CENTRO UNIVERSITÁRIO BRASILEIRO – UNIBRA

CURSO DE GRADUAÇÃO TECNOLÓGICO EM REDES DE COMPUTADORES

ARTHUR BARBOSA RIBEIRO DA SILVA
FABIANA DOS SANTOS SOUZA
MATHEUS DIAS MELO

CONHECENDO OS CRIMES CIBERNÉTICOS PRATICADOS NO BRASIL E COMO SE PROTEGER

RECIFE/2022

ARTHUR BARBOSA RIBEIRO DA SILVA
FABIANA DOS SANTOS SOUZA
MATHEUS DIAS MELO

CONHECENDO OS CRIMES CIBERNÉTICOS PRATICADOS NO BRASIL E COMO SE PROTEGER

Trabalho Conclusão de Curso apresentado ao Centro Universitário Brasileiro - UNIBRA, como requisito parcial para obtenção do título de tecnólogo em Redes de Computadores.

Professora Orientadora: Msc. Ameliara Freire Santos de Miranda

RECIFE/2022

Ficha catalográfica elaborada pela
bibliotecária: Dayane Apolinário, CRB4- 1745.

S586c Silva, Arthur Barbosa Ribeiro da

Conhecendo os crimes cibernéticos praticados no brasil e como se proteger / Arthur Barbosa Ribeiro da Silva, Fabiana dos Santos Souza, Matheus Dias Melo. Recife: O Autor, 2022.

50 p.

Orientador(a): Ameliara Freire Santos de Miranda.

Trabalho de Conclusão de Curso (Graduação) - Centro Universitário Brasileiro – UNIBRA. Tecnólogo em Redes de Computadores, 2022.

Inclui Referências.

1. Crimes cibernéticos. 2. Segurança. 3. Cybercrime. I. Souza, Fabiana dos Santos. II. Melo, Matheus Dias. III. Centro Universitário Brasileiro - UNIBRA. IV. Título.

CDU: 004

Dedicamos este trabalho aos nossos familiares e amigos que nos apoiaram desde o início da nossa graduação e aos professores que nos deram garra a cada semestre.

AGRADECIMENTOS

Agradecemos a Deus que nos permitiu alcançar mais esta etapa da vida, nossa primeira graduação, no curso Redes de Computadores, porque sem Ele nada podemos fazer e tudo que somos hoje é permissão e graça d'Ele para conosco.

Aos nossos pais e familiares que nos deram apoio para que conseguíssemos vencer mais uma etapa.

Não podemos esquecer de cada funcionário desta Instituição de Ensino, sem exceções, e principalmente aos professores, pelo esforço de cada um em passar os seus conhecimentos e ajudarem na formação e qualificação dos profissionais que estamos saindo e especialmente à professora orientadora Ameliara Freire Santos de Miranda.

“Se tu o desejas, podes voar, só tens de confiar muito em ti”.

*(**Steve Jobs**)*

RESUMO

Crimes e ataques cibernéticos são um tanto antigos, porém, a legislação de proteção não. Fizemos um recorrido dos crimes cibernéticos mais praticados no Brasil pensando na máxima que “Conhecimento é poder”, afinal saber como funciona, como vão nos ludibriar é o primeiro passo para nos protegermos. Com o advento dos computadores de mesa e dos aparelhos para uso doméstico, o risco já foi aumentando em nosso meio, afinal como estará relatado neste trabalho, o homem é um ser que busca pela vantagem. E comentaremos sobre diversas iscas e brechas que esses criminosos virtuais se utilizam, desde o *phishing* como ataques em série como web, para a evolução como o crime de *ransomware*, e a engenharia social para angariar capital. As leis que são muito novas e uma possível frouxidão dessa busca pelos criminosos virtuais, comentamos sobre as principais Leis, sendo estas a Lei Geral de Proteção de Dados, de número 13.709/2018, a Lei Carolina Dieckmann, de número 12.737/2012 e o Marco Civil da Internet, de número 12.965/2014. Conclui-se com as leis existentes e como elas impactam na sociedade em defesa do cidadão que navega no ciberespaço.

Palavras-chave: Crimes Cibernéticos. Segurança. Cybercrime.

LISTA DE FIGURAS

Figura 1 Panorama de ameaças cibernéticas no Brasil em 2020.....18

Figura 2 O movimento de e-commerce no Brasil, em janeiro de 2020 19

Figura 3 Tentativas de Fraudes no Brasil no ano de 2020.....20

Figura 4 Exemplo de *phishing* via SMS.....23

Figura 5 Golpe da Fatura Falsa.....24

Figura 6 Golpe do site falso, com link de pagamento de streaming famosa.....25

Figura 7 Golpe do FGTS via WhatsApp.....28

Figura 8 Fraude utilizando o nome de um famoso banco.....29

Figura 9 Caso de aviso em rede social de roubo de identidade: uma ‘casadinha’ de cibercrime para extorquir parentes e amigos da vítima.....30

Figura 10 Perfil oficial alerta sobre perfil fake que está se passando pelo salão.....31

Figura 11 Engenharia Social sendo desmascarada pelo Restaurante prejudicado.....32

Figura 12 Cliente solicitando a uma página falsa um atendimento.....33

Figura 13 O criminoso em contato com o cliente do banho, agora vítima.....34

Figura 14 Caso de Engenharia Social usando o nome da Receita Federal.....35

Figura 15 Ataque de ransomware ao Governo Brasileiro, em 2022.....37

Figura 16 Os preferidos para o ataque ransomware no Brasil.....38

Figura 17 Roubo de Dados é notícia como “joia do cibercrime” na pandemia.....38

Figura 18 Print da entrevista de Erick Siqueira sobre a operação Boleto Real, crime que foi disseminado no Brasil e descoberto pela Polícia Federal.....43

SUMÁRIO

1. **INTRODUÇÃO**.....10
   1.1 Objetivos Gerais e Específicos.....13
   1.2 Metodologia.....14
   1.3 Justificativa.....14
2. **REFERENCIAL TEÓRICO** 15
   2.1 O ser humano como criminoso e a criminalidade virtual: exposição inicial.....15
3. **PANORAMA DOS CRIMES MAIS COMETIDOS NO BRASIL VIA INTERNET**.....21
   3.1 Phishing.....23
   3.2 Engenharia Social.....26
   3.3 Roubo de Dados e Lei Geral de Proteção de Dados.....33
   3.4 Ransomware (Sequestro de dados) 37
   3.5 Outros crimes cibernéticos.....39
4. **CRIMES CIBERNÉTICO NA PANDEMIA E PÓS-PANDEMIA E A VISÃO DE UM AGENTE DE POLÍCIA FEDERAL SOBRE O TEMA**.....40
5. **PRINCIPAIS AÇÕES LEGISLATIVAS NO COMBATE AO CRIME CIBERNÉTICO NO BRASIL**.....44
6. **CONSIDERAÇÕES FINAIS**.....45
7. **REFERENCIAS**.....47

INTRODUÇÃO

O primeiro crime da história foi resultante da existência do homem, como rege a parábola: Caim e Abel[1], filhos de Adão e Eva. De certo que com o homem nasceu o delito, a vontade de estar acima do outro e de se sentir impune mesmo em meio ao paraíso com poucas pessoas, neste devaneio do ocultar-se, do “ninguém vai saber” e desta falsa sensação de impunidade.

E é neste ar de deus, de estar acima de tudo, que ecoamos no exposto pela mitologia grega: o mundo já nasceu marcado pela confusão, afinal no princípio de todos os mitos, antes mesmo de existir o Universo, o que inundava e abundava neste meio era o Caos. (BRANDÃO, 1991, p.184)

Se até mesmo os deuses cometiam crimes- incesto[2], parricídio[3], estupro[4] etc. - no universo físico (de certa maneira palpável), imagina os seres humanos no universo particular, do alto de sua cadeira e da potência dos seus olhos e dedos no teclado?

A situação de se sentir impune acompanhou o ser humano desde a sua formação, parece ser algo intrínseco, não poderíamos deixar de raciocinar antes de explanarmos o tema: de onde vem essa sensação de ser inalcançável?

E a resposta não é encontrada apenas em estar por trás das telas, isso é algo que apenas dá mais gosto e “facilidade”: o anonimato. E historicamente, o não te buscarem como a voz de Deus perguntando por Abel, como houve com Caim, ou outro deus mais poderoso querendo se vingar do crime cometido por um outro deus ou semideus.

Efetivamente, o que notamos é que em certas pessoas, o sangue pulsa para cometer atrocidades com outros seres, a sede de enganar e levar vantagem fala mais alto do que todas as filosofias de respeito, amor e importância dada ao próximo; conceitos

---

[1] GÊNESIS 4:8-16. In: BÍBLIA. Português. Bíblia Sagrada. São Paulo, Sociedade Bíblica do Brasil, 2018, p.5.
[2] BRANDÃO, Junito de Souza. Mitologia Grega- Volume I. Rio de Janeiro, Petrópolis. Editora Vozes, 1986, p.84.
[3] BRANDÃO (1986, p.83)
[4] BRANDÃO (1986, p.89)

estes angariados na frase atribuída ao filósofo Herbert Spencer: “A liberdade de cada um termina onde começa a liberdade do outro”.[5]

De fato, na internet, por trás das telas, não se consegue dimensionar onde inicia e termina o direito do outro, não há meios instantâneos para fazê-lo, há um *delay* na busca de quem infringiu a lei, e se agrava (no sentido de tornar trabalhoso) se o crime foi cometido nos porões da internet, o *hades*, que se conhece como *deepweb* ou em português ‘internet profunda’, segundo Chertoff e Simon (2015, APUD SILVA; FORNASIER; KNEBEL, 2020, p.228):

> “o termo Deep Web é usado para conceituar uma gama de conteúdos da Internet que, por razões técnicas, não é indexada pelos tradicionais mecanismos de pesquisa, e como qualquer forma de tecnologia, o anonimato trazido por si pode ser utilizado tanto para propósitos benéficos quanto perniciosos”.

Entretanto, como apontamos, os crimes cibernéticos não se passam apenas na *deepweb,* mas sim na internet como um todo, afinal, segundo Chertoff (2017, p.36, APUD SILVA; FORNASIER; KNEBEL, 2020, p.239), a internet é: “incapaz de dicriminar criminosos e usuários comuns” e para isso deve manter a privacidade do usuário comum, desmascarando apenas o criminoso. E ainda, afirma que “a maneira mais eficaz de fazer isso é procurar sites ilegais em vez de usuários ilegais”. Para ocorrer um crime cibernético só é preciso existir uma tela, conexão à internet, uma vítima e o autor do crime. O que quando enumeramos parece ser longo o caminho, mas é mais fácil e rápido do que imaginamos.

No País, de acordo com a Agência Brasil[6], 81% da população com mais de 10 anos tem internet em casa, o que figura mais de 152 milhões de usuários em território nacional que possuem acesso à rede[7], dados de 2020. Quanto maior o número de

---

[5] FERRARI, Márcio. Herbert Spencer: O ideólogo da luta pela vida. Nova Escola, Ed. 0186, Especial Grandes Pensadores-Matéria 94622, outubro de 2008, São Paulo: Editora Abril, 2008. Disponível em: novaescola.org.br/conteudo/1685/hebert-spencer-o-ideologo-da-luta-pela-vida. Acesso em: 9 set. 2022.

[6] Em uma matéria intitulada “Brasil tem 152 milhões de pessoas com acesso à internet”, de Lucas Pordeus León, datada em 23/08/2021. Disponível em: https://agenciabrasil.ebc.com.br/geral/noticia/2021-08/brasil-tem-152-milhoes-de-pessoas-com-acesso-internet Acesso em 03 ago. 2022

[7] Vale ressaltar que não estamos deixando de lado a informação que ainda há muitos cidadãos que não possuem acesso à internet, principalmente das classes C, D e E, de grande maioria negra, como aponta notícia da G1, em 2020. Disponível em: https://g1.globo.com/tecnologia/noticia/2022/03/21/mais-de-33-milhoes-de-brasileiros-nao-tem-acesso-a-internet-diz-pesquisa.ghtml Acesso em 03 ago. 2022

usuários maior o número de golpes, plágio, *cyber bullyng*, *malware*, vendas de produtos ilegais, *phishing* (do inglês, pescar), extorsão cibernética, incitação, produção ou posse de pornografia infantil, discurso de ódio contra LGBTQI+, xenofobia, racismo, apologia ao nazismo entre outros crimes. Como bem disse o policial e analista de sistemas: “A internet é uma grande praça pública, o maior espaço coletivo do planeta”. (CASSANTI, 2014, p.3).

E como em toda praça, dever-se-ia tomar cuidado com o espaço, onde colocamos nossos dados, fotos ou qualquer “porta aberta” para o crime; levando-se em conta as leis vigentes. Com a globalização e com a revolução que houve nos anos 90, retirando a ferramenta internet do pedestal de ser usada apenas por cientistas, e após essa década todos nós somos, de certa forma, pesquisadores, sendo aberta a ferramenta ao grande público. Com a benfeitoria vem as *maldições,* como já foi dito, fomentada por uma sensação de um lugar sem leis, e é nesta ‘oportunidade’ que surge o fruto dos absurdos, praticado pelos cibercriminosos, ocasionado pelas brechas no desconhecimento de usuários básicos da internet e quiçá usuários medianos.

Vale ressaltar o que significa o ciberespaço, para compreendermos o que seria um cibercriminoso, e para isto, conceituaremos o termo com a fala de Silvana Drumond Monteiro:

> Ciberespaço é definido como um mundo virtual porque está em presente potência, é um espaço desterritorializante. Esse mundo não é palpável, mas existe de outra forma, outra realidade. O ciberespaço existe em um local indefinido, desconhecido, cheio de devires e possibilidades. Não podemos, sequer, afirmar que o ciberespaço está presente em nossos computadores, tampouco nas redes, afinal onde fica o ciberespaço? Para onde vai todo esse “mundo” quando desligamos nossos computadores? É esse caráter fluido do ciberespaço que o torna virtual. (MONTEIRO, 2007, p.1-2)

Esse espaço é fluído, virtual, não está ‘portado’ em um aparelho eletrônico, sendo este apenas o meio que faz jorrar e ecoar este lugar de possibilidades, de consulta a uma base de dados, um método pelo qual se descobrem coisas novas a cada dia. Cheio de incertezas, impalpável, fictício, completamente abstrato, quase que um mundo paralelo em que se interpõe criações e expressões de cultura, de comércio, social e linguístico, que corre como um rio, o próprio Poseidon, deus da navegação, dos mares, e quase a personificação de Ponto, o deus do mar, segundo a mitologia grega, sendo este o próprio mar.

Continuando na analogia ao mar, ao ato de navegar, estão as enchentes – ser engolido por este rio de informações-, os terremotos – cibercrimes praticados-, e curiosamente os cavalos- se pensarmos em Poseidon-, que indicaremos como os "cavalos-de-Tróia" e demais vírus. E por ser um meio em si mesmo, sendo o mar por si só, o deus Ponto.

Logo, o ciber criminoso é alguém que comete um crime neste espaço infinito e que consegue estar presente em nossos meios eletrônicos através da internet ou de conexões de redes, é um criminoso virtual que usa da força, do poder deste meio para agredir, ir contra às leis e ganhar vantagem em cima de outras pessoas, sejam elas jurídicas ou físicas. Em uma reportagem da revista Istoé Dinheiro[8], de dezembro de 2021, o Brasil ocupava o 5º lugar dos países que mais sofreram crimes cibernéticos, de acordo com a consultoria alemã Roland Berger, no primeiro trimestre ocorreram mais de 9,1 milhões de ocorrências, em comparação aos dois semestres de 2020. E ainda, em uma nova reportagem, de 2022, na Exame[9], afirma que a estimativa foi de 32 bilhões de reais perdidos para resolver problemas com cibercrimes no ano de 2021 e que 58% dos brasileiros sofreram algum ataque cibernético, segundo estudos da Norton. E ainda mais, o Brasil se tornou o terceiro país, dentre os dez pesquisados, mais infectado por aplicativos de espionagem, ficando atrás da índia e dos EUA.

1.2 Objetivos Gerais e Específicos

É mister destacar que os crimes cibernéticos não são apenas os que se executam para ganhar dinheiro de terceiros, listamos alguns nesta introdução e temos o objetivo específico de versar sobre o que são esses crimes cibernéticos que ocorrem em maior número, como ocorrem e como podemos nos proteger, e para tal, como objetivo geral faremos um pequeno recorrido histórico, para esclarecer os términos, e de revisão da literatura sobre os temas englobados. Sendo de suma importância para a área de Tecnologia e de Sistema de Redes, afinal a internet a cada dia se expande,

[8]Matéria intitulada "Brasil foi 5º país com mais ataques cibernéticos no ano: relembre os principais", feita pelo jornalista Filipe Prado, em 20/12/2021. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/ Acesso em 03 ago. 2022

[9] Matéria intitulada "58% dos Brasileiros sofreram crimes cibernéticos, aponta estudo da Norton", pela jornalista Laura Pancini, em 11/03/20022. Disponível em: https://exame.com/tecnologia/58-dos-brasileiros-sofreram-crimes-ciberneticos-aponta-estudo-da-norton/ Acesso em: 04 ago. 2022

igualmente novos ataques são descobertos/sofridos e nosso dever é nos mantermos atualizados e desvendar as soluções para os determinados problemas que surgirem e o que nos diz as leis um tanto atuais para estes problemas manifestados com o advento da propagação do uso da internet.

1.3 Metodologia

Sendo este estudo de caráter metodológico de pesquisa bibliográfica assistemática, com contribuições científicas de diversos autores sobre a temática, de abordagem amostral, realizada através de informações de diversas fontes, entre elas o *CERT.br* (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), reportagens e pesquisas, que segundo Da Silva e Menezes (2001):“Pesquisa Bibliográfica é aquela baseada na análise da literatura já publicada em forma de livros, revistas, publicações avulsas, imprensa escrita e até eletronicamente, disponibilizada na Internet”. Ademais disso, é um estudo explicativo, o que segundo Malhotra (2001), tem como um dos objetivos possibilitar uma maior aproximação e entendimento do problema ao pesquisador, para que se consiga construir hipóteses mais adequadas.

1.4 Justificativa

Para Cassanti (2014, p. 22), “Não haverá o mínimo de possibilidade em obter êxito na luta contra os crimes virtuais se quem pretender vencê-lo primeiramente não puder entendê-lo.” Esta pesquisa justifica-se pela necessidade da comunidade, seja ela acadêmica ou geral, ser auxiliada no sentido de identificar os riscos que estão expostos e prevenindo os possíveis ataques cibernéticos e possivelmente as leis que os amparam frente a estes problemas. Uma vez que quem conhece não cai nos golpes, sejam eles de quaisquer naturezas.

2 REFERENCIAL TEÓRICO

Neste capítulo nortearemos todas as significâncias que demos para os assuntos que englobam nossa temática de forma direta ou indireta.

2.1 O ser humano como criminoso e a criminalidade virtual: exposição inicial

Sendo a internet um instrumento muito estimado pela sociedade em geral e sabendo que seu uso trouxe inúmeros benefícios para ela, tornando-se um meio de comunicação indispensável. Sendo assim, muitas vezes o elemento principal de compartilhamento de informações e de dados, ocasionando a substituição das atividades presenciais referentes a este meio. Resultado desse caminho foi a utilização da internet para praticar crimes e mostrar a conduta ilícita que muitos possuem.

Borges (2015, p.1) expõe o aproveitamento das novas tecnologias pelos criminosos:

> "É certo que a criminalidade, obviamente, não deixaria de aproveitar as oportunidades trazidas pelas novas tecnologias, e a prática de ilícitos na Internet é uma realidade perversa, com um sem número de fraudes bancárias, extorsões decorrentes de invasões de computadores, vírus e programas espalhados pela rede para obtenção de dados que permitam a prática criminosa, pornografia infantil e muitas outras condutas ilícitas ou reprováveis".

O ser humano pode mostrar seu lado deplorável na internet, isso já é algo constatado todos os dias, seja noticiado em jornais ou mesmo com uma rápida vista nas redes sociais, acompanhando os comentários acerca das fotos ou da vida de outros. A psicanalista carioca Andréa Ladislau, afirma que:

> "Todos nós temos em nosso inconsciente o bem e o mal, mas conhecemos a essa face sombria quando começamos a tornar consciente aspectos que consideramos 'ruins' ou 'errados', seja por questões educacionais, culturais ou sociais".[10]

[10] No Portal de Divulgação Científica do IPUSP, em um artigo intitulado 'Todos temos um "lado sombra" da personalidade: o que é e como lidar com ele" de Islaine Maciel. Disponível em: https://sites.usp.br/psicousp/todos-temos-um-lado-sombra-da-personalidade-o-que-e-e-como-lidar-com-ele/ Acesso em: 13 ago. 2022

Quando pensamos nas questões educacionais, culturais ou sociais para considerar, conscientemente, um crime como algo ruim ou errado, não pensamos em tão somente o que a sociedade como um todo pensa acerca dos crimes. Queremos pensar no micro, antes de tudo, pois, segundo Foucault (2014, p.14) “a certeza de ser punido é que deve desviar o homem do crime e não mais o abominável teatro; a mecânica exemplar da punição muda as engrenagens”.

O filósofo nos retrata o pensamento micro, de um homem (aquele que comete um crime), que deve se manter afastado do ato pois sabe que haverá uma punição. Seguindo a análise que Michel Foucault faz sobre a consciência do homem, agente deste crime, cita que o mal, como forma de humilhação, como ocorria antigamente e que ainda ocorrem em algumas culturas, não deve ser feito, como cortar a mão do ladrão[11], pendurá-lo em local público[12] para que seja humilhado e reconhecido pelo mal que executou- em alguns casos a justiça não é dada por um órgão regulador e sim pela própria população-[13].

Não se deve temer ou se desviar por medo à exposição. Por isso, segue afirmando que a maneira de punir muda as engrenagens sociais, e “por essa razão, a justiça não mais assume publicamente a parte de violência que está ligada a seu exercício”. (FOUCAULT, 2014, p. 14). O criminoso deve sempre pensar na punição legislativa que terá e não da humilhação pública, e isso tem mudado consideravelmente, graças a leis mais abrangentes, como por exemplo, a Lei Geral de Proteção de Dados (13.709/18), O Marco Civil da Internet (12.965/14) e a Lei de Crimes Cibernéticos, mais conhecida como Lei Carolina Dieckmann (12.737/12). E, pela mudança do espaço em que ocorrem esses crimes, o ciberespaço, que fez com que as engrenagens das leis e suas respectivas ações punitivas e até mesmo de investigação mudassem.

---

[11] Por mais que pareça muito distante e arcaica, essa punição ainda existe e podemos constatar por uma matéria intitulada “Um pé e uma mão por roubar um celular e 490 reais no Sudão”, do El País, datada de 26 jul. 2021. Disponível em: https://brasil.elpais.com/internacional/2021-07-26/um-pe-e-uma-mao-por-roubar-um-celular-e-490-reais-no-sudao.html Acesso em 11 set.2022

[12] FOUCAULT, M. Vigiar e Punir: nascimento da prisão. Petrópolis: Editora Vozes,1987, p.8

[13] Exemplo disso é o que ocorre na Bolívia, país que faz fronteira com o Brasil, em que há um linchamento para pessoas que cometem crimes como roubo, em que apanham até sua morte ou quase isso e podem, inclusive, serem queimados vivos amarrados em árvores. Exemplo disso, temos matérias como a de UGARTE, Ayala Álex. A justiça do medo. La paz, 2014. Disponível em: https://brasil.elpais.com/brasil/2014/04/01/internacional/1396313192_411524.html. Acesso em 11 set. 2022

Segundo o delegado e agente da Polícia Federal Erik Siqueira[14], na atualidade, o crime pacífico ocorre no meio virtual, não usa de violência e é um crime considerado invisível. E ainda, nesta mesma entrevista para o Security Report, afirma que, estas: “são duas características importantes que acompanhamos de perto nesse tipo de crime [cibernético] e que muitas vezes não demonstram o real impacto e dano para a sociedade e segurança pública”. O delegado quis dizer com isso que, por ser um crime cometido ‘às escondidas’, muitas vezes não tem um impacto social tão grande como aqueles que são televisionados, mostrando dinheiro no chão, dinamites e vídeos de explosões em bancos, por exemplo. As pessoas se impressionam pelo que veem e não pelo que ouvem falar, apesar do impacto de um roubo presencial ser igual, no sentido financeiro, que um crime cibernético à um banco.

É importante ressaltar o que nos diz o delegado Erick Siqueira sobre não ser um crime violento, resultando em muitas pessoas não acharem que é crime, além de estarem do alto de suas cadeiras e do falso anonimato que citamos anteriormente como facilitador para a ocorrência desses crimes ou tentativas de crimes cibernéticos.

Essa facilidade se dá pois:

> “enquanto que no mundo real há que se passar por uma porta giratória com detector de metais para se ingressar em um banco, o ingresso em qualquer instituição da sociedade virtual- seja financeira, seja governamental ou outra- está a um clique de distância” (SYDOW, 2009, p.24).

Para conceituar o que são os crimes virtuais, vamos insertar através do que nos diz Pinheiro (2010, p.46):

> “Podemos conceituar os crimes virtuais como sendo as condutas de acesso não autorizado a sistemas informáticos, ações destrutivas nesses sistemas, a interceptação de comunicações, modificações de dados, infrações aos direitos de autor, incitação ao ódio e descriminação, chacota religiosa, transmissão de pornografia infantil, terrorismo, entre diversas outras formas existentes”.

[14] Em entrevista cedida à Security Report, matéria de Letícia Cotta, datada de 2020. Disponível em: https://www.securityreport.com.br/destaques/crimes-ciberneticos-possuem-um-padrao-segundo-erik-siqueira-da-pf/#.Yvg6vkfMLIV. Acesso em 11 ago. 2022.

O panorama que temos de ameaças cibernéticas no Brasil é enorme, mas nem todas se consolidam, como podemos observar na figura 1, contamos com alguns bilhões de tentativas de ataques cibernéticos.

Figura 1- Panorama de Ameaças Cibernéticas no Brasil em 2020

Fonte: INFRA NEWS (2020)

Em uma matéria para a revista Istoé Dinheiro, afirma-se que o Brasil foi o 5º país que mais sofreu crimes cibernéticos no ano de 2021 e que segundo informações de uma consultoria alemã de organização de empresas e de gestão, houve um aumento de mais de 9 milhões de ocorrências apenas no primeiro trimestre com relação ao ano anterior.[15]

Um número alarmante para a segurança em rede, o que retira o pensamento da sociedade em geral de ser um número alarmante para a segurança das cidades e isso faz com que se tenha a falsa ilusão de que essa violência é invisível, transparente no sentido de não ser perceptível nas ruas, nas reportagens, são apenas números indicados em alguns segundos na televisão ou em jornais digitais.

Tendo em vista que a população não compreende o que está por trás destes delitos no ciberespaço, como o tráfico de drogas e as grandes facções criminosas que estão entrelaçadas nestes problemas cibernéticos, como foi ressaltado anteriormente na fala do delegado Erick Siqueira.

[15] Matéria intitulada “Brasil foi o 5º país com mais ataques cibernéticos no ano, relembre os principais”. Disponível em: https://www.istoedinheiro.com.br/brasil-foi-5o-pais-com-mais-ataques-ciberneticos-no-ano-relembre-os-principais/ Acesso em 10 ago. 2022

Vale ressaltar que a internet não está sendo um espaço de crimes apenas nesses últimos anos, Queiroz (2008, p.171) afirma que em 1994, época em que a internet passou a ter a propensão comercial no Brasil, era vista como uma facilitadora de comunicação, no sentido das relações de consumo e de estudo, e a partir daí**,** começaram a aparecer diversas infrações cibernéticas. E de acordo com a figura 2, o movimento de e-commerce no Brasil, segue em alta.

Figura 2- O movimento de e-commerce no Brasil, em janeiro de 2020

Fonte: PagBrasil (2020)[16]

Com a evolução da tecnologia, novos meios de acesso à internet foram surgindo. Outrora, o acesso era apenas através de um computador de mesa, com muito sacrifício, em que para conectar à rede, tínhamos que esperar diversas horas e até mesmo esperar pelo final de semana, por conta das altas tarifas e por esta ser conectada também ao telefone, o que fazia com que ele ficasse ocupado, se falarmos de quem possuía acesso à internet em casa.

Mas, agora é comum o uso da internet através de telefone celular, notebooks, tablets, televisões e videogames. E o acesso se popularizou, “hoje, vivemos num mundo de rapidez e fluidez” (SANTOS, 2001, p.83), a internet é a alternativa para não ir em uma

[16] Disponível em: https://www.pagbrasil.com/pt-br/insights/brasil-os-numeros-do-relatorio-digital-in-2020/ Acesso em 10 ago. 2022

loja, é a facilitadora de compras, é o lugar onde salvamos os cartões de crédito e todos os nossos dados para não perdermos tempo, além de deixar um recado rápido para alguém. E sendo este um espaço de armazenamento de dados, é mel para os criminosos.

Enquanto uns não querem perder tempo e sequer analisam o que estão fazendo, por estarem em ‘piloto automático’, há os que estudam os passos dados por todos nós, principalmente quem é ou está mais vulnerável, criando aplicativos e sites que simulam os originais – geralmente de compras ou de bancos-. Afinal, segundo Vesica (2007, p.13) “não faltam exemplos de falhas de programas exploradas para utilizar computadores para outras finalidades, e os alvos são os mais diversos(...)”.

A evolução social é clara, a sociedade como um todo já migrou para acontecer também no ciberespaço. E segundo Lévy,

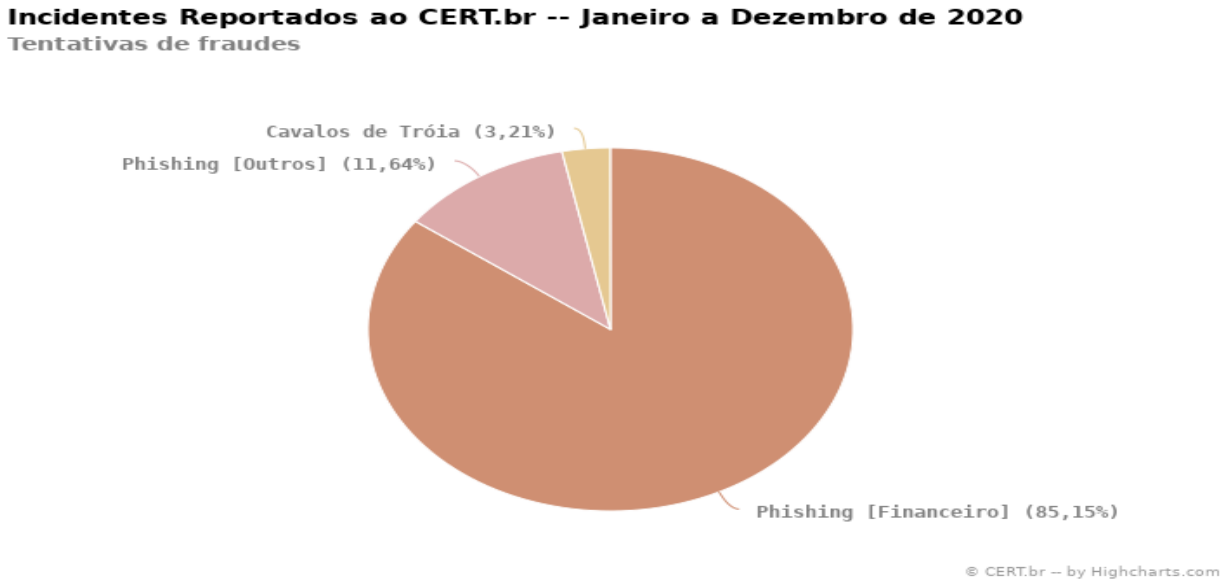
> "a extensão do ciberespaço acompanha e acelera uma virtualização geral da economia e da sociedade. Das substâncias e dos objetivos voltamos aos processos que o produzem. Dos territórios, pulamos para o nascente, em direção às redes móveis que os valorizam e as desenham. Dos processos e das redes, passamos às competências e aos cenários que as determinam, mais ainda. Os suportes de inteligência coletiva do ciberespaço multiplicam e colocam em sinergia as competências. Do design à estratégia, os cenários são alimentados pelas simulações e pelos dados colocados à disposição pelo universo digital. Ubiquidade da informação, documentos interativos interconectados, telecomunicação recíproca e assíncrona em grupo e entre grupos: ciberespaço faz dele o vetor de um universo aberto. Simetricamente a extensão de um novo espaço universal dilata o campo de ação dos processos de virtualização" (LÉVY, 1999, pp. 49-50).

3 PANORAMA DOS CRIMES MAIS COMETIDOS NO BRASIL VIA INTERNET

Para os usuários comuns, quando falamos em crimes cibernéticos, se pensa em calúnia, injúria, difamação em redes sociais ou algum golpe simples, como do pix, entretanto, para os mais experts ou para quem trabalha em grandes empresas, sabe que essa é só a ponta do iceberg. Os casos de crimes virtuais que citamos como os mais pensados por usuários comuns, são mais vinculados à problemas pessoais entre pessoas, ao preconceito, enfim, tem relação ao mundo jurídico-social.

Segundo o portal R7, em uma matéria de Filipe Siqueira (2022), “os golpes mais comuns utilizam engenharia social, para manipular psicologicamente a vítima, ou dados sigilosos obtidos por roubos de celulares”. E nestes dados sigilosos estão os dados bancários e aí ocorre outro tipo de crime: as fraudes. E vale ressaltar que dentro do crime de fraude há subcategorias de crimes, como podemos averiguar em consonância com a CERT. Br, como consta na figura abaixo:

Figura 3- Tentativas de fraudes no Brasil no ano de 2020



Fonte: CERT.br (2022)

Precisamos sumariar estes crimes e explanar como ocorrem, o que são e esclarecermos mais alguns dados informativos sobre outros crimes cibernéticos, e o faremos.

O portal R7, ainda informa que “outras modalidades de fraudes utilizam sites falsos para capturar informações confidenciais ou incitar a compra em lojas que não existem. Esse tipo de golpe cresceu 41% no ano passado, segundo a filial brasileira da Avast”.

Seguindo a ordem do que foi exposto, iremos explanar o que são estes crimes, assim teremos os crimes em tópicos e suas implicâncias ao usuário, ou melhor dito, à vítima. Segundo Leandro Kovaes (2021), para o TecnoBlog[17], os principais crimes são:

1. Fraude por e-mail e pela Internet;
2. Fraude de identidades, quando informações pessoais são roubadas e usadas;
3. Roubo de dados financeiros ou relacionados a pagamento de cartões;
4. Roubo e venda de dados corporativos;
5. Extorsão cibernética, que exige dinheiro para impedir o ataque ameaçado;
6. Ataques de ransomware, um tipo de extorsão cibernética;
7. Cryptojacking, quando hackers exploram criptomoedas usando recursos que não possuem;
8. Espionagem cibernética, quando hackers acessam dados do governo ou de uma empresa.

Nestes 8 itens destacados por Leandro Kovaes, há meios com que facilitam estes e podemos agrupá-los em outros grupos, como por exemplo, os itens 2 e 3 são o mesmo crime ou se complementam, em que primeiro se roubam informações pessoas (dados pessoais) e podem se passar por essa pessoa (geralmente em compras on-line, com os dados do cartão de crédito ou dos dados bancários, para que se haja um pagamento em débito automático, por exemplo. Os itens 5 e 6 são complementares, já que são crimes de extorsão cibernética. E o item 1 é um tipo de phishing, o item 4 um tipo de invasão de dados, ficando à parte por ser venda de dados, mas que pode

[17] KOVAES, Leandro. O que é um crime cibernético? 3 casos populares. Tecnoblog, 2021. Disponível em: tecnoblog.net/responde/o-que-e-um-crime-cibernetico-3-casos-populares/ Acesso em 13 set. 2022

ser aglutinado aos itens de roubo de dados (tanto pessoais como de corporativas), e tem a ver com o item 8, afinal, antes de existir o roubo, haverá a espionagem dos dados que acarretará uma possível extorsão. E o item que fica sozinho, é o item 7.

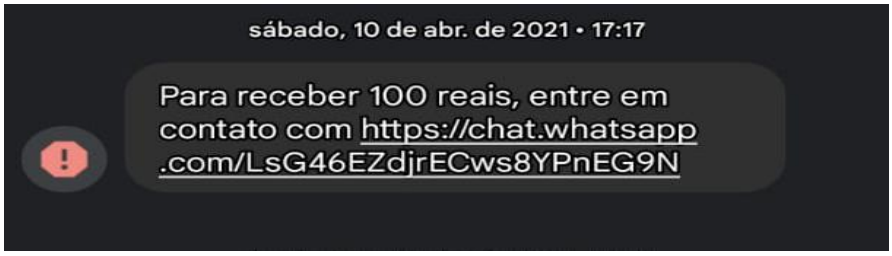
Sendo assim, iremos tratar dos crimes, falando das seguintes temáticas: Phishing, Engenharia Social, Roubo de Dados (e invasões), Rawsonware e Cryptojacking.

3.1 Phishing

Esse nome (*pishing*) vem do inglês com a ideia de “isca”, em que os bandidos usam iscas em sites para conseguirem o que tanto almejam: dados pessoais. Com estes dados os criminosos cibernéticos conseguem fazer diversas coisas e isso vale mais que dinheiro. É claro que também dados financeiros.

Exemplo disso iremos ver na figura 4, os criminosos agem como se a vítima tivesse que fazer urgentemente o que eles pedem, como clicar em links e a isca da vez é um ganho financeiro que todos sabemos que é bastante improvável receber sem ter feito nada e ainda mais acompanhado de um link que supostamente vai parar em um contato de *WhatsApp*.

Figura 4 – Exemplo de *phishing* via SMS



Fonte: Arquivo Pessoal

As fraudes por e-mail e pela internet em geral, primeiro item dos 8 que Kovaes (2021) ressalta, tem a ver com phishing, também, afinal, essa isca, podemos observar como fraude pela internet e e-mail, com um malware[18] “camuflado”, anexado ao e-

[18] Usados como intermediários dessas ações criminosas, usando da vulnerabilidade de programas instalados, *pen-drives* infectado executado no computador da vítima, acesso a páginas maliciosas sem possuir um bom antivírus instalado ou usar um navegador vulnerável, em arquivos baixados da própria internet (.doc e pdf são os mais comuns).

mail. E este malware irá burlar o sistema do computador, expondo a máquina à inseguridade. Esse tipo de ação, “com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo”[19] é crime.

Outros exemplos de phishing, por e-mail, são[20]: o golpe da fatura falsa, golpe da atualização do e-mail, golpe nigeriano, golpe do PayPal (que usa o nome desta forma de pagamento para ludibriar pessoas, como golpe da atualização do e-mail e da fatura falsa), se passar por um site etc.

Exemplo do golpe da fatura falsa é o da imagem 5, em que o cliente abre o e-mail e recebe uma fatura idêntica à da empresa de planos de saúde Unimed e crê que esse seja o seu boleto e sem verificar – até por ser realmente cliente e não se atentar ao valor-, efetua o pagamento. A empresa emitiu um alerta em seu próprio site, devido ao grande número de clientes que caíram no golpe e tiveram problemas quanto à verificação do seu pagamento ou a algum atendimento que não foi prestado justamente por não constar o pagamento.

Figura 5- Golpe da Fatura Falsa

Fonte: Unimed (2021)[21]

[19] Art. 154-A, que altera o código penal.
[20] De acordo com o Blog Usecure. Disponível em: https://blog.usecure.io/pt/the-most-common-examples-of-a-phishing-email. Acesso em 14 set. 2022
[21] Disponível em: https://www.unimedvtrp.com.br/noticias/cuidado-com-o-golpe-do-falso-boleto-por-e-mail-2/ Acesso em: 12 set. 2022

Dentro desses golpes na internet está o golpe da atualização do pagamento. Consiste em um e-mail recebido que te direciona para um site falso, isso ocorre com reativações de contas de plataformas conhecidas, como a Netflix, por exemplo, como podemos observar na figura 6. Podemos ver um e-mail remetente que não é oficial, porém, nem sempre nos atentamos a isso, focando apenas no assunto “Netflix/ Evite o bloqueio da sua conta!” e dependendo do nível do usuário, ele vai logo clicar e por seus dados sem analisar se realmente está naquela situação de suspensão por falta de pagamento.

Figura 6- Golpe do site falso, com link de pagamento de streaming famosa

Fonte: TecMundo[22] (2019)

Um outro tipo de golpe que já foi muito comum, é o nigeriano, foi amplamente divulgado nas emissoras públicas de televisão, e por este motivo tem sido um pouco esquecida ou não mais tão praticada como antes. Mas, segue sendo um exemplo de fraude/crime via e-mail e internet. É necessário sempre retornar os olhos para o passado, afinal, segundo o especialista em cibersegurança Hasnain Bokhari, para a

[22] Disponível em: https://www.tecmundo.com.br/seguranca/142323-cuidado-email-falso-netflix-diz-conta-suspensa.htm Acesso em 15 set. 2022

UOL[23], este golpe é uma variação histórica, em que se escreviam à mão cartas pedindo resgate de pessoas nobres. Santana (2021) afirma que: “o clássico email do príncipe nigeriano entra nessa categoria e envolve o convencimento da vítima para que faça depósito em moeda estrangeira”. O farsante diz ser um príncipe da Nigéria e pede ajuda para resgatar um dinheiro de familiares seus que foi depositado em uma conta no Brasil, começa a envolver a pessoa na sua conversa e inicia-se a extorsão de dinheiro.

Vale ressaltar que há outros golpes como esse de romance, usado não em e-mail, mas, na internet, em aplicativos de namoro, como por exemplo o Tinder. Você conversa com alguém que se interessou pela foto, marca em um lugar e cai no golpe que se iniciou na internet, acaba sendo roubado pessoalmente ou até mesmo sequestrado, então é um crime cibernético, na modalidade phishing. Além de que há extorsão ali mesmo no âmbito da internet, quando passam para outro aplicativo de conversas e começam os pedidos e desculpas para realizar a extorsão. O lugar onde se tem aplicado em maior número esse golpe é São Paulo, trata-se de “uma quadrilha especializada em golpes do PIX criou um perfil falso com a foto de uma garota de 13 anos para atrair homens e roubá-los”, segundo Luquesi (2022), em matéria para o G1[24].

Esses são os golpes mais conhecidos de phishing e que podemos retratar aqui, para não nos estendermos em apenas um tópico.

3.2 Engenharia Social

Com base em Mitnick e Simon (2003, APUD HENRIQUES, 2016, p.37), “é um conjunto de práticas utilizadas para a obtenção de informações relevantes ou sigilosas de uma organização ou indivíduo, por meio da persuasão, manipulação e influência das pessoas, seja com o uso ou não da tecnologia”. Cabe ressaltar que o *phishing* é

[23] SANTANA, Lucas. “O que está por trás do velho golpe do príncipe da nigéria”. Matéria disponível em: https://www.uol.com.br/tilt/noticias/redacao/2021/12/27/o-que-esta-por-tras-do-velho-golpe-do-principe-da-nigeria.htm Acesso em 14 set. 2022

[24] LUQUESI, Thaís. “PM liberta vítima de sequestro e deteve 7 suspeitos pelo crime na Zona Norte de SP”. Disponível em: https://g1.globo.com/sp/sao-paulo/noticia/2022/08/09/pm-liberta-vitima-de-sequestro-e-deteve-7-suspeitos-pelo-crime-na-zona-norte-de-sp.ghtml Acesso em 14 set. 2022

um tipo de engenharia social, e que quisemos pôr em relevo o tema, pois é a maneira mais praticada.

A engenharia social consiste em quatro passos: coleta de informação, desenvolvimento da relação, exploração de relacionamento e a execução (HENRIQUES, 2016, p.39).

Visando um alvo, o cybercriminoso prepara-se durante um tempo organizando e reunindo informações sobre uma organização ou uma pessoa física. A etapa de coleta de informação é a mais demorada, pois para lograr o que ele almeja, necessita ter informações concretas, consistentes. E realiza-se através da monitoração do tráfego da rede, do reconhecimento da rotina, do horário de trabalho das pessoas e isso pode ser alcançado por eles, os engenheiros sociais, em fontes como as redes sociais, portais, páginas web etc. (HENRIQUES, 2016)

Em suma, os olhos do cybercriminoso não desgruda do seu alvo, até encontrar e examinar as informações do seu alvo e conseguir correspondência entre eles, sem que haja incongruência, para que ele venha a cair em suas artimanhas.

Agora , já com as informações de suas vítimas analisadas e selecionadas, o criminoso parte para a segunda ação, que é a do desenvolvimento da relação, consistindo no estreitamento da relação, se passando por uma entidade pública, mascarando sua real identidade e entrando em contato com esse alvo, sendo a de fase mais prolongada aquela em que o cybercriminoso cria um perfil falso e conversa com a pessoa até garantir um certo vínculo e envolvimento capaz de passar para o penúltimo passo da engenharia social. E há também aqueles que se fazem de vítima, pedindo ajuda. (HENRIQUES, 2016, p.40-41).

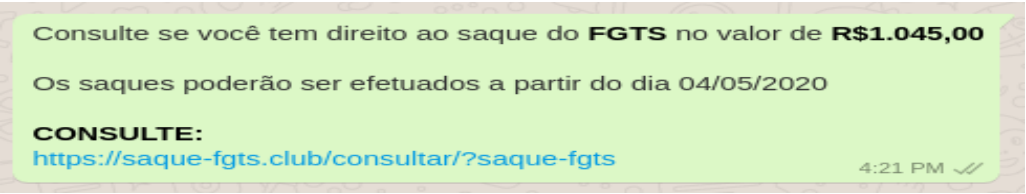
Quando nos conectamos em uma rede social e temos nossos perfis abertos, estamos dando margem à marginais e a nossa insegurança em rede, alguns cybercriminosos podem se passar por parentes distantes, por amigos, por pessoas interessadas amorosamente por nós, por refugiados e até mesmo por ‘pessoas desesperadas’ em busca de um auxílio, de um PIX para ajudar na manutenção de sua casa e de seus inúmeros filhos; bastam encontrar um ‘bom’ alvo. Após ganhar a confiança, vem estes pedidos de ajuda, tudo é feito sutilmente e envolvendo a vítima

para que esta se sinta à vontade com o criminoso, até mesmo chamando-o de amigo e crendo que ele possui os mesmos valores pessoais.

Essa é a fase da exploração de relacionamento, após ludibriar o alvo, ela tornar-se-á vítima, pois começará a revelar informações, valores, dados em que uma situação normal, uma conversa sadia, não haveria esse tipo de conversa. O engenheiro social está tecendo o relacionamento que já conquistou para ver até onde pode sugar, ele tem o dom de ludibriar, o dom das palavras. A finalidade é uma só, segundo Henriques (2016, p.42): “obter do alvo um estado emocional desejado adequado ao plano, como sentir-se triste ou feliz. Ao criar uma relação com uma estória triste, por exemplo, pode-se evocar no alvo a lembrança de um incidente infeliz e, posteriormente, entristecê-lo”. Após conseguir fazer com que a vítima se sinta emocionalmente balançada, vem a execução de maneira sutil, para que as vítimas não se previnam. O cybercriminoso tem que terminar como o bonzinho, o amigo que precisava de uma ajuda, o que veio apenas avisar uma situação ou ainda o da cartada final (de uma dívida, por exemplo).

E igualmente o crime pode ser apenas “em massa”, como phishing mesmo, como podemos ver na figura 7, uma mensagem enviada para um aplicativo de conversas, com um link suspeito, afinal, a Caixa Econômica não possui esse canal para relacionamento com seus clientes repassando links, há seu site oficial para tal dúvida ou informação sobre FGTS. Sabendo da atual situação financeira e da insegurança alimentar, por hora instalado, os engenheiros sociais buscam brechas para ‘alertar’ de ganhos aos seus alvos e conseguir praticar o crime de fato.

Figura 7- Golpe do FGTS via WhatsApp



Fonte: InfoMoney[25] (2020)

[25] Disponível em: https://www.infomoney.com.br/minhas-financas/golpes-do-novo-saque-do-fgts-ja-atingiram-quase-100-mil-pessoas-saiba-se-proteger/ Acesso em 16 set. 2022

Bem como a próxima figura indica outro caso de engenharia social, do tipo phishing, agora usando o nome do Banco Santander, pedindo o recadastramento dos dados do alvo. Este, recebido via e-mail.

Figura 8- Fraude utilizando o nome de um famoso banco

Fonte: CanalTech[26] (2021)

O roubo de identidade também faz parte da engenharia social, como a clonagem do WhatsApp, em que o cybercriminoso se passa por outra pessoa para conseguir ganhos financeiros via pix das pessoas que querem, as vezes desesperadamente, ajudar a pessoa na qual o bandido está roubando a identidade. Os crimes são quase perfeitos, utilizam a foto, sabem o nome da pessoa e até mesmo o grau de intimidade que a pessoa tem com a outra. A desculpa utilizada é que estão com problemas para acessar o banco, que irão receber a quantia que estão pedindo no outro dia e precisam com urgência desta ajuda monetária.

O crime já acometeu até mesmo dois deputados federais em 2018, segundo notícias do portal Consultório Jurídico[27], o advogado e especialista em Direito Digital Alexandre

[26] Disponível em: https://canaltech.com.br/seguranca/o-que-e-engenharia-social-195773/ Acesso em 15 set. 2022

[27] CONJUR. "Entenda como funciona golpe de WhatsApp que vitimou deputados", matéria de 2018. Disponível em: https://www.conjur.com.br/2018-fev-10/entenda-funciona-golpe-whatsapp-vitimou-deputados. Acesso em 17 set. 2022

Atheniense ressaltou que: “muitas vezes, esse golpe acontece com a conivência de alguém infiltrado dentro das operadoras de telefonia”. E informa como é feito o processo: “(...) o responsável pelo golpe consegue transferir o número da vítima para outro chip temporariamente e faz a reinstalação do aplicativo em outro aparelho, recuperando os dados e contatos”.

Figura 9- Caso de aviso em rede social de roubo de identidade: uma ‘casadinha’ de cibercrime para extorquir parentes e amigos da vítima

Fonte: Instagram pessoal de uma das vítimas

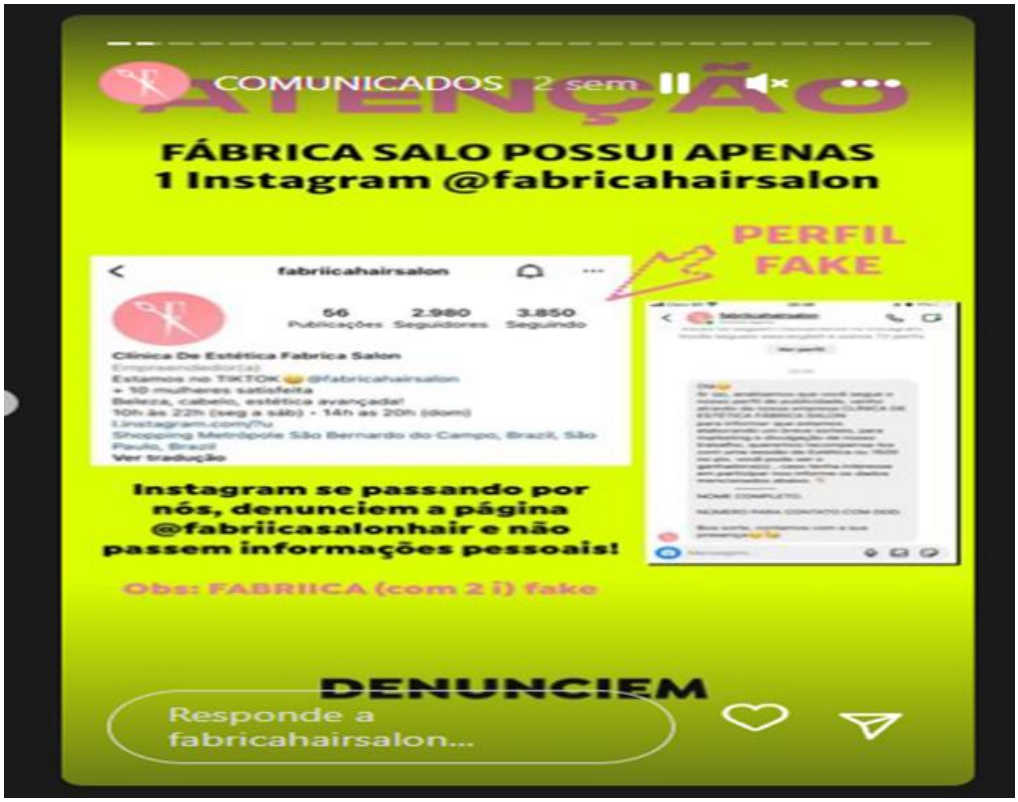
Caso semelhante ao dos deputados, é o caso deste homem que teve sua identidade roubada e estavam usando-a via WhatsApp, em março de 2022 e está alertando via redes sociais que há alguém se passando por ele e que entrou em contato com parentes de primeiro grau dele pedindo dinheiro via pix para outra pessoa, entretanto o nome que constava no telefone e foto eram dele.

Este tipo de conduta, é criminosa e está prevista no artigo 307 do Código Penal, do Decreto Lei nº 2.848, assim como, no aspecto físico, como no digital o ato constitui, sim, crime previsto no Código Penal:

> Art. 307. Atribuir-se ou atribuir a terceira 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.

A Engenharia Social também ocorre utilizando de empresas bem-sucedidas na cidade. Recentemente, foi televisionado na TV Record, no dia 17 de setembro de 2022, o caso de um salão de beleza e São Bernardo, em São Paulo, chamado *Fábrica Hair*, em que uma página se passava pelo salão pedindo as clientes seus dados pessoais para um sorteio e também, através de um link disponível nesta página fake nas redes sociais direcionado para o aplicativo de conversas, pediam 50% antes da marcação da cliente no salão e muitas clientes caíram no golpe, segundo a proprietária Letícia Lins, em reportagem. O dinheiro, claro, caía na conta dos fraudadores, segundo a TV São Bernardo, em site[28] com o resumo da matéria. Na rede social em que foi clonada, a proprietária do salão deixa o alerta para os seus clientes, conforme podemos observar na figura 10, mostrando aos seguidores, mais de 12 mil pessoas, que o outro perfil é fraudulento e pedindo para que não caíam, pois só possuem apenas uma rede social e manda prestar atenção no nome correto do perfil.

Figura 10- Perfil oficial alerta sobre perfil fake que está se passando pelo salão

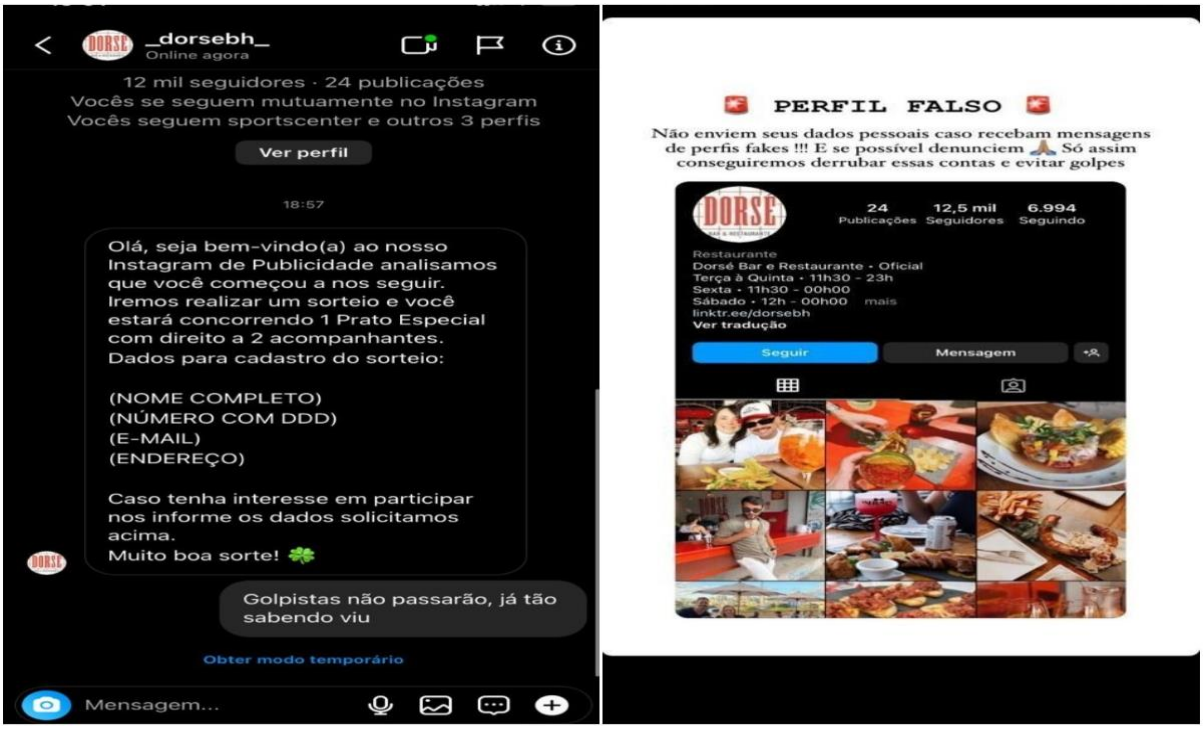


Fonte: Instagram (Story em destaque do perfil oficial do Salão de Beleza), 2022

[28] TV São Bernardo. Em São Bernardo, perfil de salão de beleza é clonado e criminosos enganam clientes. Disponível em: https://tvsaobernardo.com/em-sao-bernardo-perfil-de-salao-de-beleza-e-clonado-e-criminosos-enganam-clientes/ Acesso em 18 set. 2022

Outro exemplo disso foi o caso de um restaurante em Belo Horizonte, que segundo a jornalista Larissa Reis, para o BHAZ[29], o crime é concretizado em um “suposto sorteio e pede que os participantes enviem dados pessoais, como telefone, nome completo e endereço”. O roubo de dados é dado como participação de um sorteio e usam a imagem do restaurante para passar credibilidade, novamente usam do sentimento e do envolvimento das possíveis vítimas, como podemos observar na figura 11, em que vemos uma conversa com um cliente que não caiu no golpe e o alerta da página oficial do empreendimento alimentício.

Figura 11- Engenharia Social sendo desmascarada pelo Restaurante prejudicado



Fonte: BHAZ (2022)

Um caso de Engenharia Social que desemboca em roubo de dados, que inclusive será outro subcapítulo deste trabalho, como podemos ver a seguir.

[29] REIS, Larissa. “Restaurante de BH denuncia perfil falso que pede dados de clientes em suposto sorteio”. 2022. Disponível em: https://bhaz.com.br/noticias/bh/restaurante-de-bh-denuncia-perfil-fake/#gref Acesso em 17 set. 2022

3.3 Roubo de Dados e Lei Geral de Proteção de Dados

Vimos que a Engenharia Social também visa o roubo de dados, no caso do restaurante de Belo Horizonte, fizeram um perfil fake para roubar dados de clientes e há casos em que há a invasão da conta nas redes sociais e o roubo de dados.

Na figura 12 vemos uma página que está se passando por um determinado Banco e em seguida, na figura 13 está pedindo dados pessoais para o cliente, futura vítima. E pede para que entre em contato com eles via mensagem instantânea do *Twitter*, o cliente, infelizmente, cai no golpe e envia todos os seus dados e os do cartão de crédito, inclusive o código verificador, de três números, que serve para fazer compras online.

Figura 12- Cliente solicitando a uma página falsa um atendimento

Fonte: El Pescador (2015)

Figura 13- O criminoso em contato com o cliente do banco, agora vítima

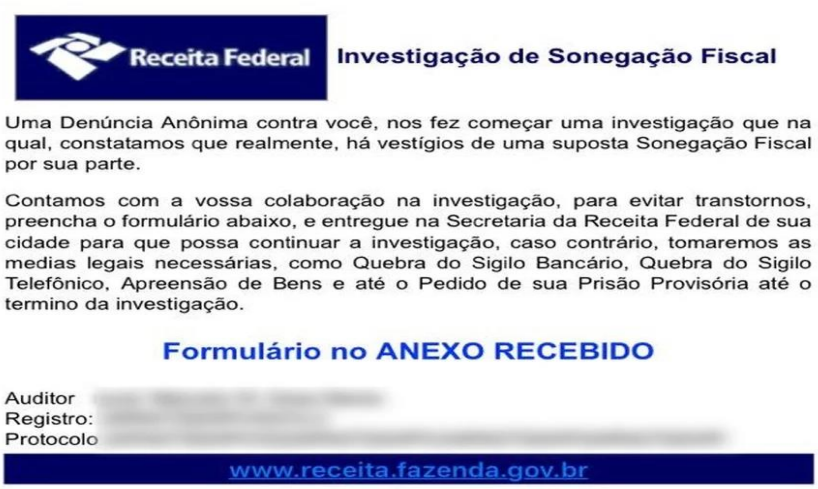
Fonte: El pescador (2015)

Parece absurdo que ainda várias pessoas caiam nesse tipo de crime, entretanto, sempre existe um desavisado e vale lembrar que há muitos que desconhecem normas de segurança em internet e do seu próprio banco ou cartão de crédito.

Outra forma muito usual é uma isca enviada para o e-mail do potencial vítima, em que o criminoso usa da engenharia social, como nos explica Fontes (2006, p.120), é o: “(...) conjunto de procedimentos, e ações que são utilizados para adquirir informações de uma organização ou uma pessoa por meio de contratos falsos sem o uso da força, do arrombamento físico ou de qualquer brutalidade”. (apud LEITE, 2017, p.2)

E isso pode ser observado na figura 14, em que os bandidos usam da boa-fé do cidadão que quer resolver qualquer situação pendente em seu nome e clica no link malicioso para ter mais informações. Essa é uma tática que usam bastante e geralmente quem cai demora a se dar conta do que houve para o roubo de dados e claro, mais um exemplo de *phishing*.

Figura 14- Caso de Engenharia Social usando o nome da Receita Federal



Fonte: Jornal Contábil (2017)

É mister destacar que os criminosos antes de praticar esse crime, estudam sobre como enviar e-mails em série, ou através de robôs de spam ou usando serviços de spam que existem na *deepweb*, como o *SafeSend*. (PHISHLABS, 2013, apud MATOS, 2017, p.40). Não parece ser difícil para quem possui a sede de poder, de conquistar sem ser descoberto e se sentir, de certa maneira, superior, por estar burlando o sistema e de fazer com que uma parte da população caia no seu golpe. Tanto que de acordo com uma notícia da TecMundo[30], datada de 2019, foi descoberto um roubo de dados de 2,3 milhões de cartões de crédito em 2,6 mil sistemas no Brasil e esse número pode ser ainda maior, segundo a empresa responsável por esta informação.

Segundo Urupá (2022), em estudos realizados pela empresa especializada em segurança da informação, chamada Syhunt, o Brasil está entre os países que mais sofreram ataques de sequestro e de vazamento de dados pessoais do mundo, em oitava posição. E tem o primeiro lugar na América do Sul, seguido do Chile.

[30] Matéria disponível em: https://www.tecmundo.com.br/seguranca/141766-cibercrime-roubou-2-milhoes-cartoes-credito-brasil-malware.htm

Geralmente, esse crime é cometido através de ransomware, que será um outro subtema trabalhado neste capítulo.

Essa tomada de cybercriminosos, vai muito além de tudo que explanamos, eles atuam, também, com invasões para sequestrar dados, na maioria das vezes, ocasionando muitos prejuízos. Além de invadir sites de companhias aéreas para fazer alterações e comprar passagens para integrantes do tráfico de drogas ou seus chamados “aviõezinhos”[31].

Eliane Saldan, nos afirma que: “o ambiente cibernético pode ser considerado, portanto, um novo domínio ou palco de batalha, depois da terra, do mar, do ar, do espaço exterior e do espectro eletromagnético”. (SALDAN, 2012, p. 68). Estamos em maior quantidade? Não sabemos, mas se é um espaço social, traz implicações e precisa de segurança para alcançar a plenitude do seu uso.

Se tratando de roubo de dados, diferente das outras leis, retratadas no penúltimo capítulo deste trabalho, deixaremos a Lei Geral de Proteção de Dados para comentar neste subtema por relacionar-se.

A Lei de Proteção de Dados, comumente chamada LGPD, é a lei de número 13.709, de 2018, que possui como objetivo defender o direito da liberdade e da privacidade seja ela social ou jurídica, é “filha” da Legislação Europeia neste mesmo sentido e regulariza as práticas de proteção de dados pessoais em todo território nacional. Por ser uma Lei que defende a imposição de limites ao acesso, ao compartilhamento, captação e uso dos dados, tem a ver com o que assegura a Constituição Federal de 1988 a partir do art. 5º, § 2º[3] o princípio da dignidade da pessoa humana, que se consagra como direito à liberdade individual e que consequentemente, se estes forem violados, expõem-se a individualidade humana.

E para que haja o cumprimento da LGPD, todas as empresas precisam de um serviço de TI para a segurança da sua rede, pois esta lei visa que os dados pessoais sejam perpassados de forma confiável, que saibamos para onde está sendo compartilhado estes dados, segurança está assegurada entre os sistemas internos e externos, garantindo assim a confidencialidade dos dados e impossibilitando o rastreamento deles por pessoas mal-intencionadas.

[31] Como são conhecidas popularmente as pessoas utilizadas para transportar drogas.

3.4 Ransomware (Sequestro de dados)

O ransomware é um tipo de malware (software causador de danos) com a finalidade de bloquear ou restringir dados de sistemas, e que geralmente consegue se infiltrar nas redes corporativas por e-mails de phishing (técnica de cybercrime para obtenção de dados já mencionada anteriormente), que, ao serem manipulados, começam a fazer a invasão e o sequestro dos dados, extorquindo, assim, as vítimas para recuperarem o acesso ao sistema ou aos arquivos. (LISKA e GALLO, 2017)

O pagamento destes resgates, geralmente, é solicitado através de Bitcoins, moeda eletrônica, sem maiores problemas com a lei e que é mais difícil de se rastrear para qual carteira está indo. Vale ressaltar que o pagamento não garante que seus arquivos sejam desbloqueados, afinal como dificilmente é possível identificar o criminoso, também não há como cobrá-lo. (TREND MICRO, 2015 APUD GUISSO, 2017, p.34)

Segundo o Relatório SonicWall de Ameaças Cibernéticas 2021, nosso país é o quarto do ranking dos que sofrem mais ataques ransomware no mundo e possuiu mais de 33 milhões de tentativas de invasões no ano do relatório.[32]

Estas ameaças vão de sites governamentais a empresas. Como podemos ver nas imagens abaixo, de reportagens sobre o tema.

Figura 15- Ataque de ransomware ao Governo Brasileiro, em 2022

Fonte: Canal Tech (2022)

[32] Dados disponíveis em: https://cryptoid.com.br/conectividade-tecnologia-criptografia-id/crime-digital-brasil-sofreu-mais-de-33-milhoes-de-tentativas-de-ransomware-em-2021/#:~:text=Brasil%20%C3%A9%20o%20quarto%20maior%20alvo%20de%20ataques%20de%20ransomware&text=O%20Relat%C3%B3rio%20SonicWall%20de%20Amea%C3%A7as%20Cibern%C3%A9ticas%202021%20revela%20que%20o,mais%20sofrer%20ataques%20de%20ransomware. Acesso em 18 set. 2022

Figura 16- Os preferidos para o ataque ransomware no Brasil

Fonte: Convergência Digital (2022)

Figura 17- Roubo de dados é noticiado como “joia do cibercrime” na pandemia

Fonte: Folha UOL (2021)

Há notícias atormentadoras de ransomware no Brasil, como vimos nas imagens, e vamos detalhar o que se passou em cada uma destas de maneira resumida para que seja alcançada a explanação. Na imagem 15, os colunistas Felipe Demartini e Claudio Yuge, noticiam que no final de agosto de 2022, o setor de inteligência de ameaças da empresa Darktraces, informou que na deepweb o grupo cybercriminoso Everest incluiu em seu arsenal de vendas de informações- estas não detalhadas- o acesso à 3 TB sobre o Governo Brasileiro. Neste sentido, LLINARES (2019, p.27) destaca o valor dos dados para o cybercrime:

> quando os terminais informáticos tiveram o protagonismo e a informação pessoal que elas podiam conter, apareceram novas formas de afetas a intimidade das pessoas, quando tais terminais e a informação contida nelas começaram a ter valor econômico e a servir para a realização de transações econômicas, surgiram diferentes formas de crimes econômicos relacionados com os computadores e especialmente a fraude informática, que a sua vez, evolucionou até

> chegar no scam, o phishing e o pharming quando apareceu a internet. (tradução nossa)

Já se foram os tempos que nossos dados pessoais ficavam dentro de uma pasta, caixa ou em uma gaveta em longos corredores, como destacou Llinares os dados e sua importância é xeque-mate para a sede de poder tocar nestes dados, e por isso o governo é o preferido para os ataques, como pudemos ver na figura 16, afinal lá é que se consegue um maior número de dados e inclusive é onde circula mais dinheiro ou possibilidade de extorquir em valores milionários. Segundo a página Convergência Digital (2022): “no Brasil, o setor governamental continuou sendo o mais alvejado pelos criminosos digitais, em junho, seguido pelas áreas de Educação e Indústria. Os segmentos de Seguros e Saúde também ficaram na mira dos atacantes”. Na figura 17, se destaca o ransomware como a joia do cybercrime justamente no período de pandemia. Nesta reportagem virtual para a folha UOL, Paula Soprana, informa que:

> “O Brasil, embora domine outros rankings de crime cibernético, virou um destaque em ransomware durante a crise de Covid-19. Foram atacados o STJ (Superior Tribunal de Justiça), o Tribunal de Justiça do Rio Grande do Sul, empresas na área de energia e a Embraer, que não pagou aos criminosos e teve documentos como contratos de aviões circulados na internet”

3.5 Outros Crimes Cibernéticos

Neste tópico entram os crimes que são mais comentados na internet, por geralmente se tratar de pessoas famosas ou por conta das entrevistas sobre crime que se veiculam na televisão é feita com advogados, exemplos como injúria racial, stalkear (perseguir uma pessoa virtualmente), homofobia, gordofobia, um comentário que chegue a difamar a uma pessoa, grupo ou empresa, crimes de compartilhamento ou de armazenamento de pornografia infantil, por exemplo.

Vale a pena lembrar, sobre esse último assunto, mais uma polêmica levantada pelo Monark, ex-membro do maior Podcast do Brasil, o Flow, que recentemente foi cancelado por apologia ao nazismo (outro crime praticado virtualmente e que se busca eliminar das redes de todas as formas possíveis) e a notícia mais atual de fala em um

Podcast (claro, no meio virtual) o Bruno Aiub**,** mais conhecido como Monark, em meados de agosto de 2022, ao comentar sobre quem consome pornografia infantil afirma que não sabe se quem consome é realmente criminoso, afinal não está praticando o ato, está apenas consumindo um conteúdo. O fato foi amplamente divulgado[33] por conta de soar como uma concordância com o fato e por ser um comentário sobre um famoso, o PC Siqueira, que está sendo investigado por este crime.

4 CRIME CIBERNÉTICO NA PANDEMIA E PÓS PANDEMIA E A VISÃO DE UM AGENTE DE POLÍCIA FEDERAL SOBRE O TEMA

Muitos aspectos mudaram mundialmente depois da longa quarentena que fizemos por conta do COVID-19, muitas restrições foram feitas a fim de sanar a pandemia, entretanto, revelou a face mais pesada de uma crise que já existia.

“Esta situação sanitária atípica, veio também provar a elevada dependência das sociedades modernas relativamente às tecnologias da informação, à internet e ao ciberespaço” (CARREIRAS *et al.,* 2020, p. 7). E com isso também veio à tona os problemas de segurança nesse ciberespaço, não que fosse inexistente ou com uma baixa porcentagem de crimes, mas tornou viável o crime quando um programa especialmente desenvolvido para uma rede – empresarial- foi rodado em uma máquina de uso pessoal destes usuários, sem terem os mínimos cuidados de segurança (boa varredura, bom antivírus e análise ao menos semanal do desempenho desta máquina).

Fora o discurso de ódio com injúria (palavras ofensivas), crime de ameaça (contra a vida, falar que vai bater, que vai arrancar cabelos ou fazer qualquer menção a tocar na pessoa como modo de repressão ou retaliação), a difamação (crime contra a honra), a clonagem de *WhatsApp* e um sem-fim de crimes.

[33] Tivemos como pauta a própria observância do Podcast, mas também, por pesquisas nas redes sobre sua fala, encontramos diversos canais comentando sobre a afirmação do Podcaster Bruno. Como fonte, nos ateremos ao Diário de Pernambuco, em matéria intitulada: “Monark defende quem consome pornografia infantil: Não sei se é criminoso”. Publicado em 14 de agosto de 2022, redigido por Natasha Werneck. Disponível em: https://www.diariodepernambuco.com.br/noticia/brasil/2022/08/monark-defende-quem-consome-pornografia-infantil-nao-sei-se-e-crimin.html Acesso em: 19 ago. 2022

E o mais aplicado: o golpe do Instagram, no qual o usuário perde a sua conta (por não ter autenticação de dois passos, para aumentar a segurança) e com a posse do perfil da vítima, o criminoso se vale da boa fama e reputação da pessoa para oferecer objetos de casa e eletrônicos: geladeira, móveis, celulares, para a venda sempre pelo PIX e só falavam por chat desta rede social, se passando por aquela pessoa dona do perfil.

Cada dia vemos, principalmente desde 2019, que o ciberespaço se tornou mais um espaço de crime passivo, de diversas vítimas se queixando, tanto de pessoas como de empresas ou supostas empresas (o que é mais provável) e até mesmo de falsos prestadores de serviço.

Veio à tona toda a falta de segurança que temos nas redes sociais e no ciberespaço em geral, há um sem-número de reportagens que provam esse aumento.

Em uma palestra do Agente de Polícia Federal Erik Siqueira, para o canal *TC Decision*, no Youtube, o policial comenta sobre as fraudes bancárias eletrônicas e fala de uma onda de ataques, inclusive ao governo, além de ataques ao próprio Estado, há o golpe contra o cidadão, o do saque do FGTS, por exemplo, que já comentamos. E segue afirmando que é um crime sem violência e que por isso, é invisível, de certa maneira, pois ninguém viu quem foi e por isso há um certo desdém e atenção a estes crimes. Passa uma sensação de “vazio”, e até mesmo de descrença que isso pode ter acontecido, parece não afetar diretamente ou sensibilizar as pessoas. A sociedade só se preocupa e visibiliza quando vê caixas eletrônicos estourados, segundo o agente de polícia. Nos informa que houve, em 2019, aproximadamente 4 bilhões de reais em fraudes bancárias eletrônicas, e que existiu uma previsão para 2020, de um aumento em 50%- 100%, valores estes que são compatíveis a 30 assaltos por ano, desses homéricos que explodem caixas e fazem uma grande armação para conseguir levar todo o dinheiro.

E ainda, o Erick Siqueira afirma que esse dinheiro está financiando criminosos reais. Segue o raciocínio, dizendo que combater esse crime é vital, afinal é um problema social, pois financia o crime não virtual, como foi afirmado anteriormente. E o que gera o aumento desses crimes cibernéticos é a lei frouxa, são as penas leves.

As fraudes bancárias são financiadoras diretas, segundo Erick Siqueira, pois as vantagens financeiras sem riscos são fáceis e conseguem angariar altos montantes para essas quadrilhas. Exemplo disso é que as fraudes atualmente há casos de fraudes entre 20 e 30 milhões em apenas uma conta bancária. E isso impacta muito a sociedade, afinal, o cidadão sofre prejuízo e ainda o Estado sofre com problemas na segurança pública, por falta de saber onde a pessoa que fraudou está. Além da demora, pois precisam alocar onde está fisicamente este IP que fez o ataque.

Organizações criminosas se beneficiam, ainda segundo expõe o agente de polícia na Palestra sobre Crimes Cibernéticos a existência de casos de pessoas que vão atrás de criminosos para pagarem dívidas, por exemplo, o cidadão que quer levar vantagem possui um boleto de uma dívida de quinhentos reais e entrega ao criminoso este boleto e paga apenas metade do valor, e se acertam desta maneira, afinal esse dinheiro será furtado da conta de um terceiro. As contas geralmente são de luz, financiamentos e impostos. Todos os envolvidos são criminosos, Erick ressalta.

Também há a *Fraude as a service*, que é aquela praticada por empresas, o lojista tem um boleto de dez mil reais para pagar por suas mercadorias e busca um criminoso para quitar essa dívida com um valor mais abaixo, seguindo o mesmo preceito do crime anterior. E é desta maneira desleal que se *quebra* a concorrência, a implicação para a sociedade é o crash econômico do país, e a vantagem financeira deste empresário, quebra a livre concorrência, a competição não é saudável e haverá a falência de outras empresas deste mesmo ramo, afetando na população como um todo, provocando o desemprego.

Essa postura não é de um cidadão de bem e que honra seus princípios e o seu país, restando as autoridades públicas irem atrás desses espertinhos para que paguem pelos seus atos ilícitos que tanto nos prejudicam como um todo.

Na imagem 18, vemos o que a polícia chama de ‘Operação Boleto Real’, em que há uma investigação em andamento – à época- sobre fraudes cometidas no internet banking, concentrada na região de Manaus.

Figura 18 – Print da entrevista de Erick Siqueira sobre a Operação Boleto Real, crime que foi disseminado no Brasil e descoberto pela Polícia Federal

Fonte: Youtube (2022)

Erick Siqueira ainda afirma, na palestra, que: “esses crimes nem sempre são fáceis de enquadrar no nosso ordenamento jurídico, e a gente tem condições de observar isso quando trabalhamos em um modelo centralizado de fraudes”. (SIQUEIRA, 2020).

Segue afirmando que há fraudes no auxílio emergencial, quitação de dívidas de campanhas eleitorais, uso de laranja etc. Todo esse dinheiro, é do crime, segundo o agente. Vale ressaltar o que Siqueira afirma: “grupos extremistas tem se beneficiado, com compras de armas, de drogas, de computadores de alta tecnologia, tudo financiam com essas condutas criminosas”.

Além de um sem-fim de más condutas, que podem ser ouvidas na palestra disponível no Youtube. Porém, uma que chama atenção é:

> “uma série de passagens aéreas compradas em diversos cartões de crédito, que se observar o trecho e comparar com o relatório da ONU sobre as drogas, podemos relacionar que os trechos comprados através de fraudes bancárias, de cartões fraudados, de terceiros, é exatamente o mesmo fluxo do tráfico de drogas internacional, ou seja, é além de ser um serviço jurídico, é o *crime to crime*. E isso reduz o custo do traficante para mandar a mula para outro país. O crime atua para obter vantagem financeira” (SIQUEIRA, 2020)

É algo que foge ao alcance, mas que precisa ser mitigado, demora; mas é descoberto, pode ser aprimorado, mas se acha tanto o alvo como o autor do crime.

5 PRINCIPAIS AÇÕES LEGISLATIVAS NO COMBATE AO CRIME CIBERNÉTICO NO BRASIL

Tudo começou quando a atriz Carolina Dieckmann sofreu um escândalo, com a invasão e posterior divulgação de fotos íntimas suas, em 2011. Teve seu computador invadido e alguém superou a barreira da senha e da proteção de seus arquivos pessoais. A partir desta lei, temos a promulgação de outro crime, como falsidade de documentos. O crime de invasão, partiu de um projeto de lei com caráter de urgência, e pune invasão de dispositivo informático (Art. 154-A, CP).

Uma sociedade é baseada em direitos e deveres e quando ferimos o outro, estamos invadindo seu espaço, o seu direito de se sentir pertencente a algum lugar. As leis servem para unir estados e unir a nação, estarmos em pé de igualdade. Nem sempre se consegue, afinal, apesar de já existir a internet e o compartilhamento de dados íntimos de pessoas (não famosas) há bastante tempo, apenas quando uma atriz de muito sucesso na época sofreu retaliações de um crime cibernético cometido por ela que chamou atenção e foram reformular as leis. Vale ressaltar que:

> “O Direito não é apenas a norma ou a letra da lei, pois é muito mais do que a mera vontade do Estado ou do povo, é o reflexo de um ambiente cultural de determinado lugar e época, em que os três aspectos – fático, axiológico e normativo – se entrelaçam e se influenciam mutuamente numa relação dialética na estrutura histórica. (Reale, 2000, s/p, apud DURAN; BARBOSA, 2015, p.7)

Houve um starter na sociedade para se atentar a esses crimes, há mudanças nas leis justamente pelo mover cultural que temos a cada época. Surge em 2012 a Lei nº 12.737/2012, rompendo paradigmas, avançando com essa nova sociedade. E para detalharmos a lei, vamos conhecê-la ou revisitá-la:

> 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.

É mister ressaltar que já no Art. 5º da nossa Constituição, há a garantia de privacidade, honra e imagem, além da inviolabilidade da intimidade no mundo não-virtual, e como um espaço social, o ambiente cibernético também deve prever todos esses pontos, e a Lei de Marco Civil da Internet assegura esses pontos que citamos além de outros princípios éticos, como a garantia de liberdade de expressão, poder manifestar seus pensamentos sem ser retaliado e nem ferindo o direito de outrem, a proteção da privacidade, dos dados pessoais – essa em forma de lei, e mais detalhada-, estabilidade, segurança e funcionalidade da rede por meio de padrões escolhidos internacionalmente.

Todos esses pontos são uma forma de assegurar o não cometimento de injustiças, que haja liberdade de expressão e o recebimento da internet que contratou. Entretanto, os servidores, as redes sociais e tantos outros sites e aplicativos não nos dá tanta privacidade como gostaríamos de ter ou que os protocolos sociais desejam.

Sabendo que muitos se sentem semi-deuses em suas cadeiras, achando que não serão nunca pegos, em 2021, houve uma tentativa de endurecimento das leis, para torna-las mais eficientes, como a Lei 14.155 de 27 de maio de 2021:

> "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. Pena – reclusão, de 1 (um) a 4 (quatro) anos, e multa. § 2º Aumenta-se a pena de 1/3 (um terço) a 2/3 (dois terços) se da invasão resulta prejuízo econômico. Pena – reclusão, de 2 (dois) a 5 (cinco) anos, e multa. Tornando a Lei de violação de dispositivo informático mais dura em suas penalidades e a definição de crime a fraude eletrônica e a de estelionato: Fraude eletrônica § 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. Estelionato contra idoso ou vulnerável § 4º A pena aumenta-se de 1/3 (um terço) ao dobro, se o crime é cometido contra idoso ou vulnerável, considerada a relevância do resultado gravoso.

Sabendo que um país pode sofrer ataques vindo de outros países, o Brasil participa e aceita o tratado internacional das leis de segurança europeia, o que faz com que mesmo ataques vindos de fora de nossa nação seja investigado com a ajuda internacional, bem como qualquer crime feito no Brasil direcionado a outro país também será passível de ser recriminado.

6 CONSIDERAÇÕES FINAIS

Conhecer os crimes, como é praticado e como se caracteriza é dever de todos nós, para repassarmos para os pais, avós, tios e pessoas menos instruídas para evitarmos que nossos parentes e conhecidos caiam em ataques ou crimes cibernéticos.

Com a expansão das atividades ilícitas no mundo digital e a repercussão de diversos casos de violações chegaram as primeiras leis com o intuito de punir, informar e coibir a prática desses atos, algumas delas trazendo mais poder e controle ao cidadão sobre seus dados digitais junto com a responsabilidade das empresas detentoras dos dados em caso de violações.

A modernidade deixou o homem cansado, querendo que a tecnologia faça tudo por ele e é muito importante limitar o acesso facilitado, como não salvando senhas automaticamente em seu celular e sem autentificar seu dispositivo, deixando-o vulnerável ou ao menos com a facilidade de sua carteira já estar aberta e, vale lembrar, que você não precisa ter medo apenas se tiver dinheiro na carteira digital, os crimes de invasão não são apenas para ganhos financeiros ou ganhos instantâneos. O golpe do empréstimo na conta corrente não acontece apenas com idosos aposentados, ocorre com quem está vulnerável.

Ter um antivírus, fazer a varredura constantemente em seu celular ou computador e evitar conteúdos duvidosos é essencial para vivermos no mundo pós-moderno. Afinal, o analfabetismo existe, para combater é necessário um maior trabalho de conscientização para os usuários pois o crime nunca vai deixar de existir, mas podemos evitá-lo seguindo boas práticas no mundo digital porem ainda é necessária uma punição mais rigorosa para os crimes mais frequentes.

REFERENCIAS

BORGES, Fabiani. **Terrorismo Cibernético e a Proteção de Dados Pessoais**. Disponível em:<https://fabianiborges.jusbrasil.com.br/artigos/218335957/terrorismocibernetico-e-a-protecao-de-dados-pessoais>. Acesso em 15 ago. 2022.

BRANDÃO, Junito de Souza. Mitologia Grega I. Rio de Janeiro: Petrópolis: Editora Vozes, 1991, p.184.

BRANDÃO, Junito de Souza. Mitologia Grega- Volume I. Rio de Janeiro, Petrópolis. Editora Vozes, 1986

BRASIL. **Constituição (1988).** Constituição da República Federativa do Brasil. Brasília: Senado, 1988.

CANAL TECH. **Governo Brasileiro sofre novo ataque de ransomware**. 2020. Disponível em: https://canaltech.com.br/seguranca/governo-brasileiro-sofre-novo-ataque-de-ransomware-224259/ Acesso em 19 set. 2022

CARREIRAS, Helena *et al.* **Cibersegurança e ciberdefesa em tempos de pandemia**. IDN Brief, 2020. Disponível em: https://comum.rcaap.pt/handle/10400.26/33350

CASSANTI, Moisés de Oliveira. **Crimes virtuais, vitimais reais**. Rio de Janeiro: BRASPORT, 2014.

COMITÊ GESTOR DA INTERNET NO BRASIL. **Cartilha de Segurança para Internet**. São Paulo, 2ª ed., 2012.

CONVERGÊNCIA DIGITAL. **Governo é o alvo preferido dos ataques ransomware no Brasil**. 2020. Disponível em: https://www.convergenciadigital.com.br/Seguranca/Governo-e-o-alvo-preferido-dos-ataques-ransomware-no-Brasil-61348.html Acesso em 19 set.2022

DURAN, Laís Baptista Toledo; BARBOSA, Laryssa Vicente Kretchetoff. **Lei Carolina Dieckmann: Atualização Jurídico-Normativa Brasileira.** 2015. Disponível em: http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/viewFile/5038/4800 Acesso em 30 ago. 2022

EL PESCADOR. **Phishing & Engenharia Social: Entenda por que essas técnicas estão interligadas.** 2015. Disponível em: https://www.elpescador.com.br/blog/index.php/phishingengenharia-social-entenda-porque-essas-tecnicas-estao-interligadas/. Acesso em: 22 ago. 2022

FOLHA UOL. **Sequestro de dados de empresas vira joia do cibercrime na pandemia**. 2021. Disponível em: https://www1.folha.uol.com.br/mercado/2021/06/sequestro-de-dados-de-empresas-vira-joia-do-cibercrime-na-pandemia.shtml Acesso em: 20 set. 2022

FRANÇA, Marcelo Luiz de. **Teda-Guardian: detectando ataques DDOs em provedores de internet.** 2020. 71f. Dissertação. Universidade Federal do Rio Grande do Norte. Instituto Metrópole Digital, Programa de Pós-Graduação em tecnologia da informação. Natal, RN, 2021. Disponível em: https://repositorio.ufrn.br/handle/123456789/31792. Acesso em: 18 ago. 2022

INFRA NEWS. **Panorama de ameaças cibernéticas no Brasil**, 2020. Disponível em: https://infranewstelecom.com.br/brasil-teve-mais-84-bilhoes-de-tentativas-de-ataques-ciberneticos-em-2020/ Acesso em 15 ago. 2022

JORNAL OPÇÃO. **Incidentes reportados a CERT.Br- Janeiro a Dezembro de 2020**. Disponível em: https://www.jornalopcao.com.br/ultimas-noticias/aumento-do-uso-da-internet-faz-crescer-o-numero-de-crimes-ciberneticos-374687/ Acesso em 12 ago. 2022

JORNAL CONTÁBIL. **Veja como se proteger dos sites falsos da Receita Federal.** Disponível em: https://www.jornalcontabil.com.br/veja-como-se-proteger-dos-sites-falsos-da-receita-federal/ Acesso em 22 ago.2022

LEITE, Bruno Pacheco Coelho. **Gestão de coleções especiais e livros raros no Brasil: Um estudo sobre engenharia social**, 2017. Disponível em: https://repositorio.febab.org.br/items/show/2871. Acesso em: 21 ago. 2022

LLINARES, Fernando Miró. **El cibercrimen: Fenomenología y criminología de la delincuencia en el ciberespacio.** Buenos Aires, Marcial Pons, 2012.

LEMOS, André. **A comunicação das coisas: teoria ator-rede e cibercultura.** SP: Annablume, 2013.

LEVY, Pierre. **Cibercultura**. São Paulo. Editora 34, 1999.

MALHOTRA, N. **Pesquisa de marketing**. 3.ed. Porto Alegre: Bookman, 2001

MATOS, Odirley Pinheiro de. **Um estudo sobre ataques de Phishing e suas medidas de contenção**, 2017. Disponível em: https://bdm.ufpa.br:8443/jspui/bitstream/prefix/3001/1/TCC_EstudoAtaquesPhishing.pdf Acesso em 30 ago. 2022

MONTEIRO, Silvana Drumond. O ciberespaço: o termo, a definição e o conceito. DataGramaZero - **Revista de Ciência da Informação**, v. 8, n. 3, p. 1-21, 2007. Disponível em: https://www.periodicos.ufpb.br/index.php/pbcib/article/view/6989/0. Acesso em 30 jul. 2022

PINHEIRO, Patrícia Peck. **Direito digital**. 4ª ed. São Paulo: Saraiva, 2010.

QUEIROZ, André. A atual lacuna legislativa frente aos crimes virtuais. Revista jurídica Unifox. Foz do Iguaçu, v.3, n.1, p. 169-178, jul./dez. 2008.

RODRIGUES, Adriano. **Comunicação e Cultura: A Experiência Cultural na era da Informação.** Lisboa: Editorial Presença,1994.

SALDAN, Eliane. **Os desafios jurídicos da guerra no espaço cibernético**. Brasília, 2012. 118 f. Dissertação de Mestrado. Instituto Brasiliense de Direito Público. Disponível em: https://repositorio.idp.edu.br/handle/123456789/1223 Acesso em 30 ago. 2022

SANTOS, Milton. **Por uma outra globalização**: do pensamento único à consciência universal. 5ª ed. Rio de Janeiro: Record, 2001.

SILVA, Fernanda Viero da; FORNASIER, Mateus de Oliveira; KNEBEL, Norberto Milton Paiva. Deep Web e Dark Web: implicações sociais e repercussões jurídicas. **REDES.** Canoas, v.8, n.2, ago. 2020, p.227-244. Disponível em: https://revistas.unilasalle.edu.br/index.php/redes/article/download/6756/pdf. Acesso em 10 set. 2022

SOARES, Orlando. **Criminologia.** Imprenta: Rio de Janeiro, Freitas Bastos,1986, p.69

SIQUEIRA, Erick. Palestra **“Crimes Cibernéticos: Fraudes Bancárias eletrônicas e o financiamento de organizações criminosas”.** Canal TV Decision. Disponível em: youtube.com/watch?v=NJFFXtEg0WE&t=1289s. Acesso em: 18 ago. 2022

STIVIANI, Mirella. **O que é worm? Entenda o malware que se multiplica sozinho**. Portal Tech Tudo, 2018. Disponível em: https:// www.techtudo.com.br/noticias/2018/11/o-que-e-um-worm-entenda-o-malware-que-se-multiplica-sozinho.ghtml. Acesso em 25 ago. 2022

SYDOW, Spencer Toth. **Delitos informáticos próprios: uma abordagem sob a perspectiva vitimodogmática**. 2009. Dissertação (Mestrado). 282 f. Universidade São Paulo, Departamento de Direito Penal, São Paulo, 2009. Disponível em: https://www.teses.usp.br/teses/disponiveis/2/2136/tde-15062011-161113/publico/Dissertacao_Mestrado_versao_final_formatada_padroes_US.pdf Acesso 12 set. 2022.

SYDOW, Spencer Toth. **Delitos informáticos e suas vítimas.** 2. ed. São Paulo: Saraiva, 2014.

URUPÁ, Marcos. Teletime. **Brasil é o país da América do Sul que mais sofre com roubo de dados, aposta estudo**. Disponível em: https://teletime.com.br/08/02/2022/brasil-e-o-pais-da-america-do-sul-que-mais-sofre-com-roubos-de-dados-aponta-estudo/ Acesso 18 set. 2022

VESICA, Fabrizio. **Desvendando o universo H4CK3R**. São Paulo: Digerati Books, 2007.

VITAL, Danilo. **OLX não responde por fraude se atuou apenas como página de classificados**. Disponível em: https:// www.conjur.com.br/2022-jul-07/olx-nao-responde-fraude-atuou-pagina-classificados. Acesso em: 21 ago. 2022

WHITRON, Gerald James. **O tempo e na história: concepções de tempo na pré-história aos nossos dias.** Rio de Janeiro, Editora Jorge Zahar, 1999