PUC

DEPARTAMENTO DE DIREITO

O DIREITO PENAL COMO INSTRUMENTO REGULADOR DAS ATIVIDADES HUMANAS NA INTERNET POR MEIO DA TIPIFICAÇÃO DOS CRIMES NO AMBIENTE VIRTUAL

Por

FELIPE PINHEIRO BORBA

ORIENTADOR: PROFESSOR SÉRGIO CHASTINET DUARTE

2022.2

PONTIFÍCIA UNIVERSIDADE CATÓLICA DO RIO DE JANEIRO

RUA MARQUÊS DE SÃO VICENTE, 225 - CEP 22451-900

RIO DE JANEIRO - BRASIL

O DIREITO PENAL COMO INSTRUMENTO REGULADOR DAS ATIVIDADES HUMANAS NA INTERNET POR MEIO DA TIPIFICAÇÃO DOS CRIMES NO AMBIENTE VIRTUAL

por

FELIPE PINHEIRO BORBA

Monografia apresentada ao Departamento de Direito da Pontifícia Universidade Católica do Rio de Janeiro (PUC-Rio) como requisito parcial para a obtenção do Título de Bacharel em Direito.

Orientador: Prof.Sérgio Chastinet Duarte

2022.2

AGRADECIMENTOS

À minha família, que cuja educação formou minha pessoa e meu caráter, prestando sempre todo o apoio emocional e amor nos momentos de festa ou de dor.

À meus professores, sem os quais minha formação acadêmica e profissional ao longo da minha vida não poderia ser concluída e cujos conhecimentos jurídicos e de vida são inestimáveis.

Aos meus amigos, cuja alegria e bons momentos propiciados sempre me fizeram acreditar no futuro e seguir enfrentando as adversidades.

RESUMO

BORBA, Felipe. *O direito penal como instrumento regulador das atividades humanas na internet por meio da tipificação dos crimes no ambiente virtual*. Rio de Janeiro, 2022. 101 p. Monografia de final de curso. Departamento de Direito da Pontifícia Universidade Católica do Rio de Janeiro – PUC-Rio.

Quando tratamos do termo "mundo globalizado", "interconectividade mundial" ou "a realidade conforme o século XXI", estamos referenciando uma mudança de paradigma dos tempos atuais em relação ao que se tinha anteriormente, esta mudança de paradigma[1], que permeia e se irradia em todos os aspectos da vida cotidiana, desde as relações mais interpessoais privadas no bojo da esfera da intimidade individual, até as relações intergovernamentais em escala global e mesmo além dela. Mas qual seria a "locomotiva" que impulsionou esta nova era das relações humanas? Quais as consequências advindas do referido vetor responsável pela mudança de paradigma? Por fim, como o Direito, como instrumento de controle social, político e econômico, em especial a esfera penal, controla e regula as relações e atividades intrinsecamente humanas que ocorrem dentro deste verdadeiro "universo paralelo"[2]? Estas são as perguntas norteadoras no qual tentaremos nos debruçar ao longo deste trabalho.

Palavras-Chave: Direito Penal; Processo Penal; Internet, tecnologias da informação, crimes virtuais, regulamentação.

[1] RODELLA, Abdo Cibele. Internet: um novo paradigma de informação. *Revistas.Usp.Br*., no. 1, v. 10, p. 41-48, 2005.

[2] SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; Cauê S. AMENI. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. *Scielo*. Disponível em: https://www.scielo.br/j/hcsm/a/TrcdX6SmXCcNqBLCcR7rb7J/abstract/?lang=pt. Acesso em: 17 ago. 2022.

SUMÁRIO

LISTA DE ABREVIAÇÕES

L. n – Lei número

CP – Código Penal

CPP – Código de Processo Penal

CRFB 88 – Constituição da República Federativa do Brasil de 1988

Art. – Artigo

PF – Polícia Federal

PC – Polícia Civil

ECA – Estatuto da criança e do adolescente

INTRODUÇÃO - TECNOLOGIA E A FENOMENOLOGIA DOS "CRIMES VIRTUAIS"

1.1 O fenômeno da internet

Por óbvio, imaginamos que ao menos a primeira das perguntas já tenham sido respondidas mentalmente por qualquer indivíduo que encontre-se atualmente vinculado a alguma atividade humana, eis que impossível se alijar totalmente do mundo social à ponto de evitar o contato com o vetor que levou a referida mudança de paradigma nas nossas relações, a internet como conhecemos hoje, permeia e percola todas as áreas de atuação do homem, é por meio deste instrumento que os cidadãos de todas as nações do globo põem em prática sua cidadania por meio do exercício de direitos e execução de deveres (em nosso país por exemplo, quase todas as atividades em âmbito administrativo ou jurídico necessariamente adentram à esfera do mundo virtual)[3], da mesma forma, as relações interpessoais e atos de natureza fundamentalmente privada também encontram-se completamente englobados dentro da interconectividade da "teia digital". Um exemplo clássico que pode ser citado é o de locação\alienação de bens imóveis, ato absolutamente solene e incrivelmente burocrático, mas que até mesmo isto atualmente se executa, em sua imensa maioria, no bojo digital dos aplicativos especializados, intermediando as ações que anteriormente dependiam de dispendiosos e complexos procedimentos administrativos e cartorários[4].

Porém importa ressaltar que nem tudo que adveio da internet é positivo, o vetor de mudança de paradigma alterou drasticamente as relações

---

[3] EVARISTO, Silvana Aparecida Cardoso; CESAR, Claudio Evaristo. Direito x internet. *Âmbito Juridico*. Disponível em: https://ambitojuridico.com.br/edicoes/revista-127/direito-x-internet/#:~:text=Desse%20modo%2C%20celeridade%20da%20internet,em%20vista%20justamente%20a%20celeridade. Acesso em: 17 ago. 2022.

[4] SISTEMA unificará vendas online de imóveis da união estados e municípios. *Governo Federal*. Disponível em: https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/04/sistema-unificara-vendas-on-line-de-imoveis-da-uniao-estados-e-municipios. Acesso em: 19 ago. 2022.

inter-humanas tanto para a prática de ato louváveis como os mencionados elementos desburocratizantes e facilitadores do cotidiano, como para a prática de atos ilícitos e reprováveis, eis que durante muito tempo, o mundo virtual encontrava-se "à margem" dos interesses e ações dos Estados nacionais, sendo este espaço tratado como mera área de atuação de profissionais especializados ou entusiastas da vanguarda tecnológica. Como consequência do vácuo gerado por legislações específicas que buscassem regular as relações e negócios virtuais, a internet logo obteve fama de ser a "última grande fronteira"[5] (aqui uma alusão a marcha para o oeste americano, onde em razão das grandes distancias entre os esparsos centros urbanos, a ausência de autoridade estatal gerou uma vida anárquica onde a "lei do revólver era a lei da terra").

De fato, nos anos iniciais da internet, com a mencionada desregulamentação e ausência de presença estatal, esta se tornou um solo fértil para todo tipo de atividades ilícitas e fenômenos repulsivos, a citar alguns: Divulgação de grupos de extermínio e assassinos de aluguel, grupos de *chats* que promoviam violência e tortura, sites de vendas de órgãos, tráfico de humanos, tráfico de entorpecentes de toda natureza e tipo, grupos e ceitas religiosas de altíssima periculosidade etc[6]. Abordaremos mais à frente, em uma análise mais profunda, alguns destes vários crimes e casos famosos.

1.2 O início da regularização e busca pelo controle, embates morais e ideológicos entre realistas e liberais

Com a maior penetração da internet nas vidas dos indivíduos e ficando os entes estatais impossibilitados de continuar ignorando o fenômeno que surgia e vinha alterando consigo todos os paradigmas das áreas por qual

[5] INTERNETS wild West days are coming close. *The Atlantic*. Disponível em: https://www.theatlantic.com/sponsored/pwc-2019/internets-wild-west-days-are-coming-close/3064/. Acesso em: 25 ago. 2022.

[6] A DEEP WEB e a relação com a criminalidade na internet. *Revista Eletrônica Direito & TI*. Disponível em: http://direitoeti.com.br/artigos/a-deep-web-e-a-relacao-com-a-criminalidade-na-internet/. Acesso em: 19 ago. 2022.

passava, ficou abundantemente claro que havia uma necessidade premente de atuação das forças do Estado dentro do mundo digital, não poderia mais haver desculpas para permitir que atos absolutamente ilícitos pudessem ser livremente praticados no ambiente virtual e que seus agentes saíssem impunes sob a justificativa de que "não há lei que regule o que ocorre por detrás das telas dos computadores"[7].

De fato, merece menção o fato de que de início, os órgãos governamentais não dispunham de qualquer meio realmente eficiente para repressão dos ilícitos que ocorriam neste "universo" completamente distinto do mundo físico, até mesmo em relação aos legisladores, agentes da lei e membros do judiciário, havia grande desconhecimento e completa desconexão com a realidade fática que ocorria nos meandros digitais.

Para piorar a situação, as forças de repressão serviam de escarnio dos agentes criminosos, que se deleitavam com o que consideravam tentativa risíveis e patéticas dos órgãos estatais para reprimir suas atividades, eis que estes como mencionado anteriormente, para além de não disporem dos meios necessários ou efetivos para o combate dos ilícitos virtuais, apresentavam completo desconhecimento de como funcionava e operavam este submundo do crime, seus sites, *links, VPN´s*, normas e mecanismos de acesso anônimos etc.[8]... Por exemplo, uma operação da polícia federal brasileira para localizar e prender um determinado traficante de órgãos poderia resultar em completo fracasso uma vez que ao detectar a intrusão de membros não cadastrados com uma chave de acesso específica para seu site, o traficante poderia com o "clicar de um botão" transferir seu servidor para a República de Burkina Faso, o que dificultaria significativamente o trabalho dos agentes.

---

[7] FERNANDES, Lauren. Exposição nas redes sociais sem autorização. *Jus Brasil*. Disponível em: https://laurenfernandes.jusbrasil.com.br/artigos/686195090/exposicao-nas-redes-sociais-sem-autorizacao. Acesso em: 20 ago. 2022.

[8] STAMILE, Natalina. *Revista Brasileira de Direito*, v. 18, n. 3, RBD. set./dez. 2022. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/2183/1839. Acesso em: 7 ago. 2022.

Sobre esse tema, surgem primordialmente dois tipos de posicionamentos dos especialistas e juristas, cujo Professor Saskia Sassen convencionou chamar de “liberais” e “realistas”[9]. De maneira breve, os liberais defendem a tese de que somente os mecanismos de auto-regulamentação da rede seriam tanto eficazes como legítimos, eis que os usuários dos sistemas, ao ingressar nas “comunidades virtuais” estariam tacitamente concordando em seguir as normas e regras regulatórias auto estipuladas para aquela comunidade\serviço, além disto, pela própria natureza descentralizada da rede aliado a notória flexibilização da *web* (universal e de acesso irrestrito) que notoriamente não respeita fronteiras nacionais, se impossibilitaria uma conexão direta com os Estados e seus burocratas, e que portanto, a própria internet já possuiria os meios para se auto regular, ficando eternamente livre das intervenções estatais e de suas regulamentações antiquadas que somente serviriam de amarras ao pleno desenvolvimento do mundo virtual. Este posicionamento ganhou grande relevância a partir da “declaração de independência do ciberespaço”, apresentada durante o fórum econômico de Davos em 1996 por John Perry Barlow que a época era o diretor da *Electronic Frontier Foundation*[10].

Já os pensadores realistas, afirmam que não existe de fato uma natureza inerente e imutável da rede, podendo esta ser alterada ou adaptada de maneira a atender as demandas e as necessidades de grupos e setores específicos conforme assim se faça necessário. Ou seja, a regulamentação estatal da web seria a maneira legitima e eficaz a ser introduzida, uma vez que esta levaria em conta aspectos e especificidades culturais, econômicas, religiosas e até mesmo geográficas. Em seu livro “*who controls de internet*”, Jack Smith e Tim Wu irão apresentar justamente o principal ponto trazido no cerne do argumento realista, quais seja: “uma internet delimitada por

[9] SASSEN, Saskia. *The impact of the internet on sovereignty*: unfounded and real worries. 2000. p. 196.
[10] BARLOW, John Perry. Declaração de Independência do Ciberespaço. *Portal DH Net*. Disponível em: http://www.dhnet.org.br/ciber/textos/barlow.htm. Acesso em: 7 ago. 2022.

fronteiras é valiosa, precisamente, porque permite que pessoas vinculadas a diferentes sistemas de valores convivam no mesmo planeta”[11].

Neste ponto, a questão torna-se iminentemente interpretativa e política, eis que os pensadores liberais têm claramente como princípio norteador as liberdades individuais e a defesa pelos direitos de auto regularização, o que é veementemente criticado pelos pensadores realistas que acreditam que o Ente estatal tem plena responsabilidade e obrigação para regular e manter uma estrutura organizada e pacífica onde se respeitem as regras e valores culturais inerentes a cada país, bem como o controle das atividades que por ventura possam decorrer para a prática de atos ilícitos.

Fato é que, em que pese a discussão doutrinário-político-jurídica, as coisas não podiam continuar como estavam, a pressão da sociedade pelo combate aos crimes virtuais, que cada dia ganhavam mais notoriedade, vinha crescendo, e os Estados se viam em uma situação de extrema vulnerabilidade em que ou se admitia a incapacidade dos órgãos públicos de atuarem na esfera digital e com isso cementar a ideia de que “na internet tudo pode” (eis que ineficazes os métodos de auto regulamentação), ou consideráveis alterações do *modus operandi* deveriam ocorrer, tanto no âmbito legislativo com a adoção e criação de instrumentos legais que permitissem as forças policiais uma atuação eficaz, delimitando o proceder e a competência de cada órgão, como no âmbito administrativo e judiciário, por meio de treinamento dos agentes da lei e fornecimento de mecanismos e meios para que estes pudessem efetivamente fazer valer de seu poder legal para combate aos crimes virtuais.

Como consequência, a própria realidade fática acabou por impor o modelo realista de controle digital, fator que pode ser visto até os dias de hoje, muito embora a discussão se mantenha em âmbito acadêmico\filosófico, e haja aqueles que defendam uma “infusão” de ambos

[11] GOLDSMITH, Jackson; WU, Tim. *Who controls the Internet?* Ilusions of a boderless world. Oxford: Oxford University Press, 2008. p. 151.

os modelos de modo a fornecer maior liberdade aos usuários, porém permitindo que os Estados possam fazer valer de suas leis, na defesa das expressões morais e culturais de cada país.

1.3 Conceito de “crime virtual” e a falta de consenso para nomenclatura na doutrina moderna

A busca por uma definição mais precisa no que diz respeito ao conceito de “crime virtual” é algo que elude a doutrina e a jurisprudência, isto pois, pela própria natureza destes tipos de fatos típicos, bem como o ambiente no qual estes são perpetrados acaba-se exigindo tanto do legislador como do operador do Direito, determinados conhecimentos de natureza altamente técnica e não trivial, que leva por dificultar a compreensão destes, e consequentemente, uma construção de uma dogmática e classificação específica.

Importa recordar que este tipo de situação não se limita apenas aos operadores do direito e acadêmicos da área, se estendendo para os demais ramos do conhecimento humano, eis que é da natureza humana não apresentar interesse em se aventurar em temas de outras áreas do saber, preferindo o conforto daquilo que já dominam. Infelizmente, isto gera grandes dificuldades ao mundo jurídico em específico, que somado a árdua missão de regular e legislar sobre todas as áreas de atividade de uma sociedade (permeando desde uma mera relação de compra e venda mercantil a regulação de instalação de centrais nucleares e atividades espaciais), sofre com a incapacidade do legislador e dos juristas em compreender de maneira mais profunda questões de natureza estritamente técnicas, inerentes a muitas destas atividades, aliado a demasiada burocracia e cerimonialistica jurídica, que resultam em um Direito engessado, desatualizado e incapaz de regular de forma concreta a área que buscou-se legislar.

1.4 Classificação dos “crimes virtuais”

Neste diapasão, a atuação de doutrinadores e juristas na área do direito da informática não poderia ser diferente, a própria nomenclatura e classificação destes tipos de ilícitos não é fixa, sendo utilizadas diversas terminologias.

Thalyta França Evangelista irá citar uma série de nomes utilizados pela doutrina e jurisprudência, tais como: “Crimes cibernéticos, crimes de informática, crimes tecnológicos, crimes cometidos por meio eletrônico, crimes cometidos por meios digitais, entre outros”. Citando o doutrinador Mendes Vieira, a autora irá definir este tipo de ilícito como:

> Aquele executado contra sistema de informática ou por meio deste, alcançando os crimes realizados contra o computador e suas ferramentas e os praticados mediante o computador. Encontra-se nesta definição os crimes executados por intermédio da internet, pois o propósito para conectar-se à rede é a serventia de um computador.

A autora irá então defender a seguinte classificação para os referidos crimes:

> A) ‘Crimes virtuais próprios’, que seriam aqueles cuja realização exige a utilização de dispositivo informático para sua execução e cujo bem jurídico tutelado é a informática, dando a autora como exemplo a invasão de e-mails e a infiltração de vírus em sistemas digitais.
> B) ‘Crimes virtuais impróprios’, que seriam aqueles que já possuem tipificação clássica e sendo bem conhecidos pelo nosso sistema jurídico criminal, eis que tais crimes podem ou não ser realizados por intermédio de um sistema informático, mas não ficando necessariamente vinculados a este meio[12].

A mesma forma de classificação é adotada por Matheus de Araújo Alves quando da classificação destes ilícitos[13].

Wendt e Nogueira trazem uma catalogação mais específica, onde apontam que as “condutas indevidas praticadas por meio de dispositivo de

---

[12] FRANÇA EVANGELISTA, Thalyta. *Crimes virtuais e o ordenamento jurídico brasileiro*. João Pessoa: Arte e diagramação, 2020. p. 17-19.

[13] DE ARAUJO ÁLVES, Matheus. *Crimes digitais, análise da criminalidade digital sob a perspectiva do Direito processual penal e do instituto da prova*. Belo Horizonte: Ed. Dialética, 2020. p. 37-61.

informática" se dividem em 2 grandes grupos que por sua vez irão se dividir em subgrupos, sendo estes:

> A) 'Crimes cibernéticos', que se subdividem em 'crimes cibernéticos abertos' (condutas típicas que podem ser realizadas de forma tradicional ou por intermédio de dispositivos de informática) e 'crimes cibernéticos fechados ou exclusivamente cibernéticos' (condutas típicas que necessariamente devem ser realizadas por intermédio de dispositivos de informática).
> B) 'Ações prejudiciais atípicas', que segundo os autores, tratariam de 'condutas que causam transtornos e\ou prejuízos e são praticadas por intermédio de dispositivos informáticos', mas que, em razão de ausência de tipificação\ regulação normativa (em partes em virtude das deficiências da ciência jurídica pelas razões anteriormente citadas), tais condutas seriam atípicas eis que não tipificadas (importa sempre recordar que a legislação pátria estipula, tanto em sede constitucional por meio do Art.5, XXXIX e XL da CRFB 88, como em sede infraconstitucional no Art. 1 do CP que 'não há crime sem lei anterior que o defina. Não há pena sem prévia cominação legal'). Isto não importa dizer que tais atos, certamente geradores de transtornos para a vítima, não possam ser levados a análise de responsabilização na esfera cível\administrativa, na busca por reparações a eventuais danos morais\materiais que o alvo destas 'ações prejudiciais' venha a sofrer[14].

Em que pese a distinção de classificação dada pelos autores, podemos perceber que na prática, os crimes virtuais propriamente ditos (atos típicos, ilícitos e culpáveis) podem ser divididos em 2 grandes grupos, que são direta ou indiretamente apresentados nas classificações destes autores:

> A) Aqueles que necessitam obrigatoriamente de meio informático para serem executados de maneira efetiva (preparo, prática e consumação no domínio informático ou a este vinculado). Podemos dar como exemplo o moderno crime previsto no Art. 154-A do CP, quais sejam, invasão de dispositivo informático, ou o crime previsto no Art. 244-B, Parágrafo primeiro do ECA (Lei n8.069\1990) que tipifica a conduta de 'aliciamento de crianças praticado por intermédio de salas\chats de bate papo na internet.
> B) Aqueles que já apresentam tipificação clássica, cujos bens jurídicos tutelados já estejam consolidados na doutrina\jurisprudência e que a utilização de meio\dispositivo informático é tão somente um instrumento disponível para o seu preparo, prática e execução, podendo vir a ser utilizado ou não, a depender das preferências e habilidades do criminoso ou grupo de criminosos que realizam o ato típico. Podemos dar como exemplo, diversos tipos de atos típicos como o estelionato, os crimes contra a honra, a pornografia, ameaça etc.

Ainda podemos entender que certos atos e condutas, em que pese reprováveis no âmbito ético\moral, não apresentam previsão legal como fatos

[14] WENDT, Emerson; NOGUEIRA JORGE, Higor. *Crimes cibernéticos, ameaças e procedimentos de investigação*. 3. ed. Rio de Janeiro: Brasport, 2021. p. 14-16.

típicos, e assim sendo, pelo consagrado princípio da legalidade e da *última ratio* (que limitam a atuação do direito penal como forma de coibir abusos a liberdade e a vida dos cidadãos), não podem ser matéria de atuação e incidência da esfera penal, ficando adstritos a uma "zona cinzenta" de repressão estatal, onde a vítima a depender do dano poderá acionar uma justa reparação em sede de juízo cível\administrativo\trabalhista, etc... porém, sem legitimidade para que o Estado inicie a persecução penal do autor. Para estas condutas, adotaremos neste trabalho o nome dado pelos doutrinadores Wendt e Nogueira e as chamaremos de "condutas prejudiciais atípicas".

Assim, sendo, entendo que apesar da dificuldade gerada pela indefinição da doutrina\jurisprudência em relação as definições e conceitos do que seriam, afinal, "crimes virtuais", evidenciado pelos mais diversos nomes trazidos a estas condutas ilícitas, podemos achar um consenso médio de que estas condutas geram enormes prejuízos para a sociedade, afetando diretamente a fábrica do tecido social, a economia, a segurança nacional e a estabilidade de nações a depender do grau de violação empregados e danos resultantes. Dessa forma, é igualmente um consenso entre os doutrinadores que os Estados busquem coibir e combater tais ilícitos.

Também podemos extrair uma clara divisão dogmática destes tipos de condutas, eis que, novamente em que pese as múltiplas classificações em sede doutrinária, percebe-se que os ilícitos tidos como "crimes virtuais" podem ser divididos em dois grandes grupos, os crimes que somente podem ser realizados por intermédio de meio eletrônico\informático e aqueles cuja realização, encontra nestes dispositivos, a faculdade de utilização para executar a empreitada criminosa e alcançar o resultado esperado. Existem ainda, ações prejudiciais atípicas, que apesar de serem reprováveis e por vezes repugnantes, não podem ser objetos de persecução penal por parte do Estado juiz, eis que não apresentam tipificação como crime, quer seja no código penal ou na legislação penal extravagante, ficando a vítima restrita a buscar indenizações\reparações morais e\ou materiais em outras esferas de atuação jurisdicional.

1.5 Bens jurídicos que se buscam proteger em decorrência dos atos ilícitos deste tipo de crime

Como nos explica Allegro:

> (...) o ser humano, quando exposto à vida em sociedade, tende a valorizar determinados elementos que geram interesses e disputas por parte de outros indivíduos). Neste sentido, quando um objeto ou coisa (tangível oi intangível) adquire algum valor e este passa a ser considerável a alguém ou a um grupo de indivíduos, surge então o interesse social pela sua proteção (tutela), que na ciência jurídica se dá por meio da normatização. Protegido pela legalidade, esse bem passa a apresentar-se como um bem jurídico, e sendo protegido pelo legislador penal a doutrina considera-o como bem jurídico penalmente tutelado[15].

Neste diapasão, não é difícil imaginar que a criação conceitual\ doutrinária de bem jurídico na ciência do Direito, advém da tentativa de combater a ameaça da criminalidade, evitando que condutas tidas como imorais ou indesejáveis\danosas para o bom convívio social, pudessem macular e afetar referidos bens, que apresentam forte significância para a estabilidade e funcionamento do tecido social no qual se encaixam.

Assim, cabe verificar as evoluções pelas quais uma sociedade passa, de maneira que se verifique a ocorrência ou não de novos riscos a bens jurídicos tutelados[16]. Conforme veremos a seguir, a informática e a criação da chamada "sociedade de risco"[17], ocasionaram novas formas de violação de bens jurídicos por meio dos crimes virtuais, mas o que se percebe com maior relevância, é o surgimento de novos bens que irão merecer especial atenção e tutela jurídico-penal por parte do Estado.

Marcelo Crespo irá dizer que:

Quando se trata de crimes digitais, as condutas delitivas atingem não só aqueles valores tradicionalmente protegidos, como a vida, a integridade

---

[15] ALLEGRO, Romana Affonso de Almeida. Bens jurídicos: o interesse estatal de tutelar bens jurídicos através de sua normatização. 2005. *Direito Net*. Disponível em: https://www.direitonet.com.br/artigos/exibir/2089/Bens-juridicos. Acesso em: 18 ago. 2022.

[16] ZÍLIO, Jackson. *Discursos sediciosos n 19, Da ilegalidade de bens à ilegalidade de direitos sobre a resistência ao movimento de expansão e modernização do Direito Penal*. Rio de Janeiro: Instituto carioca de criminologia, 2014. p. 82.

[17] DOS SANTOS, Juarez Cirino. *Direito Penal, parte geral*. ampl. e atual. Paraná: Editora Tirant lo blanch Brasil, 2014.

física, o patrimônio e a fé pública, mas também, as informações armazenadas (dados) e a segurança dos sistemas de redes informáticas ou de comunicação[18].

O que se passou a perceber, com o desenvolvimento das tecnologias e meios informacionais, é que a informação (dados computacionais) ganhou forte destaque frente a sociedade, onde passou a atuar como espécie de "mercadoria", com isto, segundo Matheus de Araújo Alves, este seria, de fato, "o principal bem jurídico a ser tutelado nos crimes digitais" e "além das informações e dos dados, a confiabilidade e a segurança dos sistemas e redes informáticas e de comunicação também carecem de tutela por parte do Direito Penal". Porém, conforme nos alerta o autor, "não quer dizer que a objetividade jurídica historicamente protegida deva ser deixada de lado"[19]. O autor ainda conclui que na prática "é possível haver uma violação conjunta de bens jurídicos tradicionais e outros, peculiares a informática"[20].

O que se conclui disto é que na realidade os crimes virtuais seriam, conforme se convencionou chamar na doutrina, "pluriofensívos", isto pois estariam atingindo sempre dois ou mais bens juridicamente tutelados. "Ao mesmo tempo em que há violação de bens jurídicos tradicionais, há também, a necessidade de proteção de novos interesses provenientes da sociedade de risco"[21].

Ou seja, enquanto o ilícito digital viola o que os autores acima citados entendem como principal bem jurídico a ser tutelado nestas circunstâncias (as informações\ dados\ confiabilidade e segurança dos sistemas e redes informáticas), estariam também, a depender do tipo de ilícito cometido, violando outros bens jurídicos (secundários) tradicionais já previamente

[18] CRESPO, Marcelo Xavier de Freitas. *Crimes digitais*. São Paulo: Saraiva, 2011. p. 56.
[19] ARAUJO ÁLVES, Matheus de. *Crimes digitais, análise da criminalidade digital sob a perspectiva do Direito processual penal e do instituto da prova*. Belo Horizonte: Ed. Dialética, 2020. p. 36.
[20] CRESPO, 2011, p. 57; ARÚS 1997, p. 190 *apud* ARAUJO ALVES, 2020, p. 36.
[21] ARAUJO ALVES, 2020, p. 36.

consolidados em nosso ordenamento, tais como a privacidade, a incolumidade pública, a liberdade sexual, a vida, o patrimônio etc.

1.6 O fenômeno da engenharia social como método primordial da prática de ilícitos digitais e obtenção de resultados

Segundo Wendt e Nogueira, engenharia social é:

> Um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e\ou aplicativo (...) enquanto certas ameaças cibernéticas utilizam vulnerabilidades localizadas em uma rede ou servidor, na engenharia social o criminoso concentra-se nas vulnerabilidades que porventura a vítima possa ter e\ou apresentar frente a determinadas situações do seu cotidiano. Nestas situações o ponto nevrálgico é a falta de conscientização do usuário de computador sobre os perigos de acreditar em todas as informações que chegam até ele[22].

Neste sentido, entendemos que a engenharia social é um dos métodos mais comuns e, porque não dizer, "humanos" do cometimento de crimes cibernéticos, sendo, portanto, de fundamental importância que se compreenda este fenômeno que é acima de tudo, antropológico, para que se possa entender a prática de determinados tipos de crimes virtuais quando formos abordá-los mais à frente.

Podemos entender, portanto, que a engenharia social é método complexo e de múltiplas vertentes por meio dos quais um agente criminoso engana a vítima para que possa obter alguma vantagem desta, que pode ou não ser o objetivo final de seu ato ilícito. Este tipo de ação não apresenta um procedimento definido a ser utilizado, ficando a criatividade do agente e sua capacidade de convencimento e persuasão as únicas forças motrizes por detrás dos atos a serem tomados para alcançar os almejados resultados.

Conforme nos lista os respeitados doutrinadores, as principais técnicas aplicadas pelos "engenheiros sociais" são baseadas na "manipulação de seus alvos". Desta forma, buscam estimular e manipular o medo, a ansiedade, a

[22] WENDT; NOGUEIRA JORGE, 2021, p. 16-17.

comiseração, a simpatia, o humanismo, e a curiosidade. A vítima, usuário do sistema de informática, influenciado e manipulado por estes sentimentos, de maneira premeditada e cuidadosamente planejada pelos "*cyber* criminosos", fornece informações pessoais sensíveis ou clicando em links que os direciona a "sites de conteúdos maliciosos e\ou para a execução de algum código maléfico em sua máquina"[23].

Uma outra estratégia muito conhecida dos criminosos é a utilização do que alguns chamam de "efeito Saliência"[24], por meio do qual os malfeitores se utilizam de assuntos e temas que estejam "em destaques na mídia mundial\nacional\regional", como a morte de um indivíduo famoso, uma catástrofe social de grandes proporções, matérias sobre conflitos geopolíticos de elevado interesse etc.

Por último, é de fundamental importância alertar para outra tática muito utilizada pelos criminosos virtuais e que inclusive são a base de "*phishig scams*" (um tipo de fraude virtual que será posteriormente abordada quando da análise dos tipos mais comuns de crimes virtuais), onde este último, de forma a dar mais credibilidade a sua ação e fortalecer as chances de sucesso da engenharia social, utiliza de imagens de empresas privadas, instituições financeiras, órgãos da administração pública direta e indireta, etc... para passar confiança a vítima e fazer com que esta aja de acordo com os interesses e em benefício do malfeitor[25].

[23] WENDT; NOGUEIRA JORGE, 2021, p. 16-17.
[24] JORGE, Higor Vinicius Nogueira; SANNINI, Francisco. Infiltração virtual de agentes representa avanço nas técnicas de investigação. *JUS*. Disponível em: https://jus.com.br/artigos/57632/infiltracao-virtual-de-agentes-representa-avanco-nas-tecnicas-especiais-de-investigacao. Acesso em: 20 ago. 2022.
[25] WENDT; NOGUEIRA JORGE, *op. cit.*, p. 16-19.

CAPÍTULO 2 - OS CRIMES MAIS COMUNS PRATICADOS NO MUNDO VIRTUAL E O FENÔMENO DA "*DARK WEB*"

2.1 Uma análise fática dos tipos mais comuns de crimes digitais segundo a classificação destes ilícitos.

Conforme sugerem Matheus de Araújo Alves e Thalyta França Evangelista, visto em capítulo anterior e os quais escolhemos utilizar neste trabalho, os crimes virtuais\digitais estariam classificados em dois tipos:

Os crimes digitais próprios onde a criminalidade irá se utilizar de meios exclusivamente informáticos para alcançar um bem jurídico tutelado vinculado a sociedade de risco digital (quais sejam, as informações\ dados\ confiabilidade e segurança dos sistemas e redes informáticas, leia-se a informática em si). E os crimes digitais impróprios, que se trata na realidade daqueles delitos que já encontram tipificação no ordenamento jurídico brasileiro, e que podem vir (ou não) a ser cometidos por intermédio de dispositivo informático, em caso da última hipótese ser positiva, estaríamos então tratando de crime digital impróprio, eis que nas palavras de Roncada:

> Diferentemente dos crimes digitais próprios, nessa modalidade delitiva, a norma penal não exige como condição para sua ocorrência o emprego de dispositivo informático, que surge de forma acidental, apenas como meio de execução do delito[26].

Desta forma passaremos a análise de alguns dos delitos informáticos mais comuns, agrupando-os em seus respectivos grupos classificatórios, de maneira a tornar mais claro a distinção entre os 2 grandes grupos.

---

[26] RONCADA, Rodiner. *A prova da materialidade delitiva nos crimes cibernéticos*. São Paulo: EMAG, 2017. p. 117.

2.2 Os delitos digitais próprios mais comuns

Conforme nos alerta Matheus de Araújo Alves, os crimes digitais próprios seriam aqueles cuja conduta delituosa atinja bens jurídicos específicos do mundo virtual caracterizado pela nossa sociedade de risco digital moderna. Assim, os sistemas informáticos e as informações automatizadas (dados) seriam os alvos a serem violados por estes tipos de ilícitos[27]. Dessa maneira, nessa classificação decaem todos os injustos penais que atinjam os sistemas computacionais em si (hardwares) e\ou os sistemas operacionais\programas (softwares), o que impede ou até mesmo neutraliza qualquer possibilidade de funcionamento.

Conforme indica o autor supramencionado, os crimes virtuais que se encaixam nesta família seriam: A intrusão informática, a inserção de malwares, o *scamming*, o *spamming* e a interceptação ilegal de e-mails[28], os quais passaremos a analisar individualmente.

Importa ainda mencionar, que os referidos tipos penais permitem a tentativa, desde que se segregue o iter criminis, ou seja, cogitação, preparação, execução e consumação[29].

2.2.1 Intrusão informática

Também conhecida como “invasão de dispositivo informático” ou *hacking*, como nos explica Sydow, refere-se ao:

> Acesso alheio, com ou sem objetivo de obter vantagem, seja ou não por meios ardilosos, violentos ou até mesmo por conta de subterfúgio que consiga enganar o

[27] ARAUJO ALVES, 2020, p. 38.
[28] Ibid., p. 38-39.
[29] DESIDERATO, João Gabriel. Prática penal, entenda o que é iter criminis. *Jus Brasil*. Disponível em: https//https://joaogabrieldesiderato.jusbrasil.com.br/artigos/1197475045/pratica-penal-entenda-o-que-e-iter-criminis#:~:text=Essas%20fases%20percorridas%20pelo%20agente,%2C%20prepara%C3%A7%C3%A3o%2C%20execu%C3%A7%C3%A3o%20e%20consuma%C3%A7%C3%A3o. Acesso em: 25 ago. 2022.

> legítimo detentor dos direitos relativos ao sistema, levando-o a permitir o ingresso, sob erro[30].

Encontra tipificação legal em nosso diploma repressivo na forma do seguinte artigo e seus respectivos incisos, adicionados ao ordenamento pátrio por meio da lei 12.737\12 (popularmente conhecida como "lei Carolina Dieckmann") e posteriormente modificada pela lei 14.155\21:

> Art. 154-A. Invadir dispositivo informático de uso alheio, conectado ou não à rede de computadores, com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do usuário do dispositivo ou de instalar vulnerabilidades para obter vantagem ilícita: (Redação dada pela Lei nº 14.155, de 2021)
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> § 1º Na 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. (Incluído pela Lei nº 12.737, de 2012)
> § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. (Redação dada pela Lei nº 14.155, de 2021)
> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido: (Incluído pela Lei nº 12.737, de 2012) Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave. (Incluído pela Lei nº 12.737, de 2012) Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. (Redação dada pela Lei nº 14.155, de 2021)
> § 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. (Incluído pela Lei nº 12.737, de 2012)
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra: (Incluído pela Lei nº 12.737, de 2012)
> I - Presidente da República, governadores e prefeitos; (Incluído pela Lei nº 12.737, de 2012) Vigência
> II - Presidente do Supremo Tribunal Federal; (Incluído pela Lei nº 12.737, de 2012) Vigência
> 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 (Incluído pela Lei nº 12.737, de 2012) Vigência
> IV - Dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal. (Incluído pela Lei nº 12.737, de 2012).

No começo da era informática, se imaginava que este tipo de delito fosse necessariamente praticado por agente com profundo conhecimento técnico na área de tecnologia digital, e que se utilizando destes conhecimentos, atacaria sistemas fechados buscando gerar "aberturas" e

[30] SYDOW, 2015, p. 113 *apud* ARAUJO ALVES, 2020, p. 39.

causando vulnerabilidades nos sistemas defensivos do software\hardware alheio. Ocorre que com o desenvolvimento da informática e da tecnologia da informação, bem como a realização de estudos mais aprofundados na área de tecnologia de segurança digital e técnicas de invasão, chegou-se à conclusão de que na realidade não são necessárias tais características para que se consiga obter acesso a um sistema alheio, eis que estes já seriam "lançados de fábrica" e disponibilizados ao mercado com o que Sydow chama de "falhas lógicas de programação"[31].

Assim, um indivíduo suficientemente habilidoso poderia, por meio de engodo, engano ou outros meios abjetos, induzirem as vítimas a acessarem dispositivos e sistemas (previamente desenvolvidos pelo criminoso) criados especificamente para instalarem\acessarem arquivos e criarem "portas de acesso livre" para o dispositivo da vítima[32].

Desta forma, conforme sugere Matheus de Araújo Alves, mencionando a análise de Sydow, a expressão "invasão de dispositivo informático" não seria a mais adequada, vez que como nos alerta o expert, "dá a entender um ato violento praticado pelo *hacker*, o que não é necessariamente verdade"[33], entretanto, conforme demonstrado anteriormente, é a atual nomenclatura que o Código penal brasileiro adotou em seu respectivo artigo. Segundo o autor, a melhor expressão para este tipo de ilícito seria a "intrusão informática", vez que traduziria de maneira mais eficaz a real natureza do crime, que é a "ação de introduzir, sem direito ou por violência, ou alternativamente, o ingresso ilegal, sem convite ou consentimento viciado"[34].

Matheus de Araújo Alves irá dizer que a intrusão informática violaria a confidencialidade do acesso particular e da segurança do dispositivo informático, gerando como consequência da ação, riscos e incertezas ao

[31] SYDOW, 2015, p. 113 *apud* ARAUJO ALVES, 2020, p. 39.
[32] Ibid., p. 39.
[33] Ibid., p. 40.
[34] Ibid., p. 40.

usuário. Ao mesmo tempo, pode gerar outras externalidades negativas, tais como a modificação de arquivos, cópia de segredos industriais e inserção de códigos maliciosos[35]. Tudo isto gera esforço e necessidade de modificação de políticas de segurança da informação, o que consequentemente, levará a tempo perdido e custos em mão de obra qualificada por parte da vítima, o que segundo Marcelo Xavier Crespo, evidenciaria o tremendo prejuízo que tais ações podem vir a causar[36].

Importa mencionar que este delito guarda profunda conexão com demais crimes digitais próprios, eis que por muitas vezes é o meio pelo qual se pratica outros ilícitos, tais como os que apresentaremos a seguir.

2.2.2 Inserção de *malwares*

Trata-se de "códigos maliciosos", cujas funções, objetivos e forma de atuação são variáveis de acordo com o que o agente deseja obter\alcançar, conforme veremos a seguir. Importa mencionar que tal ato ilícito ganhou uma maior relevância jurídica a partir da introdução da lei n 12.737\12, que foi a responsável por introduzir o crime de invasão de dispositivo informático em nosso ordenamento pátrio. Porém, conforme alerta Sydow, a introdução destes códigos maliciosos só configuraria ato típico se o agente o programa com a finalidade específica de atingir dados ou obter vantagem ilícita[37].

Neste diapasão, seria interessante analisar alguns dos tipos de códigos maliciosos que se encontram disponíveis na atualidade.

O primeiro e possivelmente mais famoso desses tipos de *malwares*, são os vírus. Trata-se de linhas de código cuja função é se anexar a programas e sistemas, de maneira que possam se propagar pelos dispositivos informáticos e contaminar assim outros sistemas[38]. Tal qual um vírus

[35] ARAUJO ALVES, 2020, p. 40.
[36] CRESPO, 2011, p. 75.
[37] SYDOW, 2015, p. 112 *apud* ARAUJO ALVES, 2020, p. 49.
[38] CRESPO, *op. cit.*, p. 74.

biológico, sua função é a de se "autorreplicar" e se espalhar da maneira mais rápida e intensa, o que pode acabar tornando os sistemas operacionais mais lentos, vez que afetam de maneira direta a memória RAM dos dispositivos. Emerson Wendt e Higor Nogueira irão dizer que existem dois tipos de vírus, cada qual com sua função específica, o "vírus de boot" e os vírus "time bombs"[39].

O segundo tipo de malware mais popular são os *worms.* Trata-se de arquivo malicioso com capacidade autorreplicante independentemente de qualquer comando dado pelo usuário vítima, Wendt e Nogueira alertam para a capacidade alta de infiltração deste tipo de *malware* em sistemas operacionais, vez que costumam se instalar em computadores em razão de vulnerabilidades previamente não identificadas pelo usuário[40].

O terceiro tipo são os *botnets*. Nesta ameaça virtual, diversos computadores são infectados por arquivos que tem como objetivo permitir ao criminoso o controle remoto do dispositivo informático. Em seguida, de posse do controle deste verdadeiro "exército" de computadores infectados, o criminoso emite comandos e requisições para sites e servidores que deseje atingir. Como os computadores controlados enviarão requisições ao mesmo tempo, o servidor alvo poderá sofrer falhas catastróficas que impeçam o de continuar funcionando, o que permite que o criminoso "tire do ar" diversos serviços essenciais a depender de que tipo de servidor se está atacado, tais como servidores utilizados por entidades públicas (ex: o servidor do corpo de bombeiros, servidor de uma instalação militar sensível etc.). Estes tipos de ataque são conhecidos no meio da criminalidade digital como "ataques DDoS", acrônimo da língua inglesa para *distributed denial of service* (negação de serviço distribuído)[41].

Importante frisar que, conforme alertam Wendt e Nogueira, as vítimas da "primeira fase" de um ataque *botnet (*leia-se, a invasão de seu sistema

[39] WENDT; NOGUEIRA JORGE, 2021, p. 19.
[40] Ibid., p. 20.
[41] Ibid., p. 21.

computacional e posterior "sequestro" deste para a realização das práticas criminosas) não tem qualquer ciência de que tal fato está ocorrendo e, portanto, absolutamente impassíveis de se ver processados pela prática do referido ato ilícito, eis que nem sequer teríamos, segundo a estruturação da moderna teoria do crime, uma conduta por parte destes indivíduos, que na realidade seriam tão vítimas dos fatos como o alvo final do ataque "DDoS"[42].

No caso concreto, no Brasil podemos listar dois grandes exemplos de ataques do tipo DDoS praticados nos últimos anos e que trazem enormes consequências no âmbito jurídico criminal. O primeiro, apelidado de "operação #Antisec" e o segundo "*Onslaught*", ambos perpetrados em conjunto pelo grupo de "cyber vigilantes" conhecidos como "*Anonymous*" em parceria com ou outro coletivo de mesma natureza chamado "*LulzSec*" e tiveram como objetivo a perpetração de bloqueios por meio da negação de serviço a sites da presidência da república, a agência brasileira de inteligência, a receita federal, dentre outros[43]. Não é de grande dificuldade portanto, imaginar o potencial lesivo deste tipo de ataque e o dano que pode gerar a prestadoras de serviços públicos e agências governamentais, que geralmente em razão da sua natureza político administrativa, acabam sendo os alvos preferidos desses tipos de organização, ou agentes, que alegam praticar tais atos na defesa de algum ideal de cunho político, religioso, filosófico etc.

Conforme apontam Wendt e Nogueira, nestes tipos de situação, haveria uma exceção à regra, por meio do qual, a prática de um ilícito tipicamente classificado como delito digital próprio, acaba se convertendo em um delito digital impróprio, eis que no caso de efetiva obtenção do resultado almejado (disrupção de sites governamentais ou de concessionárias prestadoras de serviços de natureza pública), haveria a possível incidência

[42] WENDT; NOGUEIRA JORGE, 2021, p. 20.
[43] PASSARINHO, 2011 *apud* WENDT; NOGUEIRA JORGE, 2021, p. 21.

das penas previstas no art.266, parágrafo primeiro e art. 265 caput, ambos do CP[44]:

> Art. 266 - Interromper ou perturbar serviço telegráfico, radiotelegráfico ou telefônico, impedir ou dificultar-lhe o restabelecimento:
> Pena - detenção, de um a três anos, e multa.
> § 1 o Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento. (Incluído pela Lei nº 12.737, de 2012) Vigência
> E
> Art. 265 - Atentar contra a segurança ou o funcionamento de serviço de água, luz, força ou calor, ou qualquer outro de utilidade pública:
> Pena - reclusão, de um a cinco anos, e multa.

Ainda neste tema, pode-se concluir que nas hipóteses de ataques do tipo DDoS a entidades que prestam serviços tidos como "de risco", em razão da moderna sociedade de risco[45], tais como transportadoras aéreas, fluviais\marítimas, rodoviárias, ferroviárias etc. que tenham como resultado risco de perigo de dano aos referidos meios de transporte, estaríamos diante das hipóteses dos crimes contra a segurança dos meios de comunicação e transporte previstos no capítulo II, do título VII do CP (crimes contra a incolumidade pública). De tal maneira, Wendt e Nogueira, analisando as recomendações da CERT.BR (Centro de estudos, resposta e tratamento de incidentes de segurança no Brasil), são categóricos ao afirmar que "numa análise comparativa dos malwares, os *worms* e os *botnets* são os que tem mais potencial danoso"[46].

Neste diapasão, evidencia-se a fluidez com que a classificação dos crimes virtuais\digitais acabam adotando, o que dificulta de sobremaneira uma tentativa da doutrina e jurisprudência em adotar rígidas classificações, eis que pela natureza deles, como vimos nos dois exemplos acima, não se está diante de situações "estaques", o que requer por parte dos últimos, uma análise casuística de cada tipo de ato ilícito cometido no mundo digital.

---

[44] WENDT; NOGUEIRA JORGE, *op. cit.*, p. 23.
[45] ZÍLIO, 2014. p.87
[46] CERTI.BR; NIC.BR; CGI.BR, 2020 *apud* WENDT; NOGUEIRA JORGE, 2021, p. 21.

O quarto tipo de malware são os *keyloggers*. Trata-se de um subtipo comum de *spywares*, nome genérico dado a códigos maliciosos que buscam registrar as ações do usuário naquele aparelho eletrônico, tais como rotinas de pesquisa, aplicativos mais utilizados etc.[47], que funcionam de forma a "detectar e informar toda e qualquer tecla que tenha sido acionada pelo usuário infectado"[48]. Com isto, o criminoso conseguiria obter informações sensíveis do usuário vítima, tais como as senhas por ele utilizadas, suas contas de e-mail, serviços bancários, registros de conversas de em chats de todo tipo etc.

Mateus de Araújo Alves irá concluir que os keyloggers apresentam enorme potencial de dano as suas vítimas, eis que segundo o autor: "há uma quebra na confidencialidade e disponibilidade dos serviços digitais, podendo trazer, também, prejuízos econômicos para aquele que teve sua intimidade atingida"[49].

O quinto e último tipo de malwares mais importantes, são os *ransomewares*. A função destes tipos de códigos maliciosos é a de bloquear ou até mesmo tornar inacessível permanentemente, dados de valor relevante ou estratégicos para o usuário vítima. Nas palavras da CERT.BR, os *ransomewares* buscam "tornar inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate(*ransom*) para restabelecer o acesso ao usuário". Importa mencionar que, em razão da tentativa dos criminosos em manter a anonimidade, o pagamento é, via de regra, exigido por meio de cripto moedas, tais como *bitcoin*, *etherium*, *dodgecoin*, etc...[50].

Este tipo de *malware* tem sido alvo de grande atenção e combate das autoridades no Brasil e no mundo, assim como para prestadoras de serviço de cyber segurança, vez que os métodos empregados pelos cyber criminosos

[47] Ibid., p. 26.
[48] ARAUJO ALVES, 2020, p. 48.
[49] Ibid., p. 48.
[50] CERT.BR, S. D. *apud* WENDT; NOGUEIRA JORGE, 2021, p. 38.

(criptografia de ponta e exigibilidade do uso de criptomoedas para pagamento do "resgate") dificulta "de sobremaneira a identificação dos autores"[51].

2.2.3 Engenharia social e *scamming*

Conforme relata Mateus de Araújo Alves, citando Sydow, o *scamming* é "gênero da modalidade delitiva que se utiliza do meio digital para obter alguma vantagem sobre a vítima, abarcando diversas espécies de condutas, tais como o *phishing* e o *pharming*"[52].

Portanto, seria o tipo de delito no qual:

> O ofensor e o ofendido se comunicam de forma direta ou indireta, sendo que o primeiro tenta persuadir o segundo a praticar alguma ação, geralmente a entrega de informações pessoais ou a transferência de valores econômicos[53].

Conforme nos ensina Matheus de Araújo Alves, quando aplicadas a um contexto de meio digital, estas ações adotam o nome de "engenharia social"[54]. Então o que constitui de fato engenharia social? Conforme nos explica Marcelo Crespo, é:

> Artificio intelectual para acessar informações sigilosas. (...) a engenharia social é arma para que se consigam informações sigilosas importantes, mas o faz sempre mediante artificio ou ardil, de forma sub-reptícia[55].

Ou seja, o que se convencionou chamar, em âmbito doutrinário e jurisprudencial, "engenharia social", nada mais seria do que o velho e conhecido conceito de ardil ou artifício no direito penal clássico. Como bem sintetiza Crespo, são métodos de "mascarar a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso"[56].

---

[51] WENDT; NOGUEIRA JORGE, 2021, p. 39.
[52] SYDOW, 2015, p. 126 *apud* ARAUJO ALVES, 2020, p. 49.
[53] Ibid., p. 49.
[54] ARAUJO ALVES, 2020, p. 49.
[55] CRESPO, 2011, p. 82.
[56] Ibid., p. 82.

Conforme abordado anteriormente, os esquemas *phishing* são espécies de golpe muito utilizados para a prática de engenharia social, consiste em o criminoso se fazer passar por entidades não governamentais (ONG´s), pessoa jurídica dos mais variados tipos, entidades religiosas e inclusive entes governamentais, de maneira que consiga "conquistar" a confiança da vítima e assim convence-la a fornecer dados e informações pessoais, tais como senhas, números de cartões bancários, ou como alerta Matheus de Araújo Alves, citando Crespo, "instigar a abaixar arquivos que permitam a futura subtração de dados ou acesso não autorizado ao sistema da vítima"[57].

Segundo este mesmo doutrinador, citando SYDOW, os golpes mais comuns aplicados no Brasil, no contexto da engenharia social, são:

- Alegação de que um documento do usuário foi cancelado;
- Mensagens informando que o usuário deve pagar um boleto anexado para limpar seu nome;
- E-mails de bancos em que o usuário é remetido, ao clicar na mensagem, a sites espelho, idênticos aos verdadeiros, mas fraudulentos e hospedados em servidores fora do país, em que se solicitam dados do cartão de crédito, senhas, etc...
- Envio de mensagens sentimentais que buscam tocar os leitores de um problema aparentemente real, inclusive com fotografias, como por exemplo, uma criança que precisa de algum transplante;
- Links para que o usuário acesse sites de seu interesse etc[58].

Conforme se vê, a maior parte das ações de engodo que se passam no cyber espaço, costumam ser enviadas por meio de E-mails que funcionam "como verdadeiras iscas, oferecendo vantagens ou atiçando a curiosidade do usuário"[59]. Razão pela qual, abordaremos no próximo tópico, como esse mecanismo de correio eletrônico, tão fundamental e importante no cenário atual, é objeto de um tipo específico de crime digital próprio, conforme veremos a seguir.

2.2.4 Interceptação de E-mails

[57] CRESPO, 2011 *apud* ARAUJO ALVES, 2020, p. 51.
[58] SYDOW, 2015, p. 128 *apud* ARAUJO ALVES, 2020, p. 51.
[59] ARAUJO ALVES, 2020, p. 50.

Segundo Matheus de Araújo Alves, a interceptação de E-mail se configura com "a conduta de impedir-se que a mensagem enviada pelo remetente, através do correio eletrônico, seja recebida pelo seu destinatário"[60]. Ora sabe-se que a carta magna de 1988 alçou ao rol de direitos fundamentais a chamada "inviolabilidade das comunicações", conforme se extrai do seu art.5, inciso XII, *in verbis*:

> Art. 5(...)
> XII- é inviolável o sigilo das correspondências e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma que a lei estabelecer para fins de investigação criminal ou de instrução processual penal.

Segundo entendimento da melhor doutrina, estaria superada o debate acerca da constitucionalidade de se incluir os meios digitais e de telemática no rol do artigo anterior. Mateus de Araújo Alves, citando o Professor Marcelo Crespo, afirma que esta inclusão se justifica devido a "necessidade de se incriminar tal conduta"[61] eis que a convenção de Budapeste para coibição a ilícitos digitais preceitua a incorporação de mecanismos nas legislações nacionais para que se alcancem tais objetivos.

Percebe-se ainda que a constituição abre espaço para uma autorização especial de interceptação das comunicações no geral, tratando-se de interceptação de dados telemáticos feitos pela autoridade policial competente, devidamente munida de ordem judicial para tal.

Neste diapasão, é importante citar a existência de lei específica que irá regular esta verdadeira "exceção" a regra, quando se trata da preservação da inviolabilidade das comunicações. Trata-se da lei 9.296/96, que estipulará as regras e situações em que a autoridade policial e judiciária poderão realizar e conceder a autorização, respectivamente, para que se estabeleça a violação do sigilo das informações dos investigados, bem como tipifica a conduta dos

[60] ARAUJO ALVES, 2020, p. 52.
[61] CRESPO, 2011, p. 87 *apud* ARAUJO ALVES, 2020, p. 52.

indivíduos que as violem de maneira ilegítima e ilegal, ou seja, sem a devida autorização judicial ou em desconformidade com a última.

> Art. 1º A interceptação de comunicações telefônicas, de qualquer natureza, para prova em investigação criminal e em instrução processual penal, observará o disposto nesta Lei e dependerá de ordem do juiz competente da ação principal, sob segredo de justiça
> Parágrafo único: O disposto nesta Lei aplica-se à interceptação de comunicações em sistemas de informática e telemática.
> Art. 2° Não será admitida a interceptação de comunicações telefônicas quando ocorrer qualquer das seguintes hipóteses:
> I - não houver indícios razoáveis da autoria ou participação em infração penal;
> II - a prova puder ser feita por outros meios disponíveis;
> III - o fato investigado constituir infração penal punida, no máximo, com pena de detenção.
> Parágrafo único. Em qualquer hipótese deve ser descrita com clareza a situação objeto da investigação, inclusive com a indicação e qualificação dos investigados, salvo impossibilidade manifesta, devidamente justificada.
> Art. 3º A interceptação das comunicações telefônicas poderá ser determinada pelo juiz, de ofício ou a requerimento:
> I - da autoridade policial, na investigação criminal;
> II - do representante do Ministério Público, na investigação criminal e na instrução processual penal.

Sobre a tipificação da conduta deste delito digital próprio, inova a legislação ao trazer em sem artigo décimo a seguinte estipulação:

> Art. 10. Constitui crime realizar interceptação de comunicações telefônicas, de informática ou telemática, promover escuta ambiental ou quebrar segredo da Justiça, sem autorização judicial ou com objetivos não autorizados em lei:
> Pena - reclusão, de 2 (dois) a 4 (quatro) anos, e multa.
> Parágrafo único. Incorre na mesma pena a autoridade judicial que determina a execução de conduta prevista no caput deste artigo com objetivo não autorizado em lei.

Portanto impossível seria a sustentação da tese de que tal atividade não apresenta tipificação legal na legislação pátria ou que seria impassível de punição. Isto não significa dizer, porém, que não haja debate doutrinário no âmbito da conceituação do termo “interceptar”.

Conforme aponta Mateus de Araújo Alves citando Sydow, interceptar significa “colocar-se entre, na qualidade de obstáculo, ou seja, impedir que o

curso dos dados se desenvolva, de modo a impedir que o destinatário obtenha acesso eles[62].

Neste sentido, o doutrinador irá sustentar que, em razão da própria natureza da transmissão de dados por meio de sistemas de correios eletrônicos, onde as mensagens são fracionadas em "diferentes pacotes de dados que vão ser remetidos quantas vezes forem necessárias até que seu destino seja atingido"[63], o "mero acesso e leitura dos dados referentes a um e-mail por parte de terceiro pode não impedir que o destinatário também receba a informação em uma remessa de pacotes de dados seguintes"[64], o que segundo o doutrinador, fazendo referência a análise de Sydow "haveria o afastamento da figura típica do art.10 da lei 9.296\96"[65].

Ora com a devida vênia a ambos consagrados mestres, não vislumbro possibilidade para o referido afastamento da tipicidade da conduta, eis que em que pese o conteúdo da mensagem não ser alterada ou impedida de atingir o destinatário final, nos crimes digitais próprios, por sua própria natureza, teremos como bem jurídico violado a segurança e a confiança dos meios digitais e da informação em si, conforme já abordamos quando em análise da classificação dos tipos de crimes digitais.

Desta maneira, perfeita é a letra pura da lei, que em seu artigo décimo, não exige em momento algum que a tipificação esteja vinculada a corrupção dos dados ou o impedimento da chegada destes ao seu destinatário final, mas sim o próprio ato de violação do sigilo das comunicações em si. Aqui o legislador foi bastante feliz, eis que sintetizou de maneira suscinta o cerne do artigo quinto, inciso XXI da CRFB88, pois o que se busca proteger é a inviolabilidade das comunicações (a informação), e, portanto, a disrupção dos dados ou a maculação deles constitui mero pós fato impunível[66].

---

[62] SYDOW, 2015, p. 134 *apud* ARAUJO ALVES, 2020, p. 53.
[63] ARAUJO ALVES, 2020, p. 53.
[64] Ibid., p. 53.
[65] SYDOW, 2015, p. 134 *apud* ARAUJO ALVES, 2020, p. 53.
[66] DOS SANTOS, 2014.

2.3 Os delitos digitais impróprios mais comuns

Conforme vimos anteriormente, os crimes digitais próprios são tidos pela melhor doutrina como sendo aqueles em que já existe prévia tipificação pela legislação vigente, alguns inclusive cuja previsão remonta desde a origem de elaboração e publicação do código penal vigente, em 1940. Assim, conforme cita Gimenes, seriam "as condutas as quais o computador é usado como instrumento para a execução do delito, mas não há ofensa ao bem jurídico inviolabilidade da informação automatizada"[67].

Dessa forma, o emprego de dispositivo informático durante a realização destes delitos nada mais seriam do que meios de execução para a prática do injusto, não tendo a norma penal estipulado como condição *sine qua non* o emprego destes sistemas de forma a constituir o núcleo do tipo, como vimos no caso dos crimes digitais próprios.

Vejamos então os tipos de crimes digitais impróprios mais comuns segundo a organização apresentada por Mateus de Araújo Alves.

2.3.1 Ameaça

O crime de ameaça encontra tipificação no artigo 147 do CP, *in verbis*

> Art. 147. Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave:
> Pena - detenção, de um a seis meses, ou multa.
> Parágrafo único - Somente se procede mediante representação.

Tem como cerne a ação de intimidação do autor frente a vítima, por intermédio da promessa (seja ela escrita, verbal ou até mesmo for gesto\símbolo) de lhe causar algum mal. É infelizmente bastante comum no meio digital, eis que o desconhecimento da lei e a relativa novidade dos meios de comunicação instantânea\mídias sociais, leva certos indivíduos a praticarem o ato, acreditando que em razão de se tratar do "mundo digital",

[67] GIMENES, 2013, p. 09 *apud* ARAUJO ALVES, 2020, p. 54.

não haveria de fato a materialização do fato típico, o que como sabe-se é um equívoco.

Um derivativo do crime de ameaça, é o crime de perseguição. Esta conduta típica teve por objetivo responder ao anseio popular pelo combate e fiscalização das autoridades frente um tipo de conduta que se tornou bastante difundida graças as facilidades de informação e identificação possibilitadas pelo mundo digital, o *stalking*. O ato de *stalking* constitui a perseguição de um indivíduo, com a utilização de informações pessoais deste, disponibilizadas voluntariamente ou não, de forma a se violar a intimidade e participar da vida privada da vítima sem seu consentimento. Encontra tipificação legal por meio do artigo 147-A do CP:

> Art. 147-A. Perseguir alguém, reiteradamente e por qualquer meio, ameaçando-lhe a integridade física ou psicológica, restringindo-lhe a capacidade de locomoção ou, de qualquer forma, invadindo ou perturbando sua esfera de liberdade ou privacidade. (Incluído pela Lei nº 14.132, de 2021)
> Pena – reclusão, de 6 (seis) meses a 2 (dois) anos, e multa. (Incluído pela Lei nº 14.132, de 2021)
> § 1º A pena é aumentada de metade se o crime é cometido:
> I – contra criança, adolescente ou idoso;
> II – contra mulher por razões da condição de sexo feminino, nos termos do § 2º-A do art. 121 deste Código;
> III – mediante concurso de 2 (duas) ou mais pessoas ou com o emprego de arma.
> § 2º As penas deste artigo são aplicáveis sem prejuízo das correspondentes à violência.
> § 3º Somente se procede mediante representação.

Neste diapasão, é possível que surja questionamentos a respeito da forma em que estas informações privadas são obtidas pelo *stalker*, e em caso de obtenção por meio fraudulento (Ex: violação a dispositivo informático da vítima), se estaria diante ou não de concurso de crimes.

Ora, para tal pode-se realizar uma simples correlação com o crime de furto qualificado pela destruição ou rompimento de obstáculo à subtração da coisa (art. 155, parágrafo 4, inciso I), onde entende a melhor doutrina e jurisprudência consolidada que, caso o "obstáculo" destruído seja parte integrante do objeto do furto, trata-se apenas e tão somente de crime de furto e não há que se falar no crime de dano do artigo 163 do CP, pois o vínculo

subjetivo do agente era a de usurpar para si ou outrem bem alheio móvel e não meramente danifica-lo, portanto a aplicação deste tipo penal é incabível (exemplo: O agente quebra a janela de veículo para conduzi-lo a um local de desmonte). Por outro lado, quando, para se alcançar o objeto do furto, o meliante lança mão do rompimento de obstáculo de forma ter acesso físico ao último, então teremos a qualificadora descrita sendo aplicada (exemplo: O agente quebra a janela do veículo para obter pertences de valor que se encontravam no interior do mesmo).

> EMENTA: APELAÇÃO CRIMINAL - FURTO QUALIFICADO - ABSOLVIÇÃO - IMPOSSIBILIDADE - SUFICIÊNCIA DO ARCABOUÇO PROBATÓRIO - PRINCÍPIO DA INSIGNIFICÂNCIA - INAPLICABILIDADADE - DESTRUIÇÃO DE VIDRO DE VEÍCULO PARA SUBTRAÇÃO DE OBJETO DO SEU INTERIOR - CARACTERIZAÇÃO DA QUALIFICADORA DO ROMPIMENTO DE OBSTÁCULO - PRESCINDIBILIDADE DO LAUDO PERICIAL - RECONHECIMENTO DA TENTATIVA - INVIABILIDADE - POSSE DA RES FURTIVA APÓS CESSAÇÃO DA CLANDESTINIDADE - APLICAÇÃO DO ART. 387, § 2º DO CPP - NÃO CABIMENTO. - Incabível a absolvição quando o conjunto probatório é no sentido de comprovar a autoria delitiva, ainda mais se encontrado o réu de posse da res furtiva - O princípio da insignificância (bagatela) não foi recepcionado pelo ordenamento jurídico pátrio. A insignificância é princípio orientador do Legislativo ao tipificar criminalmente as condutas, portanto, desarrazoada sua utilização pelo Judiciário, sob pena de violação dos princípios constitucionais da reserva legal e da independência dos Poderes - É desnecessária a prova pericial, para efeito de qualificar o delito de furto, quando a prova oral vai no sentido da cabal demonstração do rompimento de obstáculo para o êxito da empreitada criminosa - A destruição do vidro do automóvel para a subtração de objetos do seu interior caracteriza a qualificadora do art. 155, § 4º, I, do CPB - No crime de furto, a consumação ocorre no exato momento em que, cessada a clandestinidade, o agente se torna possuidor da coisa, sendo irrelevante que a posse não tenha sido mansa ou pacífica, ou que a coisa tenha sido retomada após imediata perseguição - Desnecessária a aplicação da regra do art. 387, § 2º do CPP, no julgamento da apelação, se o tempo de prisão provisória do acusado não interferir na definição do regime prisional, tendo sido fixado o regime mais gravoso em razão da reincidência do réu e da valoração negativa das circunstâncias judiciais, sendo de bom grado que a efetivação da detração penal fique a encargo do juízo da execução[68].

Neste sentido, seria em tese possível a aplicação de analogia, eis que *in bonam partem*, para que o agente (stalker) que obteve as informações privadas por meio de dispositivo informático, venha a responder tão somente

[68] TJ-MG. *APR: XXXXX70474472001*. Belo Horizonte, Rel. Furtado de Mendonça, Data de Julgamento: 23/11/2021, Câmaras Criminais / 6ª CÂMARA CRIMINAL, Data de Publicação: 26/11/2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-mg/1325315800. Acesso em: 8 set. 2022.

pelo crime de perseguição (art. 147-A do CP) aumentados de um sexto a dois terços, nos moldes do crime continuado (art. 71 CP), sendo incabível a incidência de concurso material (cúmulo jurídico nas hipóteses de ações criminosas diversas e independentes), de maneira a impedir que o mesmo tivesse a cumulação das penas de perseguição e violação de dispositivo informático (artigo 147-A + Art.154-A, ambos do CP, respectivamente). Em uma visão ainda mais garantista, poderia-se até mesmo defender a aplicação do princípio da consunção, onde o crime meio (invasão de dispositivo informático) é ‘’absorvido’’ ao crime fim (perseguição), vindo o autor do delito a responder tão somente pele prática do último tipo penal.

2.3.2 Furto e estelionato qualificados mediante fraude empregada por meio de dispositivo eletrônico

Dentro das diversas hipóteses de qualificadoras do crime de furto, teremos a qualificadora por meio de fraude. Importa recordar que tal modalidade não deve jamais ser confundida com o crime de estelionato previsto no art.171 do CP, pois no caso da primeira, o criminoso se utiliza de métodos e meios que tem por objetivo distrair a vítima, tirando a *res furtiva* de sua esfera de vigilância, o que possibilitará maior facilidade no momento da consumação do furto. Na segunda hipótese, o meliante irá se utilizar da já mencionada “engenharia social” (se realizada por meio digital), de engodos e artimanhas de forma a fazer com que a vítima lhe entregue, voluntariamente, vantagem econômica indevida.

Superadas as diferenças entre os distintos tipos penais, passemos a análise do crime de furto qualificado por fraude mediante uso de dispositivo informático.

É novo tipo penal, tendo sido introduzido por meio da lei 14.155\21 cujo objetivo era combater os delitos virtuais mais comuns, tornando mais graves os crimes de violação de dispositivo informático, furto e estelionato cometidos de forma eletrônica.

Diz o art. 155, parágrafo quarto B e C:

> Art. 155 - Subtrair, para si ou para outrem, coisa alheia móvel:
> Pena - reclusão, de um a quatro anos, e multa.
> § 4º-B. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se o furto mediante fraude é cometido por meio de dispositivo eletrônico ou informático, conectado ou não à rede de computadores, com ou sem a violação de mecanismo de segurança ou a utilização de programa malicioso, ou por qualquer outro meio fraudulento análogo.
> § 4º-C. A pena prevista no § 4º-B deste artigo, considerada a relevância do resultado gravoso:
> I – Aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional;
> II – Aumenta-se de 1/3 (um terço) ao dobro, se o crime é praticado contra idoso ou vulnerável.

Aqui temos a utilização por parte do cyber criminoso de meio informático para a prática da "distração" permitindo que a vítima perca de sua vigilância a *res furtiva*, o que na hipótese digital pode se referir a bens conectados ao sistema digital (*smart wearables* como eletrodomésticos inteligentes, *gadgets* etc. que estejam conectados com o provedor de internet da vítima) ou até mesmo recursos financeiros e ativos no mercado de ações.

Esta distração pode se dar de diversas formas, tais como o envio e infiltração de *malwares* (desde que o objetivo final do agente seja o de praticar o ato típico que se está tratando, caso contrário, o mero envio e distribuição constituiria tão somente invasão de dispositivo informático, sendo crime digital próprio, conforme visto anteriormente) ou esquemas mais complexos que porventura acabem por se utilizar parcial ou totalmente de sistemas digitais.

Percebe-se ainda a existência de causa especial de aumento de pena nos incisos I e II do parágrafo 4-C. Nestes casos, tendo o cyber criminoso se valido de servidores localizados fora do território nacional a pena é aumentada de um terço a dois terços, e se a empreitada criminosa tiver como vítima idoso ou vulnerável, a pena será agravada em um terço, podendo alcançar até o dobro.

Aqui acredita-se que, na primeira hipótese, o legislador estivesse buscando desencorajar a utilização de servidores localizados fora do país

para a prática de atividades ilícitas, em razão da enorme dificuldade de se processar e julgar tais casos (fato que abordaremos mais a frente quando tratarmos das dificuldades em se combater os crimes digitais). Já na segunda hipótese, se estaria reconhecendo a vulnerabilidade dos indivíduos mais idosos, eis que por não estarem acostumados com as inovações tecnológicas atuais, tornam-se "presas" fáceis dos meliantes.

Em se tratando da prática de estelionato por meio de meios eletrônicos e informáticos, teremos a seguinte dicção da legislação repressiva:

> Art. 171 - Obter, para si ou para outrem, vantagem ilícita, em prejuízo alheio, induzindo ou mantendo alguém em erro, mediante artifício, ardil, ou qualquer outro meio fraudulento:
> Pena - reclusão, de um a cinco anos, e multa, de quinhentos mil réis a dez contos de réis.
> § 2º-A. A pena é de reclusão, de 4 (quatro) a 8 (oito) anos, e multa, se a fraude é cometida com a utilização de informações fornecidas pela vítima ou por terceiro induzido a erro por meio de redes sociais, contatos telefônicos ou envio de correio eletrônico fraudulento, ou por qualquer outro meio fraudulento análogo.
> § 2º-B. A pena prevista no § 2º-A deste artigo, considerada a relevância do resultado gravoso, aumenta-se de 1/3 (um terço) a 2/3 (dois terços), se o crime é praticado mediante a utilização de servidor mantido fora do território nacional.

Percebe-se, portanto, que o tipo penal trata de combater as práticas por meio dos quais os malfeitores tentem, por meio de "esquemas" e engenharia social, obter vantagem indevida da vítima, ao fazer com que entregue voluntariamente algo que os cyber criminosos tenham interesse de obter.

Dentre as causas especiais de aumento de pena, teremos novamente hipótese de utilização e emprego de servidor localizado fora do território nacional, pelas mesmas razões e motivos que foram levantadas anteriormente.

2.3.3 Incitação e apologia ao crime

A figura típica de incitação à prática de crime e o delito de apologia ao crime, encontram previsão expressa nos artigos 286 e 287 do código repressivo, respectivamente.

> Art. 286 - Incitar, publicamente, a prática de crime:
> Pena - detenção, de três a seis meses, ou multa.
> Parágrafo único. Incorre na mesma pena quem incita, publicamente, animosidade entre as Forças Armadas, ou delas contra os poderes constitucionais, as instituições civis ou a sociedade.
> Art. 287 - Fazer, publicamente, apologia de fato criminoso ou de autor de crime:
> Pena - detenção, de três a seis meses, ou multa.

São figuras típicas que carregam, por sua própria natureza, grande polêmica, eis que segundo alguns doutrinadores, não teriam sido recepcionadas pelo ordenamento pátrio atual em virtude de serem incompatíveis com os princípios da liberdade de expressão e de reunião, expressamente definidos em sede constitucional. Entretanto, a maioria da doutrina e jurisprudência entende que os tipos penais são válidos, desde que aplicados com muita parcimônia avaliando o caso concreto e equilibrando os princípios mencionados acima com o da preservação da ordem e da segurança pública.

Em razão da enorme interconectividade e facilidade que internet e as mídias sociais proporcionaram, indivíduos dos mais amplos espetros ideológicos, políticos e sociais puderam interagir entre si e encontrar seus "nichos de interesse". Infelizmente, refletindo a vida real material, o mundo virtual tornou-se meio pelo qual indivíduos ou grupos de indivíduos, mal-intencionados ou cujos apreços pessoais por determinados conceitos, ideias ou figuras, pudessem colocar em público suas questionáveis preferencias.

Isto acabou por resultar na existência de páginas e grupos sociais que se dedicam a incitação e apologia a crimes e\ou figuras de criminosos, exemplos clássicos e conhecidos são os notórios perfis "camisas do tráfico", "relógios do tráfico", perfis dedicados a patrocínio de grupos terroristas, organizações criminosas, defesa de ações de membros do narcotráfico etc.

2.3.4 Violação de direitos autorais

Trata-se, pois, de todo o tipo de ato que busque violar os direitos do autor, devidamente estipulados pela legislação civil pátria bem como tratados

internacionais que regem questões como a propriedade intelectual (aqui englobando tanto as questões de propriedade industrial tais como patentes, desenho industrial e marcas, e também questões que envolvam direitos autoriais propriamente ditos).

Encontra previsão legal no artigo 184 do CP:

> Art. 184. Violar direitos de autor e os que lhe são conexos:
> Pena – detenção, de 3 (três) meses a 1 (um) ano, ou multa

Segundo Matheus de Araújo Alves e Marcelo Crespo, os tipos mais comuns que envolvem estes delitos é a pirataria, o uso indevido de marcas e documentos e outras questões relativas a violações a propriedade intelectual[69].

2.3.5 Falsidade ideológica e falsa identidade

Trata-se de tipos penais previstos nos artigos 299 e 307 do CP respectivamente.

> Art. 299 - Omitir, em documento público ou particular, declaração que dele devia constar, ou nele inserir ou fazer inserir declaração falsa ou diversa da que devia ser escrita, com o fim de prejudicar direito, criar obrigação ou alterar a verdade sobre fato juridicamente relevante:
> Pena - reclusão, de um a cinco anos, e multa, se o documento é público, e reclusão de um a três anos, e multa, de quinhentos mil réis a cinco contos de réis, se o documento é particular.
> Parágrafo único - Se o agente é funcionário público, e comete o crime prevalecendo-se do cargo, ou se a falsificação ou alteração é de assentamento de registro civil, aumenta-se a pena de sexta parte.

e

> Art. 307 - Atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:
> Pena - detenção, de três meses a um ano, ou multa, se o fato não constitui elemento de crime mais grave.

[69] ARAUJO ALVES, 2020, p. 56; CRESPO, 2011, p. 89.

No primeiro caso, como se pode extrair do texto da lei, se constitui o fato típico por meio da "inserção" de dados incorretos (falsos) ou então tem-se a omissão de dados que sejam relevantes e que deveriam constar no documento público\particular e que, conforme nos alerta Matheus de Araújo Alves, tenham "a intenção de prejudicar direito, criar obrigações ou alterar a verdade sobre fato juridicamente relevante"[70].

É crime relativamente comum de ocorrer, pois em razão de aplicativos de manipulação de texto, imagens e dados, um cyber criminoso devidamente instruído e treinado, é capaz de alterar todo e qualquer documento, inclusive oficiais do governo, de modo a tornar os documentos falsos quase indistinguíveis dos originais autênticos.

No segundo caso, temos um tipo penal que se encontra ainda mais em voga no mundo virtual na atualidade, muito por conta de aplicativos de relacionamento e chats de mensagem instantâneos online. No crime de falsa identidade, nas palavras de Matheus de Araújo Alves, "uma pessoa se faz passar por quem ela não é, utilizando-se de dados e até mesmo de senha de um terceiro, em proveito próprio ou alheio, ou até para causar algum dano"[71]. No contexto atual, e em especial decorrência da pandemia de COVID-19 que afetou as relações interpessoais de bilhões de pessoas mundo afora, para muitos o único meio de interação social disponível eram aplicativos de relacionamento e sites de chats instantâneos. Muitos indivíduos, inseguros com suas próprias aparências, usariam fotos de outros usuários que entendessem ser "esteticamente mais aprazíveis" ou até mesmo fotos de indivíduos famosos, e se fariam passar por estes últimos, como se eles fossem, de forma a acumular mais *likes* e interações dos demais usuários.

Estes perfis falsos acabaram recebendo a alcunha de "*fakes*", sendo até os dias atuais, algo bastante comum de se encontram nestes aplicativos e sites. Nestas hipóteses entretanto, somente haverá crime se ficar evidenciado

[70] ARAUJO ALVES, 2020, p. 56.
[71] ARAUJO ALVES, 2020, p. 56.

obtenção de efetiva vantagem indevida ou danos a terceiro, caso contrário trataria-se, tão somente, de mera conduta prejudicial atípica.

2.3.6 Crimes contra a Honra

Os crimes contra a honra são os delitos de calúnia, difamação e injúria e encontram tipificação, de maneira respectiva, nos artigos 138, 139 e 140.

> Art. 138 - Caluniar alguém, imputando-lhe falsamente fato definido como crime:
> Pena - detenção, de seis meses a dois anos, e multa.
> § 1º - Na mesma pena incorre quem, sabendo falsa a imputação, a propala ou divulga.
> § 2º - É punível a calúnia contra os mortos.
> § 3º - Admite-se a prova da verdade, salvo:
> I - se, constituindo o fato imputado crime de ação privada, o ofendido não foi condenado por sentença irrecorrível;
> II - se o fato é imputado a qualquer das pessoas indicadas no nº I do art. 141;
> III - se do crime imputado, embora de ação pública, o ofendido foi absolvido por sentença irrecorrível.

e

> Art. 139 - Difamar alguém, imputando-lhe fato ofensivo à sua reputação:
> Pena - detenção, de três meses a um ano, e multa.
> Exceção da verdade
> Parágrafo único - A exceção da verdade somente se admite se o ofendido é funcionário público e a ofensa é relativa ao exercício de suas funções.

e

> Art. 140 - Injuriar alguém, ofendendo-lhe a dignidade ou o decoro:
> Pena - detenção, de um a seis meses, ou multa.
> § 1º - O juiz pode deixar de aplicar a pena:
> I - quando o ofendido, de forma reprovável, provocou diretamente a injúria;
> II - no caso de retorsão imediata, que consista em outra injúria.
> § 2º - Se a injúria consiste em violência ou vias de fato, que, por sua natureza ou pelo meio empregado, se considerem aviltantes:
> Pena - detenção, de três meses a um ano, e multa, além da pena correspondente à violência.
> § 3º Se a injúria consiste na utilização de elementos referentes a raça, cor, etnia, religião, origem ou a condição de pessoa idosa ou portadora de deficiência:
> Pena - reclusão de um a três anos e multa.

A calúnia busca proteger o que se convencionou chamar na doutrina de “honra objetiva”, isto é, aquilo que indivíduos de um grupo social pensam

sobre um dos seus membros. Difere-se da “honra subjetiva” que em sua essência é aquilo que o indivíduo pensa\sente de si mesmo.

Por este motivo, a calúnia somente irá operar quando o agente imputa, falsamente a vítima, um fato que seja tipificado como crime. Importa mencionar que o crime de calunia não admite a modalidade culposa, outro ponto a se ter em mente é que o fato típico só se consuma quando um terceiro obtém conhecimento do suposto crime praticado pela vítima, portanto se este não se consuma por questões alheias a vontade do agente (dificuldade de transmissão de dados, queda de luz, falta de conexão de internet etc.). não há em que se falar em “crime de calunia tentado”. O crime de calunia admite exceção da verdade, isto é, o agente tem a possibilidade de provar que o crime que imputou a vítima de fato ocorreu.

A difamação, que tal qual a calunia, protege a honra objetiva da vítima, se dá quando o agente imputa fato ofensivo a reputação da última, porém sem que este fato constitua um crime. Exemplo clássico é quando o criminoso afirma que a vítima se prostitui ou que apresenta algum tipo de personalidade repulsiva socialmente. Tal qual o tipo anterior, também se consuma quando o fato ofensivo imputado a vítima alcance terceiro, caso isto não ocorra, não haverá difamação, também não existe previsão legal para a prática culposa. Importante distinção com relação a calunia se dá pelo fato de que o crime de difamação não admite exceção da verdade, salvo se a “difamação” for direcionada a funcionário público e em razão do exercício de seu ofício.

A injúria, que diferentemente das hipóteses anteriores, tutela a honra subjetiva da vítima, se dá quando o agente ofende a “dignidade ou decoro”. Por esta razão, não é necessário que a ofensa chegue ao conhecimento de terceiros, necessitando, porém, que chega ao conhecimento da vítima. Pela própria natureza que constitui o crime, não é admitida exceção da verdade.

Conforme alerta Matheus de Araújo Alves, no contexto da ocorrência destes tipos de ilícitos por meio de dispositivos informáticos:

> Os criminosos motivados pelo anonimato, cometem os crimes através de chats, blogs, e-mails, dentre outros meios de postagem digital. Assim como nos crimes de ameaça, possuem maior incidência nas redes sociais, como, por exemplo, quando há divulgação de informações falsas que prejudicam a reputação de um terceiro.

Neste diapasão, importa mencionar a existência de causa geral de aumento de pena introduzida pela lei 13.964/19, onde se estipula que, caso qualquer uma das modalidades delitivas do rol dos crimes contra a honra, vier a ser praticada por meio de dispositivo informático (sendo as falsas informações vinculadas por meio de redes sociais ou pela internet), a pena aplicada será aumentada em até 3 vezes. *In verbis:*

> Art. 141(...)
> § 2º Se o crime é cometido ou divulgado em quaisquer modalidades das redes sociais da rede mundial de computadores, aplica-se em triplo a pena.

O objetivo do legislador foi o de reprimir a prática de tais atos por meios digitais, em especial aqueles que possam vir a alcançar muitos acessos e divulgações das falsas e nocivas imputações.

2.3.7 Pornografia infantil

O crime de pornografia infantil, faz referência as ações de divulgação e arquivamento de imagens, vídeos, áudios etc. que apresentem conteúdo de natureza pornográfica que envolvam crianças e adolescentes. O referido crime faz-se presente em diversas condutas tipificadas em artigos ao longo do ECA (estatuto da criança e adolescente – lei 8.069/90), especificamente os artigos 240, 241,241-A,241-B e 241-C, *in verbis:*

> Art. 240. Produzir, reproduzir, dirigir, fotografar, filmar ou registrar, por qualquer meio, cena de sexo explícito ou pornográfica, envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> § 1º Incorre nas mesmas penas quem agencia, facilita, recruta, coage, ou de qualquer modo intermedeia a participação de criança ou adolescente nas cenas referidas no caput deste artigo, ou ainda quem com esses contracena.
> § 2º Aumenta-se a pena de 1/3 (um terço) se o agente comete o crime:
> I – no exercício de cargo ou função pública ou a pretexto de exercê-la;
> II – prevalecendo-se de relações domésticas, de coabitação ou de hospitalidade; ou
> III – prevalecendo-se de relações de parentesco consanguíneo ou afim até o terceiro grau, ou por adoção, de tutor, curador, preceptor, empregador da vítima ou de

> quem, a qualquer outro título, tenha autoridade sobre ela, ou com seu consentimento.
> Art. 241. Vender ou expor à venda fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 4 (quatro) a 8 (oito) anos, e multa.
> Art. 241 - A. Oferecer, trocar, disponibilizar, transmitir, distribuir, publicar ou divulgar por qualquer meio, inclusive por meio de sistema de informática ou telemático, fotografia, vídeo ou outro registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 3 (três) a 6 (seis) anos, e multa.
> § 1º Nas mesmas penas incorre quem:
> I – assegura os meios ou serviços para o armazenamento das fotografias, cenas ou imagens de que trata o caput deste artigo;
> II – assegura, por qualquer meio, o acesso por rede de computadores às fotografias, cenas ou imagens de que trata o caput deste artigo.
> § 2º As condutas tipificadas nos incisos I e II do § 1º deste artigo são puníveis quando o responsável legal pela prestação do serviço, oficialmente notificado, deixa de desabilitar o acesso ao conteúdo ilícito de que trata o caput deste artigo.
> Art. 241-B. Adquirir, possuir ou armazenar, por qualquer meio, fotografia, vídeo ou outra forma de registro que contenha cena de sexo explícito ou pornográfica envolvendo criança ou adolescente:
> Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa.
> § 1º A pena é diminuída de 1 (um) a 2/3 (dois terços) se de pequena quantidade o material a que se refere o caput deste artigo.
> § 2º Não há crime se a posse ou o armazenamento tem a finalidade de comunicar às autoridades competentes a ocorrência das condutas descritas nos arts. 240, 241, 241-A e 241-C desta Lei, quando a comunicação for feita por:
> I – agente público no exercício de suas funções;
> II – membro de entidade, legalmente constituída, que inclua, entre suas finalidades institucionais, o recebimento, o processamento e o encaminhamento de notícia dos crimes referidos neste parágrafo;
> III – representante legal e funcionários responsáveis de provedor de acesso ou serviço prestado por meio de rede de computadores, até o recebimento do material relativo à notícia feita à autoridade policial, ao Ministério Público ou ao Poder Judiciário.
> § 3º As pessoas referidas no § 2º deste artigo deverão manter sob sigilo o material ilícito referido.
> Art. 241-C. Simular a participação de criança ou adolescente em cena de sexo explícito ou pornográfica por meio de adulteração, montagem ou modificação de fotografia, vídeo ou qualquer outra forma de representação visual:
> Pena – reclusão, de 1 (um) a 3 (três) anos, e multa.
> Parágrafo único. Incorre nas mesmas penas quem vende, expõe à venda, disponibiliza, distribui, publica ou divulga por qualquer meio, adquire, possui ou armazena o material produzido na forma do caput deste artigo

Importa mencionar que a aplicação ou não da legislação repressiva frente uma determinada conduta que, em tese, se encaixa nos moldes dos artigos acima mencionados, irá depender do local de hosteamento do servidor, do país no qual a conduta é praticada, da nacionalidade da vítima

etc. Isto pois, em certos países, não existe limitação a idade de consentimento ou até mesmo limites para consumação de ato de conjunção carnal.

Países que tenham a aplicação da sharia islâmica ou que culturalmente interpretem a maturidade sexual de maneira distinta, acabam sendo casos que devem ser vistos com cuidado quando se busca investigar e penalizar um suposto "pedófilo", eis que pelas normas de territorialidade da lei penal brasileira, somente se pune crimes cometidos por brasileiro no estrangeiro, se o fato for igualmente punível como crime no país em que foi praticado (dicção do art. 7, parágrafo 2, alínea B do CP).

Esta celeuma jurídica internacional será melhor tratada mais à frente, quando a respeito da discussão das dificuldades para se investigar e punir os cyber criminosos, tempo e local do crime, jurisdição e competência (ponto 3.2)

2.3.8 Racismo e preconceito

O crime de racismo, que não pode ser confundido com o crime de injúria racial (uma forma qualificada do crime de injúria), encontra tipificação legal no artigo 20 da lei 7.716/89, que estipula:

> Art. 20. Praticar, induzir ou incitar a discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional.
> Pena: reclusão de um a três anos e multa

Trata-se, portanto, da prática de indução e\ou citação a discriminação de indivíduos de um determinado grupo social em razão de sua cor de pele, credo professado, origem nacional etc. Deve, entretanto, ter sempre caráter de generalidade, ou seja, deve ser proferida contra um grupo de indivíduos e nunca contra uma pessoa tão somente. Dentre exemplos de segregação e preconceito, Matheus de Araújo Alves, citando Marcelo Crespo, irá citar toda e qualquer "condutas que impeçam acesso a lugares públicos, empregos, meios de transporte, clubes, bares, restaurantes, sempre por conta de

preconceito de raça, cor, etnia, religião ou procedência nacional"[72]. Assim sendo, no contexto das mídias digitais e dos meios de comunicação na internet, postagens em mídias sociais e participação em grupos promovedores de tais ideias podem, em tese, configurar o referido crime.

A dúvida aqui expressa se dá pela necessidade de avaliação do local da prática da conduta, onde os servidor esteja localizado etc. pois tal como no caso do crime de pornografia infantil vistos anteriormente, existem países cuja conduta acima descrita não configura fato típico.

2.4 Uma análise a respeito das "ações prejudiciais atípicas"

Quando tratamos da classificação dos delitos digitais, pudemos observar que a doutrina majoritária classifica estes fatos típicos subdividindo-os em crimes digitais\virtuais próprios e impróprios. Ocorre que por vezes, uma ação de cunho altamente negativa e moralmente\eticamente reprovável no cunho social, pode não ter sido suficientemente grave para que seja tipificada segundo a legislação repressiva vigente, como um delito informático.

Outra situação relativamente comum, é a de que estas ações simplesmente sequer tenham previsão legal como fatos típicos, e, portanto, segundo a teoria do crime, não podem ser consideradas como delitos puníveis pelo estado juiz. Outrossim, isto não quer dizer que tais atitudes e ações perpetradas não despertem repulsa e aversão no "seio social" e no imaginário popular, ou que não apresentem potencial lesivo, quer dizer tão somente, que estas "externalidades negativas" oriundas do convívio social, não podem ser passíveis de punição e persecução penal.

A este tipo de conduta, Wendt e Nogueira irão classificar, na esquemática de condutas criminosas do cyber espaço, como "ações

[72] CRESPO, 2011, p. 91 *apud* ARAUJO ALVES, 2020, p. 61.

prejudiciais atípicas". Nas palavras dos doutrinadores as referidas condutas são quelas:

> Praticadas por intermédio de dispositivos informáticos, que causam algum transtorno e\ou prejuízo para a vítima, porém não existe uma previsão penal, ou seja: O indivíduo causa algum problema para a vítima, mas não pode ser punido, no âmbito criminal, em razão da inexistência de norma penal com essa finalidade[73].

Entretanto, importa recordar que tais atitudes não impedem a atuação do judiciário em outras esferas de atuação, sendo por exemplo perfeitamente possível que a vítima de algum ato semelhante, busque reparação em âmbito cível por danos morais ou materiais que lhe foram causados. Conforme lecionam Wendt e Nogueira:

> O indivíduo que invade o computador de um conhecido sem o objetivo de obter, adulterar ou destruir dados ou informações não será indiciado nem preso, pois estes fatos não são criminosos, por não se adequarem ao art.154-A do código penal. Por outro lado, o causador do transtorno pode ser responsabilizado na esfera civil, como por exemplo, ser condenado a pagar indenização em virtude dos danos morais\materiais produzidos[74].

Algumas situações que seriam tipicamente entendidas como meras "ações prejudiciais atípicas" podem, em decorrência das atitudes tomadas pelos seus perpetradores, ou dos meios de linguagem\violência empregados contra a vítima, bem como a alteração do vínculo subjetivo do autor para com o objetivo do ato, evoluir para algum crime digital. Isto acaba ocorrendo com alguma frequência nos chamados "fenômenos de *cyberbullying* e *cyberstalking*".

Neste contexto, é erro comum do imaginário popular acreditar que a violência somente pode ser cometida por meios físicos. Existem modalidades distintas de violência que podem acabar ocorrendo, tais como a agressão moral, que por obvio, como visto anteriormente, é facilmente realizável por meios eletrônicos\cibernéticos, e é neste sentido que surge o fenômeno do *cyberbullying*.

---

[73] WENDT; NOGUEIRA JORGE, 2021, p. 15.
[74] WENDT; NOGUEIRA JORGE, 2021, p. 15.

Segundo a Dra. Fabiana F. Brotto, o conceito de *bullying* é:

> Uma prática violenta que pode compreender uma série de atitudes agressivas praticadas de forma repetitiva por um aluno ou grupo de alunos contra um estudante específico ou mesmo um grupo (...) para se constituir bullying, a atitude agressiva deve acontecer de forma repetitiva(...)[75].

Ainda segundo a expert, o bullying pode se apresentar de muitas formas, dentre eles o *bullying* físico, o *bullying* psicológico e o *cyberbullying*.

O *bullying* físico "não necessariamente inclui agressões que levam a machucados sérios, mas também pode caracterizar empurrões e beliscões, além de chutes, socos e tapas"[76], já o psicológico se caracteriza por "agressões como a intimidação por ameaça ou chantagem, até perseguições e manipulações"[77]. Já o *cyberbullying* acaba sendo a aplicação do *bullying* psicológico, porém praticado por intermédio de meios digitais e informáticos, conforme nos alerta a Dra. Brotto, este é potencialmente a forma mais lesiva e perigosa, em especial quando se trata de vítimas crianças, eis que, nas palavras da *expert*:

> Atinge a criança em locais onde ela costuma se sentir segura e protegida dos *bullies*: fora da escola, em casa, com os pais. Isso acontece porque por meio de um simples aparelho conectado à internet, como um smartphone, as mensagens violentas e agressivas chegam aonde a criança estiver[78].

Neste diapasão, conforme mencionamos acima, quando tratamos de agentes maiores e capazes, e cujas atitudes acabem por serem demasiado violentas ou tenham algum outro objetivo mais reprovável por de trás da ação, o *cyberbullying* pode, nas palavras de Wendt e Nogueira, romper "os limites da licitude" acabando por se enquadrar em alguma hipótese prevista como crime[79]. Segundo os prestigiados doutrinadores, as formas de delitos digitais (quer sejam eles próprios ou impróprios) mais comuns que acabem

---

[75] F. BROTTO, Thaiana. Bullying na escola: conheça os tipos e saiba como lidar. *Psicologo e Terapia*. Disponível em: https://www.psicologoeterapia.com.br/blog/bullying-na-escola-conheca-os-tipos-e-saiba-como-lidar/. Acesso em: 23 set. 2022.
[76] F. BROTTO., Acesso em: 23 set. 2022.
[77] Ibid., Acesso em: 23 set. 2022.
[78] Ibid., Acesso em: 23 set. 2022.
[79] WENDT; NOGUEIRA JORGE, 2021, p. 80.

decorrendo das ações mais estremadas de *cyberbullying* são: Os crimes contra a honra injúria, calunia, difamação (arts.140,138 e 139, respectivamente, do CP), a ameaça (art.147 do CP), o constrangimento ilegal (art.146 do CP), falsa identidade (art. 307 do CP), perseguição (art. 147-A do CP) e pôr fim à violência psicológica contra a mulher (art.147-B), muito embora importe ressaltar a forte divergência doutrinária enquanto a constitucionalidade desta última figura típica e os embates políticos e ideológicos que decorrem de sua polêmica recém incorporação no diploma repressivo, mas que fogem do escopo deste trabalho.

Uma novidade advinda em virtude de alteração do Art.122 do CP trouxe à tona a possibilidade de maior punição para os casos em que se estimule o suicídio e\ou a autolesão pelo meio digital. Isto pois, infelizmente, é demasiado comum que os perpetradores de cyberbullying estimulem suas vítimas para a prática de tais atos.

2.5 A *dark web*

Antes que se possa tratar das formas e de combate aos delitos digitais e os enormes e complexos desafios que as autoridades competentes costumam enfrentar, é necessária uma breve análise a respeito da chamada "*dark web*", local onde muitos dos cyber criminosos costumam operar, em especial para prática de delitos digitais mais sórdidos e reprováveis.

A internet como um todo nada mais é do que a junção de servidores que se encontram interconectados por meio de conexões via satélite ou fisicamente por meio de cabos de fibra ótica que circundam todos os continentes do globo. Conforme abordados em análise introdutória, este verdadeiro universo de dados, que coexiste de maneira simbiótica com o mundo real\físico, é espaço para os mais diversos fins, seja para a prática de atividades comerciais e profissionais, a divulgação científica e de ensino, o aprimoramento pessoal, a conexão interpessoal e criação de relacionamentos, bem como as mais diversas formas de entretenimento possíveis.

Ocorre que, tal qual o universo físico que se vincula, o mundo digital da internet também apresenta seu lado obscuro, escondidos dos "holofotes e luz solar" dos grandes serviços e algoritmos de busca, criminosos dos mais diversos perfis, tipos e origem social\nacional, cometem variados tipos de ilícitos. Se pudermos traçar paralelos entre o mundo físico e o mundo digital, enquanto a *web* como a maioria dos indivíduos a conhece seria a "rua bem iluminada do bairro central de uma cidade", a dark web é a "viela obscura do bairro afastado do centro urbano, onde a criminalidade impera sob a ausência dos olhos vigilantes do Estado".

Importa mencionar que a internet como um todo se subdivide em duas grandes "camadas de dados":

A) Surface web (web de superfície): É aquela onde a maior parte dos usuários trafegam em seu dia a dia de atividades virtuais, é acessável por todas as grandes *engines* de pesquisa (também chamados de 'motores de busca') e navegadores comuns, tais como o '*google'*, o '*bing*', o '*mozila firefox*', a atualmente extinta '*internet explorer*', o '*opera*', dentre outros. Por meio destes motores de busca, se é possível a qualquer indivíduo, que conheça o endereço completo do domínio do site que se pretenda acessar, possa ter acesso ao referido site. Os portais de serviços governamentais abertos ao público, os aplicativos de produtos e serviços privados, sites de relacionamento mais populares etc. se concentram em sua esmagadora maioria nesta 'camada' da internet.

B) Deep web (web profunda): É aquela onde um gigantesco fluxo de dados (alguns autores costumam citar ser até 10 vezes maior que a quantidade de dados da web de superfície) transitam, de maneira sigilosa, sorrateira e de difícil acesso aos indivíduos que não possuam conhecimentos específicos ou saibam de sua existência para acessá-los, razão pela qual muitos estudiosos no tema a chamam de 'internet não indexável'. Sites e serviços que estejam *hosteados* em servidores vinculados a deep web somente pode ser acessados por meio de motores de busca especializados (tais como a *engine tor*), capazes de realizar decifrações matemáticas complexas que mascaram os nomes de domínio dos sites que operam na deep web.

A deep web em si não é necessariamente a área de prática de delitos virtuais, muitas vezes é apenas e tão somente um setor do universo digital (internet) que possibilita o *hosteio* de serviços específicos tais como sites governamentais de acesso restrito, serviços de comunicação militares, e até mesmo sites de produtos e serviços que, em razão da complexidade de sua execução, especificidades próprias ou raridade\sensibilidade dos bens ofertados, se veem forcadas a operar de maneira discreta e servindo tão

somente clientes mais “seletos” que já conhecem previamente da existência daquele produto e\ou serviço (exemplo: Sites para compra e venda de minério de urânio empobrecido, leilões para compra e venda de armamentos e serviços de segurança, instrumentos musicais e obras de arte raríssimas etc.).

O grande problema se dá quando, em razão da grande anonimidade e segurança oferecida pela deep web, cyber criminosos se aproveitam para realizar seus ilícitos ou ofertar seus serviços a quem queira. Neste contexto, teremos a existência da temida *dark web*, que, portanto, nada mais é do que a coletânea de todos os sites e hosts nos quais se pratiquem ou visem praticar os mais variados tipos de cyber crimes, desde os menos graves como violações de direitos autorais (como a distribuição não autorizada de livros, músicas, propriedade industrial etc.) aos mais repulsivos como a prática de venda ilegal de órgãos, tráfico internacional de pessoas\drogas\armas, bem como a existência de sites de organizações terroristas e grupos de extermínio, *chats* de promoção e divulgação de pornografia infantil, serviços de *hacking*, assassinatos de aluguel etc.

Portanto, compreende-se a dark web como sendo um setor específico da deep web, que por sua vez, trata-se de uma das duas grandes “camadas de dados” que se encontram disponibilizadas no mundo digital (internet), com variações de graus de dificuldade para acesso de seus respectivos conteúdo.

CAPÍTULO 3 - COMPETÊNCIAS PROCESSUAIS E INVESTIGATIVAS DOS ENTES ESTATAIS PARA ANÁLISE DE ATOS TÍPICOS PRATICADOS NO MUNDO VIRTUAL, SEGUNDO O ORDENAMENTO JURÍDICO PÁTRIO E LEGISLAÇÃO INTERNACIONAL

3.1 As dificuldades para se investigar e punir os cyber criminosos

Como pudemos observar, a expansão das fronteiras do mundo digital e o desenvolvimento tecnológico trouxe novos paradigmas para a sociedade moderna, e no contexto da criminalidade e segurança pública, não poderia ser diferente. O fenômeno dos crimes digitais apesar de ser algo relativamente recente na história e consequentemente do direito penal (sendo o direito um reflexo da sociedade que regula), encontra-se lamentavelmente em flagrante expansão. Por este motivo, as diversas legislaturas dos países que compõem a comunidade internacional vêm se debruçando cada vez mais em criar mecanismos que deem amparo legal as forças de segurança e ao poder judiciário de forma que seja possível uma maior eficácia na prevenção e repreensão dos delitos informáticos.

Entretanto, estas ações depreendem enorme esforço e junção de conhecimentos tanto da área jurídica como da ciência da computação, que podem estar sujeitas a críticas (quer seja em âmbito acadêmico ou profissional). Ressalta-se ainda que muitas vezes, tais “inovações legais” acabam sendo ineficazes para corrigir aquilo que se propunham, em razão da demasiada demora oriunda da burocracia estatal e das complexidades vinculadas a atuação e interesses de atores políticos no âmbito legislativo.

Neste sentido, trazemos alguns dos principais pontos que os professores Wendt e Nogueira apontam e que revelam a enorme dificuldade e desafio no qual o poder público se depara quando se trata do combate e repressão aos ilícitos cibernéticos.

3.1.1 Ausência de legislação mais específica

Muito embora seja possível enquadrar quase todos os tipos de atos prejudiciais realizados no mundo virtual, muitos deles continuam sem previsão normativa e tipificação. Tais exemplos foram tratados no capítulo dois, especificamente no ponto 2.4, quando abordamos as ações prejudiciais atípicas. Wendt e Nogueira citam em sua obra[80], o exemplo da chamada "Lei Azeredo", que apesar do nome, teve como elaborador da proposta original o então deputado federal Luís Piauhylino.

Tal inovação legislativa foi apresentada ao legislativo federal como proposta de lei em 1999 sob o número PL 84 e trazia em seu escopo mecanismos jurídico-processuais bem como operacionais de forma a oferecer as autoridades competentes, condições mais adequadas para a investigação, repreensão e prevenção de delitos informáticos.

A proposta de lei então passou pelos devidos tramites legais, sendo por fim aprovada e sancionada em 30 de novembro de 2012 se tornando então a Lei n 12.735\12. Ocorre que em razão de pressões de natureza estritamente políticas, o texto da PL foi severamente alterado e seus mecanismos restringidos de maneira que, como bem apontam os doutrinadores anteriormente mencionados, tinham apenas e tão somente 2 artigos em seu escopo, sendo um deles relacionado a melhor estruturação das policias civis estaduais e a polícia federal para repreensão e investigação de crimes virtuais, ficando o outro artigo responsável por estipular que o poder judiciário pudesse, ouvidos o *parquet*, determinar a cessação de transmissões radiofônicas, televisivas e eletrônicas em caso de prática de crime de racismo por tais meios. Por tais razões, os doutrinadores irão entender que a "lei Azeredo" teria sido absolutamente "defenestrada pelo nosso legislador pátrio"[81].

[80] WENDT; NOGUEIRA JORGE, 2021, p. 197.
[81] Ibid., p. 197.

Em sentido contrário, Thalyta França Evangelista irá afirmar que, muito embora a "lei Azeredo" tenha tido, em seu cerne e objetivo, a repressão e combate aos criminosos virtuais, a maneira como esta foi originalmente estruturada bem como os poderes que conferia aos órgãos de investigação e repressão estatais acabariam por fim na violação da liberdade de expressão e a intimidade. A doutrinadora vai mais a fundo e compara o texto originariamente proposto como um "novo AI-5", em referência a histórica emenda institucional incorporada na antiga constituição de 1967 ao qual restringia muitos dos direitos e garantias fundamentais previstos naquela magna carta[82] ().

Ainda sobre a temática de legislações inadequadas, o professor Wendt e o professor Nogueira irão citar as penas demasiado brandas destes ilícitos digitais. Para tal, citam como exemplo a lei n 12.737, popularmente conhecida como "lei Carolina Dieckmann", uma vez que a iniciativa para sua elaboração se deu em razão do clamor popular pela divulgação de fotos íntimas da celebrada atriz. Os doutrinadores, citando a análise crítica de Renato Opice Blum, concluem que as penas previstas na referida inovação legislativa seriam "exacerbadamente brandas"[83].

Por outro lado, os professores elogiam as iniciativas dos legisladores em se aprofundarem mais sobre o tema e buscarem fornecer meios e procedimentos de forma a combater os cyber criminosos. Citam como exemplos destas iniciativas positivas a lei 11.829\08 que alterou o ECA criando figuras típicas para reprimenda de pornografia infantil, como o art.241-B. Citam ainda as leis 13.718 e 13.722, ambas do ano de 2018, que introduzem ao código repressivo os arts.16-B e 218-C, respectivamente, que tratam de tipificar a divulgação não consentida da intimidade.

Ainda trazem à tona as alterações trazidas pela nova redação do art.122 do CP trazendo atenção ao incentivo a suicídio e autolesão, a

[82] EVANGELISTA, 2020, p. 66.
[83] WENDT; NOGUEIRA JORGE, 2021, p. 198.

tipificação da conduta de stalking por meio do art.147-A. Por fim, elogiam a *novatio legis* advinda com a lei n 14.155\21, que não só alterou e corrigiu problemas relativos ao art.154-A, acrescenta também parágrafos nos art. 155 e 171 do CP, criando as qualificadoras de "furto mediante fraude" e "estelionato eletrônico", respectivamente[84].

3.1.2 Falta de capacitação dos agentes policiais e outros atores da persecução penal

Conforme nos aponta Wendt e Nogueira, é público e notório que persiste em nossa sociedade uma falta de "educação digital do usuário da internet". A ausência de conhecimentos específicos, em especificamente aspectos da segurança dos meios informáticos (segurança da informação), por boa parte se não a maioria dos atuais usuários destes meios, torna o universo digital um meio próspero para que cyber criminosos possam atuar e tirar vantagens ilícitas de suas vítimas. Por este motivo, os doutrinadores irão alertar que:

> A falta de capacitação dos policiais e de outros atores da persecução penal, como o Ministério público e o judiciário, representam um grande desafio, na medida em que pode impedir a punição dos cyber criminosos e, por consequência, causar impunidade[85].

Neste diapasão, entendemos que a capacitação de agentes bem como a contínua criação e aperfeiçoamento de divisões especializadas dentro dos órgãos de persecução, assim como a correta distribuição de recursos e disponibilização dos meios adequados ao seu funcionamento e operacionalidade, são obrigações aos quais os agentes políticos não podem se desincumbir, sob pena de descumprir estipulações normativas por eles mesmos criadas, com o objetivo de combater a prática dos delitos digitais. Nas palavras dos professores Wendt e Nogueira:

---

[84] WENDT; NOGUEIRA JORGE, 2021, p. 199.
[85] Ibid., p. 199.

> (...) espera-se que com a Lei n 12.735/12, possam os órgãos policiais se adequar às exigências sociais de investigação eficaz dos crimes cibernéticos, especialmente em razão da pulverização da Internet e uso cada vez maior, principalmente o provocado pela pandemia do coronavírus. A instalação de delegacias e/ou laboratórios de inteligência cibernética nos estados é fundamental para o atendimento a essa demanda[86].

3.1.3 Colaboração e integração entre cyber criminosos de várias localidades

Em razão da própria natureza interconectada da *web*, é tão somente natural que criminosos e malfeitores ao redor de todo o planeta possam, ainda que não estabeleçam contato físico uns com os outros, elaborar, planejar e executar os mais diversos delitos. Como nos alerta Wendt e Nogueira:

> Os recursos tecnológicos permitem que cyber criminosos, espalhados por diversas localidades, comuniquem-se e realizem ações criminosas em parceria e organizadamente[87].

Organizações criminosas e seus agentes podem e irão atuar neste ambiente, cientes e motivadas pelas dificuldades enfrentadas pelos órgãos de segurança pública e da interconectividade acima mencionada, para instruir seus operadores em diversas regiões do planeta a praticar atos ilícitos. *Hackers* especializados podem se juntar em grupos de "justiceiros sociais" para a prática de "banditismo social", bem como serem contactados e contratados por grandes empresas cujos diretores inescrupulosos desejem contratar serviços de lavagem internacional e/ou evasão de divisas com uso de cripto moedas não lastreáveis/rastreáveis. Círculos de extremistas e terroristas podem espalhar suas ideologias e princípios em sites de suas organizações etc.

Como se vê, os investigadores não têm uma tarefa fácil, devendo enfrentar um verdadeiro "exército" de delinquentes, dos mais variados tipos, porém muitas vezes interconectados e interessados no fracasso, humilhação e desmoralização dos órgãos fiscalizatórios e punitivos do Estado, pois ao

[86] WENDT; NOGUEIRA JORGE, 2021, p. 200.
[87] Ibid., p. 200.

manterem a “espada” das autoridades longe do domínio virtual, estes estão garantindo que o *status quo* do sistema de “vale tudo” permaneça vigente no mundo virtual[88].

3.1.4 Falta de diálogo entre os órgãos que realizam a investigação criminal

Sob a falta de integração entre os órgãos púbicos com competência investigativa e repressiva aos delitos digitais, os professores Wendt e Nogueira afirmam ser:

> Voz uníssona entre os órgãos que promovem a investigação de crimes praticados pela internet que, diferentemente dos criminosos, não existe uma atuação integrada entre os responsáveis pela persecução penal, mesmo aqueles pertencentes ao mesmo setor[89].

A falta de estabelecimento de uma doutrina operacional padrão, dificulta consideravelmente a integração, esta praticamente inexistente, entre os agentes estatais legitimados para investigar os delinquentes digitais. Cabe ainda destacar que a competição entre os órgãos por recursos, bem como o eventuais conflitos de competência, seja esta positiva ou negativa, afeta de sobremaneira a eficiência e eficácia da luta do Estado frente a criminalidade informática.

3.2 Tempo e local do crime

A definição do tempo e local da prática de um ilícito é fundamental para determinação de questões de extrema importância para o processo penal e direito penal como um todo, questões como incidência ou não da legislação penal brasileira, a definição de competência entre os órgãos da persecução penal, o tempo de prescrição da pretensão punitiva etc.

---

[88] WENDT; NOGUEIRA JORGE, 2021, p. 200.
[89] Ibid., p. 200.

Neste sentido, o que todo operador do direito deve se perguntar e analisar quando se esta diante de uma cena de crime é:

A) Onde o ilícito foi cometido:

Esta questão é fundamental para que se possa definir se a legislação pátria é aplicável ao caso concreto, isto pois o código penal em seu arts. 6 e 7 irá definir o conceito de "lugar do crime" e as regras relativas à extraterritorialidade penal, respectivamente.

> Lugar do crime
> Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado
> E
> Extraterritorialidade
> Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro: (
> I - os crimes:
> a) contra a vida ou a liberdade do Presidente da República;
> b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público;
> c) contra a administração pública, por quem está a seu serviço;
> d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil;
> II - os crimes:
> a) que, por tratado ou convenção, o Brasil se obrigou a reprimir;
> b) praticados por brasileiro;
> c) praticados em aeronaves ou embarcações brasileiras, mercantes ou de propriedade privada, quando em território estrangeiro e aí não sejam julgados.
> § 1º - Nos casos do inciso I, o agente é punido segundo a lei brasileira, ainda que absolvido ou condenado no estrangeiro.
> § 2º - Nos casos do inciso II, a aplicação da lei brasileira depende do concurso das seguintes condições:
> a) entrar o agente no território nacional;
> b) ser o fato punível também no país em que foi praticado;
> c) estar o crime incluído entre aqueles pelos quais a lei brasileira autoriza a extradição;
> d) não ter sido o agente absolvido no estrangeiro ou não ter aí cumprido a pena;
> e) não ter sido o agente perdoado no estrangeiro ou, por outro motivo, não estar extinta a punibilidade, segundo a lei mais favorável.
> § 3º - A lei brasileira aplica-se também ao crime cometido por estrangeiro contra brasileiro fora do Brasil, se, reunidas as condições previstas no parágrafo anterior:
> a) não foi pedida ou foi negada a extradição;
> b) houve requisição do Ministro da Justiça.

Portanto, conforme se extrai da dicção dos artigos acima listados do diploma repressivo, é de fundamental importância que se estabeleça o lugar onde o crime se deu, pois a depender da situação enfrentada no caso concreto,

sequer teremos que falar na prática de crime, eis que não aplicável a legislação pátria.

B) Tempo no qual o crime foi cometido

Aqui trata-se de questão fundamental para a o ordenamento penal brasileiro, em especial seus dois pilares mais sagrados: A segurança jurídica, vez que deve-se prever aos indivíduos a segurança trazida pela figura da prescrição e decadência, bem como ao Estado juiz o estímulo de fazer valer a lei de maneira eficiente e o Estado de Direito, que na esfera penal se concretiza por meio da garantia ao contraditório e a ampla defesa que caracterizando o sistema acusatório contemplado pela constituição de 1988.

Como exemplos da aplicação destes relevantes institutos jurídicos em nossa legislação repressiva, podemos citar o art. 4 do título I, o art.103 do título VII bem como todos os artigos relativos à extinção da punibilidade previstos no título VIII, notadamente os arts. 107, 109, 110, 111, 112, 115 e 117. Todos do CP.

Neste diapasão, conforme nos alerta o doutrinador Matheus de Araújo Alves, dentre as diversas teorias que buscam estabelecer o momento em que um delito é praticado, o código penal brasileiro adotou em seu art.4 a chamada "teoria da ação ou da atividade"[90].

In verbis:

> Tempo do crime
> Art. 4º - Considera-se praticado o crime no momento da ação ou omissão, ainda que outro seja o momento do resultado.

Ou seja, caso uma conduta seja praticada em um dado momento histórico onde esta conduta era lícita, seu resultado não poderia ser punível, se este viesse a ocorrer em momento histórico distinto no qual a conduta fosse então tipificada. Evitando-se assim, a violação a máxima estipulada pelo art. 5, inciso XL: "a lei penal não retroagirá, salvo para beneficiar o réu".

[90] ARAUJO ALVES, 2020, p. 66.

O doutrinador explica ainda que, nos casos dos delitos informáticos, a observação das regras acima descritas é extremamente importante, pois por muitas vezes:

> O período de tempo entre a ação e o resultado é relativamente grande (...) na já citada conduta de inserção de *malware*, por exemplo, a inserção de código malicioso ou sabotagem de um dispositivo informático alheio pode gerar resultados apenas tempos depois dessa inserção, quando o usuário acessar determinada página ou abrir um arquivo fechado[91].

No que tange ao local do cometimento do crime, como visto anteriormente, o art. 6 do código repressivo adota a teoria da ubiquidade, também chamada por alguns de unitária ou mista, ao dizer que "praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir o resultado"[92].

De tal maneira, se previne que ocorram conflitos de jurisdição e, conforme informa Matheus de Araújo Alves: "Soluciona-se a questão do crime a distância, em qua a ação e o resultado realizam-se em lugares distintos"[93]. Ainda segundo o autor, citando o renomado professor Bittencourt: "Caso haja uma eventual duplicidade de julgamento, esta é superada pela regra presente do art. 8 do mesmo código, que estabelece a compensação de penas, como modalidade especial de detração penal"[94].

Dessa forma, trazendo um exemplo aplicável da legislação pátria a um caso de delito digital praticado em país distinto da vítima, tal como um hacker que na índia viola dispositivo informático de brasileiro, basta aplicarmos as regras estabelecidas pelos artigos acima mencionados de maneira a facilmente estabelecer as regras de competência para se fazer processar e julgar o malfeitor, evidentemente desde que em ambos os mencionados países tal ato seja tipificado penalmente.

---

[91] ARAUJO ALVES, 2020, p. 67.
[92] BRASIL. Decreto-Lei n 2.848, de 07 de dezembro de 1940. *Código Penal*. 1940.
[93] ARAUJO ALVES, *op. cit.*, p. 67.
[94] BITENCOURT, 2017, p. 254 *apud* ARAUJO ALVES, 2020, p. 67.

O problema entretanto se dá quando a severidade da legislação de um país frente aos atos praticados não encontre paralelos com a do Brasil. Matheus de Araújo Alves, citando um exemplo levantado pelo professor Renato Leite Monteiro, onde um e-mail contendo artefato malicioso é enviado, por um *cyber criminoso,* de um país "X" para vários destinatários, cada qual em uma nação soberana distinta, irá dizer que: "atos foram praticados em diversos locais com resultados que puderem ser percebidos em diferentes jurisdições"[95].

Neste tipo de situação altamente complexa e delicada, o doutrinador entende que não há critério específicos que definam o local da prática do delito e nem o local onde este se consumiu, vez que "várias teorias são adotadas por diferentes países, e cada um tem competência para determinar se tem ou não autoridade para processar o delito em seu território"[96].

Importa mencionar que tal opinião não chega sequer próxima de ser unanime, pois como aponta o mesmo doutrinador logo em seguida, outros grandes juristas de renome como Túlio Lima Vianna irão defender que as normas penais sempre devem ser interpretadas de forma restritiva. Neste sentido, "caso haja duas interpretações possíveis e perfeitamente lógicas para um mesmo fato jurídico, o intérprete tem o dever de optar por aquela que menos restringir a liberdade do cidadão"[97].

Na esteira deste raciocínio, o doutrinador irá adotar a mesma visão que o professor Vianna sobre o assunto, pois conclui que a interpretação do art. 6 não permitiria outro sentido de compreensão, vez que há clara adoção da teoria da ubiquidade e assim sendo, só será crime aquele ato assim tipificado tanto no local da conduta como no local onde se produziu o resultado. Dessa forma, somente seria possível a responsabilização penal de um agente, pela justiça brasileira, caso tanto a legislação nacional como a estrangeira tenham

[95] MONTEIRO, 2010, p. 48 *apud* ARAUJO ALVES, 2020, p. 68.
[96] Ibid., p. 68.
[97] VIANNA, 2001, p. 100 *apud* ARAUJO ALVES, 2020, p. 69.

a conduta por este praticada, tipificada penalmente, caso contrário se estaria tratando de "ofensa direta ao princípio da legalidade"[98].

Conforme conclui De Araújo Alves, baseando-se nos ensinamentos de Vianna, quando em análise da limitação do poder punitivo estatal e aplicação do princípio da *ultima ratio*:

> Para as condutas praticadas no Brasil, que são tipificadas no ordenamento jurídico brasileiro, mas que produzem resultados em países onde não são consideradas ilícitas, também se aplica o princípio da exclusiva proteção a bens jurídicos. Caso um Estado soberano entenda que a proteção a determinado bem jurídico não seja necessária, o Brasil não pode querer protegê-lo, quando o resultado ocorra nas fronteiras desse país, sob pena de violação do art. 4, inciso III, da constituição da República Federativa do Brasil[99].

3.3 jurisdição e competência para investigação, combate e julgamento de delitos informáticos

Nas palavras de Matheus de Araújo Alves, a internet "por sua essência não possui fronteiras e assim foi projetada para que fosse acessada de qualquer parte do mundo"[100]. De fato, todo o sistema e modelo pelo qual a *web* se estrutura atualmente tem por objetivo tornar possível, para qualquer indivíduo no planeta, o acesso a rede mundial de computadores, independentemente do seu local de acesso.

Por este mesmo motivo, como visto em capítulo anterior, um determinado conteúdo ou ação pode ser tipificado como um delito em um país "A" enquanto a mesma seja perfeitamente legal em "B". Por este motivo, a doutrina e a jurisprudência em sua maioria identificam que existe forte caráter de "transnacionalidade" nos crimes digitais, devido às fortes probabilidades de que o delito seja cometido em mais de um país (quer seja pelo fato dos sujeitos ativo e passivo se localizarem em nações distintas, quer seja pelo fato dos meios empregados envolverem servidores e prestadores de serviços sem representatividade no solo pátrio).

---

[98] VIANNA, 2001, p. 100 *apud* ARAUJO ALVES, 2020, p. 69.
[99] Ibid., p. 69.
[100] ARAUJO ALVES, 2020, p. 70.

É fundamental que se compreenda que apesar da internet aparentar ser uma “rede imaterial” onde ocorre a transmissão de bits e dados de informação, para que a mesma possa funcionar, se faz -se necessária lançar mão de uma complexa infraestrutura de cabos que cortam leitos submarinos, provedores de comunicação, frotas de satélites em baixa orbita terrestre e\ou orbita geoestacionária e, obviamente, servidores físicos onde todas estas informações são armazenadas para distribuição e acesso dos consumidores. Portanto, para que um indivíduo possa acessar a *web*, este precisa ter acesso a servidores de conexão de rede, que “atribuem ao usuário um número IP (internet protocol) utilizado para ingresso no cyber espaço” (...) “estrutura disponibilizada pelos provedores que, a partir de então, passam a deter as informações referentes aos passos que o usuário percorreu na rede, como histórico de navegação, postagens e comunicações”[101].

São, portanto, tais informações as quais os provedores de internet têm sob seu domínio que irá permitir aos agentes e autoridades competentes que possibilita descobrir os criminosos por trás de operações ilícitas na web. Ocorre que, por vezes, tais provedores não possuem representação no Brasil ou então em que pese terem representação jurídica em solo nacional, o mesmo não pode ser dito de seus servidores que podem encontrar-se espalhados ao redor do planeta. Torna-se evidente portanto a enorme dificuldade para que se possa estabelecer qual nação teria a competência (e também a possibilidade\interesse legal) de ordenar a entrega destes dados.

Matheus de Araújo Alves, citando La Chapelle e Fehlinger, irá dizer que para este tipo de “nó górdio” existem quatro saídas jurídicas válidas, porém cada qual com suas devidas limitações e problemas, são estas a aplicação:

> (...) da lei local em que está o usuário, do qual se pretende obter os dados; a lei do local onde estão os servidores que armazenam os dados; a lei do local de

[101] DOMINGOS RODER, 2017, p. 62 *apud* ARAUJO ALVES, 2020, p. 71.

> incorporação da empresa que presta o serviço; e a lei do local dos registros de onde o domínio foi registrado[102].

Como resultado, o doutrinador, citando Domingos e Roder irá dizer que:

> Todos os critérios apresentados por La Chapelle e Fehlinger, ao assumirem que, para o fornecimento de dados digitais, as empresas provedoras de internet devem obedecer aos parâmetros legais de variadas jurisdições do local onde os fatos ocorreram ou tiveram o serviço prestado, acarretam a necessidade de pedidos de cooperação jurídica internacional[103].

3.3.1 Competência segundo o ordenamento jurídico nacional.

Matheus de Araújo Alves, citando as lições do professor Túlio Lima Vianna irá dizer que ao se falar em jurisdição se está falando de "expressão da soberania de um Estado. Poder este que é único, mas em sua aplicação, por uma questão de ordem prática, repartida entre vários órgãos do corpo estatal"[104].

O professor Mirabete e Fabbrini definem jurisdição e competência da seguinte forma:

> Como poder soberano do Estado, a jurisdição é uma e, investido do poder de julgar, o juiz exerce a atividade jurisdicional. Sendo evidente, porém, que um juiz não pode julgar todas as causas e que a jurisdição não poder ser exercida ilimitadamente por qualquer juiz, o poder de julgar é distribuído por lei entre os vários órgãos do Poder Judiciário, através da competência. A competência, é assim, a medida e o limite da jurisdição[105].

Matheus de Araújo Alves, inspirando-se nas lições do professor Túlio Vianna irá definir competência como sendo, portanto, o "limite do poder de cada órgão jurisdicional" (...) "a distribuição dos poderes jurisdicionais do Estado se dá de acordo com a natureza do crime praticado, com a qualidade

---

[102] LA CHAPELLE FEHLINGER, 2016 *apud* ARAUJO ALVES, 2020, p. 72.
[103] DOMINGOS; RODER, 2017, p. 66 *apud* ARAUJO ALVES, 2020, p. 73.
[104] ARAUJO ALVES, 2020, p. 70.
[105] MIRABETE, Júlio Fabbrini; FABBRINI, Renato N. *Código Penal interpretado*. 9. ed. São Paulo: Atlas, 2015. p. 136.

das pessoas incriminadas e com o local em que o delito foi praticado ou se consumou, ou ainda o local da residência de seu ator"[106].

O que se percebe é que, no contexto dos crimes virtuais, a fixação da competência em razão da matéria e em razão do local do delito são as fundamentalmente mais importantes formas de definição de competência processual para investigação, combate, julgamento e prevenção destes tipos de crime.

O mesmo doutrinador, ao tratar sobre o tema da competência para processar e julgar os delitos informáticos, irá dizer que a justiça federal sempre se fará competente para tal, isto pois segundo o autor, a constituição da república, definiu por meio do seu art. 109, inciso IV, a competência dos juízes federais em razão da matéria, ou seja, da natureza dos delitos praticados[107].

> Art. 109. Aos juízes federais compete processar e julgar:
> IV - os crimes políticos e as infrações penais praticadas em detrimento de bens, serviços ou interesse da União ou de suas entidades autárquicas ou empresas públicas, excluídas as contravenções e ressalvada a competência da Justiça Militar e da Justiça Eleitoral.

Neste sentido, o doutrinador, citando Vianna, propõe o entendimento de que a internet, ao se tratar de serviço público de telecomunicação, fica sujeita a regulamentação da ANATEL (autarquia especial\reguladora, vinculada a administração pública indireta), o que criaria, na visão destes autores, "incontestável interesse da União em protegê-la juridicamente. Desta forma, os processos relativos à intrusão informática, quando praticadas através da internet, deverão ser conhecidos e julgados pela justiça federal"[108].

Por outro lado, o autor alerta que isto não quer dizer que a justiça estadual comum não possa atuar no julgamento de causas que envolvam delitos informáticos, eis que "caso o agente não se utilize da internet (...) a

---

[106] VIANNA, 2001, p. 102 *apud* ARAUJO ALVES, 2020, p. 70.
[107] ARAUJO ALVES, 2020, p. 73.
[108] VIANNA, 2001, p. 102-103 *apud* ARAUJO ALVES, 2020, p. 74.

competência passa a ser da justiça comum"[109], entretanto a maior parte da doutrina entende que o fato do delito ter sido praticado pela internet não bastaria para justificar a competência da justiça federal, devendo para tanto ficar caracterizada a natureza de transnacionalidade do delito e que este seja tipificado como tal pela legislação repressiva, seja por força de lei ou tratado\convenção internacional do qual o Brasil tenha ratificado.

Nas palavras de Thalyta Evangelista, citando Barros:

> Se não existe convenção\tratado internacional, o delito será de competência da Justiça Estadual, mesmo possuindo dispositivo para originar resultados em outro país. Tomamos por exemplo, uma pessoa que calunia outrem em sua página virtual, esta calunia pode ser vista por qualquer indivíduo, em todo lugar do mundo. Portanto, como não existe uma convenção\tratado internacional no qual o Brasil possua vínculo para poder cessar esse crime, não será designada a competência da justiça federal' (...) 'de outro modo, mesmo que persista convenção internacional\tratado que defina a repressão do delito, se não houver a transnacionalidade do crime, também não transcorrerá a competência da Justiça federal. Ilustrando: O sujeito A envia, através de e-mail, imagens com teor de pornografia infantil para o sujeito B, os dois encontram-se no Brasil[110].

De toda sorte, a competência da justiça comum se verifica em todos os delitos informáticos em que a internet não é o meio utilizado para sua prática ou em sendo, não se verifique a transnacionalidade do delito e que o ato seja tipificado penalmente pela legislação pátria. Há de se convir entretanto, que tais limitações tornam, na prática, a competência da justiça estadual comum para processar e julgar os crimes digitais em algo altamente residual, haja vista a própria natureza da infraestrutura da *web*, onde ao menos em relação a característica de transnacionalidade do delito se faz presente na imensa maioria dos casos, seja em razão da infraestrutura (o servidor utilizado se encontram em território estrangeiro e\ou a empresa prestadora do serviço não possui representação jurídica no Brasil), ou de natureza prática (a ação ou o resultado do ato não se dá dentro do território nacional e\ou atingem um nacional brasileiro).

Neste sentido entendeu o STJ:

---

[109] KUROKAWA et al., 2006, p. 41 *apud* ARAUJO ALVES, 2020, p. 74.
[110] BARROS, 2013 *apud* EVANGELISTA, 2020, p. 92-93.

PROCESSUAL PENAL. CONFLITO DE COMPETÊNCIA. CRIME PREVISTO NO ART.
241, CAPUT, E § 1º, II, DA LEI 8.069/90 (NA REDAÇÃO ANTERIOR À DA LEI 11.829/2008). CONVENÇÃO SOBRE OS DIREITOS DA CRIANÇA, SUBSCRITA PELO BRASIL. INEXISTÊNCIA DE TRANSNACIONALIDADE DO CRIME DE CAPTAÇÃO E ARMAZENAMENTO, EM COMPUTADORES DE ESCOLAS MUNICIPAIS, DE VÍDEOS DE CONTEÚDO PORNOGRÁFICO DE CRIANÇAS E ADOLESCENTES, ADVINDOS DA REDE INTERNACIONAL DE COMPUTADORES (INTERNET). COMPETÊNCIA DA JUSTIÇA ESTADUAL.
I. O art. 109, V, da Constituição Federal estabelece que compete aos Juízes Federais processar e julgar 'os crimes previstos em tratado ou convenção internacional, quando, iniciada a execução no País, o resultado tenha ou devesse ter ocorrido no estrangeiro, ou reciprocamente'.
II. Para fixar a competência da Justiça Federal, não basta o Brasil ser signatário de tratado ou convenção internacional que prevê o combate a atividades criminosas relacionadas a pedofilia, inclusive por meio da Internet. O crime há de se consumar com a publicação ou divulgação, ou quaisquer outras ações previstas no tipo penal do art. 241, caput e §§ 1º e 2º, da Lei 8.069/90, na rede mundial de computadores (Internet), de fotografias ou vídeos de pornografia infantil, dando o agente causa ao resultado da publicação, legalmente vedada, dentro e fora dos limites do território nacional.
Precedentes do STF e do STJ.
III. Na hipótese dos autos, e pelo que se apurou, até o presente momento, o material de conteúdo pornográfico, em análise no apuratório, não ultrapassou os limites dos estabelecimentos escolares, nem tampouco as fronteiras do Estado brasileiro.
IV. Não obstante a origem do material em questão seja, em tese, advinda da Internet, a conduta que se pretende apurar consiste no download realizado, pelo investigado, e na armazenagem de vídeos, em computadores de escolas municipais - o que se amolda ao crime previsto no art. 241, § 1°, II, da Lei 8.069/90, cuja redação, vigente ao tempo dos fatos, é anterior a Lei 11.829/2008 -, inexistindo, por ora, como destacou o Ministério Público Federal, indícios de que o investigado tenha divulgado ou publicado o material pornográfico além das fronteiras nacionais.
V. Assim, não estando evidenciada a transnacionalidade do delito - tendo em vista que a conduta do investigado, a ser apurada, restringe-se, até agora, à captação e ao armazenamento de vídeos, de conteúdo pornográfico, ou de cenas de sexo explícito, envolvendo crianças e adolescentes, nos computadores de duas escolas -, a competência, in casu, é da Justiça Estadual.
VI. Conflito conhecido, para declarar a competência do Juízo de Direito da Vara de Crimes contra Criança e Adolescente da Comarca de Curitiba/PR, o suscitante.
(CC 103.011/PR, Rel. Ministra ASSUSETE MAGALHÃES, TERCEIRA SEÇÃO, julgado em 13/03/2013, DJe 22/03/2013)
E
CONFLITO NEGATIVO DE COMPETÊNCIA. CRIME DE INJÚRIA PRATICADO POR MEIO DA INTERNET, NAS REDES SOCIAIS DENOMINADAS ORKUT E TWITTER. AUSÊNCIA DAS HIPÓTESES DO ART. 109, INCISOS IV E V, DA CF. OFENSAS DE CARÁTER EXCLUSIVAMENTE PESSOAL. COMPETÊNCIA DA JUSTIÇA ESTADUAL.
1 - O simples fato de o suposto delito ter sido cometido por meio da rede mundial de computadores, ainda que em páginas eletrônicas internacionais, tais como as redes sociais 'Orkut' e 'Twitter', não atrai, por si só, a competência da Justiça Federal.
2 - É preciso que o crime ofenda a bens, serviços ou interesses da União ou esteja previsto em tratado ou convenção internacional em que o Brasil se comprometeu a

> combater, como por exemplo, mensagens que veiculassem pornografia infantil, racismo, xenofobia, dentre outros, conforme preceitua o art. 109, incisos IV e V, da Constituição Federal.
> 3 - Verificando-se que as ofensas possuem caráter exclusivamente pessoal, as quais foram praticadas pela ex-namorada da vítima, não se subsumindo, portanto, a ação delituosa a nenhuma das hipóteses do dispositivo constitucional, a competência para processar e julgar o feito será da Justiça Estadual.
> 4 - Conflito conhecido para declarar a competência do Juízo de Direito do Juizado Especial Cível e Criminal de São Cristóvão/SE, o suscitado[111].

No caso de análise de aplicabilidade da lei penal brasileira em conjunto com a análise de jurisdição e competência, Matheus de Araújo Alves, citando mestre Vianna, alerta que diferentemente do código penal, que adota a teoria da ubiquidade, o código de processo penal define quanto a competência em razão do local, a teoria do resultado. Desta forma, a competência seria fixada não mais pelo local de origem do comando (de onde partiu a ordem de ação pelo cyber criminoso), mas sim da localização onde se encontra o dispositivo eletrônico da vítima afetada[112].

Neste sentido, o doutrinador irá vislumbrar três hipóteses possíveis, dando a cada uma delas a devida solução legal[113]:

> A) O sistema computacional está situado no Brasil: Neste caso a competência será da justiça brasileira.
> B) A ordem parte de um sistema computacional situado no Brasil, e o resultado se dá em dispositivo localizado em outro país: Neste caso se aplica o disposto no art. 70, parágrafo único do CPP que dispõe:
> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 1o Se, iniciada a execução no território nacional, a infração se consumar fora dele, a competência será determinada pelo lugar em que tiver sido praticado, no Brasil, o último ato de execução.

De igual maneira, se o dispositivo no qual se partiu a ordem esteja localizado em território estrangeiro, mas o sistema afetado esteja no Brasil, aplicar-se-á o disposto no parágrafo segundo do artigo citado acima:

---

[111] STJ. *CC 121.431/SE*, Rel. Ministro Marco Aurélio Bellizze, Terceira Seção, julgado em 11/04/2012, DJe 07/05/2012.
[112] VIANNA, 2001, p. 103 *apud* ARAUJO ALVES, 2020, p. 75.
[113] Ibid., p. 76.

> § 2o Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado.

Neste sentido, conclui Thalyta Evangelista que não existe de fato uma previsão normativa de competência exclusiva para se processar e julgar delitos informáticos, sendo a justiça federal competente para julgamento nas hipóteses de existência de convenção\tratado internacional e concomitantemente, o caráter de transnacionalidade do delito, o que se dá na maior parte dos casos. Sendo entretanto, necessária uma análise casuística para que se possa determinar sobre qual órgão judicial recai o *ius puniendi* estatal[114].

No âmbito jurisprudencial, já é pacífico o reconhecimento da intensa natureza transnacional dos delitos envolvendo o meio virtual da *deep web* quando os servidores utilizados estejam em território estrangeiro, quando a ação o resultado se dê em locais que não em solo pátrio ou quando os provedores do serviço não possuam representação no Brasil, o que acaba ocorrendo na esmagadora maioria dos casos que envolvam a internet não indexável.

Neste sentido, relevante decisão que julgou um dos primeiros casos de investigação no Brasil, de cyber criminoso que atuava nos escuros meandros da *deep web*, assentou o entendimento que hoje é unanimidade no mundo jurídico. Referimo-nos, ao julgamento do Recurso Extraordinário N. 628.624, cuja íntegra se apresenta a seguir:

> 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.

[114] EVANGELISTA, 2020, p. 94.

> 1. À luz do preconizado no art. 109, V, da CF, a competência para processamento e julgamento de crime será da Justiça Federal quando preenchidos 03 (três) requisitos essenciais e cumulativos, quais sejam, que: a) o fato esteja previsto como crime no Brasil e no estrangeiro; b) o Brasil seja signatário de convenção ou tratado internacional por meio do qual assume o compromisso de reprimir criminalmente aquela espécie delitiva; e c) a conduta tenha ao menos se iniciado no Brasil e o resultado tenha ocorrido, ou devesse ter ocorrido no exterior, ou reciprocamente.
> 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[115].

Conforme se observa pela leitura do julgado acima, o Supremo tribunal federal em julgado de extrema importância para a segurança jurídica e combate à criminalidade digital, reconhece que a competência investigativa

[115] STF. *RE: 628.624 MG*, Rel.: Marco Aurélio, Data de Julgamento: 29/10/2015, Tribunal Pleno, Data de Publicação: 06/04/2016.

e processual relativa a delitos virtuais recai, via de regra, a justiça federal, em razão de existência flagrante da natureza transnacional intrínseca a maioria dos crimes informáticos. Como consequência, a Polícia federal, será na maioria dos casos, o órgão policial investigativo para vigiar e combater os cyber criminosos. Entretanto, isto não significa dizer que as policiais civis dos Estados da federação não possam realizar aberturas de inquéritos ou praticar outros atos investigativos em ralação a tais crimes.

Muito pelo contrário, por vezes são estes mesmos os primeiros a receberem notícias crime relativos à prática de delitos informáticos, sendo estes órgãos então os que iniciam os procedimentos investigativos iniciais, que podem ou não, em seguida, serem repassados a Polícia federal (na hipótese de reconhecimento do carácter transnacional do delito pelo delegado de polícia) de maneira que a PF participe das investigações e realize os atos que entender cabíveis.

Com base neste julgado, outros de igual importância foram decididos pela justiça de igual maneira, eis que reconhecida a natureza de repercussão geral quando do julgamento do RE. 628.624. Abaixo, apresenta-se o julgado do Habeas corpus N. 615857, proveniente do estado de São Paulo, efetuado após sentença que condenou um dos investigados pela operação "*darknet*", a pena de reclusão pelas práticas de pornografia infantil em site próprio na *darkweb* (área não indexável da internet, cuja definição e conceito foi abordado no ponto 2.5 deste trabalho).

> HABEAS CORPUS Nº 615857 - SP (2020/XXXXX-7) DECISÃO Trata-se de habeas corpus, com pedido liminar, impetrado em favor de HECTOR MOYANO contra acórdão proferido pelo Tribunal Regional Federal da 3ª Região, no julgamento da Apelação Criminal n. XXXXX37.2016.403.6181.
> Depreende-se dos autos que o paciente foi condenado, pela prática do crime tipificado no art. 241-A da Lei n. 8.069/1990, por nove vezes, na forma continuada, à pena de 7 anos e 6 meses de reclusão, em regime inicial semiaberto, e multa. Irresignada, a defesa interpôs o recurso de Apelação perante o TRF-3, alegando, preliminarmente, nulidades do processo, em razão da infiltração policial em ambiente virtual e da incompetência da Justiça Federal para processar e julgar o feito.
> No mérito, sustentou a tese do crime impossível, bem como não haveria provas suficientes para a condenação. Em caráter subsidiário, aduziu que a pena deveria ser reduzida, por inexistirem elementos que lastreassem a majoração da pena no

patamar imposto na sentença. Em sessão de julgamento realizada no dia 30/1/2020, a Décima Primeira Turma do TRF-3, à unanimidade, deu parcial provimento ao recurso, fixando a reprimenda definitiva em 6 anos e 3 meses de reclusão, e multa, mantidos os demais termos da sentença.
O acórdão restou assim ementado (e-STJ fls. 112/113): DIRFATO PLNAL. APELAÇÃO CRIMINAL. PORNOGRAFIA INFAMO-R IVFNIL. LEI 8.069/90. ARTIGOS 24 I-A. DIVI LGAÇÃO. LINKS. CONEXÕES DE ACESSO. DEEP WEB. MATERIALIDADE INCONTROV142SA. AUTORIA E DOLO. COMPROVAÇÃO. CONDENAÇÃO MANTIDA. DOSIMETRIA. PENA-BASE. REDUÇÃO. RECURSO DA DEFESA PARCIALM1T5flt PROVIDO.
1. Réu que teria compartilhado links" (conexões para acesso virtual direto) para conteúdo de pornografia infanto-juvenil, no âmbito da chamada “deep web".
2. O Supremo Tribunal Federal enfrentou a questão da competência da Justiça Federal em crimes como os imputados ao réu, em caso que teve repercussão geral reconhecida (RE 628.624). Com base no entendimento da Suprema Corte, fica clara a competência da Justiça Federal no caso concreto, porquanto a imputação diz com a divulgação, em foro virtual aberto aos frequentadores da "deep web" (desde que se cadastrassem para acesso ao "fórum"), de conteúdos pornográficos infantis que poderiam ser acessados, virtualmente. em qualquer parte do mundo. Reconhecida a competência da Justiça Federal.
3. "Operação Darknet". Criação de "fórum" na deep web para que fosse possível identificar quais eram os indivíduos que potencialmente compartilhavam ou divulgavam os materiais criminosos de pornografia infantil. Infiltração de agentes realizada com autorização judicial c com amparo legal. Artigos 10 e seguintes da Lei 12.850/13. Atuação válida. Ausente qualquer nulidade na conduta dos agentes de investigação, ou na colheita de provas.
4. Crimes previstos nos arts. 241-A. Materialidade comprovada. Inexistente o flagrante preparado. posto que ausentes atos de instigação policial ou ausência de potencial lesivo nas condutas praticadas no âmbito do referido "fórum". Materiais efetivamente divulgados c visualizados por diversos usuários.
5. Autoria e elemento subjetivo. Comprovação. Circunstâncias concretas, provas documentais e teor do próprio interrogatório no que tange ao conhecimento informático e ao uso exclusivo da conta por meio da qual foram divulgados os conteúdos pornográficos infantis.
6. Dosimetria. 6.1 Pena-base mantida acima do mínimo legal, mas reduzida em relação ao quantum cominado na sentença. Pena de multa reduzida, para que seu estabelecimento se dê com obediência dos mesmos parâmetros utilizados na fixação da pena privativa de liberdade. 6.2 Tratando-se de nove práticas amoldadas ao art. 241-A, em circunstâncias similares de modo, tempo e lugar, em nexo de unitariedade, incide o art. 71 do Código Penal, no patamar máximo de dois terços.
7. Recurso provido em parte. Condenação mantida; pena reduzida. Segundo a inicial, foi certificado o trânsito em julgado. No presente habeas corpus substitutivo de recurso próprio, a defesa sustenta a nulidade do julgamento da Apelação, visto que, após a interposição do referido recurso, os causídicos do ora paciente, que foram constituídos no curso da ação penal, não foram mais intimados a respeito dos andamentos processuais, o que impossibilitou a defesa realizar sustentação oral, bem como interpor recursos contra o acórdão ora impugnado, resultando em cerceamento de defesa. Ao final, requer (e-STJ fls. 14-15):
a) Deferimento do Pedido Liminar para Decretar a Anulação dos seguintes atos processuais: 1º: v. Acórdão de fls. 366/372 que julgou o Recurso de Apelação do Paciente; 2º: Certidão que atestou o Trânsito em Julgado às fls. 378; 3º Decisão do MM. Juízo de primeira instância que determinou a expedição de Mandado de Prisão Definitivo de fls. 379 e; por conseguinte, 4º: anulação do Mandado de Prisão Definitivo expedido às fls. 380; assim como Conceder a Ordem de Salvo Conduto,

> com imediata determinação de expedição e comunicação a autoridade coatora e a autoridade judiciária para conhecimento;
> b) Subsidiariamente, suspender o feito originário nº 0012168-37.2016.403.6181/SP, com sustação do Mandado de Prisão Definitivo expedido às fls. 380, até o julgamento definitivo do Mérito do writ;
> c) No Mérito, conceder a ordem pleiteada de forma definitiva, julgando nulo o feito nº 0012168-37.2016.403.6181/SP a partir do v. Acórdão de fls. 366/372 que julgou o Recurso de Apelação do Paciente; ou qualquer outra entre as hipóteses de nulidades pleiteadas, devendo anular em todas elas, no mínimo a Certidão que atestou o Trânsito em Julgado às fls. 378; a r. Decisão do MM. Juízo de primeira instância que determinou a expedição de Mandado de Prisão Definitivo de fls. 379, assim como o Mandado de Prisão Definitivo expedido às fls. 380.Determinado por último a remessa dos autos do processo a Secretaria da 11ª Turma do Colendo Tribunal a quo, para proceder conforme tese acolhida, como consagração do princípio da ampla defesa.
> d) Por fim, requer a juntada das Cópias do Processo originário nº 0012168-37.2016.403.6181/SP a partir da constituição destes Patronos como Defensores do Paciente, assim como após tais cópias, junta também neste ato o comprovante de pesquisa junto ao site Recorte Digital, bem como os e-mails encaminhados pela empresa Recorte Digital nos dias onde não houve publicação do TRF 3º Região em seus nomes, os quais provam o alegado. É o relatório. Decido.
> A liminar em recurso ordinário em habeas corpus, bem como em habeas corpus, não possui previsão legal, tratando-se de criação jurisprudencial que visa a minorar os efeitos de eventual ilegalidade que se revele de pronto na impetração. Em um juízo de cognição sumária, não visualizo manifesta ilegalidade no ato ora impugnado a justificar o deferimento da medida de urgência, que se confunde com o próprio mérito. É cediço que o conhecimento do habeas corpus pressupõe prova pré-constituída do direito alegado, devendo a parte demonstrar de maneira inequívoca a pretensão deduzida e a existência do evidente constrangimento ilegal, o que, a princípio, não foi observado na hipótese.
> Assim, não obstante os fundamentos apresentados pela defesa, mostra-se imprescindível uma análise mais aprofundada dos elementos de convicção constantes dos autos, a fim de se aferir a existência de eventual constrangimento ilegal, notadamente após a vinda das informações da Corte Regional. Por fim, o pedido liminar confunde-se com o próprio mérito da impetração, o qual deverá ser apreciado em momento oportuno, por ocasião do julgamento definitivo deste writ.
> Ante o exposto, indefiro a liminar. Solicitem-se informações pormenorizadas ao Tribunal impetrado acerca do alegado na presente impetração, em especial sobre a ausência de intimação da defesa sobre os atos processuais em segundo grau, notadamente acerca do despacho que designou a data do julgamento e sobre a publicação do acórdão, devendo ser remetida a senha para acesso aos dados processuais constantes do respectivo portal eletrônico, se for o caso, tendo em vista a restrição determinada pela Resolução n. 121 do CNJ. Após, encaminhem-se os autos ao Ministério Público Federal. Intimem-se. Brasília, 25 de setembro de 2020. Ministro REYNALDO SOARES DA FONSECA Relator[116].

Destaco também uma breve síntese sobre a Operação Darknet, citada no primeiro julgado.

[116] STJ. *HC: 615857 SP 2020/XXXXX-7*, Rel. Ministro Reynaldo Soares da Fonseca, Data de Publicação: DJ 29/09/2020.

No dia 13/05/2022 teve início a operação *Darknet* pela polícia civil do DF para investigar um homem suspeito de envolvimento na venda de pornografia infantojuvenil. A apuração se iniciou quando a Agência de Investigações de Segurança Interna (*Homeland Security Investigations – HSI*), da Embaixada dos Estados Unidos, em Brasília, obteve informações sobre indivíduo que estaria promovendo a compra e venda de arquivos contendo pornografia infantil na chamada *Deep Web*, localizada na camada não indexável da internet.

A DIPO-DF (Departamento de inquéritos policiais da polícia civil do Distrito federal) verificou que um usuário, localizado em Brasília, morador do bairro Guará, teria efetuado a compra e possível venda de material de abuso sexual infantil por meio de site da Darknet. Após individualizar o suspeito, a PCDF representou pedido de expedição de mandado de busca e apreensão, que foi deferido pelo Judiciário. O mandado foi cumprido nos bairros Sudoeste e Guará, na cidade de Brasília, tendo os agentes encontrado materiais relacionados à pedofilia infantil armazenados em um celular. O investigado foi então autuado em flagrante delito por armazenar imagens e vídeos de crianças com cunho sexual. No interior da residência, os agentes apreenderam ainda equipamentos eletrônicos que foram e estariam sendo utilizados na prática das condutas criminosas.

A operação levou a alcunha "*Darknet*" em razão do indiciado, estudante de Análise e Desenvolvimento de Sistemas, confessar que adquiria os packs (pacotes de dados), com arquivos de pornografia infantojuvenil, em sites fornecedores da Deep Web[117].

[117] PCDF deflagra operação Darknet. *Polícia Civil do Distrito Federal*. Disponível em: https://www.pcdf.df.gov.br/noticias/11059/pcdf-deflagra-operacao-darknet. Acesso em: 2 out. 2022.

3.3.2 Legislação internacional

No que tange ao mundo jurídico que permeia a comunidade internacional, destaca-se a existência da convenção de Budapeste, promulgada em 23 de novembro de 2001, que busca em seu cerne, segundo Thalyta Evangelista, em análise dos escritos de Dias, a "concepção de uma política criminal comum, com o propósito de resguardar a sociedade contra a criminalidade no mundo virtual"[118].

Importa destacar porém, que o Brasil não ratificou o mencionado tratado, não sendo portanto aplicáveis suas disposições a casos que envolvam brasileiros ou cujo resultados se deem em solo nacional. Neste sentido, Thalyta Evangelista irá criticar a falta de iniciativa por parte do Brasil para sua ratificação, eis que no cenário internacional atual, diante das incertezas da insegurança jurídica, muitas entidades e empresas de tecnologia da informação, deixam de investir e instalar suas representações em países que não possuam uma regulação mais aprofundada no tema.

A autora cita a tentativa do congresso nacional em estabelecer legislação que regule as atividades digitais, sejam elas de carácter penal ou cível, tais como a lei n. 12.737/12 (lei Carolina Dieckmann), a lei n. 12.9645/14 (marco civil da internet) e a lei n. 13.709/18 (Nova lei de proteção de dados pessoais), porém trazendo fortes críticas ao fato de que todas estas inovações legislativas terem surgido muito tardiamente e que a atenção ao fato somente ter sido introduzida aos congressistas por meio do texto original da PL 84/1999, que nas palavras da doutrinadora, tratava-se de um:

> Regresso absoluto perante a legislação da Convenção de Budapeste (...) o que se objetivava com o consentimento dessa Lei, era instaurar um total vigilantíssimo, dessa forma, cessaria a navegação anônima (...) falta de respeito notório aos direitos fundamentais e as autonomias civis(...) é evidente a discrepância entre esses dispositivos normativos, tal como a inconstitucionalidade de preceitos do projeto em questão[119].

[118] EVANGELISTA, 2020, p. 64.
[119] Ibid., p. 66.

Segundo a autora, a convenção apresenta a seguinte estrutura de classificação normativa para os delitos virtuais:

A) Infrações contra a confidencialidade, integralidade e disponibilidade de sistemas informáticos e dados informáticos;

- Acesso ilegal: É o acesso irregular e doloso a computadores e redes
- Interceptação ilegal: É a captura irregular e dolosa de dados
- Interferência de dados: É o ataque de '*cracker*', com destruição ou captura
- Interferência em sistemas: É a captura, bombardeio ou negação de serviços (ataques DDoS)
- Uso abusivo de dispositivos: É a venda ilegal de dados, códigos e senhas

B) Infrações relacionadas com computadores

- Falsidade informática: É a falsificação de dados
- Burla informática: é o estelionato na versão cibernética

C) Infrações relacionadas com o conteúdo

- Pornografia infantil
- Racismo e xenofobia
- Apologia ao genocídio ou outros crimes contra a humanidade

D) Infrações relacionadas com a violação do direito de autoria e direitos conexos[120].

Conforme se extrai da leitura interpretativa, o que se percebe é que na prática, muito embora não signatário da convenção, o Brasil já prevê muitos dos atos acima mencionados como delitos digitais, quer seja por meio da introdução de novas leis (legislação penal extravagante) que assim o fazem, quer por meio do próprio código repressivo.

Entretanto, Thalyta Evangelista irá defender que a falta de uma legislação coerente e unificada, tal como a proporcionada pela convenção de Budapeste, faz com que haja maior dificuldade dos órgãos de repressão e prevenção para o combate dos ilícitos digitais, uma vez que, segundo a autora, os conceitos legais atualmente presentes no código penal e leis

[120] EVANGELISTA, 2020, p. 64-65.

esparsas necessitam de “maiores argumentações e edificações, pois os crimes estão evoluindo”[121].

Em razão disto, alerta a autora que:

> Mesmo sem existir uma legislação coerente que possa discorrer, apreciar e proibir de maneira adequada os crimes virtuais em sua totalidade, os acontecimentos coletivos e constitucionais têm determinado que os juristas lançassem mãos de afirmações indefinidas e insuficientes, concedendo oportunidades à defesa do criminoso que se nutri com as imperfeições constitucionais revolucionárias, propiciando uma grande desordem no espaço virtual[122].

3.4 O instituto das provas no âmbito dos delitos digitais

Como é cediço a todos os juristas que militam na área das ciências criminais, a ocorrência de um fato delituoso que atinge a bem juridicamente tutelado, motiva ao Estado agir no caminho de combater e impedir as condutas criminosas, sempre que possível prestando amparo para a vítima do delito, que suporta os danos materiais e/ou pessoais decorrentes do ato ilícito. Neste contexto, o Estado juiz, faz-se mão do processo penal de maneira a aplicar a jurisdição penal que lhe é exclusiva, de forma a se punir o meliante, remediar os danos no que for possível e atingir assim a pacificação social, esta última sendo entendida como a razão pela qual a ciência do Direito existe.

Neste sentido, a investigação criminal é meio pelo qual os órgãos competentes lançam mão de estratégias e meios pelos quais se poderá investigar a autoria, bem como a existência de materialidade do delito, de maneira que se possa, por meio destas provas coletadas, munir o Estado juiz em sua decisão quanto a inocência ou culpa do acusado(s) investigado(s). Assim sendo, a prova da autoria e materialidade delitiva são condições *sine qua non* para o sucesso ou não da pretensão punitiva estatal.

---

[121] EVANGELISTA, 2020, p. 67.
[122] DIAS, 2017, *apud* EVANGELISTA, 2020, p. 67-68.

3.4.1 O conceito de prova para o direito processual penal

Nas palavras de Aury Lopes Junior, citado por Matheus de Araújo Alves, o processo penal seria "instrumento de retrospecção em que há uma tentativa de se reconstruir, de forma aproximada, um determinado fato"[123], ou seja são as provas que permitiram a reconstrução de fato pretérito que se busca reprimir, leia-se o crime.

No modelo adotado pelo Direito pátrio, quais seja, o Sistema penal acusatório, o órgão repressor acusador e/ou o particular legitimado, nas hipóteses em que é constitucional e legalmente competente para tal, devem comprovar de maneira inequívoca que houve de fato a ocorrência de um injusto penal, e para tal deverá lançar mão de todos os meios de prova aceitos, de forma a romper o estado de presunção de inocência que é garantido constitucionalmente a toda pessoa ou entidade dotada de personalidade jurídica.

Importa ressaltar que o contraditório e a ampla defesa, princípios basilares do instituto do devido processo legal ao qual se embasa o sistema penal acusatório brasileiro, são fundamentais para o instituto das provas, e não um empecilho a este como alguns defendem, eis que na realidade, estes princípios servem de instrumentos para uma correta e efetiva obtenção de provas, ao se permitir o debate de evidencias e alegações em âmbito processual, se permite que a verdade dos fatos possa ser alcançada com uma maior precisão, evitando assim abusos e erros por parte do Estado juiz.

A produção de provas é prevista em sede constitucional devido a sua expressa previsão no art.5, incisos XXXV, LIV e LV da constituição da república de 1988, constituem direito fundamental e que embasa o sistema penal pátrio (que adota o sistema acusatório) e que por sua vez é uma das expressões mais cristalinas do estado democrático de direito. Nas palavras de Jorge Luiz da Silva, citado por Matheus de Araújo Alves, a elaboração de

[123] LOPES JR., 2017, p. 285 *apud* ARAUJO ALVES, 2020, p. 79.

provas "constitui direito fundamental consubstanciado no contraditório, na ampla defesa, no devido processo legal e no acesso à justiça"[124].

É, entretanto, justamente por conta da vinculação deste instituto jurídico com o princípio da legalidade, da moralidade etc. que, nas palavras do doutrinador citado acima, "sua produção não tem carácter absoluto, sendo sujeita a determinados limites"[125].

Nesta linha de pensamento, Roseiro Pereira Leal irá colocar que:

> A lei constitucional é elemento e instrumento de prova da existência ou não do Estado de Direito. Se a lei é produzida por meio do devido processo legislativo, na acepção aqui estudada, é ela também elemento e instrumento de prova da existência do Estado de Direito Democrático. Quando o NCPC (art. 369) contempla 'meios moralmente legítimos' e 'livre' conjectura do juiz (art. 370) para se provarem fatos, além de cometer a impropriedade de afirmar a existência de uma moral válida sem norma jurídica definidora, permite coleta de prova numa realidade externa ao direito, em critérios personalíssimos e sumaríssimos (instantâneos), com negativa de vigência do princípio da legalidade estrita adotada pelo art. 5, II, da CF/88[126].

Portanto, com base nos argumentos trazidos pelo doutrinador acima descrito, bem como avaliando o cenário constitucional pátrio, jurisprudencial e doutrinário em vigência, pode-se concluir que as provas:

> São elementos que permitem a reconstrução histórica e sobre os quais recai a tarefa de verificação das hipóteses, com o objetivo de convencer o magistrado (...) uma vez que provar é assumir a difícil missão de representar os elementos da realidade objetiva pelos meios intelectivos autorizados pela legislação[127].

3.4.2 Meios de obtenção de prova no mundo virtual

Como visto em ponto anterior, uma das grandes dificuldades relativas a prevenção e punição dos delitos informáticos se dá justamente em razão da dificuldade de obtenção de provas da autoria e materialidade do delito, seja porque as autoridades e os órgãos competentes não possuem o conhecimento técnico e os meios matérias que permitam que estes atuem em paridade com

[124] DA SILVA, 2017, p. 03 *apud* ARAUJO ALVES, 2020, p. 87.
[125] ARAUJO ALVES, 2020, p. 87.
[126] LEAL, 2018, p. 265 *apud* ARAUJO ALVES, 2020, p. 86.
[127] ARAUJO ALVES, *op. cit.*, p. 81-82.

os cyber criminosos, como também pelas especificidades do mundo virtual, onde todas as provas se constituem em pulsos elétricos (os *bits*) que são por sua vez armazenados de maneira efêmera em servidores que por vezes nem sequer encontram-se em território nacional.

Neste diapasão alerta Matheus de Araújo Alves que "existe uma limitação no que tange à obtenção de provas pelo sistema judiciário nos casos que envolvam crimes digitais"[128], limitação esta de cunho estritamente prático, em razão das especificidades do mundo digital, da infraestrutura e sistemas postos para servir o mesmo, tais como a existência de criptografia e sistemas de proteção ao anonimato e dados sensíveis.

Por esta razão, em que pese a maior parte dos delitos informáticos já apresentarem classificação e tipificação na legislação repressiva pátria (sejam estes delitos digitais próprios ou impróprios), ainda irão ser caracterizados por particularidades que os diferem dos delitos tradicionais praticados no mundo material/físico. Por esta razão, a "persecução penal e probatória passam a ser diferentes"[129].

Seguindo esta linha de raciocínio, Matheus de Araújo Alves, citando a professora Adriana Shimabukuro irá alertar que:

> Enquanto no crime tradicional, praticado no mundo material, se encontram informações essenciais para sua investigação, como vestígios, indícios e testemunhas, nos crimes digitais, as evidências podem estar alocadas em inúmeros dispositivos como computadores, celulares, *pendrives*, provedores de internet, registros de equipamento de infraestrutura de rede como roteadores, firewalls e servidores de e-mail. O material probatório, além de volátil, é bastante variado, histórico de navegação, fotos, vídeos, e-mails, entre outros (...) devido as particularidades das provas no meio digital, caso esta não seja prontamente preservada, pode ser rapidamente danificada, alterada ou até suprimida, impedindo qualquer investigação ou identificação do autor do delito. Com isto, a coleta do material probatório nos crimes digitais segue rigorosos critérios de preservação e controle para que não haja perda de sua veracidade[130].

Portanto, conforme se extrai das informações, é evidente o fato de que a prova de autoria e materialidade dos delitos informáticos são de notória

---

[128] ARAUJO ALVES, 2020, p. 100.
[129] DA SILVA, 2017, p. 06 *apud* ARAUJO ALVES, 2020, p. 91.
[130] SHIMABUKURO, 2017, p. 23 *apud* ARAUJO ALVES, 2020, p. 91.

complexidade, quer seja pela dificuldade de obtenção destas, da falta de meios materiais para tal pelos órgãos competentes, ou pela falta de legislação processual específica que melhor se adeque a natureza volátil das provas no mundo virtual da *web*.

Ainda segundo o autor, a análise dos artigos 158-184 do CPP permite inferir que o meio de prova mais "adequado" para se comprovar a prática de um injusto penal, é o exame de corpo de delito[131], que deve sempre ser realizado por um especialista na sua área de atuação, cuja conclusão é emitida por meio de parecer técnico. Conforme leciona o professor Rodier Roncada, corpo de delito é "o conjunto dos vestígios resultantes da infração penal, enquanto o exame de corpo de delito é a análise e o registro feito por peritos sobre esses vestígios"[132].

Neste diapasão, Matheus de Araújo Alves irá concluir que "não se faz prova da existência de crimes digitais sem o devido exame de corpo de delito, formalizado em laudo técnico pericial"[133], isto pois conforme conclui o doutrinador, todo delito informático acaba envolvendo aspectos técnicos, cuja comprovação de sua execução exige "conhecimento científico de informática para atestar a existência"[134].

O referido doutrinador, citando o professor Roncada, ao tratar do tema, afirma que, muito embora haja previsão expressa no CPP, especificamente o art. 167, para que seja dispensado o exame de corpo de delito para crimes em que tenha havido desaparecimento dos vestígios materiais, podendo neste caso ser substituído por prova testemunhal, nos casos estritamente relacionados a delitos informáticos, o doutrinador entende que o exame de corpo de delito se faz essencial, pois:

> (...) não há como confirmar de modo seguro a sua ocorrência e seu alcance sem constatar o caminho lógico percorrido pelo autor dentro do ambiente digital, até mesmo determinando a origem dos atos executórios, primordiais para determinar

[131] ARAUJO ALVES, 2020, p. 92.
[132] RONCADA, 2017, p. 180.
[133] ARAUJO ALVES, *op. cit.*, p. 92.
[134] Ibid., p. 92.

> a autoria do crime. Isso só seria possível através de um exame técnico em que os vestígios são analisados por profissional habilitado em informática e tecnologia da informação, que tem a função de elaborar uma opinião crítica e fundamentada sobre os fatos observados[135].

Em mesmo sentido se expressa Thalyta Franca Evangelista ao afirmar que:

> A prova pericial é fundamental nas práticas de crimes virtuais, visto que, possibilita que o especialista beneficiado de capacidades técnicas que, constantemente, fogem do conhecimento do magistrado, desempenhe uma análise minuciosa do modo pelo qual o delito foi executado[136].

Portanto, nas hipóteses de investigações relacionadas a delitos informáticos, em razão de tudo que foi apresentado, ficariam restritas os meios de obtenção de provas, sendo estas adstritas tão somente a provas materiais obtidas por meio de exames de corpo de delito, que devem ser realizados pela autoridade competente, de maneira mais célere possível, como forma de evitar a degradação ou perda destas evidencias materiais que podem ser identificadas por agentes com conhecimentos técnicos e científicos específicos.

Importa mencionar que os crimes virtuais não apresentam normas processuais próprias para procedimentos investigativos, e assim sendo, são aplicáveis a estes tipos de delitos as regras genéricas previstas no código de processo penal e legislação estravagante (lei 12.850/13- Lei das organizações criminosas e lei 12.965/15 -Marco civil da internet), que como bem aponta Matheus de Araújo Alves, possuem “importantes instrumentos de apuração de crimes digitais previstos em seus artigos”[137], tais como a infiltração de agente policial em sites onde se suspeita ocorrência de atividades criminosas ou estipulação de obrigação dos servidores localizados no Brasil de atenderem a ordens judiciais para acesso de conteúdo dos seus registros.

---

[135] RONCADA, 2017, p. 183 *apud* ARAUJO ALVES, 2020, p. 94.
[136] EVANGELISTA, 2020, p. 88.
[137] ARAUJO ALVES, 2020, p. 95.

A legislação pátria, embora omissa, na maior parte das vezes, em relação a regulação específica de métodos processuais próprios para a investigação e processamento de crimes praticados em ambiente digital, ao menos estipula que não existe impedimentos legais para a utilização de provas coletadas neste "ambiente imaterial". Isto se extrai da leitura do art. 225 do código civil, onde se estipula que:

> As reproduções fotográficas, cinematográficas, os registros fonográficos e, em geral, quaisquer outras reproduções mecânicas ou eletrônicas de fatos ou de coisas fazem prova plena destes, se a parte, contra quem forem exibidos, não lhes impugnar a exatidão.

Seguindo em mesma linha, o legislador estipula no código de processo civil, por meio do art. 369 que:

> As partes têm o direito de empregar todos os meios legais, bem como os moralmente legítimos, ainda que não especificados neste Código, para provar a verdade dos fatos em que se funda o pedido ou a defesa e influir eficazmente na convicção do juiz.

Neste sentido, conclui Matheus de Araújo Alves, citando Da Silva, que todas as provas "obtidas no ambiente digital são aceitas, desde que respeitados alguns padrões técnicos para sua coleta e armazenamento, com o objetivo de resguardar sua integridade, validade e/ou licitude"[138].

Na seara da ciência criminalística forense, cabe destacar a existência da modalidade conhecida como "computação forense". Nas palavras de Matheus de Araújo Alves, citando o professor Jorge Luís da Silva, computação forense é "uso de técnicas analíticas e de investigação para identificar, coletar, analisar e preservar as provas, informação que é armazenada magneticamente ou codificada"[139]. Neste sentido, entende-se que a ciência criminal da computação forense, é meio para identificar, validar, coletar analisar etc. evidências digitais, que possam então resultar em indícios e eventualmente provas periciais (devidamente produzida conforme

[138] DA SILVA, 2017, p. 08 *apud* ARAUJO ALVES, 2020, p. 96.
[139] Ibid., p. 96.

rígidos critérios técnico-científicos) que podem, pôr fim, ser utilizados para a conclusão do processo criminal com a decisão do magistrado.

Falando sobre a formação das evidências eletrônicas, os professores Wendt e Nogueira irão explicar que "A maioria dos *hosts* da rede (máquinas) não possuem funções de monitoramento, que são em grande parte invisíveis e automáticos. Porém, quase toda atividade de rede acaba sendo registrada em algum lugar"[140]. Nesse diapasão, os professores irão listar diversos métodos pelos quais a criminalística aplicada da computação forense pode acessar as evidências que se procuram, tais como:

- Registros de login (logs)
- Amostras de registros de sessão
- Registros de navegação na internet (diretórios de cache, arquivos de históricos, registros detalhados para cada pedido por qualquer página, data/hora/número de *bytes*)
- Endereço de IP do sistema que solicitou o dado

Ao tratar do caso em que os servidores encontram-se fora do território nacional, os doutrinadores mencionam que no caso especifico dos Estados Unidos, existe acordo bilateral de cooperação entre as justiça pátria e deste pais estrangeiro (decreto n 3810 de 02 de maio de 2001), de maneira que, em que pese certas dificuldades burocráticas, o Ministério da Justiça e segurança pública possa (por meio do Departamento de Recuperação de ativos e cooperação jurídica internacional) a pedido de autoridade policial e/ou judiciária competente, representar perante a justiça daquele país, para que os provedores dos servidores que se pretendem investigar, forneçam os dados listados anteriormente. Tal procedimento vem sendo realizado, com graus variados de sucesso, haja vista a relutância da justiça de alguns estados americanos em fornecer dados de natureza pessoal, considerando a grande importância dada a anonimidade na legislação de muitos desses entes federais[141].

[140] WENDT; NOGUEIRA JORGE, 2021, p. 97.
[141] Ibid., p. 99-100.

Como conclusão, Matheus de Araújo Alves, irá dizer que:

> O processo de investigação e julgamento de um delito informático deve ser pautado na ampla liberdade probatória outorgada às partes e no livre convencimento do órgão julgador para que este possa apreciar essas provas, fundamentados os motivos de sua decisão[142].

3.4.3 A "engenharia social" como método investigativo (infiltração de agentes segundo a lei das Org. Criminosas Lei n 12.850 e Estatuto da criança e do adolescente Lei n 8.069/90)

O conceito de "engenharia social", hoje tão comentada e utilizada por doutrinadores e juristas, nada mais é do que ardil ou artifício no direito penal clássico. Como bem sintetiza Crespo, são métodos de "mascarar a realidade para explorar ou enganar a confiança de uma pessoa detentora de dados importantes a que se quer ter acesso"[143]. A engenharia social portanto é a criação, em ambiente virtual, de uma falsa situação, uma "peça" no qual o agente ativo simula uma realidade para o agente passivo, que acreditando estar diante de uma situação verídica, fornece ao primeiro tudo que este deseja obter ou ver realizado.

É portanto mecanismo social de satisfação de um objetivo, este último podendo ser um objetivo lícito ou ilícito. Quando estamos diante de um exemplo ilícito, possivelmente estaremos tratando de hipóteses para incidência de algum delito informático, tais como o furto mediante fraude eletrônica, ou estelionato digital (ambos os tipos já abordados em pontos anteriores). Entretanto, o ordenamento jurídico pátrio prevê que em determinadas situações, agentes públicos vinculados aos órgãos competentes possam se utilizar desse mecanismo para se infiltrarem em sites, salas de *chats* etc. onde determinados tipos de delitos estejam sendo praticados por grupos criminosos organizados.

---

[142] ARAUJO ALVES, 2020, p. 98.
[143] CRESPO, 2011, p. 82.

Estas hipóteses estarão previstas na legislação referente ao estatuto da criança e adolescente (Lei. n 8.069/90), que passou a prever a possibilidade de infiltração de agentes policiais disfarçados na web, com a intenção de investigar crimes relacionados a dignidade sexual dos jovens e crianças. Tal inovação legislativa se deu a partir da Lei n. 13.441/17 e obteve tamanho êxito que posteriormente motivou o legislador a introduzir mecânica semelhante na lei de repressão a organizações criminosas (Lei n. 12.850/13) que passou a prever a infiltração eletrônica de agentes policiais a fim de possibilitar maiores investigações em meio digital dos crimes previstos no referido diploma repressivo.

Aqui cabe trazer a distinção entre a infiltração de agente e o flagrante preparado ou montado. No flagrante preparado, o que se tem é a autoridade policial instigando o "criminoso" a realizar a prática do crime (exemplo: Um policial suspeita que um indivíduo está comercializando produtos em desacordo com as normas técnicas, logo este simula interesse para que o investigado lhe venda tais materiais de forma a possibilitar o flagrante).

Nas palavras de Renato Brasileiro de Lima, neste tipo de "flagrante" o "suposto autor do delito não passa de um protagonista inconsciente de uma comédia, cooperando para a ardilosa averiguação da autoria de crimes anteriores, ou a simulação da exterioridade de um crime"[144]. Acerca do flagrante preparado, tem-se o teor da Súmula 145 do Supremo Tribunal Federal em que se pacificou o entendimento de que não seria constitucional:

> S.145: Não há crime, quando a preparação do flagrante pela polícia torna impossível a sua consumação.

Portanto, ao se realizar uma infiltração virtual (ou até mesmo uma infiltração física tradicional), o agente policial em momento algum deverá estimular a prática do delito por parte dos investigados, ficando sua atuação

[144] LIMA, Renato Brasileiro de. *Manual de processo penal*: Volume único. 10. ed. rev., ampl., e atual. São Paulo: Ed. Jus Podivm, 2021. p. 898.

restrita a verificar ou não a ocorrência dos ilícitos, que deverão ser praticados de livre e espontânea vontade pelos investigados.

Conforme se deduz de análise da inovação advinda da lei 13.441/17, é possível observar que a infiltração policial virtual será possível em 3 distintas categorias de delitos previstos no ECA[145]. Sendo estas:

- Pedofilia: (ECA, art. 240, 241, 241-A, 241-B, 241-C, e 241-D).

- Crimes contra a dignidade sexual de vulnerável: estupro de vulnerável (CP, art.217-A), corrupção de menores (CP, art.218), satisfação de lascívia (CP, art.218-A) e favorecimento da prostituição de criança ou adolescente ou de vulnerável (CP, art.218-B).

- Invasão de dispositivo informático (CP, art.154-A).

- Conforme nos alerta mestre Renato Brasileiro de Lima, sobre os aspectos processuais da infiltração virtual de agente, cabe ressaltar que tal mecanismo investigativo previsto no art.190-A do ECA não pode exceder o prazo de 90 dias, podendo ser renovado, desde que o prazo máximo não exceda a 720 dias e fique cabalmente demonstrada a efetiva necessidade perante a autoridade judicial competente, conforme também se extrai da leitura do art.190-A, III, ECA. (LIMA, 2021, p. 801).

  Art. 190-A. A infiltração de agentes de polícia na internet com o fim de investigar os crimes previstos nos arts. 240, 241, 241-A, 241-B, 241-C e 241-D desta Lei e nos arts. 154-A, 217-A, 218, 218-A e 218-B do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal), obedecerá às seguintes regras:

  I – será precedida de autorização judicial devidamente circunstanciada e fundamentada, que estabelecerá os limites da infiltração para obtenção de prova, ouvido o Ministério Público;

  II – dar-se-á mediante requerimento do Ministério Público ou representação de delegado de polícia e conterá a demonstração de sua necessidade, o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas;

  III – não poderá exceder o prazo de 90 (noventa) dias, sem prejuízo de eventuais renovações, desde que o total não exceda a 720 (setecentos e vinte) dias e seja demonstrada sua efetiva necessidade, a critério da autoridade judicial.

  § 1º A autoridade judicial e o Ministério Público poderão requisitar relatórios parciais da operação de infiltração antes do término do prazo de que trata o inciso II do § 1º deste artigo.

  § 2º Para efeitos do disposto no inciso I do § 1º deste artigo, consideram-se:

[145] LIMA, 2021, p. 801.

> I – dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão;
>
> II – dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão.
>
> § 3º A infiltração de agentes de polícia na internet não será admitida se a prova puder ser obtida por outros meios.

No que tange a infiltração virtuais de agentes em sites ou domínios administrados por organizações criminosas, o Pacote Anticrime inovou ao adicionar o art.10-A a lei 12.850/13, de maneira que se passou a permitir a infiltração de agentes policiais, desde que obedecidos os requisitos estipulados no *caput* do art. 10, com o objetivo de se investigar e coibir a prática dos tipos penais e ilícitos que estejam conexos a tal diploma repressivo e praticados por organizações criminosas ou entidade que se assemelhe.

Alerta Renato Brasileiro de Lima que tal medida deverá ainda preceder de demonstração cabal da efetiva necessidade bem como o alcance das tarefas que serão realizados pelos infiltrados tais como os dados pessoais dos investigados, os supostos delitos que se acreditem estar sendo realizados, dados de conexão e cadastrais, endereços de IP do site ou sistema a ser infiltrado etc. A infiltração deverá ser realizada em prazo de até 6 meses, renováveis mediante autorização judicial, desde que não excedam 720 dias. Importa ainda mencionar que conforme estipulado no art.10-C do diploma repressivo, não comete crime (falsidade ideológica e demais crimes de falso) o agente policial que oculta sua identidade, fornecendo dados falsos aos investigados, para que possa colher os indícios de autoria e materialidade dos delitos, entretanto conforme nos alerta o professor Renato, isto não impede que o policial não possa responder por eventuais excessos cometidos no curso da sua infiltração[146].

[146] LIMA, 2021, p. 802.

> Art. 10-A. Será admitida a ação de agentes de polícia infiltrados virtuais, obedecidos os requisitos do caput do art. 10, na internet, com o fim de investigar os crimes previstos nesta Lei e a eles conexos, praticados por organizações criminosas, desde que demonstrada sua necessidade e indicados o alcance das tarefas dos policiais, os nomes ou apelidos das pessoas investigadas e, quando possível, os dados de conexão ou cadastrais que permitam a identificação dessas pessoas.
>
> § 1º Para efeitos do disposto nesta Lei, consideram-se:
>
> I - dados de conexão: informações referentes a hora, data, início, término, duração, endereço de Protocolo de Internet (IP) utilizado e terminal de origem da conexão;
>
> II - dados cadastrais: informações referentes a nome e endereço de assinante ou de usuário registrado ou autenticado para a conexão a quem endereço de IP, identificação de usuário ou código de acesso tenha sido atribuído no momento da conexão.
>
> § 2º Na hipótese de representação do delegado de polícia, o juiz competente, antes de decidir, ouvirá o Ministério Público.
>
> § 3º Será admitida a infiltração se houver indícios de infração penal de que trata o art. 1º desta Lei e se as provas não puderem ser produzidas por outros meios disponíveis.
>
> § 4º A infiltração será autorizada pelo prazo de até 6 (seis) meses, sem prejuízo de eventuais renovações, mediante ordem judicial fundamentada e desde que o total não exceda a 720 (setecentos e vinte) dias e seja comprovada sua necessidade.
>
> § 5º Findo o prazo previsto no § 4º deste artigo, o relatório circunstanciado, juntamente com todos os atos eletrônicos praticados durante a operação, deverá ser registrados, gravados, armazenados e apresentados ao juiz competente, que imediatamente cientificará o Ministério Público.
>
> § 6º No curso do inquérito policial, o delegado de polícia poderá determinar aos seus agentes, e o Ministério Público e o juiz competente poderão requisitar, a qualquer tempo, relatório da atividade de infiltração.
>
> § 7º É nula a prova obtida sem a observância do disposto neste artigo.

Findo a investigação, os dados coletados deverão então ser encaminhados ao juiz competente para que este então tome as medidas legais cabíveis, devendo para tal manter o sigilo das investigações.

CAPÍTULO 4 - SÍNTESE DO ESTUDO E REVELAÇÃO DA IMPORTÂNCIA DO DIREITO PENAL COMO INSTRUMENTO REGULADOR DAS ATIVIDADES HUMANAS NA INTERNET

A conclusão que se pode chegar após a análise dos pontos apresentados nos capítulos que formam este trabalho é que o processo de globalização e a revolução tecnológica, iniciada ainda nas décadas finais do século anterior, trouxeram grandes inovações e possibilidades para a humanidade como um todo. Porém, como não poderia deixar de acontecer em qualquer grande inovação e revolução social em nossa história como espécie, a dura realidade fática do mundo leva que indivíduos mal-intencionados acabem se utilizando da revolução digital e do surgimento do cyberespaço para o planejamento e execução de práticas ilícitas, estejam estas tipificadas ou não nos diplomas repressivos dos entes nacionais.

Neste sentido, a nova realidade forçou grandes mudanças no campo do Direito Penal, em especial pela introdução de novos tipos penais ou então adicionando a previsão de novas formas de cometimento de delitos previamente tipificados. Entretanto, como visto em capítulo anterior, ainda permeia discussão em âmbito doutrinário/político a respeito da relevância ou necessidade dos Estados nacionais em controlar e vigiar o fluxo de atividades no universo informático, com fortes debates ideológicos e filosóficos em pleno desenvolvimento.

De início, se acreditava que os próprios usuários poderiam se autorregular e evitar a prática de condutas negativas, tal como sustentado pelos pensadores liberais, entretanto com o passar do tempo, isto acabou se mostrando um equívoco, as informações e os dados que transitam na internet possuem grande valor seja econômico ou político, o que torna a cyber criminalidade um perigo real que deve ser reconhecido e combatido pelas autoridades nacionais, eis que nos encontramos em uma sociedade de risco pois o correto funcionamento de setores estratégicos da economia e do

cotidiano dependem da confiabilidade e segurança dos sistemas informáticos, o que torna a informação e a segurança desses sistemas e sua infraestrutura novos bem jurídicos tutelados pelo Direito Penal, ponto sustentado pelos pensadores realistas ao longo de seus embates com os liberais.

Muito embora haja reticência de alguns em aceitar, fato é que a internet é uma extensão da sociedade em que vivemos e logo os mesmos problemas e desafios vividos no mundo físico é refletido de maneira paralela no mundo digital, sendo a anonimidade da web (muito embora mecanismo importante de proteção pessoal de dados e manutenção da privacidade alheia) motiva e possibilita ao cyber criminoso atuar com fins de realizar seus reprováveis objetivos.

Entende-se que os delitos digitais seriam ações típicas, antijurídicas e culpáveis, seguindo exatamente o modelo da teoria analítica de crime adotado pela doutrina majoritária e pelo ordenamento jurídico pátrio. Pode-se ver que a doutrina ainda não se decidiu em relação a nomenclatura para esses tipos de crimes, estando porém a subdivisão entre eles algo relativamente pacificado, sendo os crimes virtuais subdivididos em dois grandes grupos: os delitos que são praticados contra bem jurídico informático tais como sistemas informacionais, dados e infraestrutura digital (crimes digitais próprios) e os delitos cometidos contra algum bem jurídico tradicionalmente previstos pela legislação penal clássica, não relativos a tecnologia da informação, mas que se utiliza desta última para fazer alcançar seus objetivos (crimes digitais impróprios).

Pode-se observar ainda a grande dificuldade em se investigar e punir os agentes que realizam suas nefastas atividades em ambiente digital, haja vista a falta de legislação internacional vigente que busque regular e unificar entendimentos jurisprudenciais e doutrinários entre os membros da comunidade internacional, tendo a convenção/protocolo de Budapeste de 2001 o que melhor se chegou deste objetivo, mas que por razões de interesse

geopolíticos, ideológicos e religiosos deixou de ser ratificado pela maioria dos países do mundo, inclusive o Brasil.

Com isto, a definição do tempo da ação, do local do crime e da competência para julgamento se faz extremamente dificultada quando está-se diante de um delito que apresente forte carácter de transnacionalidade, o que traz grandes transtornos e dificuldades aos órgãos repressivos competentes para realizar suas diligencias investigativas, reforçando a natureza volátil das provas digitais, facilmente manipuláveis e destrutíveis, levando em muitos casos a impunidade dos autores dos delitos, fato este que é “elevado a nona potência” quando tratamos de atividades criminosas praticadas na área não indexável da internet, a *deepweb*.

A falta de cooperação jurídica internacional e a inexistência de conceitos unificados entre distintas legislações nacionais em razão de diferenças culturas, religiosas, políticas e econômicas, aliadas a barreiras burocráticas intransponíveis da transnacionalidade somente intensifica a dificuldade de condenação dos cyber criminosos e proteção de suas vítimas.

Neste diapasão, cabe ressaltar que enquanto não se formaliza um entendimento entre os países e seus diferentes sistemas jurídicos, o ordenamento jurídico pátrio deve continuar se utilizando de conceitos, práticas e princípios já utilizadas, sendo estas tão somente adaptadas a atuação no mundo informático, tais como regras processuais de obtenção de meios de prova ou definições de competência para investigar, julgar e punir cyber criminosos. Importa ressaltar que em razão da existência de infraestrutura necessária ao correto funcionamento da tecnologia da informação, ao escolher implantar tal estrutura em solo pátrio, a empresa prestadora passa necessariamente a seguir os princípios e regras da legislação nacional, fato que facilita consideravelmente a obtenção de provas por meio de exame de corpo de delito (meio de prova estabelecido pelo CPP como sendo o mais adequado para se demonstrar a ocorrência de prática criminosa) e infiltração de agentes (quando previsto pela legislação penal estravagante),

no momento em que um delito informático é praticado, em seu todo, em solo nacional.

CONCLUSÃO

Conclui-se que, muito embora ainda se permeie no imaginário popular a ideia de que a web seja um espaço “anárquico” onde tudo vale e prevalece a impunidade, em especial com relação ao setor não indexável da internet, a deepweb, e sua parcela mais obscura, a darkweb, tal visão vem sendo gradualmente alterada.

Apesar de todas as adversidades e dificuldades trazidas neste trabalho, (seja por dificuldades técnico materiais para que os órgãos investigativos realizem suas diligências em paridade de armas com os meliantes, seja pela ausência de tipificações adequadas nas leis penais em vigor ou inexistência de tratado internacional que auxilie na pacificação e unificação de conceitos, entendimentos e cooperação jurídica internacional), o judiciário tem procurado combater a sensação de impunidade e reprimir a cyber criminalidade por meio de adaptações da legislação existente, enquanto tanto o executivo e legislativo vem atuando de maneira a introduzir modernizações normativas que melhor adequem os órgãos do Estado para impedir que os meliantes virtuais possam continuar impunes, seja pela criação de agencias unificadas especializadas em cyber crimes ou pela introdução de novos tipos penais que buscam em seu cerne o combate aos delitos informáticos.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAUJO ÁLVES, Matheus de. *Crimes digitais, análise da criminalidade digital sob a perspectiva do Direito processual penal e do instituto da prova*. Belo Horizonte: Ed. Dialética, 2020.

BRASIL. Decreto-Lei n 2.848, de 07 de dezembro de 1940. *Código Penal*. 1940.

BRASIL. Decreto-Lei n 3.689 de 03 de outubro de 1941. *Código de Processo Penal*. 1941.

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

DOS SANTOS, Juarez Cirino. *Direito Penal, parte geral*. ampl. e atual. Paraná: Tirant lo Blanch, 2014.

FRANÇA EVANGELISTA, Thalyta. *Crimes virtuais e o ordenamento jurídico brasileiro*. João Pessoa: Arte e diagramação, 2020.

LIMA, Renato Brasileiro de. *Manual de processo penal*: Volume único. 10. ed. rev., ampl., e atual. São Paulo: Ed. Jus Podivm, 2021.

MIRABETE, Júlio Fabbrini; FABBRINI, Renato N. *Código Penal interpretado*. 9. ed. São Paulo: Atlas, 2015.

RONCADA, Rodiner. *A prova da materialidade delitiva nos crimes cibernéticos*. São Paulo: EMAG, 2017.

TAVARES, Juarez. *Fundamentos da teoria do delito*. 4. ed. rev. e atual. São Paulo: Tiranch lo Blanch, 2018.

VIANA, Túlio Lima. *Discursos sediciosos nº 14, A era do controle*: Introdução crítica ao direito penal cibernético. Rio de Janeiro: instituto carioca de criminologia. 2004.

VIANA, Túlio Lima. *Do acesso não autorizado a sistemas computacionais*: Fundamentos do direito penal informático. Belo Horizonte: Faculdade de Direito da UFMG, 2001.

WENDT, Emerson; NOGUEIRA JORGE, Higor. *Crimes cibernéticos, ameaças e procedimentos de investigação*. 3. ed. Rio de Janeiro: Brasport, 2021.

ZÍLIO, Jackson. *Discursos sediciosos n 19, Da ilegalidade de bens à ilegalidade de direitos sobre a resistência ao movimento de expansão e modernização do Direito Penal*. Rio de Janeiro: Instituto carioca de criminologia, 2014.

Referencias de internet:

A DEEP WEB e a relação com a criminalidade na internet. *Revista Eletrônica Direito & TI*. Disponível em: http://direitoeti.com.br/artigos/a-deep-web-e-a-relacao-com-a-criminalidade-na-internet/. Acesso em: 19 ago. 2022.

ALLEGRO, Romana Affonso de Almeida. Bens jurídicos: o interesse estatal de tutelar bens jurídicos através de sua normatização. 2005. *Direito Net*. Disponível em: https://www.direitonet.com.br/artigos/exibir/2089/Bens-juridicos. Acesso em: 18 ago. 2022.

BARLOW, John Perry. Declaração de Independência do Ciberespaço. *Portal DH Net*. Disponível em: http://www.dhnet.org.br/ciber/textos/barlow.htm. Acesso em: 11 set. 2022.

DESIDERATO, João Gabriel. Prática penal, entenda o que é iter criminis. *Jus Brasil*. Disponível em: https//https://joaogabrieldesiderato.jusbrasil.com.br/artigos/1197475045/pratica-penal-entenda-o-que-e-iter-criminis#:~:text=Essas%20fases%20percorridas%20pelo%20agente,%2C%20prepara%C3%A7%C3%A3o%2C%20execu%C3%A7%C3%A3o%20e%20consuma%C3%A7%C3%A3o. Acesso em: 25 ago. 2022.

EVARISTO, Silvana Aparecida Cardoso; CESAR, Claudio Evaristo. Direito x internet. *Âmbito Juridico*. Disponível em: https://ambitojuridico.com.br/edicoes/revista-127/direito-x-internet/#:~:text=Desse%20modo%2C%20celeridade%20da%20internet,em%20vista%20justamente%20a%20celeridade. Acesso em: 17 ago. 2022.

F. BROTTO, Thaiana. Bullying na escola: conheça os tipos e saiba como lidar. *Psicologo e Terapia*. Disponível em:

https://www.psicologoeterapia.com.br/blog/bullying-na-escola-conheca-os-tipos-e-saiba-como-lidar/. Acesso em: 23 set. 2022.

FERNANDES, Lauren. Exposição nas redes sociais sem autorização. *Jus Brasil*. Disponível em: https://laurenfernandes.jusbrasil.com.br/artigos/686195090/exposicao-nas-redes-sociais-sem-autorizacao. Acesso em: 20 ago. 2022.

GOLDSMITH, Jackson; WU, Tim. *Who controls the Internet?* The ilussions of a boderless world. Oxford: Oxford University Press, 2006.

INTERNETS wild West days are coming close. *The Atlantic*. Disponível em: https://www.theatlantic.com/sponsored/pwc-2019/internets-wild-west-days-are-coming-close/3064/. Acesso em: 25 ago. 2022.

JORGE, Higor Vinicius Nogueira; SANNINI, Francisco. Infiltração virtual de agentes representa avanço nas técnicas de investigação. *JUS*. Disponível em: https://jus.com.br/artigos/57632/infiltracao-virtual-de-agentes-representa-avanco-nas-tecnicas-especiais-de-investigacao. Acesso em: 20 ago. 2022.

PCDF deflagra operação Darknet. *Polícia Civil do Distrito Federal*. Disponível em: https://www.pcdf.df.gov.br/noticias/11059/pcdf-deflagra-operacao-darknet. Acesso em: 2 out. 2022.

RODELLA, Abdo Cibele. Internet: um novo paradigma de informação. *Revistas.Usp.Br.*, no.1, v10., p. 41-48, 2005.

SASSEN, Saskia. *The impact of the internet on sovereignty*: unfounded and real worries. 2000.

SEGURADO, Rosemary; LIMA, Carolina Silva Mandú de; Cauê S. AMENI. Regulamentação da internet: perspectiva comparada entre Brasil, Chile, Espanha, EUA e França. *Scielo.* Disponível em: https://www.scielo.br/j/hcsm/a/TrcdX6SmXCcNqBLCcR7rb7J/abstract/?lang=pt. Acesso em: 17 ago. 2022.

SISTEMA unificará vendas online de imóveis da união estados e municípios. *Governo Federal*. Disponível em: https://www.gov.br/pt-br/noticias/financas-impostos-e-gestao-publica/2021/04/sistema-unificara-vendas-on-line-de-imoveis-da-uniao-estados-e-municipios. Acesso em: 19 ago. 2022.

STAMILE, Natalina. *Revista Brasileira de Direito*, v. 18, n. 3, RBD. set./dez. 2022. Disponível em: https://seer.imed.edu.br/index.php/revistadedireito/article/view/2183/1839. Acesso em: 25 ago. 2022.

STF. *RE: 628.624 MG*, Rel.: Marco Aurélio, Data de Julgamento: 29/10/2015, Tribunal Pleno, Data de Publicação: 06/04/2016.

STJ. *CC 121.431/SE*, Rel. Ministro Marco Aurélio Bellizze, Terceira Seção, julgado em 11/04/2012, DJe 07/05/2012.

STJ. *HC: 615857 SP 2020/XXXXX-7*, Rel. Ministro Reynaldo Soares da Fonseca, Data de Publicação: DJ 29/09/2020.

TJ-MG. *APR: XXXXX70474472001*. Belo Horizonte, Rel. Furtado de Mendonça, Data de Julgamento: 23/11/2021, Câmaras Criminais / 6ª CÂMARA CRIMINAL, Data de Publicação: 26/11/2021. Disponível em: https://www.jusbrasil.com.br/jurisprudencia/tj-mg/1325315800. Acesso em: 8 set. 2022.