais à determinação da competência territorial nos crimes informáticos impróprios, existem alguns pontos em que a doutrina e jurisprudência tratou de forma mais específica, a seguir então serão observadas essas considerações.

5.2.2.1 Nos crimes contra a honra e racismo

No caso dos crimes informáticos contra a honra, calúnia, difamação e injúria, conforme assinala Fabiano Kummer[243], o Superior Tribunal de Justiça vem entendendo, que, a competência territorial para apreciação desses delitos se dá a partir do local em que estão sendo alimentadas as informações ofensoras, ou seja, local do domínio sob o qual o site, ou serviço está hospedado, nesse sentido foi a decisão do Conflito de Competência 136700/SP:

> CONFLITO DE COMPETÊNCIA. CRIMES CONTRA HONRA PRATICADOS PELA INTERNET. COMPETÊNCIA. VEICULAÇÃO DO CONTEÚDO OFENSIVO. FIXAÇÃO NO LOCAL DO TITULAR DO PRÓPRIO DOMÍNIO E QUE CRIOU A HOME PAGE ONDE É ABASTECIDO SEU CONTEÚDO.
> 1. Tratando-se de crimes contra a honra praticados pela internet, a competência deve ser firmar de acordo com a regra do art. 70 do Código de Processo Penal, segundo o qual "A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução". Isso porque constituem-se crimes formais e, portanto, consumam-se no momento de sua prática, independentemente da ocorrência de resultado naturalístico. Assim, a simples divulgação do conteúdo supostamente ofensivo na internet já é suficiente para delimitação da competência.
> 2. Esse local deve ser aquele de onde efetivamente partiu a publicação do conteúdo, o que ocorre no próprio local do domínio em que se encontra a home page, porquanto é ali que o titular do domínio alimenta o seu conteúdo, independentemente do local onde se hospeda o sitio eletrônico (provedor).
> 3. No caso, a veiculação da reportagem que deu ensejo ao inquérito policial partiu de sítio eletrônico cujo domínio era de empresa situada no Mato Grosso, razão pela qual a competência é do Juízo Federal da 5ª Vara da Seção Judiciária do Estado do Mato Grosso.[244]

Assim, se o indivíduo que reside em Junqueirópolis/SP, publica difamações em sua rede social, com sede em São Paulo, a outrem, de regra o local competente será o do domínio da rede social, no caso São Paulo.

---

[243] KUMMER, 2017, **op. cit.,** s/p.

[244] STJ, Superior Tribunal de Justiça. **CC 136.700/SP, Rel. Ministro ROGERIO SCHIETTI CRUZ, TERCEIRA SEÇÃO, julgado em 23/09/2015**, DJe 01/10/2015, Brasília: STJ, 2015. Disponível em: <https://bit.ly/2RO8w5w> Acesso em 12/10/2018 às 17h59min, s/p.

Analisando a estrutura dos delitos de racismo tanto a injúria racial, quanto os descritos na Lei 7.716/1989, em que pese algumas diferenças entre esses crimes, como a abrangência e as formas específicas dos crimes de racismo, faz sentido seguir a mesma lógica acima, já que não deixa de ser, ainda que como questão secundária, uma ofensa à honra[245], e foi realmente essa a postura adotada pelo Superior Tribunal de Justiça no CC. 107938, ao se posicionar que o órgão competente é do local de onde partiram as ofensas, ou seja, do domínio a partir do qual elas foram vinculadas.

5.2.2.2 Nos crimes de ameaça

Em recente decisão, o Superior Tribunal de Justiça no julgamento do Conflito de Competência nº 156.284/PR, entendeu que no caso do delito de ameaça, artigo 147 do Código Penal, quando for praticado pela via informática, através de sites e aplicativos de mensagens como Facebook, Whatsapp, email, o foro competente será do local em que o indivíduo tomou conhecimento da ameaça, independentemente do local em que tenha sido vinculada, assim é a decisão:

> CONFLITO DE COMPETÊNCIA. CRIME DE AMEAÇA PRATICADO POR WHATSAPP E FACEBOOK. ÂMBITO DE APLICAÇÃO DA LEI MARIA DA PENHA. DELITO FORMAL.
> CONSUMAÇÃO NO LOCAL ONDE A VÍTIMA CONHECE DAS AMEAÇAS. CONFLITO DE COMPETÊNCIA CONHECIDO. DECLARADA A COMPETÊNCIA DO JUÍZO SUSCITADO.
> 1. O crime de natureza formal, tal qual o tipo do art. 147 do Código Penal, se consuma no momento em que a vítima toma conhecimento da ameaça. 2. Segundo o art. 70, primeira parte, do Código de Processo Penal, "A competência será, de regra, determinada pelo lugar em que se consumar a infração". 3. No caso, a vítima tomou conhecimento das ameaças, proferidas via Whatsapp e pela rede social Facebook, na Comarca de Naviraí, por meio do seu celular, local de consumação do delito e de onde requereu medidas protetivas. 4. Independentemente do local em que praticadas as condutas de ameaça e da existência de fato anterior ocorrido na Comarca de Curitiba, deve-se compreender a medida protetiva como tutela inibitória que prestigia a sua finalidade de prevenção de riscos para a mulher, frente à possibilidade de violência doméstica e familiar. 5. Conflito conhecido para declarar a competência do Juízo da 1º Vara Criminal da Comarca de Naviraí/MS, ora suscitado.[246]

---

[245] VIANNA, 2013, **op. cit.,** p. 52.

[246] STJ, Superior Tribunal de Justiça. **CC 156.284/PR, Rel. Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 28/02/2018 DJe**, Brasília: STJ, 2018. Disponível em: <https://bit.ly/2pPZeZF> Acesso em 12/10/2018 às 14h27min, s/p.

Logo, se A ameaçar B pelo Facebook e esse tomar conhecimento da ameaça enquanto estiver viajando por Maringá/PR, o foro competente para apreciar tal crime, será a cidade de Maringá, perceba, um entendimento que adota um viés prático oposto ao observado nos crimes contra a honra e racismo, cujo órgão competente é o do domínio em que os fatos foram vinculados.

5.2.2.3 Nos crimes contra o patrimônio

Do ponto de vista dos crimes contra o patrimônio, merecem destaque duas considerações, a primeira no que concerne o crime furto mediante fraude realizado no meio informático, artigo 155, §4º do Código Penal, no qual o agente se vale dos mecanismo informáticos para subtrair valores de contas bancárias, nesse caso o Egrégio Superior Tribunal de Justiça entendeu que o foro competente é o do local da agência bancária da qual os valores foram subtraídos, pois, é nesse que o crime se consuma, nesse sentido é o informativo nº 0326 de agosto de 2007, do Superior Tribunal de Justiça:

> **COMPETÊNCIA. FRAUDE ELETRÔNICA. *INTERNET*. CONTA CORRENTE. BANCO.**O cerne da questão consiste em se determinar o juízo competente para processar e julgar crime de transferências eletrônicas bancárias sem consentimento do correntista para outra pessoa via *internet* em detrimento da CEF. No caso dos autos, a fraude foi usada para burlar o sistema de proteção e vigilância do banco sobre os valores mantidos sob sua guarda, configurando crime de furto qualificado por fraude e não estelionato. Assim, considera-se consumado o crime de furto no momento em que o agente torna-se possuidor da *res furtiva*, ou seja, no momento em que o bem subtraído sai da esfera de disponibilidade da vítima. No caso, a conta-corrente da vítima estava situada em Porto Alegre-RS, local da consumação do delito (art. 155, § 4º, II, do CP). Com esse entendimento, em sintonia com o parecer do MPF e a jurisprudência deste Superior Tribunal, a Seção declarou competente o Juízo Federal suscitante. Precedente citado: CC 67.343-GO. CC 72.738-RS**,** Rel. Min. Maria Thereza de Assis Moura, julgado em 8/8/2007.[247]

Outro entendimento consolidado acerca da determinação da competência “ratione loci” nos crimes informáticos, é com relação ao delito de estelionato praticado no âmbito informático, artigo 171 do Código Penal, segundo

[247] STJ, Superior Tribunal de Justiça. **Informativo nº 326, Terceira Seção – COMPETÊNCIA. FRAUDE ELETRÕNICA. INTERNET. CONTA-CORRENTE. BANCO,** Brasília: STJ, 2017. Disponível em: < https://bit.ly/2J4P7Jw> Acesso em 09/10/2018 às 15h27min, s/p.

Túlio Viana[248], o foro competente será o do local onde o agente obteve a vantagem indevida, nesse sentido foi o entendimento Superior Tribunal de Justiça:

> CONFLITO NEGATIVO DE COMPETÊNCIA. JUSTIÇA ESTADUAL X JUSTIÇA ESTADUAL. INQUÉRITO POLICIAL. ESTELIONATO. VENDA DE PRODUTO PELA INTERNET. ENVIO DE E-MAIL COM FALSA COMPROVAÇÃO DE PAGAMENTO. CONSUMAÇÃO DO DELITO (ART. 70, CPP): LOCAL DA OBTENÇÃO DA VANTAGEM ILÍCITA, QUE, NO CASO CONCRETO, CORRESPONDE AO LOCAL DE RECEBIMENTO DA MERCADORIA. 1. Situação em que a vítima vendia mercadoria pela internet e, após receber uma falsa confirmação de pagamento por e-mail, remeteu a mercadoria para o endereço do estelionatário, que foi preso em flagrante quando a recebia do agente dos Correios. 2. Nos termos do art. 70 do CPP, a competência será de regra determinada pelo lugar em que se consumou a infração e o estelionato, crime material tipificado no art. 171 do CP, consuma-se no momento e lugar em que o estelionatário aufere proveito econômico em prejuízo da vítima. 3. Há que se diferenciar a situação em que o estelionato ocorre quando a vítima é ardilosamente induzida a, voluntariamente, depositar na conta do estelionatário o preço de uma mercadoria que jamais chega a receber, da hipótese (como a dos autos) em que a vítima, também iludida por um ardil, é levada a crer que o pagamento pelo produto por ela vendido foi devidamente efetuado e, em consequência disso, voluntariamente entrega a mercadoria. Na primeira das situações (em que pagamentos são feitos pela vítima ao estelionatário), a obtenção da vantagem ilícita ocorre no momento em que o dinheiro sai efetivamente da disponibilidade financeira da vítima. Tratando-se de pagamento por meio de cheque, transferência bancária ou cartão de crédito, isso ocorre quando os valores saem da entidade financeira sacada. Por esse motivo, em tais casos, entende-se que o local da obtenção da vantagem ilícita é aquele em que se situa a agência bancária onde foi sacado o cheque, seja dizer, onde a vítima possui conta bancária. Já na segunda hipótese, em que a vítima é a vendedora do produto, o estelionatário aufere proveito econômico em prejuízo da vítima quando recebe a mercadoria e não chega a pagar por ela. Em tais situações, por óbvio, o local em que é obtida a vantagem ilícita é o local da retirada do produto. A esse segundo tipo de conduta, corresponde a hipótese com base na qual foi editada a súmula n. 48 desta Corte, segundo a qual compete ao juízo do local da obtenção da vantagem ilícita processar e julgar crime de estelionato cometido mediante falsificação de cheque. Nesse diapasão: CC 113.947/PA, Rel. Ministro MARCO AURÉLIO BELLIZZE, TERCEIRA SEÇÃO, julgado em 26/02/2014, DJe 06/03/2014; CC 101.900/RS, Rel. Ministro JORGE MUSSI, TERCEIRA SEÇÃO, julgado em 25/08/2010, DJe 06/09/2010 e CC 96.109/RJ, Rel. Ministro ARNALDO ESTEVES LIMA, TERCEIRA SEÇÃO, julgado em 26/08/2009, DJe 23/09/2009. 4. De mais a mais, as investigações preliminares, no caso concreto, permitiram concluir que a ação dos investigados atingiu vítimas de vários Estados da Federação, parecendo mais proveitoso à investigação, à compreensão de seu modus operandi, e à coleta de provas que o Inquérito permaneça no local em que os investigados residem e operavam seu esquema criminoso. 5. Conflito conhecido, para declarar a competência do Juízo de Direito da 2ª Vara Criminal de Curitiba/PR, o suscitado, para conduzir o presente Inquérito Policial e, eventualmente, julgar a ação penal dele derivada.[249]

[248] VIANNA, 2013, **op. cit.,** p. 50.

[249] STJ, Superior Tribunal de Justiça. **CC: 160053 SP 2018/0194677-4, Relator: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 22/08/2018, S3 - TERCEIRA**

Interessante frisar que o referido Tribunal recentemente passou a entender que a conduta de abrir lojas virtuais com fim de enganar a sociedade e não entregar os produtos vendidos, não configura o crime do artigo 171 do Código Penal, mas sim o crime contra economia popular descrito no artigo 2º, inciso IX, da Lei nº 1.521/1951. No aspecto da competência, como ambos os crimes se destinam a obtenção de uma vantagem ilícita, é possível dizer que o critério definido pelo STJ para o crime de estelionato se estende ao referido crime contra economia popular da Lei nº 1.521/1951, sendo o foro competente o do local em que o agente recebeu a vantagem indevida, no caso, os valores provenientes das vendas fraudatórias.

5.2.2.4 Dos crimes contra a criança e adolescente

Já finalizando o estudo acerca da competência dos crimes informáticos impróprios, resta tecer observações acerca da competência territorial nos crimes contra à criança e o adolescente, mais precisamente os descritos nos artigos 241, 241-A, 241-B, do Estatuto da Criança e do Adolescente.

Quanto às práticas descritas nos artigos 241, 241-A, que são os delitos relacionados à difusão de material pornográfico, segundo Fábio Kummer[250], o Superior Tribunal de Justiça, no conflito de competência 29.886/SP[251], pacificou que tais crimes se consumam no momento da difusão do material, ou seja, dá inserção nos meios virtuais, devendo a competência “ratione loci” ser fixada no local em que ocorre a propagação do conteúdo pornográfico. O autor[252] também assevera, que nas situações em que esse local da difusão for estrangeiro, serão aplicadas as regras de extraterritorialidade do artigo 7º do Código Penal, pois, como mencionado anteriormente, o Brasil ratificou a Convenção Sobre os Direitos da Criança da ONU, dessa forma, serão aplicadas às regras mencionadas às páginas 81 e 82 do presente trabalho, quais sejam, os artigos 70, § 2º e 3º, e 88 do Código de Processo Penal.

SEÇÃO, Data de Publicação: DJe 27/08/2018, Brasília: STJ, 2018. Disponível em: < https://bit.ly/2NH2O25 > Acesso em 13/10/2018 às 10h15min, s/p.

[250] KUMMER, 2017, **op. cit.,** s/p.

[251] STJ, Superior Tribunal de Justiça. **CC 29.886/SP, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, TERCEIRA SEÇÃO, julgado em 12/12/2007, DJ 01/02/2008, p. 427,** Brasília, 2007. Disponível em: <https://bit.ly/2ygZJRc> Acesso em 12/10/2018 às 12h10min, s/p.

[252] [252] KUMMER, 2017, **op. cit.,** s/p.

Em relação ao crime descrito no artigo 241-B, armazenagem de conteúdo pornográfico, Túlio Vianna, diz que a regra de análise de competência se altera um pouco, pois, tal delito é de mera conduta, ou seja, se consuma com a simples ação de armazenar, de forma que o foro competente será o do local do armazenamento do conteúdo, não excluindo o que foi dito quanto a possibilidade de aplicação da extraterritorialidade no caso do local de depósito do material estar no estrangeiro.

5.3 Ultimas Considerações Acerca da Competência dos Crimes Informáticos

Essa foi a análise da competência nos crimes informáticos, no que pese o foco ter sido nos delitos de caráter impróprio, a maioria das regras mencionadas se aplicam aos crimes informáticos em geral.

Dessa análise, fica evidente a existência de poucas regras processuais para a disciplina dos crimes digitais, os critérios apresentados em sua maioria advêm de interpretações da jurisprudência e doutrina, o que é prejudicial, pois, não traz segurança jurídica, já que os entendimentos jurisprudenciais comumente se alteram, podendo, inclusive, se chocar em algum momento.

Também deve se ressaltar novamente que a opção do legislador pela adoção da teoria do resultado no artigo 70 do Código de Processo Penal, dificulta o estudo da competência dos delitos informáticos, dadas as suas especificidades, parecendo mais vantajoso que o Código de Processo Penal entrasse em sincronia total com o artigo 6º do Código Penal, e adotasse a teoria da ubiquidade. Contudo, apesar da crítica à postura do legislador, todos os problemas parecem se resumir à falta de legislação específica, talvez o problema maior não seja a adoção da teoria do resultado como regra do Código de Processo Penal, mas sim, a falta de regras que determinem a competência nos crimes informáticos, tanto em relação à competência “*ratione loci”*, quanto à competência de justiça.

6 CONCLUSÃO

Depois de uma longa análise, o trabalho chega ao momento de destaque de suas principais conclusões.

Em um primeiro momento foi possível compreender que de um longo processo evolutivo, que teve por cenário o homem e seus dilemas matemáticos, emergiu a computação e a internet que inauguraram a chamada “era da informação”. Conforme observado essa nova era revolucionou o modo de viver da sociedade, o mundo passa a estar inteiramente conectado, tendo por principal atributo a velocidade, tanto no aspecto de acesso e circulação de informações, quanto no aspecto evolucional, pois, grandes evoluções que ocorriam em décadas e séculos, passam a ocorrer em dias, horas, e daí nasce um ponto temeroso ao Direito, que acaba por ter dificuldades de acompanhar evoluções tão marcantes e rápidas, nascendo lacunas e problemas como a dificuldade de atribuição da competência nos crimes informáticos.

Da análise estrutural e caracterológica feita na segunda parte, foi possível compreender que os crimes informáticos são, pelo seu rápido avanço, uma realidade que vem provocando temor global e nacional.

O principal objeto desses crimes, é a integridade e sigilo de dados, que são as informações decodificadas no mundo digital, a partir daí, foi observado que as práticas que ofendem esse bem jurídico e que em razão disso dependem do mundo informático, são chamadas de crimes informáticos próprios, existindo a contrário sensu os crimes informáticos impróprios, crimes comuns que lesam outros bens jurídicos, mas que acabam por ser praticados âmbito informático aproveitando de uma série de peculiaridades desse meio.

Da confluência entre bem jurídico e classificações, os crimes informáticos puderam ser conceituados como todas aquelas práticas que se utilizam dos aparatos tecnológicos com o fim de agredir o sigilo e a integridade de dados e informações. Tais fatores também explicam a adoção do “nomen juris” crimes informáticos, dado que essa se adequa melhor a conceito e ao bem jurídico, e ao meio em que tais práticas são realizadas, qual seja o ambiente informático, diferente do que ocorre com expressões como “crimes cibernéticos”, que possui caráter genérico e impróprio, pois, como visto, a cibernética é uma ciência ampla da qual um dos objetos pode ser o meio digital e seus crimes.

Ficou claro também, que em razão das peculiaridades do cenário informáticos, muitos criminosos comuns acabaram migrando para esse meio, quebrando o estigma do criminoso informático com vasto conhecimento técnico da computação. Também foi notado, que a comunidade informática, categoriza alguns criminosos de acordo com periculosidade e conhecimento, como os “crackers”, “internals”, e “professional criminals”.

Das considerações sobre sujeição passiva, foi possível extrair a importante conclusão de que a vítima tem um papel muitas vezes determinante nesse tipo de crime, pois muitas vezes inobserva os cuidados essenciais de uso, acessando links e fornecendo dados à paginas suspeitas, de forma que a prevenção se torna um dos elementos essenciais para a redução dos crimes informáticos.

Ao final da segunda parte, foi possível compreender que o ambiente informático é dotado de características, como a internacionalidade, a velocidade, o anonimato, a intangibilidade, a pluralidade e à ubiquidade, que o diferenciam de qualquer outro meio, rompendo barreiras geográficas, físicas e temporais, de forma que fazem necessárias normas específicas, pois, ainda que o crime seja impróprio, essas peculiaridades rompem com preceitos dos quais o Direito já estava adequado, surgindo inúmeros problemas, como o da dificuldade de atribuição de competência nos crimes informáticos.

Na terceira parte foi traçado o cenário legal brasileiro acerca dos crimes informáticos, em que pese o destaque às Leis 12.735/12 e 12.737/12 como as primeiras normas a tratarem com maior especificidade essa modalidade de delito, ficando latente que a legislação brasileira é prematura e atrasada em matéria dos crimes informáticos, sendo os principais motivos, a timidez, e a dissidia do legislador, que teve oportunidades de alterar e evoluir o ordenamento, mas não fez; e o fato do Brasil não ser signatário da importante Convenção de Budapeste, tratado internacional destinado à uniformização das normas de combate aos crimes informático, ficando o Brasil atrás de vários países como Argentina e Chile.

No último capítulo, o trabalho chegou ao seu objeto, a análise competência nos crimes informáticos impróprios. Da primeira parte, onde foram feitas as considerações gerais sobre competência, foi possível compreender que a jurisdição é o mecanismo adotado pelo Estado, para solucionar as divergências e pacificar o meio social, e que se entende por competência, as parcelas de jurisdição

distribuídas a cada órgão do judiciário, tendo em vista a impossibilidade prática de um único juiz apreciar todos conflitos sociais.

Nos aspectos gerais foi possível observar que a atribuição da competência passa por três principais critérios, em razão da pessoa (“ratione personae”), em razão da matéria (‘ratione materiae”) e em razão do território (“ratione loci”). Sendo os dois primeiros, critérios de competência absoluta, que de regra não podem ser alterados, e o último de competência relativa, admitindo a prorrogação.

Desse modo, foi demonstrado que a competência em razão da pessoa, se vincula a chamada “competência por prerrogativa de função”, ou seja, a função, cargo ocupado pode atrai a origem do julgamento para outro órgão, como o Superior Tribunal Federal no caso de um deputado federal. Além da atuação na competência originária, atua ao lado do critério “ratione materiae” na determinação da competência de justiça, determinando se serão competentes justiças especializadas, como a Militar e a Eleitoral, ou as comuns, Federal e Estadual.

No campo da competência por matéria, que como dito se apresenta como importante critério de determinação da competência de justiça, ficou claro que alguns conteúdos serão analisados pelas justiças especificas, tendo a Justiça Comum Estadual competência residual, ou seja, julga toda matéria que não se enquadrar de alguma forma nas outras justiças.

Por fim na análise da competência territorial, foi observado que esse critério se dedica a determinar o órgão jurisdicional de qual território que julgará o caso, a chamada competência de foro.

A regra geral, como observado, é a do artigo 70 do Código de Processo Penal, ou seja, o local da consumação ou último ato da execução, o que evidencia a adoção da teoria do resultado, e não da ubiquidade como o Código Penal preferiu.

Além da regra, foram observadas exceções, as primeiras destacadas, foram as descritas parágrafos 1º e 2º do referido artigo, nos casos de crime à distância, aqueles que atingem além do Brasil algum outro país, a teoria da ubiquidade é utilizada, sendo competente foro do local em que o crime tocou no Brasil.

No caso de crimes totalmente internacionalizados, foi observado que se estiverem presentes os requisitos da extraterritorialidade do artigo 7º do Código

Penal, será competente o último local em que o indivíduo residiu ou, caso esse não exista, o foro da capital do país, sendo aplicado o artigo 88 do Código de Processo Penal.

Por fim, como últimas exceções, foi possível concluir que não sendo possível auferir o local do crime, como no caso dos crimes plurilocais, serão utilizadas duas regras, o local em que o réu domiciliado, artigo 72 do Código de Processo Penal, e o critério da prevenção, artigos 72, §1º e 2º e 83 do referido código, sendo competente para julgar, o foro que primeiro tiver contato com a causa.

Traçados os critérios gerais de competência, partiu-se para a análise de competência específica dos crimes informáticos, feita em dois ângulos de maior discussão, a competência de justiça e a competência de foro.

Do viés da competência de justiça, foi observado que o cerne da discussão se dá entre competência da federal e estadual, como a última é residual, restou a determinação dos casos de competência federal.

Sendo possível concluir que a justiça federal será competente em duas hipóteses: a primeira, descrita no artigo 109, IV da Constituição Federal, quando do crime informático resultar lesão ou ameaça de lesão, importante aos interesses, bens e serviços da União, autarquias e empresas públicas, é o que o ocorre no furto qualificado mediante fraude, realizado no âmbito digital contra correntista da Caixa Econômica Federal. A segunda, quando o crime informático tiver caráter internacional relevante, com certa publicidade, e estiver previsto em tratado internacional do qual o Brasil tenha se comprometido a combater e a reprimir aquela conduta, como ocorre nos casos de pedofilia dos artigos 241, 241-A, 241-B, do Estatuto de Criança e do Adolescente, e nos crimes de racismo.

No plano da competência de foro, foi possível compreender que esse é um dos campos de maior discussão, dado que as peculiaridades do ambiente informáticos tornam o local do crime difuso, daí o olhar negativo à adoção do critério do resultado, e não o da ubiquidade pelo Código de Processo Penal, pois, tal medida dificulta a determinação de competência, por restringir as hipóteses de foro, quando que aos crimes informáticos, o ideal seria ter múltiplas possibilidades.

Ficou nítido que grande parte das regras de competência geral são aplicadas aos crimes informáticos, sendo utilizadas tanto a regra do artigo 70 do Código de Processo Penal, como as exceções já destacadas nessa conclusão, cabendo ressaltar a importância da ubiquidade trazida nos parágrafos do artigo 70, a

exceção do artigo 72, o foro internacional do artigo 80 e, principalmente, o critério da prevenção, pois, muitas vezes o crime informático assumirá papel plurilocal e de difícil determinação, aí atribuir a competência ao órgão que primeiro apreciar se torna medida positiva.

Por fim foram destacados específicos de atribuição da competência territorial nos crimes informáticos impróprios, chegando a quatro principais conclusões:

A primeira conclusão é que nos crimes contra a honra e racismo, de regra, o foro competente será o do local do domínio do site ou serviço em que as agressões estão sendo proferidas, independentemente do local do agressor ou do servidor em sob qual o site, ou serviço estejam hospedados;

A segunda, é que nos crimes de ameaça, o foro competente será o do local em que a vítima tomou conhecimento da ofensa, independentemente de onde tenham partido as agressões.

A terceira, é que no caso do crime de furto mediante fraude realizado pelo meio digital com saques irregulares, artigo 155, §4º do Código Penal, o Superior Tribunal de Justiça entendeu que será competente o foro do local da agência a qual pertence a conta, da qual os valores foram desviados.

Por fim, nos caso de estelionato praticado pelo meio informático, o foro competente é o do local em que o agente auferir a vantagem ilícita, mesmo raciocínio para o do crime contra a economia popular disciplinado no artigo 2º, inciso IX da Lei 1.521/1951, lembrando que o Superior Tribunal de Justiça entende que abrir lojas virtuais com ânimo de obter vantagem indevida sem entregar os produtos configura esse delito e não estelionato.

Calha salientar, que em que pese as regras de atribuição de competência tenham sido estudadas no prisma dos crimes informáticos impróprios, muitas das disposições atingem os crimes informáticos como um todo.

Dessa forma, nota-se em conclusão final que o problema da atribuição da competência nos crimes informáticos é fruto de vários fatores como: a evolução rápida da era da informação, as peculiaridades do meio informático, e até o fato da adoção da teoria do resultado pelo artigo 70 do Código de Processo Penal.

Contudo, todos esses desdobramentos se resumem a uma raiz, a deficiência e atraso normativo, o legislador teve oportunidades de atualizar o ordenamento e não fez. Não se deve abraçar o pensamento de que em crimes

impróprios não são necessárias normas específicas, pois, as peculiaridades do meio informático e da era da informação tornam essa realidade muito distinta de qualquer outra já vivida, sendo possível concluir que a melhor solução ao problema da competência e outros advindos dos crimes informáticos, é que sejam feitas profundas alterações legislativas no ordenamento brasileiro de modo a adequá-lo essa nova era que vive em constante evolução.

REFERÊNCIAS

AVENA, Norberto Pâncaro. **Processo Penal**/Norberto Avena, 9.ed. Rio de Janeiro: Método, 2017. (Recurso Eletrônico – “Minha Biblioteca”).

BENTO, Beatrice Helena Silveira**. A nova lei de proteção de dados no Brasil e o general data protection regulation da União Europeia,** Migalhas, 2018. Disponível em:< https://bit.ly/2Rd0stE> Acesso em 23/10/2018 às 22h15min

BITENCOURT, Cezar Roberto. **Tratado de direito penal,** v.1 parte geral. 21. São Paulo: Saraiva, 2015.

BRASIL**. Código de Processo Penal. decreto lei nº 3.689, de 03 de outubro de 1941.** 1941. Disponível em: <https://bit.ly/2pPI2Uh> Acesso em: 15/082018 às 16h21min.

_____. **Código Penal. Decreto-Lei 2.848, de 07 de dezembro de 1940**, 1940. Disponível em: <https://bit.ly/1dqm1Rx> Acesso em 09/10/2018 às 14h29min.

_____**. Constituição da República Federativa do Brasil, de 5 de outubro de 1988.** 1988. Disponível em <https://bit.ly/1dFiRrW> Acesso em: 12/10/2018 às 16h52min.

_____. **Decreto nº 99.710, de novembro de 1990.** Promulga a Convenção sobre os Direitos da Criança, 1990. Disponível em: <https://bit.ly/28TFYGb> Acesso em 10/10/2018 às 15h16min.

_____. **Lei nº 7.716, de 5 de janeiro de 1989.** Define os crimes resultantes de preconceito de raça ou de cor. 1989. Disponível em: <https://bit.ly/28TFYGb> Acesso em 10/10/2018 às 15h16min

_____. **Lei nº 11.829, de 25 de novembro de 2008.** Altera a Lei nº 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente, para aprimorar o combate à produção, venda e distribuição de pornografia infantil, bem como criminalizar a aquisição e a posse de tal material e outras condutas relacionadas à pedofilia na internet. 2008. Disponível em: <https://bit.ly/2EkYqpN> Acesso em 11/10/2018 às 15h16min

_____. **Lei nº 12.735, de 30 de novembro de 2012.** Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências, 2012. Disponível em: < https://bit.ly/1sUwjhz> Acesso em 11/10/2018 às 22h16min.

_____. **Lei nº 12.737, de 30 de novembro de 2012.** Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. 2012. Disponível em: <https://bit.ly/2NqkqDaz> Acesso em 11/10/2018 às 22h16min.

_____. **Lei nº 13.709, de 14 de agosto de 2018.** Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet), Brasília, 2018. Disponível em < https://bit.ly/2NH4yIF> Acesso em 23/10/2018 às 22h20min.

BRITO, Auriney. **Direito penal informático,** *1ª edição,* São Paulo: Saraiva, 2013. (Recurso Eletrônico – "Minha Biblioteca").

CANALTECH. **O que é DoS e DDosS?,** Canaltech. Dispnível em: <https://bit.ly/2GP6lt8> Acesso em 22/09/2018 às 16h29min.

CARDI, Marilza de Lourdes. **Evolução da computação no Brasil e sua relação com fatos internacionais**. 2002. Dissertação (Mestrado em Ciência da Computação) - Universidade Federal de Santa Catarina, Santa Catarina, 2002. Disponível em: < https://bit.ly/2yA9BVK > Acesso em 12/03/2018 às 18h39min.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas Reais,** 1.ed. Rio de Janeiro: BRASPORT, 2013. (Recurso Eletrônico – "Edição do Kindle").

CERT, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. **Estatísticas dos Incidentes Reportados ao CERT.br**, 2017. Disponível em: <https://bit.ly/2EWbOMn> Acesso em 13/10/2018 às 15h42min.

CORPORATION, Symantec. **Norton Cyber Security Insights Report 2017 Global Results** 2017. Disponível em: <https://symc.ly/2G8VNnU> Acesso em 25/08/2018 às 22h53min.

COSTA, Fernando José da. **Locus delicti nos crimes informáticos**. 2011. Tese (Doutorado em Direito Penal) - Faculdade de Direito, Universidade de São Paulo, São Paulo, 2011. Disponível em: < https://bit.ly/2A83hXr > Acesso em: 11/03/2018 às 20h59min.

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

EUROPE, **Council of. Chart of signatures and ratifications of Treaty 185,** Council of Europe, 2018. Disponível em: <https://bit.ly/2NYqlKp> Acesso em 13/10/2018 às 11h38min.

FONSECA FILHO, Cléuzio. **História da computação: O Caminho do Pensamento e da Tecnologia**, 1. ed, Porto Alegre: EDIPUCRS, 2007.

FORTES, Carlos José e Silva**. Lei 11.829 de 25 de outubro de 2018 – "Lei da Pornografia Infantil",** Todos Contra a Pedofilia, 2011. Disponível em: <https://bit.ly/2RKLUTf> Acesso em 28/08/2018 às 19h42min.

G1, Globo. **Ataque hacker foi o maior já sofrido por sites do governo na internet**, São Paulo: G1. Globo, 2011. Disponível em: <http://glo.bo/joEpHt> Acesso em 25/08/2018 às 17h41min.

G1, Globo. **Carolina Dieckmann fala pela 1ª vez sobre fotos e diz que espera 'justiça'**, São Paulo: G1. Globo, 2012. Disponível em: <http://glo.bo/KXcf5Z> Acesso em 25/08/2018 às 16h51min.

GARCIÁ, Miquel Barceló. **Una história de la informática**, 1.ed. Barcelona: Editorial UOC, 2008.

GIL, Gilberto. **Pela Internet,** álbum: Quanta Gente Veio Ver, 1998. Disponível em: <https://bit.ly/2RluFGZ> Acesso em 21/10/2018, às 15h16min.

IBGE, Instituto Brasileiro de Geografia e Estatísticas. PNAD – **Pesquisa Nacional por Amostra de Domicílios Contínua - Acesso à Internet e à Televisão e posse de telefone móvel celular para uso pessoal,** 2016. Disponível em: < https://bit.ly/2QOxb8x> Acesso em 22/08/2018 às 14h02min.

JESUS, Damasio de. **Manual de crimes informáticos**, 1. ed. São Paulo: Saraiva, 2016. (Recurso Eletrônico – "Minha Biblioteca").

KASPAROV, Garry. **O poder da tecnologia para o bem ou para o mal depende de quem a controla.** Avast Blog, 2016. Disponível em: < https://bit.ly/2EhEXGD> Acesso em 06/08/2018 às 19h42min.

KESSLER, Glenn. **Trump's 'spygate' claim is latest off-target salvo at Russia probe**, Chiacago: Chicago Tribune, 2018. Disponível em: <https://trib.in/2J2NrTU> Acesso em 25/09/2018 às 16h58min.

KOHN, Karen; MORAES, Cláudia Herte de. **O impacto das novas tecnologias na sociedade: conceitos e características da Sociedade da Informação e da Sociedade Digital,** artigo científico, Santos: Intercom – Sociedade Brasileira de Estudos Interdisciplinares da Comunicação, XXX Congresso Brasileiro de Ciências da Comunicação. Disponível em: < https://bit.ly/2Kxm4SF> Acesso em: 08/03/2018 às 20h02min.

KUMMER, Fabiano Ratton. **Direito Penal na Sociedade da Informação**. 1.ed. Paraná: Publicação Independente, 2017. (Recurso Eletrônico – “Edição do Kindle”).

LIMA, Djalba. **Comoções sociais influenciaram punição de crimes hediondos,** Agência Senado, 2010. Disponível em: <**https://bit.ly/2vWdpT1> Acesso em 12/09/2018 às 13h02min.**

LIMA, Mariana. **Brasil já tem mais de um smartphone ativo por habitante, diz estudo da FGV,** São Paulo: O Estado de São Paulo, 2018. Disponível em: < https://bit.ly/2JZALdf> Acesso em 30/07/2018 às 22h12min

LIMA, Renato Brasileiro de. **Manual de processo penal:** volume único. 5.ed. rev., ampl. e atual. Salvador: Ed. JusPodivm, 2017.

LUCA, Cristina. **Brasil sofreu 264,9 mil ataques DDoS em 2017, 34% gerados no próprio país,** NIC.BR, 2018. Disponível em: <https://bit.ly/2yfA2Ay> Acesso em 17/09/2018 às 14h29min.

MARCÃO, Renato. **Curso de processo penal,** 3.ed. São Paulo: Saraiva, 2017. (Recurso Eletrônico – “Minha Biblioteca”).

MARÇULA, Marcelo. **Informática**: Conceitos e Aplicações **/** Marcelo Marçula, Pio Armando Benini Filho. 4. ed. São Paulo: Érica, 2013.

MOSSIN, Heráclito Antônio. **Compêndio de Processo Penal:** Curso Completo. Barueri: Manole, 2010. (Recurso Eletrônico – “Minha Biblioteca”).

MOUGENOT, Edilson. **Curso de Processo Penal,** 12. ed. São Paulo: Saraiva, 2017. (Recurso Eletrônico – “Minha Biblioteca”).

MPF. Ministério Público Federal. Câmara de Coordenação e Revisão, 2. Roteiro de atuação**: crimes cibernéticos,** 2. ed. Ver, Brasília: MPF/2ªCCR, 2013. Disponível em: <https://bit.ly/2IV5Xu2> Acesso em 28/08/2018 às 18h12min.

NOTÍCIA. Expresso da. **Justiça do Trabalho não tem competência para julgar ações penais,** JusBrasil, 2006. Disponível em: <https://bit.ly/2CHoqKC> Acesso em 26/08/2018 às 21h48min.

OPPERMANN, Daniel. **Governança multisetorial e o processo de governança da internet: um estudo de caso sobre crime cibernético e filtragem na internet entre 1990 e 2010**. 2012. 264 f., il. Tese (Doutorado em Relações Internacionais), Brasília: Universidade de Brasília, 2012. Disponível em: <http://repositorio.unb.br/handle/10482/11696> Acesso em: 08/04/2018 às 18h42min.

PAESANI, Liliana Minardi. **Direito e Internet**: liberdade de informação, privacidade e responsabilidade civil / Liliana Minardi Paesani. 7. ed. São Paulo: Atlas, 2014.

PALFREY, John**. Nascidos na era digital**: entendendo a primeira geração de nativos digitais / John Palfrey, Urs Gasser; tradução: Magda França Lopes; revisão técnica: Paulo Gileno Cysneiros: Dados eletrônicos. Porto Alegre: Artmed, 2011.

PINHEIRO, Patricia Peck. **Direito Digital**, 6.ed. São Paulo: Saraiva, 2016.

PRIETO, Xavier Molero. **Un viaje a la história de la informática,** 1.ed. Valência: Editorial Universitat Politècnica de València, 2016.

REALE, MIGUEL. **Filosofia do Direito,** 20ª ed. São Paulo: Saraiva, 2002. (Recurso Eletrônico - Minha Biblioteca).

SAFERNET. **Indicadores Safernet, 2017**, Disponível em: <https://bit.ly/1q6AeeW> Acesso em: 29/09/2018 às 19h09min.

SEBRAE. **Meios de Pagamento Digitais**, Brasília, 2012. Disponível em: < https://bit.ly/2z0gq0W > Acesso em 15/09/2018.

SILVA, Patrícia Santos da. **Direito e crime cibernético:** análise da competência em razão do lugar no julgamento de ações penais [recurso eletrônico] / Patrícia Santos da Silva, Matheus Passos Silva (coord.). Brasília: Vestnik, 2015. Disponível em: <https://bit.ly/2CcoQHD> Acesso em: 25/08/2018 às 18h22min

STF. Supremo Tribunal Federal. **RE 628624, Relator(a):** Min. MARCO AURÉLIO, Relator(a) p/ Acórdão: Min. EDSON FACHIN, Tribunal Pleno, julgado em 29/10/2015, ACÓRDÃO ELETRÔNICO REPERCUSSÃO GERAL - MÉRITO DJe-062 DIVULG 05-04-2016 PUBLIC 06-04-2016, Brasília: STF, 2015. Disponível em: <https://bit.ly/2RL8uLo> Acesso em: 15/09/2018 às 14h25min.

STJ, Superior Tribunal de Justiça. **CC 29.886/SP, Rel. Ministra MARIA THEREZA DE ASSIS MOURA, TERCEIRA SEÇÃO, julgado em 12/12/2007, DJ 01/02/2008, p. 427,** Brasília, 2007. Disponível em: <https://bit.ly/2ygZJRc> Acesso em 12/10/2018 às 12h10min

_____, Superior Tribunal de Justiça. **CC 136.700/SP, Rel. Ministro ROGERIO SCHIETTI CRUZ, TERCEIRA SEÇÃO, julgado em 23/09/2015**, DJe 01/10/2015, Brasília: STJ, 2015. Disponível em: <https://bit.ly/2RO8w5w> Acesso em 12/10/2018 às 17h59min.

_____, Superior Tribunal de Justiça. **CC 156.284/PR, Rel. Ministro RIBEIRO DANTAS, TERCEIRA SEÇÃO, julgado em 28/02/2018 DJe**, Brasília: STJ, 2018. Disponível em: <https://bit.ly/2pPZeZF> Acesso em 12/10/2018 às 14h27min.

_____, Superior Tribunal de Justiça. **CC: 145516 ES 2016/0050531-4, Relator: Ministro JOEL ILAN PACIORNIK, Data de Publicação: DJ 28/04/2017**, Brasília: STJ, 2017. Disponível em: <https://bit.ly/2RMYNMv> Acesso em 12/10/2018 às 9h06min.

_____, Superior Tribunal de Justiça. **CC: 160053 SP 2018/0194677-4, Relator: Ministro REYNALDO SOARES DA FONSECA, Data de Julgamento: 22/08/2018, S3 - TERCEIRA SEÇÃO, Data de Publicação: DJe 27/08/2018**, Brasília: STJ, 2018. Disponível em: < https://bit.ly/2NH2O25 > Acesso em 13/10/2018 às 10h15min.

_____, Superior Tribunal de Justiça. **Enunciado de Súmula nº 53,** Brasília: STJ, 1992. Disponível em: <https://bit.ly/2Ejr62E> Acesso em 21/09/2018 às 19h39min.

_____, Superior Tribunal de Justiça. **Informativo nº 326, Terceira Seção – COMPETÊNCIA. FRAUDE ELETRÕNICA. INTERNET. CONTA-CORRENTE. BANCO,** Brasília: STJ, 2017. Disponível em: <https://bit.ly/2J4P7Jw> Acesso em 09/10/2018 às 15h27min

_____, Superior Tribunal de Justiça. **RHC 19846 / GO RECURSO ORDINARIO EM HABEAS CORPUS 2006/0153072-3**, Brasília: STJ, 2006. Disponível em: < https://bit.ly/2P3e9hH> Acesso em: 13/10/2018.

SYDOW, Spencer Toth. Col. Saberes monográficos - **Crimes informáticos e suas vítimas,** 2. ed. São Paulo: Saraiva, 2015. [Recurso Eletrônico – “Minha Biblioteca”].

VIANNA, Túlio; MACHADO, Felipe. **Crimes informáticos**. Belo Horizonte: Fórum, 2013.