INOCUIDADE NAS INVESTIGAÇÕES CONTRA FRAUDES BANCÁRIAS: direitos fundamentais X estrito cumprimento do dever legal e falta de controle dos perigos decorrentes dos avanços sociais e tecnológicos

Cristino Costa Ribeiro[1]

Humberto César Machado[2]

RESUMO: Esse trabalho faz levantamento de dados para mostrar visão crítica do senário atual em relação a controle de dados e fraudes eletrônicas, entender metodologia aplicada para tentativas de cessar crimes cibernéticos, apresentar leis previstas para coibir e mostrar diversas contradições em que pesa na dificuldade de incriminar o autor, como as demandas em grande proporção, atrapalham as autoridades ter êxito com menor tempo. Inovações tecnológicas são feitas para progresso social, porem conhecimento em mãos erradas acarreta em infrações, indicar em como usuários poderão navegar com maior tranquilidade no mundo virtual.

PALAVRAS-CHAVE: Crimes. Cibernéticos. Avanços. Tecnológicos. Pessoais.

1 INTRODUÇÃO

O presente trabalho, objetiva expor, refletir e indicar antinomia entre as leis e os métodos utilizados para investigações no espaço virtual nas searas Constitucional, Penal e Processual penal, apresentando o tema sobre os crimes cibernéticos observando fraudes bancárias e dados pessoais. Colocar em prática as determinações legais pode acarretar alguns empecilhos como demonstrar a materialização dos crimes desse porte, pois nos sujeita a oposições sob alguns direitos fundamentais na execução do objetivo de demostrar o fato jurídico.

Como por exemplo, direito a privacidade, umas das maiores dificuldades de lidar nesse tipo de cyber crime, pois as pessoas têm direito de sigilo de suas correspondências,

[1] Centro Universitário Alfredo Nasser. E-mail: cristinoribeiro@outlook.com.

[2] Pós-Doutor em Psicologia pela Pontifícia Universidade Católica de Goiás – PUC-GO (2016); Doutor em Psicologia pela PUC-GO (2013); Mestre em Psicologia pela PUC-GO (2006); Especialista em História pela Universidade Federal de Goiás - UFG (2002); Graduado em Filosofia pela UFG (1996); Graduado em Pedagogia pela ISCECAP (2018); Elemento Credenciado Fatores Humanos e Prevenção de Acidentes Aéreos pelo CENIPA (Centro de Investigação e Prevenção de Acidentes Aeronáuticos); Professor Coreógrafo e Dançarino de Salão; Membro do Comitê de Ética e Pesquisa e Professor do Centro Universitário Alfredo Nasser – UNIFAN; e, Professor da PUC-GO. E-mail: humberto.cesar@unifan.edu.br.

celulares, computadores, agendas etc. e como demonstrar autoria desse crime? A coleta de informações é de extrema importância, e deve ter cautela na observação dos direitos constitucionais e regras processuais que devem ser cumprida durante fase probatória do crime.

Independentemente de ser criminoso eles tem os mesmos direitos que todos, como devemos prosseguir para resolver esse "algoritmo", tão bom as vezes, mas ruim pela liberdade com que usam para aplicação do crime desejado. Hoje informações em grosso modo é muito fácil obter, uma pesquisa em algum browser como Google ou Fire Fox, Tor Browser entre diversos sistemas e maquinas que coletam e transmitem informações o dia inteiro.

Cotidiano hoje é você acordar utilizando um dispositivo e dormir com ele, a dependência de uma máquina para nos comunicarmos, seja navegando nas redes sociais, lazer, pesquisas ou trabalho, é nítido visualizarmos isso, onde nele se encontra diversos dados, inclusive os seus dados leitores estão em todo lugar, lojas, sites, escolas, faculdades, bancos.

A inviolabilidade do seu dispositivo eletrônico informático é a maior questão. Ele foi mesmo invadido? E como conseguiu obter seus dados? Informações podem ser obtidas fisicamente ou pode ser também através de uma navegação na internet que onde maior se propaga. Segundo Siqueira (2014),

> os tipos de vínculos numa abordagem investigativa podem ser diretos ou indiretos. Os vínculos diretos independem de complemento, como: transferência entre contas, registros de logs no servidor ..., utilizando na conexão com a vítima, conexão de internet (IP), pagamentos (transações bancárias) e recargas de celulares.

2 METODOLOGIA

O presente trabalho utiliza a metodologia exploratória por meio da pesquisa de artigos científicos e suas referências bibliográficas, atentando-se a não clonagem de ideias para evitar a não “descoberta” de dados já inseridos em trabalhos anteriores, sendo assim suscetível de novo conhecimento e ideias, contribuindo para o conhecimento, trabalhando a partir de contribuição dos autores de artigos, teses, livros, Leis, Jurisprudências, Súmulas.

3 DISCUSSÕES, RESULTADOS E/OU ANÁLISE DE DADOS

Os bancos adotam diversos tipos de protocolos para evitarem as fraudes, porem os *Hackers* e *Crakers* se atualizam todos os dias pois necessitam do crime para obter a vantagem desejada, uma das atualizações que as agências bancárias adotaram é o QRCode, onde tem um código de barras específico, ou mesmo *Tokens* para você ter acesso ao aplicativo ou site do banco. Para o fraudador, são necessários dados pessoais, senhas e logs ou número dos cartões, não necessariamente necessita de tudo, mas alguns dados são necessários dependendo do tipo de crime.

Já a polícia adota também alguns critérios para demonstrar o crime como dispõe Dantas *et al*. (2007), por exemplo no vinculo indireto: "necessita de outra técnica investigativa para ser comprovado, como: história-cobertura, infiltração, interrogatório, busca e apreensão, etc. São vínculos indiretos: localidade das agências das contas beneficiadas e os endereços das pessoas beneficiadas. Aplica-se AD no mapeamento criminal tendo como finalidade mostrar a densidade ou concentração de fatos, parte de um fenômeno, em um determinado espaço e tempo".

A nossa carta magna em seu artigo 5º e incisos X e XII, por exemplo, dispõe que: Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes: X - são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação; XII - é inviolável o sigilo da correspondência 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 instrução processual penal;

Observando, nota se que a inviolabilidade da intimidade e segurança ao quebrar sigilo de correspondências físicas ou eletrônicas, somente pelo fato de ele armazenar ou ter acesso já viola o direito, independente se ele mesmo que fez a captação das informações ou se lhe foi fornecido por terceiro. Conforme artigo do nosso código penal dispõe: 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: tipificando crime pela invasão do dispositivo eletrônico seja de qualquer tipo.

Trata-se também crime de estelionato quando estamos falando de fraudes bancárias, pois o criminoso se passa pela vítima utilizando os dados dela para obter a vantagem ilícita e que gera prejuízo a terceiros que no caso as agencias bancárias, então dois polos são atingidos se não mais dependendo do caso, como compras por aplicativo entre envolve mais uma vítima.

> 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:
> […]
> § 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.

As agências bancárias também tentam desenvolver seu papel para a proteção de dados, investindo em tecnologia para melhoria dos seus recursos antifraudes, identificar o *modus operandi* nem sempre é simples para a Polícia Federal, inviável por muitas vezes prender o indiciado preventivamente, pois o prazo é menor, sendo que muitas vezes a notificação do boletim de ocorrência pode ser demorado em relação ao prazo da data do crime cometido. E tentar provar compulsoriamente que um dispositivo que está sob sua posse que ligará ele a diversos crimes sem prévia autorização judicial poderá ser usada em desfavor como prova anulável e abuso de autoridade entre diversos argumentos de defesa.

Porém existe um padrão e uma constância com que cometem as fraudes, por isso ainda conseguem identificar o modus operante, uma compra feita no exterior, por exemplo, ela tem um rastreio para entrega, visualizando que terá um destinatário, surge a oportunidade de descobrir autoria, achando o receptador, provável que saiba quem é o estelionatário, dentro do mundo

Virtual também existe crime organizado, um sistema de logística implantado e criado por eles mesmos.

Importa para o processo de onde foi feito, onde se finalizou o crime, contudo eles cometem de onde estiverem, só precisam de uma máquina e acesso à internet, tudo isso deve ser pautado nas audiências, mas em razão do lugar do crime no casos de estelionato pelas dificuldades enfrentadas por nosso judiciário para definir quem seria competente pra julgar, ficou mais fácil determinando competente pra jugar o foro do lugar onde ocorreu o prejuízo e não do lugar onde executou.

4 CONSIDERAÇÕES FINAIS

Considerando que cada vez mais a evolução da ciência da informação faz com que criminosos continuem no anonimato sem ser punido, merece atenção para que não ocorra superdecadência nos créditos bancários, tanto que já previsto isso pela Circular nº 3.979, de 30 de Janeiro de 2020, trata-se dos riscos sob operações financeiras. Ótimos projetos realizados pela Polícia Federal, porém não deixam de ter milhares de casos sem uma conclusão, entendendo que a demanda de casos é superior à quantidade de resoluções com mérito, carecendo de mais profissionais e capacitados, com vasto conhecimento assim como os Hackers e Crackers, para a erradicação desse crime seja cumprida com porcentagem maior no cenário atual.

REFERÊNCIAS

ARAGÃO, David Farias. Monografia (Bacharelado em Ciências Econômicas) - Universidade Federal do Paraná, Setor de Ciências Sociais Aplicadas, Curso de Ciências Econômicas. Disponível em: https://tedebc.ufma.br/jspui/handle/tede/tede/667.

COSTA, Marcus Vinicius Gebaile. Disponível em: https://www.gutenberg.com.br/_files/200000391-85d8485d88/Bank%20Fraud-5.pdf.

GRECO FILHO, Vicente. **Manual de processo penal**. 9. ed. rev. e atual. São Paulo: Saraiva, 2012. p. 163.

LIMA, Iluy Manoel de Castro. **O processo de inovação tecnológica dos bancos brasileiros a partir das fraudes eletrônicas**. 49 f. Monografia (Bacharelo em Ciências Econômicas) - Universidade Federal do Paraná, Setor de Ciências, Curso de Ciências Econômicas, Curitiba, 2016. Disponível em: http://hdl.handle.net/1884/46841. Acesso em: 4 maio 2021.

REVISTA TECNOLOGIA DA INFORMAÇÃO, Ano VII, n. 7, Série Estudos, Software 2007. Edição Anual de Setembro de 2007

SIQUEIRA JÚNIOR, Paulo Hamilton. O direito na sociedade da informação**. Revista do curso de direito do centro universitário das faculdades metropolitanas reunidas**. Ano XVII, n, 25. São Paulo: UniFMU, 2003.

SOARES JÚNIOR, R. P.; VIANNA, W. B. Representação sistemográfica para gestão da informação: o projeto tentáculos da polícia federal. **Encontro Nacional de Pesquisa em Ciência da Informação**, n. XX ENANCIB, 2019. Disponível em: http://hdl.handle.net/20.500.11959/brapci/124442. Acesso em: 05 jun. 2021