

ALEX ALVES OLIVEIRA

DESAFIOS LEGAIS NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS PELA POLÍCIA

Ji-Paraná-RO

2024

ALEX ALVES OLIVEIRA

**DESAFIOS LEGAIS NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS PELA
POLÍCIA**

Trabalho de Conclusão de Curso
apresentado ao Centro universitário São
Lucas Ji-Paraná, para obtenção de grau
na disciplina Trabalho de Conclusão de
Curso – TCC, em Direito.

Prof. Orientador: Esp. Weliton do
Nascimento Alexandre.

Ji-Paraná-RO

2024

Dados Internacionais de Catalogação na Publicação - CIP

O48d	Oliveira, Alex Alves. Desafios legais na investigação de crimes cibernéticos pela polícia. / Alex Alves Oliveira. – Ji-Paraná, 2024. 23 p. Trabalho de Conclusão de Curso (Graduação em Direito) – Centro Universitário São Lucas Ji-Paraná, 2024. Orientador: Prof. Esp. Weliton do Nascimento Alexandre. 1. Crimes cibernéticos. 2. Investigação policial. 3. Legalidade. 4. Formação especializada. 5. Cooperação internacional. I. Alexandre, Weliton do Nascimento. II. Título. CDU 34:681.51
------	--

DESAFIOS LEGAIS NA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS PELA POLÍCIA

Alex Alves Oliveira¹

Weliton do Nascimento Alexandre²

RESUMO: Esse estudo tem por objetivo compreender a legitimidade das investigações para com os crimes cibernéticos pela polícia, quais áreas estão autorizadas de serem investigadas por essas autoridades e a importância do treinamento e aprimoramento além de trabalhar em conjunto com autoridades internacionais para erradicar e elucidar esses crimes. Além disso, é válido considerar importante a atualização das leis para que fique paralela e equiparada ao avanço tecnológico que a sociedade vive hoje em dia. Aportou-se metodologicamente na pesquisa bibliográfica descritiva para realização desse trabalho a fim de compreender e expor de forma eficiente a temática proposta. Assim, esperou-se apresentar uma completa análise dos empecilhos que os policiais se deparam ao investigar esses delitos e sugerir meios de vencê-los e alcançarem êxito no seu trabalho.

Palavras-chave: Crimes cibernéticos. investigação policial. Legalidade. formação especializada. cooperação internacional.

LEGAL CHALLENGES IN THE INVESTIGATION OF CYBER CRIMES BY THE POLICE

ABSTRACT: This study aims to understand the legitimacy of investigations into cybercrime by the police, which areas are authorized to be investigated by these authorities and the importance of training and improvement as well as working together with international authorities to eradicate and elucidate these crimes. In addition, it is worth considering the importance of updating laws so that they are parallel and in line with the technological advances that society is experiencing today. This work was based on descriptive bibliographical research in order to efficiently understand and expose the proposed theme. In this way, we hope to present a complete analysis of the obstacles that police officers face when investigating these crimes and suggest ways of overcoming them and achieving success in their work.

Keywords: Cybercrime. police investigation. Legality. specialized training. international cooperation.

¹Acadêmico do 10º período do curso de Direito no Centro Universitário São Lucas Ji-Paraná/RO. E-mail: alex_oliveirajp@hotmail.com

² Professor Orientador, Especialista em Direito Processual Civil, Pós-graduando em Docência no Ensino Superior, ambos pela Faculdade FAVENI (2022), Bacharel em Direito pelo Centro Universitário São Lucas Ji-Paraná (2021). E-mail: weliton.alexandre@saolucasjiparana.edu.br.

INTRODUÇÃO

Tem-se como origem da internet uma rede criada pela Arpanet com o intuito de troca de informações, desenvolvida para conectar na década de 1960, instalações de pesquisas militares com o pentágono nos EUA. À época, esteve vinculada principalmente a disputa por tecnologia entre as nações dos Estados Unidos e União Soviética dentro do espaço temporal da Guerra Fria.

Nos anos de 1970 militares e pesquisadores fizeram uso da Arpanet concordando que o e-mail seria a mais propícia maneira de comunicação, pois possibilitava envio de mensagens de forma mais veloz entre os usuários. Para além disso, criou-se aplicativos destinados ao uso em computadores que possuíam conexão com a Arpanet. O NPC foi o protocolo de comunicação utilizado para essa finalidade.

Na perspectiva de Lins (2023) a conectividade entre bilhões de dispositivos ao redor do mundo tornou a internet uma infraestrutura indispensável para o cotidiano da sociedade. Cenários como educação, comércio, trabalho, atividades de lazer fazem uso desse recurso para melhor fluxo e alcance os objetivos propostos. Nesse sentido, é inegável a expansão de conexão dela em dispositivos eletrônicos e também, para veículos automotores, eletrodomésticos, sistemas segurança etc.

Nesse sentido, é válido dizer que no cenário social e político da atualidade a internet sem sombra de dúvidas é uma ferramenta amplamente usada, seja na organização de protestos, compartilhamento de informações, elaborar campanhas etc. Dentre os caminhos que são recorridos pelos usuários, as redes sociais estão no topo da lista, haja vista que são as plataformas que os indivíduos estão em contato desde o despertar até o dormir.

Esse estudo tem por objetivo compreender a legitimidade das investigações para com os crimes cibernéticos pela polícia, quais áreas estão autorizadas de serem investigadas por essas autoridades e a importância do treinamento e aprimoramento além de trabalho em conjunto com autoridades internacionais para erradicar e elucidar esses crimes. Além disso, é válido considerar importante a

atualização das leis para que fique paralela e equiparada ao avanço tecnológico em que a sociedade vive hoje em dia. Aportou-se metodologicamente na pesquisa bibliográfica descritiva para realização desse trabalho a fim de compreender e expor de forma eficiente a temática proposta. Assim, esperou-se apresentar uma completa análise dos empecilhos que os policiais se deparam ao investigar esses delitos e sugerir meios de vence-los e alcançarem êxito no seu trabalho.

1. CONTEXTO HISTÓRICO DA INTERNET NO BRASIL E NO MUNDO

1.1. ORIGEM DA INTERNET

Tem-se como origem da internet uma rede criada pela Arpanet com o intuito de troca de informações, desenvolvida para conectar na década de 1960, instalações de pesquisas militares com o pentágono nos EUA. À época, esteve vinculada principalmente a disputa por tecnologia entre as nações dos Estados Unidos e União Soviética dentro do espaço temporal da Guerra Fria. Em âmbito de corrida espacial, lançou-se no espaço, pela União Soviética, o primeiro satélite artificial nomeado *Sputnik*. Assim, como forma de resposta, o governo norte-americano se empenhou na elaboração de um projeto que superasse o feito do até então rival direto, que resultou postumamente na criação da internet que hoje é usada mundialmente (ANNES, 2022).

Em 1958, ocorreu a implementação da *Advanced Research Projects Agency* (Arpa), a qual na atualidade atende pela sigla Darpa. Tal agência foi responsável pelo estabelecimento de um programa que objetiva desenvolver um sistema ao qual fosse possível enviar dados e informações relevantes para os centros militares bem como os de pesquisa e também, para o Pentágono. Almejava-se ainda seu uso como ferramenta de defesa e proteção do país caso houvesse, por exemplo, uma guerra nuclear. A iniciativa criada pela Arpa chamada Arpanet foi coordenada por Robert Taylor e Lawrence Roberts, e também contou com a contribuição de vários outros pesquisadores. Na ocasião, foram utilizadas *Wide Area Networks* (WAN) como meio de transmissão de informações (ANNES, 2022).

A Arpanet foi lançada em 1969, e naquele momento, apenas quatro computadores nos Estados Unidos tinham capacidade para enviar dados através

dessa rede. No momento, a comunicação foi feita de um computador da UCLA para um computador no SRI em Menlo Park, ambos na Califórnia. A primeira avaliação ocorreria com a transmissão da frase “*log win*”, porém o sistema na universidade de Stanford falhou ao processar e travou ao receber a letra “g”. Um teste adicional, feito logo em seguida, teve êxito. A partir desse momento, foi estabelecida uma conexão de instabilidade entre UCLA e SRI. (ANNES, 2022).

Assim surgiu a internet, com o objetivo principal de simplificar a comunicação entre esses locais e, conseqüentemente, estabelecer um sistema de proteção contra os soviéticos durante a Guerra Fria.

1.2. EVOLUÇÃO DA INTERNET

Nos anos de 1970 militares e pesquisadores fizeram uso da Arpanet concordando que o e-mail seria a mais propícia maneira de comunicação, pois possibilitava envio de mensagens de forma mais veloz entre os usuários. Para além disso, criou-se aplicativos destinados ao uso em computadores que possuíam conexão com a Arpanet. O NPC foi o protocolo de comunicação utilizado para essa finalidade. Em decorrência do aumento significativo da utilização da Arpanet, viu-se a indiscutível necessidade de implementação de protocolos que fossem padronizados a todos que dela desprendessem, foi então que, no ano de 1983 começou-se o uso do *Internet Protocol* (IP) e também, do *Transmission Control Protocol* (TCP) ambos contemplando as metas estipuladas pelos criadores. Por falar em metas, a aplicação desses protocolos visava ler e encaminhar mensagens significativas a época de um usuário ao outro, de maneira segura, a fim de evitar vazamento de dados “privados” (RODRIGUES, 2008)

No final da década dos anos 1980 os primeiros passos para utilização da Arpanet para fins comerciais começaram a ser vivenciados. Até então, os usuários restringiram-se a pesquisadores. Esse uso para fins comerciais propiciaram uma expansão de comunicação entre aqueles que a esse serviço tinham acesso, fazendo com que impreterivelmente os utilizadores trocassem mensagens por meio dessa ferramenta, a nível mundial. Dado esse fato, a National Science Foundation se viu no cenário de estudos serem feitos para viabilizar a expansão da conectividade

dessa rede ao público geral (sociedade civil e que tivessem os recursos necessários para adquiri-lo) A NSFNET, tida como base da internet atual, foi estabelecida em 1986 a partir dessas pesquisas. A NSFNET também permitiu a expansão da utilização da internet (RODRIGUES, 2008).

1.3. INTERNET NO BRASIL

A internet foi introduzida no Brasil em 1988. Esse fato importante para a história brasileira se deu por uma conexão entre a rede da Universidade Maryland nos Estados Unidos com um computador da Universidade Federal do Rio de Janeiro, no respectivo ano. Em São Paulo a conexão na internet também se iniciou nesse ano por meio da Faesp (Fundação de Amparo à Pesquisa do Estado de São Paulo). Nota-se então um cenário de conexões por parte de universidades e instituições de pesquisa gradualmente ampliadas por meio da utilização do Alternex. Sua origem também ocorreu nessa respectiva data (CARVALHO, 2021).

Em 1989 com o intuito de criar uma infraestrutura em território nacional de internet, o Ministério da Ciência e Tecnologia (MCT) fundou a Rede Nacional de Pesquisa (RNP). É preciso dizer que se limitou esse serviço a sociedade acadêmica e pesquisadora brasileira, até o ano de 1995. Realizada na cidade do Rio de Janeiro, a Rio-92 ou Eco-92 foi um evento designado que marcou por ser o primeiro com acesso à internet no Brasil. Esse evento era parte da Conferência da ONU (Organização das Nações Unidas) a qual tratava da temática de desenvolvimento e meio ambiente. O teste de internet comercial no território brasileiro ocorreu no dia 20 de dezembro de 1994 sob a responsabilidade da empresa Embratel. Nesse evento, compareceram o quantitativo de cinco mil pessoas. Cabe destacar que essa empresa perdeu a exclusividade de oferecer tal serviço mediante decisão do ministro das comunicações da época (CARVALHO, 2021).

A disponibilidade da internet no Brasil para fins comerciais só começou entre 1994 e 1995. A organização da RNP se expandiu além do meio acadêmico e começou a ser utilizada para necessidades do mercado. Em 1995, foi criado o Canal Vip, o domínio comercial pioneiro registrado no Brasil. Durante essa fase, sites de notícias, bancos, empresas e bandas como o Barão Vermelho já disponibilizaram

seus sites na internet. No final de 2021, aproximadamente 120 mil indivíduos já tinham acesso à internet no Brasil (ANNES, 2022).

O CGI foi implementado em 1995 com o objetivo de discutir sobre a segurança e o progresso da internet. O Grupo de Coordenação da Internet inclui membros da comunidade, indústria e universidade e trabalha para realizar pesquisas e oferecer sugestões sobre segurança online. Em 1996, foi lançado o site do Jornal do Brasil, sendo o pioneiro entre os jornais brasileiros a estar online. Depois disso, os sites dos grupos UOL e Terra foram criados. Gilberto Gil foi um dos primeiros artistas brasileiros a disponibilizar músicas na internet com a canção "Pela internet". (ANNES, 2022).

Em 1997 teve um marco significativo na história eleitoral do Brasil, o primeiro resultado que foi divulgado via internet. Ainda nesse ano, as primeiras remessas de declarações recolhidas de Imposto de Renda via online. Já em 2004 as redes sociais em seus primórdios expansivos chegaram ao país com a inauguração da rede social Orkut que pertencia a empresa Google, tal feito foi tão significativo na sociedade que, o Brasil se tornou uma das nações com mais usuários do aplicativo no mundo. Outro evidente acontecimento evolutivo da internet nacional foi o surgimento da conexão móvel, ou seja, poder se conectar de qualquer lugar fora de casa, essa conexão ficou conhecida como 3G e a pioneira dessa viabilização conectiva foi a empresa de telefonia Vivo. No ano seguinte em 2005, uma pesquisa realizada pela empresa Ibope, uma estimativa de onze milhões de pessoas faziam uso da navegação da internet em suas residências. Ainda nesse estudo divulgado, calculava-se uma média de quinze horas e quatorze minutos semanais de tempo gasto na rede. Por meio da lei nº. 12.965/2014 direitos, obrigações, princípios e garantias quanto a utilização da internet no Brasil foi direcionada, sendo considerado assim, o marco civil da internet no país. (ANNES, 2022).

2. INTERNET NOS DIAS ATUAIS

Na perspectiva de Lins (2023) a conectividade entre bilhões de dispositivos ao redor do mundo tornou a internet uma infraestrutura indispensável para o cotidiano da sociedade. Cenários como educação, comércio, trabalho, atividades de lazer

fazem uso desse recurso para melhor fluxo e alcance os objetivos propostos. Nesse sentido, é inegável a expansão de conexão dela em dispositivos eletrônicos e também, para veículos automotores, eletrodomésticos, sistemas segurança etc.

Hoje, a pauta quanto a avanços tecnológicos está em torno da IA (Inteligência Artificial) e, da big data. Com o uso dos algoritmos, a expansividade da exibição de marketings e propagandas comerciais é fomentando pelas empresas que da IA utilizam, atingido todos os indivíduos online. Já a big data, fica responsável pela análise da grande massa de dados/informações e direcionar decisões estratégicas e mais bem informadas (LINS, 2023).

Nesse sentido, é válido dizer que no cenário social e político da atualidade a internet sem sombra de dúvidas é uma ferramenta amplamente usada, seja na organização de protestos, compartilhamento de informações, elaborar campanhas etc. Dentre os caminhos que são percorridos pelos usuários, as redes sociais estão no topo da lista, haja vista que são as plataformas que os indivíduos estão em contato desde o despertar até o dormir.

É pertinente destacar o cenário brasileiro no mercado da internet. Nas concepções de Anne (2022) o país é um dos maiores mundialmente falando. Isso ocorre em razão da grande massa da comunicação entre os usuários como por exemplo, via whatsapp, um aplicativo de mensagens instantâneas muito popular da atualidade. Além desse fato, o surgimento do varejo online como Magazine Luiza, Mercado Livre, por exemplo, é outro ponto favorável a expansão do uso da navegação no território nacional e assim, estar no patamar em que se encontra.

3. ORIGEM E EVOLUÇÃO DOS CRIMES CIBERNÉTICOS

A definição de crimes virtuais é algo atual em comparação com os conceitos de crimes tradicionais, os quais têm sido treinados por longo período. Uma definição popular é fornecida por Krone (2005), que caracteriza crimes virtuais como transgressões que abarcam desde ataques contra dados até proteção de conteúdo e direitos autorais. No entanto, a definição é ampla e inclui atividades como fraude,

acesso não autorizado, exploração infantil e assédio online. É um crime virtual, isto é, um crime que utiliza tecnologia eletrônica.

Na sua obra "Crimes virtuais, vítimas reais", Moisés Cassanti define crimes virtuais como qualquer ação em que um computador ou rede de computadores seja usada como instrumento, ponto de ataque ou forma de crime. Os primeiros atos violentos ligados à complexidade nos anos 1960 nos EUA. Naquele período, os primeiros incidentes de computadores sendo usados para práticas criminosas, como sabotagem e espionagem, foram documentados na imprensa e na literatura científica nos Estados Unidos. Apenas nos próximos dez anos, estudos sistematizados e científicos foram realizados em relação ao assunto. Desde 1980, houve um aumento nas atividades criminosas, com foco em fraudes bancárias, pirataria de software, manifestamente em redes de comunicação e exploração de crianças (BICUDO, 2012).

Apesar de relatos de atividades criminosas virtuais desde os anos 1970, foi apenas durante uma reunião do G-8 no final dos anos 90, para combater crimes online, que o termo "crime cibernético" foi criado para designar como divulgado na internet. (D'URSO, 2017).

O *ciberbullying*, com o suporte da tecnologia da informação, ultrapassa os limites temporais mantendo a ofensa presente indefinidamente no ambiente virtual, assim como ultrapassa os limites geográficos do espaço físico (Silva; Mascarenhas, 2010). Existem diversas formas de se chamar a prática dessas infrações penais atualmente, mas a maioria dos escritores as caracteriza como "crimes digitais".

O escritor complementa ao abordar a questão: "Crimes virtuais são atos ilegais de homicídios via internet que podem se enquadrar no Código Penal Brasileiro, resultando em sanções como multas ou detenção." (CASSANTI, 2016). Desta forma, os crimes cometidos ou facilitados pela internet ou por sistemas de computador podem prejudicar diferentes aspectos legais, como as pessoas (vida, privacidade, liberdade individual, entre outros) e o patrimônio (tangível e intangível).

Os delitos informáticos ocorrem no ambiente virtual, por meio da internet ou sistemas informáticos, sendo praticados não apenas através dos computadores, mas também através das plataformas móveis, tais como celulares, *smarthphones*, tablets, por meio das mais diversas formas, sendo alguns exemplos: vírus, *spam*, *botnet*, *phishing*, *spyware*, *worm*, entre outros.

O cybercriminoso é aquele agente que pratica conduta típica, antijurídica e culpável, virtualmente, e será processado, julgado e punido por suas ações. Esses agentes não possuem um perfil padrão, podendo ser tanto pessoas possuidoras de um conhecimento técnico mais profundo a respeito da internet, os chamados hackers ou crackers, quanto usuários comuns que, por meio de seus atos no âmbito virtual, praticam os mais variados crimes (estelionato, crimes contra honra, pedofilia, racismo) contra outros usuários.

Dessa forma, entende-se que se tratam de pessoas as quais empenham seus saberes acerca da tecnologia da informação a fim de acessar legalmente sistemas de segurança, senhas de redes, códigos criptografados sendo oriundas de ações criminosas.

No entanto, esses indivíduos não possuem conexão com subtração de dados ou até mesmo acessar sem autorização sistemas, sendo nesse caso o oposto do que o senso comum pensa. Podem ser definidos como um programador de sistemas e desenvolvedor de proteção e *softwares*, ou seja, o *hacker* utiliza todo seu conhecimento técnico para aperfeiçoar softwares licitamente e elaborar soluções inteligentes para um problema de programação e segurança.

Com o aprimoramento e popularização dos meios eletrônicos e surgimento da internet, se tornou cada vez mais frequente a prática de atos delituosos por meio da esfera digital em que os agentes se utilizam de todos os recursos e meios possíveis proporcionados pela internet e outros instrumentos tecnológicos, para cometerem os mais diversos tipos de infrações.

Não é necessário, no entanto, ter um notório conhecimento de informática. Os criminosos usam do anonimato ou até mesmo do equivocado pensamento de

estarem protegidos por uma tela digital para disseminarem ódio, para difamar, ofender, piratear, roubar informações, divulgar dados pessoais de outrem sem a devida permissão, entre outros inúmeros delitos.

Com a chegada da *dark web*, parte anônima da deep web, crimes mais graves contra a confiança e a propriedade passaram a ser realizados e planejados, como pedofilia, terrorismo, apologia ao crime, venda ilegal de produtos, armas, drogas, entre outros. A expressão “Deep Web” refere-se à parte da internet que não está disponível para pesquisa através de ferramentas como Google, Chrome, Safari ou Edge. Por conter conteúdos sigilosos, difíceis de serem acessados e descobertos, passou a ser usado por pessoas perigosas com intuito de praticar condutas criminosas sem serem descobertas.

Muitos indivíduos passaram a utilizar a rede para ferir o direito do outro, com o pensamento de que ali estariam impunes, podendo cometer as mais variadas infrações e não serem “pegos”.

Portanto, no Brasil, com a promulgação da Constituição em 1988 que estabeleceu que as questões de informática deveriam ser de competência do Estado, vem tomando medidas para lidar com essa nova realidade, tentando alcançar os infratores no plano virtual e aplicando punições no mundo real.

O Ordenamento Jurídico brasileiro já conta com algumas normas, as quais preveem direitos, deveres, sanções quanto ao uso da internet no Brasil. Entretanto, essas normas não acompanham as necessidades sociais e a complexidade que se trata o cybercrime.

4. FUNDAMENTOS LEGAIS E NORMATIVOS DA INVESTIGAÇÃO DE CRIMES CIBERNÉTICOS

A influência da tecnologia ao cotidiano da sociedade, isso é, no modo de interação, questões de trabalho e de atividades diárias é algo pertinente na atualidade. Isso se dá pelo avanço que essa área sofre de maneira constante, desde sua fundação. Nesse aspecto, o mundo dos crimes online é um campo que traz consigo severas batalhas na área jurídica. Dentre as tipificações de crimes

cibernéticos, pode-se ter como exemplo hacking, invasão de sistemas, phishing, pornografia infantil etc.

Junto com as oportunidades ímpares que vieram acompanhando a evolução tecnológica, também trouxe para o mundo, desafios complexos de lidar no universo do ciberespaço. As autoridades que são incumbidos de combater e proteger a população frente a esse delito afirmam ser prioridade estudos a fim de compreender senão em sua totalidade, maior parte do funcionamento dessa situação para que dessa maneira, crie-se estratégias intervencionistas para sua erradicação.

Uma adaptação já está em andamento quanto a legislação brasileira para que se possa ter punições adequadas aos infratores que esse crime praticarem. Dessa forma, assegura-se a conservação dos direitos dos cidadãos e interliga eficientemente as instituições que trabalham nessa área.

4.1. MARCO CIVIL DA INTERNET

No ano de 1999, o Projeto de Lei n. 84/99, também conhecido como "PL Azeredo", foi introduzido no Senado, sendo desenvolvido pelo ex-deputado Luiz Piauhyllino e com Eduardo Azeredo como relator. Esse projeto, que tratava dos crimes online e suas punições, recebeu muitas críticas por ser considerado "criminalizador", "vigilante" e repressivo, o que infringiu os direitos fundamentais dos usuários. Por causa dessas características, a sociedade rejeitou o projeto e o chamou de "AI-5 Digital", mostrando a oposição do público a um modelo legislativo que favorece a repressão em vez de proteger as liberdades individuais.

Uma movimentação interinstitucional em prol de assegurar direitos e liberdades e também, regulamentar a internet no país, foi realizada em 29 do mês de junho do ano de 2009. Como resultado dessa ação, houve a promulgação da lei de nº 2.126/11 sancionada apenas no ano 2014. Ainda nesse respectivo ano, promulga-se a legislação conhecida como marco civil da internet, por meio da lei de nº 12.965/14 a qual direcionava como deveria ser aplicada o uso desse recurso em todo território nacional (BRASIL, 2014).

O principal objetivo dessa Lei é proteger a privacidade do usuário na internet e busca assegurar a inviolabilidade e o sigilo das comunicações, conforme determina o inciso X, do artigo 5º, da CF/88.

A Lei nº 12.965/14 ficou conhecida como “Constituição da Internet” e estabelece que os provedores não podem violar os direitos dos indivíduos à intimidade e privacidade dos usuários, sendo vedado, para tanto, a monitoração dos dados compartilhados pela rede, bem como realizar a divulgação destes. Ademais, assegura a exclusão dos dados quando as partes encerram com as atividades.

O Marco Civil se assenta em três pilares: “a garantia da neutralidade da rede; proteção à privacidade do usuário da Internet; e a garantia da liberdade de expressão”. (MAIA, 2017).

5. LEI CAROLINA DIECKMANN

No ano de 2011 houve um episódio em que ocorreu o vazamento de 36 fotos da atriz Carolina Dieckman, que na época, teve seu computador invadido por hackers, e o fizeram através do e-mail de Carolina. Antes de ter suas fotos vazadas, ainda, os hackers tentaram extorqui-la, pedindo dinheiro em troca da não publicação das fotos.

Em decorrência de alguns episódios em meados de 2011, ocorrendo vários ataques na navegação de serviços nos sites do governo brasileiro que ficaram

instáveis até saírem do ar, bem como, nos inúmeros outros casos de atos criminosos no âmbito virtual, foi apresentado um novo projeto de lei, em 29 de novembro de 2011 na Câmara dos Deputados.

Esse projeto era de autoria dos Deputados Federais Paulo Teixeira, Luiza Erundina, Manuela D’Ávila, João Arruda, Brizola Neto e Emiliano José, e visava a necessidade de criar uma legislação que regulamentasse de forma mais específica o uso “criminoso” dos meios cibernéticos.

O PL nº 2.793/11 diferencia-se do PL nº 84/99 no tratamento das tipificações penais e sugere redução no quantitativo de tipologias penais.

A PL intitulada “Lei Carolina Dieckman”, foi sancionada em 30/11/12 e se tornando assim a lei nº 12.737/12. Seu intuito partia do princípio de adequação das punições com base na gravidade do delito com base no CP brasileiro, sem assim ser necessários criar novas categorias criminais e mudar o que já estava posto. (Brasil, 2011). Com o alcance que o caso da atriz teve nos veículos de comunicação, a sensação de fragilidade entre os cidadãos foi iminente o que levou o legislativo agir de maneira rápida quanto a aprovação da referida lei.

Criou-se nessa legislação, os art. 154-A e 154-B que tratavam de tipificar os crimes de invasão de dispositivo informático e também se alterou itens no código 266 e 298 a fim de atingir detalhes oriundos dessa prática delituosa em computadores.

Assim, incorporou-se a previsão de crime de invasão de computadores, celulares, dispositivos alheios em geral no ordenamento jurídico do Brasil. Parte-se da premissa de não haver nesse caso, consentimento do proprietário ou até mesmo sem motivo algum. As penas possuem variação de três meses a um ano de detenção, podendo ser aumentada em caso de prejuízos econômicos a vítima.

O bem jurídico tutelado referia-se à violação da liberdade do usuário do dispositivo informático, através de outro dispositivo informático (Nucci, 2014). É crime comum, o qual pode ser praticado por qualquer pessoa, não se exigindo uma qualidade ou condição especial do agente para ser sujeito ativo, ou seja, não necessita que o invasor seja um especialista, conhecido como hacker (Junior, 2013, Nucci, 2014).

Ademais, o sujeito passivo também pode ser qualquer pessoa que seja responsável pelo bem jurídico que foi violado (NUCCI, 2014) seja ele o proprietário ou detentor do bem, como nos casos de equipamentos fornecidos por empresas aos seus funcionários (Prado, 2013).

Para a caracterização desse crime é fundamental o dolo (não cabendo, portanto, a forma culposa) (Reis, 2014).

5.1. LEI GERAL DE PROTEÇÃO DE DADOS

Um conjunto de leis a fim de assegurar privacidade e proteção de dados existem no Brasil, podendo se exemplificar, código do consumidor, marco civil da

internet, lei Carolina Dieckman etc. Porém, esse emaranhado de legislações causa complexidade para entendimento e ações com base nele. Assim sendo, com o objetivo de simplificar as coisas, cria-se a Lei Geral de Proteção de Dados (LGPD).

Promulgada em 14/08/18 pelo presidente na época, Michel Temer, a lei designava um prazo de 18 meses para adaptação e aplicação da legislação em todo território nacional nos vieses públicos e privados. Inclui-se nessa lei, o termo privacidade, que não se fazia presente no marco civil da internet, no seu sistema legal. Desejava-se enquadrar legalmente o tratamento de dados pessoais a fim de evitar danos aos cidadãos nas mais diferentes esferas (SÁ, 2019; TEFFÉ; VIOLA, 2019; PINHEIRO, 2020).

Em seus princípios, direitos e obrigações estabelecidas, anseia-se por proteger os dados pessoais da população, considerado um dos bens mais valiosos que um indivíduo tem, no âmbito digital. Implica essa lei que todos os departamentos que tenham contato com os dados pessoais de alguém, independentemente de origem do departamento e se, pessoa física ou jurídica, deverá ter uma base legal para tratar tais dados, assegurando a privacidade deles. (PINHEIRO, 2020; TEFFÉ e VIOLA, 2019).

Cabe ressaltar que a lei está sob o fundamento da liberdade e privacidade, classificados como fundamentais na CF 88 brasileira. Contudo, também se escora no fomento ao desenvolvimento econômico e tecnológico do país. Dessa maneira, as instituições que com dados pessoais tenham contato, tem que ponderar entre esses dois pilares para que se possa tramitar o processo de maneira respeitosa, transparente e sem intempéries. (BRASIL, 2018).

Outro elemento essencial da LGPD é o consentir. Mas há algumas exceções a isso. No entanto, cabe ressaltar que situações dão brechas para tratamento de dados sem consentimento do cidadão, como é o caso de executar política pública (respaldada por lei), contratos, proteger o crédito, defesa de direitos em processos etc.

Uma equipe eficiente e capacitada se faz necessária para fiscalizar e punir aqueles que descumprem as diretrizes e o regimento da LGPD. Para isso, criou-se a Autoridade Nacional de Proteção de Dados Pessoais- ANPD por meio da lei nº 13.853/19.

Adoção de medidas preventivas, elaboração de planos de contingência, resolver imprevistos com agilidade e replicar boas práticas são algumas das incumbências do responsável por gerir dados pessoais.

As falhas de segurança podem gerar multas de até 2% do faturamento anual da organização no Brasil limitado a R\$ 50 milhões por infração.

5.2. LEI DE STALKING (LEI 14.132/21)

A palavra “*stalk*”, em inglês significa perseguir. Desse modo, coação, ataque, perseguição são algumas das ações praticadas pelos criminosos praticantes desse crime e que, sempre estiveram no tópico de proibições.

O principal público vítima de stalking é feminino. Isso se dá pelo fato de historicamente serem colocadas como “propriedade” do homem e da sobressalência do machismo para com o dia a dia da sociedade. O olhar das mulheres quanto a essa conduta dos homens começou ser mais empregado após os anos 80 pois, anteriormente a luta por direitos ao voto, ao trabalho, aos métodos contraceptivos etc. eram as prioridades das feministas em suas batalhas contra o sistema.

Portanto, o Brasil, abraçou uma luta estrangeira e, junto com ela, trouxe ao seu ordenamento jurídico, um nome que já estava em uso mundo afora. Dessa forma, em abril de 2021 sanciona-se a lei nº 14.132/21 a qual inclui o art. 147-A do CP brasileiro e exclui o art. 65 da LCP.

Da simples leitura do texto legal, é possível notar o quanto o legislador se debruçou sobre os problemas para que as mais diversas possibilidades pudessem ser tuteladas pelo tipo penal. Primeiro, pela substituição do termo “molestar”, por “perseguir”. Segundo, pois, apesar de impor algumas condicionantes (quais sejam a prática reiterada; a ameaça à integridade física ou psicológica e a restrição da

capacidade de locomoção), o trecho final do caput volta a deixar o crime extremamente abrangente quando diz que também será perseguição quando o agente, não incorrendo nas possibilidades e condicionantes anteriores, de qualquer forma, invadir ou perturbar a privacidade ou a liberdade da vítima.

Pois bem, com toda a riqueza de detalhes do novo texto legal, o que mais inovou foi o termo “por qualquer meio”, isto é: presencialmente, virtualmente ou por qualquer outro modo que venha a existir eventualmente.

Contudo, nota-se que antes a prática de perseguição, inclusive na internet, era classificada como perturbação da tranquilidade e tinha uma punição branda e o advento da nova lei enquadra a ação como delito, e aumenta a punição para até 3 anos de reclusão.

6. ATUAÇÃO DA POLÍCIA INVESTIGATIVA

Garantir a eficiência das leis e proporcionar a paz aos indivíduos, têm se tornado cada vez mais uma tarefa difícil e custosa aos cofres públicos, por causa do aumento significativo dos crimes virtuais, como evidenciado através dos dados no ano de 2020 que apresentava o registro de denúncias anônimas contabilizando 156.692 casos, segundo os dados da Central Nacional de Denúncias de Crimes Cibernéticos. (SAFERNET, 2020).

Se faz necessário ter em posse do Estado recursos/ferramentas que viabilizem uma ampla investigação no âmbito virtual dos delitos nele cometidos, contando com apoio internacional e usando técnicas atualizadas e de alto nível para suas perícias. A punição dos crimes cibernéticos torna-se dificultosa se não existirem profissionais especializados em todos aspectos técnicos do mundo digital.

Para que a persecução penal seja bem sucedida, é essencial que as provas digitais sejam claras e possibilitem a comprovação da materialidade e da autoria dos delitos praticados através da rede mundial de computadores. As provas digitais apresentam traços específicos que permitem sua verificação, ou seja, elas deixam

marcas e se caracterizam como o rastro dos crimes cibernéticos (DOMINGOS,2017).

Com isso, é fundamental enfatizar que quando uma informação é registrada na internet ou em algum dispositivo informático, tal informação poderá ser recuperada dentro de um certo período, ainda que tenha sido apagada. Isso possibilita que a perícia forense analise as provas digitais, verificando sua autenticidade e integridade, propiciando a determinação do seu grau de confiabilidade (DOMINGOS, 2017).

Independente do motivo, seja para boas ou más finalidades, quando alguém se conecta à internet, o faz através de ISP (*Internet Protocol Provider*), ou provedor de acesso à internet, sendo que este atribui ao usuário um endereço de IP (*Internet Protocol*), “em uma determinada faixa de data e horário, comumente enquanto durar a conexão à internet. Tal atribuição pode ficar no provedor de conexão (registro de conexão associados a dados cadastrais)” (JESUS; MILAGRE, 2016).

Existe também a possibilidade de se obter informações acerca do acesso à internet através do registro do servidor do *proxy*. Há situações em que o delinquente cibernético faz uso de conexão direta, oportunidade na qual os logs de registro de navegação identificam quais os locais que o usuário esteve e os serviços utilizados por ele (MALAQUIAS, 2015).

Além disso, os *cookies*, pequenos registros de informações, são armazenados cada vez que o usuário acessa os *sites da internet*. Através dessas informações “é possível traçar o *user profile* (perfil do usuário) que se consolida em determinado espaço de tempo em virtude de comparação de dados estatísticos comparativos de suas preferências” (MALAQUIAS, 2015).

O papel da perícia forense em analisar as evidências que são colhidas no decorrer da investigação, essa tendo por indispensabilidade a presença de peritos nas buscas e apreensões, tem caráter essencial para assegurar clareza, transparência e não deixar que haja corrompimento ou perda de informações/dados relevantes a elucidação do caso. Outro fator importante é o tempo na obtenção das

evidências deixadas pelo agente, uma vez que a prova digital é extremamente volátil (DOMINGOS, 2017).

A perícia judicial pode ser até mesmo efetuada no computador pessoal, smartphone ou qualquer outro dispositivo que seja objeto de investigação e possa ter sido usado, por exemplo, para compartilhar conteúdos de pornografia infantil, incitação ao ódio, mensagens difamatórias vê-se aí então a necessidade da ordem judicial que determina a busca e apreensão como cautela, para averiguar a procedência dos fatos ou refutá-la por e-mail, arquivo ou programa que possa ter sido objeto do crime (MALAQUIAS, 2015).

Após a promulgação da Lei nº 12.850, de 2 de agosto de 2013, a infiltração de agentes poderá ser utilizada como forma de investigação nos crimes de pornografia infanto-juvenil via *internet*, considerando a transnacionalidade envolvida no delito, bem como a existência de tratado internacional que obriga o Brasil a promover a sua erradicação (WOLFF, 2017).

No caso concreto, o agente policial infiltrado tenta criar uma relação de confiança para que seja possível desvendar as ações criminosas ou introduzir-se no universo da organização criminosa, para que seja possível compreender seu funcionamento. Essa tarefa pode ser extremamente perigosa, razão pela qual necessita de agentes treinados para a sua execução (WOLFF, 2017).

Porém, o uso de agente infiltrado é procedimento de investigação excepcionalíssimo, sendo imprescindível a autorização judicial, que deverá ser circunstanciada, motivada e sigilosa, estabelecendo os limites a serem respeitados conforme norteia o art. 10 da lei nº 12.850/13. Ainda, observa-se que o §2º estabelece os requisitos para que a infiltração seja cabível: “será admitida a infiltração se houver indícios de infração penal de que trata o artigo 1º e se a prova não puder ser produzida por outros meios disponíveis”.

Desse modo, é possível o uso de infiltração de agentes para investigar o crime cibernético de pornografia com envolvimento crianças e adolescentes em razão da caracterização da internacionalidade da conduta. Por óbvio, para que se

possa utilizar desse método de investigação, deverá ser comprovada a impossibilidade de produzir a prova por outros meios. Afinal, “o uso de ardil por parte do Estado não deverá ser a regra, mas sim a última opção” (WOLFF, 2017).

Salienta-se, inclusive, que houve um avanço em relação ao combate os crimes digitais com a promulgação da Lei nº 12.735, de 30 de novembro de 2012, que prevê, em seu artigo 4º, que os órgãos da polícia judiciária poderão estruturar, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

7. CONSIDERAÇÕES FINAIS

Ao final dessa produção pode-se verificar que novas brechas têm sido encontradas pelos infratores no que diz respeito a crimes da internet quanto a vulnerabilidade e a ludibriação das vítimas. Isso ocorre dado ao avanço tecnológico vivenciado na sociedade atualmente. Assim, esse texto evidenciou a importância da multifase e da integralização de entidades na batalha contra a erradicação desse tipo de delito.

É imprescindível que haja investimento em capacitação profissional dentro das polícias, a fim de que os agentes saibam lidar com esses processos complexos, já que se trata do mundo digital. Utilizar inovações tecnológicas bem como recursos atualizados fomentam a taxa de sucesso na atuação da segurança pública frente a ação criminosa que é cometida nesse universo.

Inter institucionalizar a ação de combate ao crime cibernético é um caminho bem indicado para ter resultados positivos, isso é, agências nacionais e internacionais devem trabalhar em conjunto haja vista que esse tipo de delito percorre o mundo todo. A participação da comunidade civil também é fundamental pelo fato de serem agentes que podem auxiliar a polícia na captura dos suspeitos e assim, a investigação avançar e ter bons frutos.

8. REFERÊNCIAS

9.

ANNES, Franciso. **Origem da internet: saiba como tudo começou.** Disponível em: <https://inforchannel.com.br/2022/11/11/origem-da-internet-saiba-como-tudo-comecou/>." Acesso em: 20. set. 2024.

BRANT, Marcos Henrique Caldeira. **Stalking–perseguição obsessiva.** Belo Horizonte, 2013.

BRITO, A. L. A. **Stalking no Brasil: uma análise dos aspectos psicológicos e jurídico-penais.** 2013. 75 f. Monografia (Graduação em Direito) - Faculdade de Direito, Universidade Federal do Ceará, Fortaleza, 2013. Disponível em: <https://repositorio.ufc.br/handle/riufc/27193>. Acesso em: 04 out. 2024.

CASSANTI, Moisés de Oliveira. **Crimes Virtuais, Vítimas reais.** Rio de Janeiro: Brasport, 2014.

DOCUSIGN. **Descubra aqui qual é a história por trás da criação da internet.** Disponível em: <https://www.docusign.com.br/blog/criacao-da-internet>." Acesso em: 20 set. 2024.

D'URSO, Luiz Augusto Filizzola. **Cibercrime: perigo na internet.** Publicado em 2017.

Disponível em <http://politica.estadao.com.br/blogs/faustomacedo/cibercrime-Perigona-internet/>>. Acesso em: 27 set. 2024.

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

Lei que criminaliza stalking é sancionada. Senado Notícias, 05 abr. 2021. Disponível em: <https://www12.senado.leg.br/noticias/materias/2021/04/05/lei-que-criminaliza-stalking-e-sancionada>. Acesso em: 04 out. 2024.

RODRIGUES, V. **A origem da internet. Ministério da Educação:** 2008. Disponível em: <http://www.grupoescolar.com/pesquisa/a-origem-da-internet.html>. Acesso em: 25 set. 2024