CRIMES CIBERNÉTICOS E O ESTELIONATO VIRTUAL

Jamile Amorim Barata
Discente do Curso de Direito da Faculdade da Alta Paulista (FAP) - Tupã

José Luís Junqueira de Andrade Filho
Docente do Curso de Direito da Faculdade da Alta Paulista (FAP) - Tupã

1. INTRODUÇÃO

Com o avanço da tecnologia, o processo de comunicação também vem se expandido exponencialmente nas últimas décadas. Foi incrível a transformação dos meios de comunicação via cartas, as quais demoravam dias para serem entregues, para as mensagens instantâneas que recebemos em menos de segundos.

As empresas, tomando conhecimento de quão vasta é essa tecnologia, passaram a utilizar essa velocidade e qualidade de informação para um diferencial competitivo em seus negócios, o que facilitaria a entrega e divulgação de seus produtos até a residência de seus clientes.

Chiavenato (2002, p. 571), discorre sobre informação sugerindo que:

> As informações podem provir do ambiente externo (de fora da organização, como o mercado de trabalho, concorrentes, fornecedores, agências reguladoras, outras organizações etc.) ou do ambiente interno (de dentro da organização, como o organograma de cargos e respectivos salários na organização, pessoas que nela trabalham homens/horas trabalhadas, volume de

> produção e de vendas, produtividade alcançada, etc.).

Com esse avanço exponencial da tecnologia, despertou o interesse em algumas pessoas, de agir de má fé, obtendo vantagem ilícita. Capez (2020) ensina que, a vantagem ilícita, trata-se do objeto material do crime e, caso o agente esteja agindo em razão de uma vantagem devida, a conduta é tipificada como exercício arbitrário das próprias razões, delito previsto no art. 345, do Código Penal.

Esse interesse, da abertura para uma nova "tendência", de invadir redes bancárias, e subtrair informações confidenciais de grandes empresas ao redor do mundo. Vem crescendo uma técnica que é a razão desse artigo, o estelionato, situação em que a identificação de seus autores e sua punição ainda é algo além do controle da legislação vigente.

2. DO CRIME DE ESTELIONATO E A FRAUDE ELETRÔNICA

2.1 Crime de Estelionato

Trata-se de um crime patrimonial pautado, primordialmente na fraude, e com o intuito de obter vantagem ilícita.

Observe o que dispõe o art. 171 do CP.

> 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.

O estelionato não é um crime novo na cultura brasileira. No entanto, é possível notar uma crescente dessa infração, junto com o desenvolvimento da tecnologia, bem como a facilidade do acesso à internet.

2.2 Fraude eletrônica

A Lei 14.155/21 alterou o Crime de Invasão de Dispositivo Informático, aumentando significativamente suas penas em seu art. 154-A do Código Penal. Além disso, foram fracionados e criados os crimes específicos de Furto Mediante Fraude Eletrônica (art. 155, § 4º-B do CP) e de Fraude Eletrônica (art. 171, § 2º-A do CP) a qual recebeu o *nomen iuris*, cuja definição legal se dá por:

> **§ 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. (Incluído pela Lei nº 14.155, de 2021)

Consoante ao que foi apresentado, no dispositivo em análise, a elementar "fraude" não se apresenta como tempo verbal, sendo designada da ação ou comportamento humano. Sendo assim, pode ser caracterizada como “qualquer ato ardiloso, enganoso, de má-fé, com o intuito de lesar ou ludibriar outrem, e de não cumprir determinado dever; logro", afirma o doutrinador Houaiss.

O mesmo, utiliza a construção do furto mediante fraude eletrônica para classificar que se o furto praticado mediante fraude eletrônica é cometido, então há remissão expressa ao furto, ou seja,

fica subentendido que incidirá uma qualificadora, esse sim, quando ocorrer, de fato, a subtração de coisa alheia móvel para si ou para outrem.

Em complemento, a qualificadora estabelecida, não pode ser considerada uma norma penal em branco, de modo que em nenhuma hipótese a complementação normativa pode incidir sobre o núcleo de tipo. Ademais, é perceptível que não há no ordenamento um conceito normativo de "fraude", de modo a permitir a complementação clara sobre o comportamento delitivo.

Segundo Enrique Bacigalupo:

> La ley penal tiene una función decisiva en la garantía de la libertad. Esa función suele expresarse en la máxima nullum crimen, nulla poena sine /ege.'Esto quiere decir que sin una ley que lo haya declarado previamente punible ningún hecho puede merecer una pe -na del derecho penal.
>
> O direito penal tem um papel decisivo na garantia da liberdade. Essa função é geralmente expressa na máxima nullum crime, nulla poena sine /ege. Isso significa que sem uma lei que tenha anteriormente declarado punível, nenhum ato pode merecer punição na do direito penal.

Doutrinador, esse, que faz alusão ao princípio da Legalidade, com o objetivo de reduzir ao mínimo a possibilidade de decisões pessoais e subjetivas, dos tribunais, na configuração concreta do que fato que se proíbe.

Sustenta Bacigalupo:

> Desta forma, o princípio nulla poena sine lege ou princípio da legalidade adquiriu caráter fundamental no direito penal, como princípio constitucional e como princípio propriamente penal, independentemente de qualquer teoria de punição. A consequência prática deste princípio é a seguinte: não. A condenação pode ser proferida mediante aplicação de pena que não se baseia em uma lei anterior, ou seja, uma lei em que o fato acusado do autor é ameaçado de punição. Em outras palavras, deve começar pela lei, pois só assim a condenação pode ser baseada no direito penal.

Em conclusão, conforme apresentado anteriormente, diante a deficiência terminológica e por ofensa ao princípio da legalidade, as condutas que são caracterizadas fraudes eletrônicas, no feito legal atual, devem ser enquadradas na figura simples do crime de estelionato, no que tange o art. 171 do Código Penal.

2.3 Do crime cibernético.

Os crimes cibernéticos consistem no cometimento de atividades ilícitas por meio do computador ou rede de internet e classificam-se, de acordo com a sua forma de cometimento (WENDT; JORGE, 2012).

De acordo com uma pesquisa desenvolvida pelo site Safernet, entre os principais crimes cibernéticos, está o estelionato. (SANTOS; MARTINS; TYBUCSH, 2017)

Tratando-se do crime de estelionato, no ambiente da internet, o sujeito ativo mantém a vítima em erro, sob a finalidade de obter vantagem ilícita para si próprio. Também se considera crime cibernético exaltar ou elogiar criminoso ou ato criminoso de maneira

pública, caracterizando crime de apologia de crime ou de criminoso. Outro exemplo, consiste no oferecimento, utilizando a internet, de consumo a substância entorpecente, ou que sujeite a pessoa a depender-se fisicamente ou psicologicamente, caracterizando tráfico de drogas (SANTOS; MARTINS; TYBUCSH, 2017).

A internet se tornou a promessa de um futuro melhor para a humanidade, por ser uma espetacular ferramenta de troca de conhecimento. A liberdade é a característica mais atribuída à internet. Como um mundo sem fronteiras. Mas há um lado nocivo trazido por esta ausência de normas e regras (SILVA, 2015).

2.4 A LEI 12.737/2012, Lei Carolina Dieckmann.

A Lei n. 9.983/03, somente no ano de 2012, foi editada e sancionada com a intenção de ser a primeira lei específica de crime cibernético no sistema brasileiro, Lei n. 12.737/2012, Lei Carolina Dieckmann. Ganhou esse codinome por consequência de uma situação de invasão, por meio de Hackers, no dispositivo de uma atriz brasileira, que ainda, sofreu ameaças e chantagens.

A referida Lei criou o artigo 154-A, que fora acrescido no Código Penal brasileiro, in verbis:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita: Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa. (BRASIL,2021)

Vale ressaltar que a invasão consiste mediante a violação indevida de um mecanismo de segurança, a obtenção da senha de bloqueio de um celular, por exemplo. Esse tipo penal, configura-se com dolo específico, já que o agente tem vontade de obter ou destruir dados e informações alheias, de modo a afetar a vulnerabilidade para obter vantagem indevida.

O doutrinador Guilherme Nucci (2014) aborda, em sua obra, o tipo penal definido no caput do artigo 154-A:

> [...] crime comum (pode ser cometido por qualquer pessoa); formal (delito que não exige resultado naturalístico, consistente na efetiva lesão à intimidade ou vida privada da vítima, embora possa ocorrer); de forma livre (pode ser cometido por qualquer meio eleito 129 pelo agente); comissivo (as condutas implicam ações); instantâneo (o resultado se dá de maneira 47 determinada na linha do tempo), podendo assumir a forma de instantâneo de efeitos permanentes, quando a invasão ou a instalação de vulnerabilidade perpetua-se no tempo, como rastro da conduta; unissubjetivo (pode ser cometido por uma só pessoa); plurissubsistente (cometido por vários atos); admite tentativa (NUCCI, 2014, p. 814).

O tipo penal fora mal redigido e com o abuso de elementos normativos, contrariando a taxatividade. Dentre esses tipos penais elencados, o que se pode perceber é que todos possuem como elemento subjetivo a modalidade dolosa. Não quis o legislador brasileiro incriminar a modalidade culposa. O legislador da referida codificação, possui pouca informação sobre o sistema informático, e isso é agravado pela falta de reflexão por parte da Dogmática Penal Brasileira, refletindo a lacuna normativa e a falta de debate em torno

da moralidade das condutas cibernéticas, bem como as consequências e prejuízos causados por essas condutas (CASTRO, 2018).

2.5 O gerador do estelionato

Um exemplo curioso e comum de ransomware de criptografia, um tipo de software malicioso (malware), muito utilizado por criminosos para extorquir dinheiro é o famoso Ransomware *WannaCry*.

Ele ataca computadores com sistema operacional Microsoft Windows e tem a função de criptografar arquivos do seu software e bloquear o seu acesso, de modo que se torne impossível de usá-lo. Como tantos outros ransomwares de criptografia, o *WannaCry* faz seus reféns e só promete devolvê-los, após o pagamento de uma quantia a ser estipulada em Bitcoins.

No ano de 2017 aconteceu uma epidemia global de ataques do ransomware *WannaCry*, que afetou mais de 200.000 computadores no mundo inteiro, causando pânico geral, e os remetentes de spam aproveitaram a oportunidade de imediato. Pesquisadores detectaram uma grande quantidade de mensagens que ofereciam serviços como proteção contra os ataques do *WannaCry*, recuperação de dados, além de workshops e cursos de treinamento para os usuários. Os remetentes de spam também implementaram com êxito um esquema tradicional de ofertas fraudulentas para instalar atualizações de software nos computadores afetados. No entanto, os links redirecionavam os usuários para páginas de phishing, onde os dados pessoais das vítimas seriam roubados. (KASPERSKY, 2017.)

Darya Gudkova, analista de spam da Kaspersky Lab, declara

> "Durante o segundo trimestre do ano, observamos que as principais tendências nos ataques de spam e phishing continuaram crescendo. O uso do *WannaCry* em mensagens em massa demonstra que os criminosos virtuais estão muito atentos e reagem rápido aos eventos internacionais. Eles também começaram a focar mais no setor B2B, considerado lucrativo. Nossa expectativa é de que essa tendência continue aumentando, e que a quantidade total e a variedade de ataques corporativos cresçam",

O *WannaCry* tomou vida, quando um grupo de hackers chamado Shadow Brokers se aproveitou de uma deficiência no sistema operacional Microsoft Windows, usando um Hack, desenvolvido pela *Agência de Segurança Nacional dos Estados* Unidos, conhecido como *EternalBlue*.

Dois meses antes da invasão, a Microsoft gerou uma correção de segurança que permitia proteger os usuários contra qualquer tipo de ataque, mas inúmeras pessoas não atualizaram regularmente os seus sistemas operacionais, o que permitiu ficarem expostas e cada vez mais vulneráveis ao ataque do Ransomware.

Durante a invasão, os agentes exigiam US$ 300 em bitcoins e, mais tarde, aumentaram o valor do resgate para US$ 600 em bitcoins. Se as vítimas não pagassem esse valor dentro do prazo estipulado de três dias, os responsáveis ameaçavam excluir os arquivos permanentemente. Consta que, a codificação usada no ataque estava com defeito, mesmo após o pagamento das vítimas os invasores não tinham como associar ao computador daquela pessoa física.

2.6 O caso do golpista do Tinder

Baseado em um caso real de 2018, a Netflix produziu um documentário voltado para depoimentos de vítimas do israelense Shimon Hayut, ou Simon Liev que fingia ser um milionário russo no app de relacionamento.

As vítimas relatam que o golpista começou com o match, fingiu ser um milionário russo que ostentava com viagens, jatinhos, estadias em hotéis de luxo, festas, joias e presentes de grandes valores, e se demonstrava como o "Principe" dos Diamantes, estando envolvido na extração da joia, em regiões da África e no comércio de armas.

Shimon se aproxima das mulheres, a fim de se tornar o namorado de confiança, e inicia seu golpe dizendo estar sendo perseguido por inimigos e precisa de ajuda de suas mulheres. Elas, prestativas e apaixonadas, emprestam seus cartões de crédito, e dinheiro vivo, coisas que não são rastreáveis.

Uma das vítimas enviou cerca de R$ 1,4 milhão para o criminoso, e muitas outras faziam empréstimos de grandes quantias para enviar a Simon. Ao todo, foram mais de US$ 10 milhões roubados.

Em uma de suas viagens, quando havia sido descoberto por suas vítimas e entregue para a polícia, Simon resolve fazer um passaporte falso, e parte voo com uma identidade que não era a sua. O criminoso foi detido e levado preso pelo porte de documento falso.

Mesmo com todas as provas, Leviev está livre e nega ter roubado qualquer dinheiro. No país de origem, ele negou todas as

acusações contra ele, dizendo que nunca tirou nada das mulheres e que elas apreciavam a sua companhia.

"Tenho o direito de escolher o nome que quiser, nunca me apresentei como filho de ninguém, mas as pessoas usam a imaginação", relatou ao Channel 12 News.

"Talvez seus corações tenham partido durante o processo… Eu nunca tirei um centavo delas; essas mulheres se divertiram na minha companhia, viajaram e conheceram o mundo com meu dinheiro", completou.

2.7 O Robô do Pix

A partir do momento em que as pessoas entram no mundo virtual, mais passam a ser vítimas de crimes como este e ficam mais vulneráveis a qualquer invasão por meio dos dispositivos. Golpes envolvendo pagamentos por meio de Pix têm crescido nos últimos anos. Os relatórios identificam uma rede de perfis falsos com mais de 600 mil seguidores que usa a promessa de dinheiro fácil como isca para roubar dados confidenciais das vítimas. A prática, conhecida como "Robô do Pix", configura estelionato virtual, porque busca induzir as vítimas a realizar transferências bancárias ou fornecer informações sensíveis. Após capturarem dados pessoais e financeiros, os criminosos os utilizam em fraudes e processos de clonagem de cartão. (PSafe, 2022).

Um dos mecanismos utilizados pelos criminosos, é a divulgação de posts com promoções, em que a vítima faz um pagamento de uma quantia mínima a ser revertido em investimentos

de criptomoedas, em seguida garante que será revertido um valor 10 vezes maior.

Há, também, casos em que a vítima é direcionada para outros sites e deverá inserir dados bancários e pessoais, além do número do cartão de crédito. Essas informações são armazenadas pelo agente, que posteriormente fará seu alvo de fraudes e clonagens.

Propõe definir o que são os dados pessoais, e designar cuidados específicos a alguns deles, como os dados pessoais sensíveis e dados pessoais sobre crianças e adolescentes.

Deixa claro que, independentemente da sede de uma organização ou o centro de dados dela estarem localizados no Brasil ou exterior, se existe o processamento de informações de pessoas que estejam no território nacional, a LGPD deverá ser observada. Ainda, permite o compartilhamento de dados pessoais com organismos internacionais de outros países, desde que seja mantida a segurança e melhor observação dos requisitos que são estabelecidos.

No desenrolar da LGPD, a principal regra se trata do consentimento do titular dos dados, trazendo assim diversas garantias, das quais temos: a solicitação de que sejam excluídos seus dados pessoais, transferir dados para outros fornecedores de serviços, revogar o consentimento e outras ações. É de total compreensão que tenha uma certa finalidade e uma necessidade a serem previamente calculados e decididos junto ao titular.

Tem sido um dos assuntos mais discutidos desde que foi instaurada em 14 de agosto de 2018, no governo do Temer. Resumidamente, ela diz como os dados podem ser coletados, armazenados e manipulados, bem como a penalidade variando de

multa até 2% sobre o faturamento da empresa que a infringir, limitando um valor de R$ 50 milhões.

O fato é que, as empresas ainda não têm total noção do que deve ser feito, e nesse contexto, elas devem apenas se preocupar em proteger os dados de seus clientes e colaboradores. Desse modo, as organizações devem implementar uma solução de privacidade, desde a coleta de dados, por padrões potencializados, utilizando a automatização robótica de inteligência artificial.

3. RESULTADOS E DISCUSSÕES.

É de fácil compreensão as didáticas da prática do crime, dispostas no decorrer do artigo, além de discorrer a respeito dos mecanismos de investigação.

A proposta é trazer para o desenrolar do artigo, as jurisprudências que tratam expressamente do caso, e refletir sobre a maneira de atuação dos agentes responsáveis pela solução dessas situações; bem como demonstrar a importância da investigação para que possa, de maneira correta solucionar esses conflitos.

De acordo com a coleta de dados, alguns jornais em sua plataforma digital, disponibilizaram estatísticas voltadas aos índices desses crimes em nosso país. CORREIO DO POVO (2022) divulgou que: Pesquisadores, junto da Secretaria de Segurança Pública, analisaram um total de 100 mil habitantes para efeitos de comparação entre as unidades da federação. Chegaram à conclusão de que os casos quase triplicaram no Brasil, desde 2018, e 2021, tendo um aumento percentual de 179%.

Ainda, o jornal MIGALHAS (2022) afirma que a alta dos crimes de estelionato virtual, foram acometidas por golpes através do PIX, sendo crimes potencialmente lucrativos e de fácil realização. Um exemplo, são as centenas de mensagens enviadas para atrair consumidores, o que, uma vez dominada, pode ser uma técnica realizada diversas vezes pelo mesmo indivíduo. Além disso, o mecanismo do PIX, atualmente, tem como principal função, a facilidade e a prática, que permitem a transição de dinheiro e valores para diversas contas.

Em total análise, os criminosos buscam na internet meio de obter informações e dados a respeitos de suas possíveis vítimas, visando que a todo momento pessoas do mundo inteiro guardam e compartilham informações pessoais, em suas redes sociais, por exemplo. Além de que, 24h por dia, as pessoas costumam comprar ou vender coisas e objetos, de modo que se cadastram em diversos sites, fornecendo senhas e dados pessoais.

Todas essas formas de utilidade da internet podem ser, por sua vez, inofensivas, o que as tornam, em um plano paralelo rodeado por pessoas de más intenções, um grande risco aos usuários, nos expondo cada vez mais, a fim de aumentar a nossa vulnerabilidade.

4. CONSIDERAÇÕES FINAIS

Em total análise do presente artigo científico, podemos ressaltar a imensa necessidade de nos precaver de ataque futuros. Vivemos num mundo incerto e cheio de surpresas, onde todo cuidado é pouco.

A que se questionar a respeito da nossa vulnerabilidade, que se limita aos mecanismos de segurança dos quais, geralmente, deixamos passar despercebidos e só fazemos questão no momento em que somos atacados.

Os delitos cometidos através da internet estão presentes no mundo todo, englobando inúmeras situações, a fim de alcançar o maior número de pessoas. No entanto, o presidente do Brasil, no dia 27 de maio de 2021, sancionou a Lei n. 14.155/2021, que altera o Código Penal e torna mais rigorosa a punição para os crimes de violação de dispositivo informático, furto e estelionato cometidos pela internet ou por meio de dispositivos eletrônicos.

Sobre o crime de estelionato, inclui ao Código Penal a pena de reclusão de quatro a oito anos e multa, quando a vítima for enganada e fornecer informações por meio de redes sociais, estando passível de majoração, quando o crime for realizado por meio de servidor localizado em outro país. Ainda, a legislação acrescenta um dispositivo ao Código de Processo Penal, a fim de definir a competência para processar e julgar determinadas modalidades de crimes de estelionato.

Diante da expansão do espaço cibernético, é de suma importância que cada indivíduo atualize seus mecanismos de proteção. Além disso, em matéria investigativa, existe uma falta de infraestrutura para que sejam efetivados alguns procedimentos, como os equipamentos tecnológicos e agentes capacitados.

Por fim, é possível concluir que, ainda que o Brasil esteja avançando juridicamente, quanto às relações criminosas no espaço cibernético, há muito que evoluir. De modo que haja investimento na

área específica, com aprofundamento investigativo na legislação, assim a sanção de impunibilidade, causada pelo meio virtual, diminuirá, o que consequentemente impossibilitaria futuros ataques.

5. REFERÊNCIAS BIBLIOGRÁFICAS.

ALVES, M.H. **A evolução dos crimes cibernéticos e o acompanhamento das leis específicas no Brasil.** JUS BRASIL.18 de mar. 2018. Disponível em: < https://jus.com.br/artigos/64854/a-evolucao-dos-crimes-ciberneticos-e-oacompanhamento-das-leis-especificas-no-brasil >. Acesso em: 2 set 2022.

BARATTA, Alessandro. **Criminologia crítica e crítica do direito penal introdução à sociologia do direito penal.** 3. ed. Rio de Janeiro: Revan, 2002.

BRASIL. **Tribunal Regional Federal da 3ª Região TRF-3. Recurso em Sentido Estrito: RES 0013241-15.2014.4.03.6181.** JUS BRASIL. São Paulo. 2018. Disponível em: < https://trf-3.jusbrasil.com.br/jurisprudencia/624509523/recurso-em-sentido-estrito-rse-132411520144036181-sp. Acesso em 2 set. 2022.

BRASIL. **Manual de cooperação jurídica internacional e recuperação de ativos: cooperação em matéria penal.** Brasília: Departamento de Recuperação de Ativos e Cooperação Jurídica Internacional, 2008.

BRENOF, Ann. **Como um golpe bilionário na internet está partindo corações e esvaziando contas bancárias**. São Paulo. 08 de Abr. 2017. Disponível em: < https://www.huffpostbrasil.com/2017/08/04/como-um-golpe-bilionario-na-internet-esta-partindo-coracoes-e-es_a_23063731/ >. Acesso em: 2 set. 2022.

CAPEZ, Fernando Prado. **Código Penal Comentado**. São Paulo: Saraiva, 2016.

CASTRO, Aldemario Araujo. **A internet e os tipos penais que reclamam ação criminosa em público.** 2018. Disponível em: https://egov.ufsc.br/portal/sites/default/files/anexos/13308-13309-1-PB.pdf. Acesso em 11 de novembro de 2022.

CUNHA, Rogério Sanches. **Manual de Direito Penal: Parte Geral**. Salvador: Juspodivm, 2014.

GRECO, Rogério. **Curso de Direito Penal.** 17. ed. Rio de Janeiro: Impetus, 2015.

MOREIRA, Paulo. **Estelionato praticado por meio da internet: uma visão acerca dos crimes digitais.** MIGALHAS. Brasil, 16 fev. 2022. Disponível em: https://www.migalhas.com.br/depeso/359821/estelionato-praticado-por-meio-da-internet. Acesso em: 02 set. 2022.

NUCCI, Guilherme de Souza. **Código penal comentado.** 14. ed. Rio de Janeiro: Forense, 2014.

NUCCI, Guilherme de Souza. **Manual do Direito Penal**. 7. ed. São Paulo: Revista dos Tribunais, 2011.

RONDON FILHO, E. B.; KHALIL, K. P. SCAMMERS: ESTELIONATO SENTIMENTAL NA INTERNET. **Revista Direito e Justiça: Reflexões Sociojurídicas**, v. 21, n. 40, p. 43-57, 2 de set. 2022.

SALES, Luiz. **Da necessidade de tipificação do crime de estelionato praticado na internet**. CONTEUDO JURÍDICO. São Paulo. 16 de set. 2010. Disponível em: https://conteudojuridico.com.br/consulta/Monografias-TCC-Teses-E-Book/19147/da-necessidade-de-tipificacao-do-crime-de-estelionato-praticado-na-internet. Acesso em: 2 set. 2022.

SANT'ANNA, Paulo. **Remetentes de spam usaram epidemia WannaCry para promover serviços fraudulentos no 2º trimestre.** KASPERSKY. 22 de ago. 2017. Disponível em: https://www.kaspersky.com.br/about/press-releases/2017_kaspersky-

lab-wannacry-epidemic-used-to-promote-fraudulent-services-in-q2. Acesso em: 02 de set. 2022.

SANTOS, Liara Ruff dos; MARTINS, Luana Bertasso; TYBUCSH, Francielle Benini Agne. **Os crimes cibernéticos e o direito a segurança jurídica: uma análise da legislação vigente no cenário brasileiro contemporâneo.** 2017.

SILVA, Patrícia Santos da. **Direito e crime cibernético: análise da competência em razão do lugar no julgamento de ações penais**. Brasília: Vestnik, 2015.

SOUZA, Alina. **Crimes virtuais e pix impulsionam aumento de 179% dos estelionatos.** CORREIO DO POVO. Brasília, 29 jun. 2022. Disponível em: https://www.correiodopovo.com.br/not%C3%ADcias/pol%C3%ADcia/crimes-virtuais-e-pix-impulsionam-aumento-de-179-dos-estelionatos-1.847362. Acesso em: 02 set. 2022.

WENDT, Emerson; JORGE, Higor Vinícius Nogueira. **Crimes cibernéticos: Ameaças e procedimentos de investigação**. Rio de Janeiro: Brasport, 2012. p 10.