Crimes Digitais e a Segurança do Usuário

Leonardo Feitosa de Almeida

Faculdade de Computação – Universidade Federal Pará (UFPA)
Castanhal - PA - Brasil

leonardofeitosa638@gmail.com

Abstract. *This paper focuses on presenting the context of digital crimes in Brazil. The existing laws that protect the victims are pointed out, as well as the methods that can be used to prevent the incident of a misdemeanor and the user's accessibility when they have to deal with a possible situation involving a cybercrime.*

Resumo. *Este artigo tem foco em mostrar a respeito do contexto dos crimes digitais no Brasil. São apontadas as leis existentes que amparam as vítimas, assim como os métodos que podem ser utilizados para evitar o acontecimento de um delito e a acessibilidade do usuário ao ter que lidar com uma possível situação envolvendo um crime cibernético.*

Palavras Chaves: Crimes digitais. Usuário. Internet. Vítima.

1. Introdução

Com o crescimento da tecnologia e a internet ficando cada vez mais acessível a um grande número de usuários, os riscos e perigos que esse advento podem oferecer também ganham cada vez mais força. Crimes digitais são ataques feitos por meio de um dispositivo de informática ou um sistema ligado a internet.

Atualmente o tema ainda não é abordado da maneira como deveria para que mais pessoas possam ficar cientes sobre algo tão presente na rotina do ser humano, como é o caso da vulnerabilidade do usuário em um ambiente repleto de informações e serviços. No Brasil, existem leis que amparam as vítimas de crimes cibernéticos, no entanto, o resultado desses delitos na sociedade ainda causam um impacto que demanda uma lei regulamentadora específica para esse tipo de crime.

Levando isso em consideração, neste artigo são discutidos determinados pontos a respeito dos crimes digitais no Brasil, como leis e dados concretos do delito no país, além de demonstrar a importância em se prevenir contra crimes cibernéticos e em como se comportar no mundo virtual para evitar ter que lidar com esse tipo de situação.

1.1. Objetivos

1.1.1. Objetivo Geral

Analisar o contexto dos crimes cibernéticos no Brasil, levando em consideração as leis existentes e a acessibilidade dos usuários com relação as ferramentas disponíveis e os riscos que estas tecnologias podem trazer.

1.1.2. Objetivos Específicos

1- Mostrar os principais crimes cibernéticos cometidos atualmente;

2- Ressaltar as leis de amparo existentes e o marco civil regulatório da internet, assim como a competência jurídica ao tratar desses casos;

3- Salientar sobre a acessibilidade e mostrar ao usuário métodos para evitar ser vítima de um crime digital.

2. Justificativa

Na mesma medida em que a tecnologia ganha mais força e se torna mais presente na vida das pessoas, novos sistemas, sites e aplicativos podem ser disponibilizados por qualquer tipo de usuário, e em alguns casos este usuário age com más intenções para prejudicar outro indivíduo. Ao somar esse cenário com o fato de que grande parte dos usuários inocentes e sem muito conhecimento sobre tecnologia podem ser vítimas de um crime, o resultado é um alto índice de crimes envolvendo o mundo virtual. Este trabalho busca informar a respeito dos crimes cibernéticos, a fim de melhorar o conhecimento dos usuários ao utilizar uma ferramenta digital de forma correta e segura.

3. O que configura um crime digital e as leis existentes

É considerado crime digital qualquer ato previsto na lei que é reconhecido como ilícito usando algum meio de tecnologia, como ataques à sistemas e bancos de dados informatizados, ou quando é feito o uso de ferramentas digitais para outros tipos de crimes mais conhecidos (difamação, pedofilia, golpes, etc.), que podem ser denominados como crimes cibernéticos.

No Brasil, duas leis voltadas para crimes digitais foram sancionadas em 2012 onde o código penal foi alterado e penas foram estabelecidas para os crimes como invasão de computadores, propagação de vírus ou códigos para roubo de senhas de usuários e utilização de cartões de crédito e débito sem que o titular esteja ciente do ato.

A primeira dessas leis é a Lei dos Crimes Cibernéticos (12.737/12), também conhecida como Lei Carolina Dieckmann, que é centrada em tratar de atos como invasão de computadores, violação de dados dos usuários ou promover a “queda” de um site. O texto deste crime já existia antes do caso da atriz em virtude da alta taxa de roubos de senhas e golpes na internet, porém, após o acontecido o crime foi renomeado com seu nome. A segunda lei é a Lei 12.735/12, que foi sancionada para tratar de crimes que fazem uso de sistemas eletrônicos, digitais ou similares para invadir ou atacar sistemas informatizados.

Crimes considerados não tão graves, como invasão de dispositivos informáticos, dispõem de penas com prisão de três meses a um ano de prisão e multa. Já os delitos mais graves perante a lei, como conseguir acesso à informações confidenciais, segredos comerciais e etc, são penalizados com seis meses a dois anos de prisão e multa.

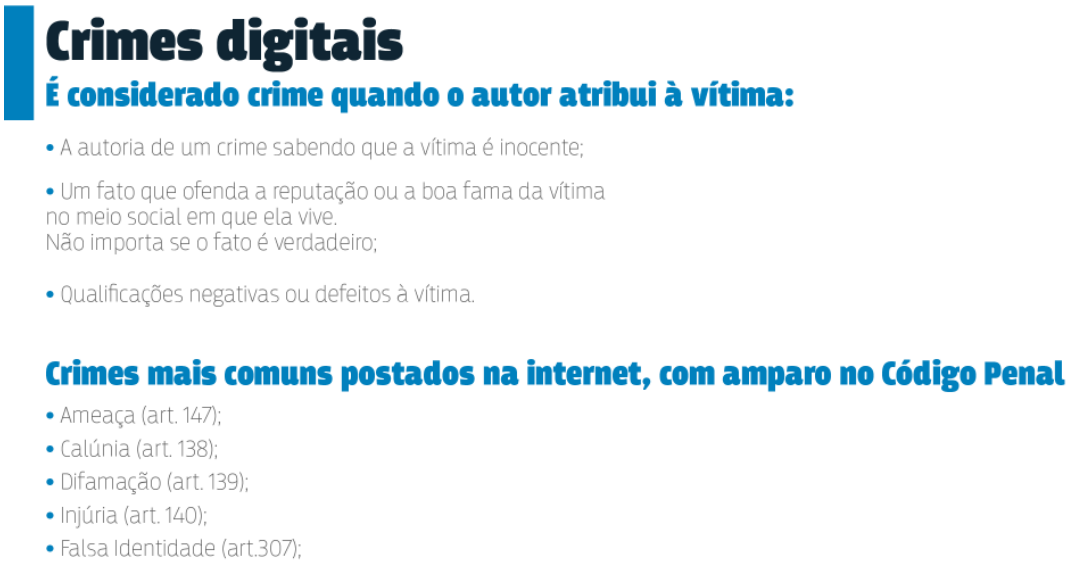

Figura 1. Fonte: Delegacia de Repressão aos Crimes Informáticos (DRCI).

Em 2021 foi sancionada a Lei 14.155/21, uma nova lei mais rigorosa com maiores penas para crimes cibernéticos. Delitos como violação de dispositivo informático, furto e estelionato realizados de maneira eletrônica ou via internet passaram a ser mais graves, onde a pena passou a ser de um a quatro anos de prisão e multa. A pena é a mesma para situações de estelionato onde um determinado usuário é induzido pelo criminoso a disponibilizar informações e dados pessoais como senhas de contas, além do fato de que as penas podem ser aumentadas caso o crime tenha sido praticado em um servidor de outro país, ou se foi realizado contra uma pessoa idosa ou vulnerável.

4. Os crimes mais frequentes

Muitos dos crimes feitos por meio da tecnologia já eram cometidos antes mesmo dos computadores ganharem popularidade na vida do ser humano, e com o surgimento das novas ferramentas, esses delitos começaram a se estender ao mundo virtual. É possível citar como os principais crimes feitos de maneira online os seguintes casos:

- Calúnia - Previsto no artigo 138 do Código Penal onde a pena pode ir de seis a dois anos de reclusão e multa, é o delito em que uma pessoa é apontada como responsável por um crime que não realizou;
- Difamação - Previsto no artigo 139 do Código Penal onde a pena pode ir de três meses a um ano de prisão e multa, é o crime em que um fato que possa prejudicar a reputação ou honra é designado a alguém;
- Injúria - Previsto no artigo 140 do Código Penal onde a pena pode ir de um a seis meses de prisão e multa, é o crime em que a dignidade de uma pessoa possa ser afetada através de insultos, humilhações, xingamentos e etc.;
- Injúria Qualificada - Previsto no parágrafo terceiro do artigo 140 do Código Penal, é considerado um delito mais grave de injúria e a pena pode ir de um a três anos de prisão e multa. Se encaixa como injúria qualificada o ato onde uma pessoa é ofendida por conta de sua raça, cor, etnia, religião e etc.;

- Ameaça - Previsto no artigo 147 do Código Penal onde a pena pode ir de um a seis meses de prisão e multa, é o crime em que há uma ameaça de agressão, seja física ou psicológica voltada à uma pessoa ou alguém conhecido da vítima;
- Falsa Identidade - Previsto no artigo 307 do Código Penal onde a pena pode ir de três meses a um ano de prisão e multa, é o delito em que alguém mente à respeito de sua identidade ou da identidade de outra pessoa para prejudicar um terceiro ou para obter algum tipo de benefício indevido.

Entre os crimes cibernéticos mais cometidos, ainda pode-se destacar que existem dois tipos de crimes, sendo estes os crimes próprios e impróprios. Os crimes próprios são aqueles delitos que demandam de uma prática por meio de algum tipo de dispositivo tecnológico ou é feito contra um sistema, o que seria uma invasão no sistema para ter acesso à informações e dados; já os crimes impróprios são aqueles delitos realizados através de um sistema, mas o computador pode ou não ser utilizado para fazer tal ato.

5. Marco Civil e Competência Jurídica

Sancionado em 2014, o Marco Civil da Internet (Lei 12.965/2014) determina os direitos e deveres dos usuários online, onde dados e informações privadas são protegidos contra atos criminosos. A partir da criação do Marco Civil, informações e dados de qualquer tipo de sistema podem ser acessados por terceiros somente com ordem judicial para fins jurídicos.

Com o Marco Civil sancionado, tornou-se mais prático fazer a remoção de conteúdos da internet, uma vez que até a lei ser aprovada não existia um método mais claro a respeito de como tratar casos do tipo. Após o regimento, um conteúdo é excluído de um ambiente online apenas com ordem judicial, exceto em casos em que a vítima teve sua intimidade violada e tem poder de demandar a remoção do conteúdo ao serviço que armazena esse conteúdo.

A partir do Marco Civil da Internet, foi determinado que os Juizados Especiais passariam a ser encarregados de decidir a respeito se um ato pode ser considerado crime ou não, o que se encaixa nos casos de ofensa e injúria, que terão procedimentos exatamente da mesma maneira como se o crime tivesse sido cometido sem uso de um dispositivo de informática.

O estabelecimento da competência jurídica não está interligado com o local do provedor de acesso ao âmbito da tecnologia, local reconhecido como a esfera onde o crime é realizado, de acordo com o termos do artigo 70 do Código de Processo Penal. Casos de delitos que envolvam violação de privacidade ou de ações que podem afetar bens e interesses de empresas privadas ou públicas ficam como responsabilidade da Justiça Federal de realizar o processo do crime.

Figura 2. Principais direitos dos titulares na LGPD (Lei Geral de Proteção de Dados Pessoais).

6. Acessibilidade e proteção do usuário

Na mesma medida em que a internet é o instrumento utilizado para cometer uma série de crimes, é por meio dela que também é possível se defender dos mais variados tipos de crimes cibernéticos. Atualmente uma série de sites e ferramentas online se encontram disponíveis 24 horas por dia para que a vítima consiga denunciar um caso de forma anônima ou não, além das delegacias físicas especializadas em situações de crimes digitais.

A pessoa que sofreu o crime precisa juntar o máximo possível de informações a respeito do ocorrido e registrar um boletim de ocorrência que é encaminhado a um órgão próprio para tratar do delito. No Brasil, esse tipo de órgão não é encontrado em todos os estados do país, e em circunstâncias assim é necessário que o usuário registre as informações em cartório mediante a uma ata notarial em que esse documento possibilita o uso das informações como evidência em uma possível ação judicial.

Outro meio para denunciar crimes cibernéticos é utilizando o site SaferNet, uma ferramenta com cooperação de empresas como Google Brasil, Facebook, Twitter, Telefônica, Instagram e entre outras que oferece ao usuário a possibilidade de denunciar um crime que lhe ocorreu de maneira online, sem precisar ir até uma delegacia física

6.1. Como evitar ser uma vítima

Diante do vasto campo de ferramentas que é a internet, é preciso que o usuário sempre tenha cautela ao fazer o uso de determinado serviço ou simplesmente fazer uma

publicação em uma rede social. São vários os métodos existentes para evitar ser vítima de um crime cibernético, como por exemplo:

- Manter um uso saudável de suas redes sociais para evitar situações que possam gerar atritos mais sérios com outra pessoa e não compartilhar dados pessoais com um público desconhecido;
- Não compartilhar a imagem de um terceiro desconhecido sem que este tenha dado autorização para tal ato, o que pode se enquadrar no Direito de Imagem e Direito Autoral;
- Jamais colocar senhas e dados em locais que não fazem parte do serviço oficial da empresa ou banco, por mais que o usuário tenha recebido uma solicitação para isso;
- Não repetir senhas em muitos sites e serviços;
- Deixar dispositivos sempre atualizados, assim como os antivírus e firewalls;
- Procurar imediatamente a polícia caso algum crime tenha sido cometido contra o usuário.

7. Ataques cibernéticos na pandemia

Com o surgimento do COVID-19 em 2020, a dependência de uma infraestrutura digital por parte das empresas acabou resultando no crescimento do uso da internet para a realização de atividades feitas dentro de casa, também conhecido como Home Office. Esse novo estilo de trabalho foi visto por criminosos digitais como uma oportunidade para agir de forma maliciosa contra esse grupo de pessoas, principalmente aquelas em situações mais vulneráveis e sem conhecimento necessário para poder se defender desse tipo de ataque.

Segundo um relatório divulgado pela Symantec, já em 2019, antes do início da pandemia, o Brasil era o terceiro país com índice mais alto no ranking de países que mais sofrem ataques cibernéticos, atrás apenas da China e Estados Unidos. No entanto, pouco mais de um ano depois, em 2020, esse tipo de ataque virtual obteve um aumento significativo no cenário brasileiro, onde o Brasil sofreu mais de 3,4 bilhões de tentativas de ataques na internet durante os meses de janeiro e setembro de 2020 de acordo com a Fortinet Threat Intelligence Insider Latin America. Durante janeiro e abril de 2021, a Interpol identificou mais 907 mil spams, 737 mil casos ligados a malwares, e 48 mil links considerados suspeitos.

7.1. Ataques mais frequentes na pandemia

Crimes cibernéticos existem há anos e existem diversos tipos e maneiras de cometer uma infração desse tipo, todavia, com o início da pandemia certos tipos de crimes tornaram-se mais “populares” por serem considerados mais eficientes em afetar as vítimas.

7.1.1. Phishing

Considerada uma das técnicas mais utilizadas entre os crimes digitais, o phishing funciona recolhendo dados de usuários de determinada empresa ou produto. Geralmente

é enviado um e-mail à vítima dizendo que este usuário ganhou algum prêmio junto de um link que vai direcioná-lo a um site para informar os seus dados.

Phishing chega ao usuário de forma que ele não vai exitar em acessar o link e informar todos os seus dados ao criminoso, uma vez que esses e-mails são todos formatados e escritos de maneira que transmita uma confiança ao leitor.

Os ataques de phishing são realizados por meio de uma sequência de ações que colocam aquele usuário no lugar de vítima de um crime desse tipo. A princípio, é feito um planejamento onde é definido como o ataque será operado e quem será a vítima, além de estipular qual o tipo invasão a ser cometida, uma vez que o crime pode ser feito roubando informações bancárias ou dados pessoais do usuário, por exemplo. O próximo passo é escolher o meio utilizado para afetar a vítima: envio de e-mail, arquivos em anexo, sites e links maliciosos e etc; logo após é realizado o ataque usando um dos métodos citados anteriormente; então é feita um apanhado de todas as informações roubadas para definir o que será feito com esses dados; e por fim os criminosos realizam a última etapa, apagando todos os rastros que possam ter sido deixados para trás e serem usados como prova.

O phishing pode ser praticado em diversos casos, sendo alguns deles:

- **Blind phishing:** onde o criminoso consegue passar a falsa impressão que uma empresa ou pessoa está entrando em contato com o usuário e faz ele passar seus dados pessoais;
- **Spear phishing:** é quando o golpe está direcionado a uma pessoa específica que possui dados e informações expostos em redes sociais ;
- **Whaling:** golpe semelhante ao spear phishing, no entanto, o que difere um do outro é que o whaling foca em atingir pessoas específicas com alto poder aquisitivo, onde o ataque é realizado por meio de intimações judiciais ou notificações da empresa;
- **Pharming:** é o tipo de ataque onde os criminosos encontram mais trabalho para colocar em prática, uma vez que ele visa invadir o sistema DNS dos servidores da empresa mudando o encaminhamento do servidor em que estão hospedadas as URLs. A partir do momento que o ataque foi bem sucedido, ao tentar acessar o site a princípio confiável, o usuário é redirecionado para o site feito pelos criminosos.

7.1.2. Golpe do cartão de crédito ou boleto bancário

Esse tipo de golpe é realizado na maioria dos casos por meio de um software malicioso que atinge as máquinas e rouba dados como senhas bancárias ou até mesmo do cartão. Já nos casos de golpe por meio de boletos bancários, o ataque é feito criando um documento aparentemente confiável da compra de um e-commerce ou da compra de algum produto que o usuário fez na internet, onde o código de barras do boleto é modificado e o valor pago acaba indo para a conta criada pelo criminoso.

Ainda nos primeiros passos para cometer o delito, os criminosos coletam informações pessoais como número do CPF, nome completo, telefone e endereço,

deixando a vítima com a sensação de confiabilidade para seguir as próximas etapas do que seria um pagamento de uma dívida atrasada em alguma loja ou banco. O pagamento, que seria para pagar a suposta dívida, acaba sendo depositado nas contas dos criminosos.

Sendo um golpe com um campo de operação bastante vasto, a quantidade de usuários com chances de se tornarem vítimas é muito alta. Para evitar sofrer com esse tipo de situação, os bancos recomendam que o cliente sempre verifique as informações do beneficiário no boleto para ter certeza do destino do pagamento, além de checar número de CPF ou CNPJ, assim como data de vencimento e o valor da cobrança de fato. É válido se atentar no código do boleto, verificando se os três primeiros dígitos estão de acordo com o código do banco emissor, sendo possível fazer essa busca no site Busca Banco, da Febraban.

7.1.3. Mobile Malware

O mobile malware é um tipo de vírus criado por hackers que infecta celulares e computadores com o objetivo de ter acesso e roubar todas as informações sigilosas do usuário, como dados e senhas de banco. A seguir, alguns dos tipos mais comuns:

- **Ferramentas de Acesso Remoto (RATs):** onde os criminosos possuem acesso amplo aos dados de dispositivos infectados dos usuários e há uma coleta dessas informações de maneira frequente. Por meio da técnica dos RATs, os criminosos conseguem ter acesso a aplicativos instalados, histórico de chamadas, endereços, histórico de navegação e dados de mensagens de texto, além de ter o poder de enviar sms, controlar câmeras dos dispositivos e registrar dados de GPS.
- **Bank Trojans:** também conhecido como cavalo de tróia envolvendo sistemas bancários em que aplicações semelhantes às originais chegam ao acesso da vítima, deixando esse usuário sob o risco de ter seus dados de login e senha roubados.
- **Ransomware:** é o tipo de malware que invade o dispositivo da vítima e exige um pagamento em troca do resgate do sistema, geralmente utilizando bitcoins onde não é possível rastrear o recebedor. Uma vez que o pagamento do resgate foi feito, os criminosos liberam códigos de acesso para que o usuário tenha acesso ao dispositivo novamente.
- **Cryptominig Malware:** nesse tipo de malware os invasores conseguem executar cálculos no dispositivo da vítima, fazendo o dispositivo criar criptomoedas. Na maioria dos casos, essa mineração de criptomoedas é feita por meio de códigos de cavalo de Troia escondidos em aplicações aparentemente legítimas.
- **Cliques em anúncios falsos:** onde o malware age por meio de cliques em anúncios falsos, permitindo que o invasor tenha acesso ao dispositivo e gere dinheiro com cliques em propagandas não legítimas.

Os métodos de distribuição de um vírus do tipo mobile malware em grande parte dos casos se dá devido ao fato de que é muito comum, principalmente no período pós-pandemia, funcionários usarem seus dispositivos pessoais para trabalhar. Sendo assim, os criminosos encontram nessas situações uma ótima oportunidade de invadir o aparelho e obter acesso aos dados da empresa, uma vez que apenas uma brecha é

suficiente para comprometer todo um sistema e gerar uma perda significativa de dados para a organização.

Entre alguns dos métodos utilizados pelos criminosos para distribuir o código malicioso, o Mobile Phishing and Spoofing (falsificação) é um dos mais comuns. Nesse tipo de ataque o usuário é levado a acreditar que está repassando seus dados e informações para uma fonte confiável, quando na verdade está sendo vítima de um golpe que leva esses dados para fazer uso indevido. Diferente do phishing, o spoofing além de conseguir obter informações também é capaz de ir além nos ataques, como por exemplo, induzir o usuário a clicar em um link malicioso armazenado dentro de um e-mail aparentemente confiável. Outro método comumente usado para distribuir códigos maliciosos se chama Jailbroken/Rooted Devices, onde o próprio dono do dispositivo "burla" as regras do sistema operacional ao não respeitar as proteções internas do aparelho para baixar aplicativos de terceiros não aprovados pelo sistema operacional ou para fazer modificações na aparência do software do telefone que não são permitidas pela proteção padrão.

8. Resultados

A partir das informações obtidas, é possível destacar que os crimes digitais crescem na mesma medida em que a internet ganha mais força na rotina do ser humano. O tempo todo o usuário está suscetível a ser vítima ou de praticar um delito virtual, seja qual for o contexto em que ele está inserido.

De acordo com dados da Central Nacional de Denúncias de Crimes Cibernéticos, em 2020, o número de denúncias anônimas de crimes cometidos na internet teve um crescimento mais do que dobrado com relação a 2019, onde de janeiro a dezembro foram 156.692 denúncias anônimas, enquanto no ano anterior foram apenas 75.428. Os tipos de denúncias variam de um para o outro, porém, o caso com mais frequência é o de pornografia infantil, sendo 98.244 no ano de 2020 e 48.576 no ano de 2019.

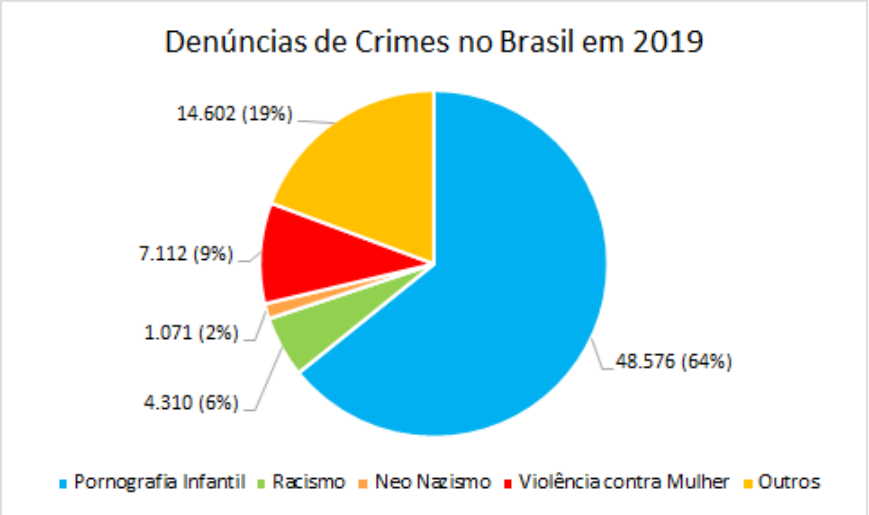

Figura 3. Denúncias anônimas de crimes cibernéticos registradas em 2019.

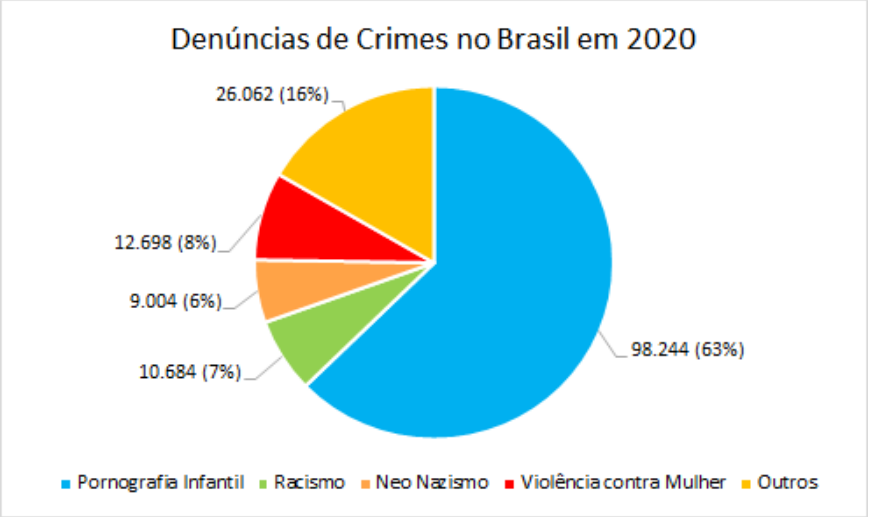

Figura 4. Denúncias anônimas de crimes cibernéticos registradas em 2020.

Ainda na mesma pesquisa, foi constatado que entre os maiores crescimentos de percentual nos crimes cibernéticos, se destacam os crimes de neonazismo, que tiveram um aumento de 740% em 2020, e os crimes de racismo, que tiveram um aumento de 147,8%. Já os crimes de violência ou discriminação contra a mulher tiveram uma taxa de 78,5% maior com relação ao ano anterior. De acordo com Thiago Tavares, diretor-presidente da SaferNet Brasil "As vítimas são crianças e adolescentes, mas também jovens e pessoas idosas que estão expostas a todo tipo de golpe, principalmente, utilizando dados pessoais e violação de senhas e outros tipos de invasões que tenham acontecido tanto em celulares, como em computadores".

9. Conclusão

Com o estudo em questão, é possível analisar que o cenário dos crimes digitais no Brasil cada vez mais vem tomando maiores proporções, afetando a experiência e até mesmo a vida pessoal das vítimas desse tipo de crime. O usuário que sofrer com um delito pode procurar meios para realizar denúncias anônimas e acompanhar o andamento do caso através de ferramentas virtuais disponibilizadas para esse tipo de situação. Com o crescimento dos crimes digitais, as leis também passaram a ser mais rigorosas, o que pode ser considerado como um avanço no combate a essas infrações.

Referências

CNJ. (2018). Crimes digitais: o que são, como denunciar e quais leis tipificam como crime?. Disponível em: <https://www.cnj.jus.br/crimes-digitais-o-que-sao-como-denunciar-e-quais-leis-tipificam-como-crime/>. Acesso em: 14 mai. 2021.

Guia do Estudante. (2020). Crime digital: o que é e como se proteger. Disponível em:<https://guiadoestudante.abril.com.br/atualidades/crime-digital-o-que-e-e-como-se-proteger/>. Acesso em: 14 mai. 2021.

Sindicomércio. (2021). Lei que endurece penas para crimes cibernéticos é sancionada. Disponível em: <https://sindicatodocomercio.org.br/noticias/lei-que-endurece-penas-para-crimes-cib

erneticos-e-sancionada>. Acesso em: 4 jun. 2021.

Justificando. (2018) Crimes digitais: quais são, quais leis os definem e como denunciar. Disponível em: <https://www.justificando.com/2018/06/25/crimes-digitais-quais-sao-quais-leis-os-definem-e-como-denunciar/>. Acesso em: 16 mai. 2021.

G1. (2021) Denúncias de crimes cometidos pela internet mais que dobram em 2020. Disponível em: <https://g1.globo.com/economia/tecnologia/noticia/2021/02/09/numero-de-denuncias-de-crimes-cometidos-pela-internet-mais-que-dobra-em-2020.ghtml>. Acesso em: 18 mai. 2021.

Crypto ID. (2021). Crescimento de crimes cibernéticos na pandemia. Disponível em: <https://cryptoid.com.br/identidade-digital-destaques/crescimento-de-crimes-ciberneticos-na-pandemia-como-nao-ser-uma-vitima/>. Acesso em: 16 ago. 2021.

NAGLI, L. S. D. (2020). PANDEMIA NA PANDEMIA: A ESCALADA DE ATAQUES CIBERNÉTICOS PÓS COVID-19. Disponível em: <http://bibliotecadigital.fgv.br/ocs/index.php/ctd/ctd2020/paper/viewFile/7614/2308>. Acesso em: 16 ago. 2021.

Neoway. (2020) Phishing: O que é, quais os principais tipos e como detectar . Disponível em: <https://blog.neoway.com.br/phishing/>. Acesso em: 14 set. 2022.

CrowdStrike. (2022) What is mobile malware?. Disponível em: <https://www.crowdstrike.com/cybersecurity-101/malware/mobile-malware/>. Acesso em: 15 set. 2022.

Correio Braziliense. (2022) Golpe do ‘boleto adulterado’: saiba como identificar e se prevenir. Disponível em: <https://www.correiobraziliense.com.br/brasil/2022/06/5012371-golpe-do-boleto-adulterado-saiba-como-identificar-e-se-prevenir.html>. Acesso em: 15 set. 2022.

Olhar Digital. (2021) Novo golpe do boleto: Procon-SP cobra explicações a Nubank, Itaú, Febraban e outros. Disponível em: <https://olhardigital.com.br/2021/09/07/seguranca/novo-golpe-do-boleto-procon-sp-cobra-explicacoes-a-nubank-itau-febraban-e-outros/>. Acesso em: 15 set. 2022.

CRUZ, D. e RODRIGUES, J. (2018). CRIMES CIBERNÉTICOS E A FALSA SENSAÇÃO DE IMPUNIDADE. Disponível em: <http://faef.revista.inf.br/imagens_arquivos/arquivos_destaque/iegWxiOtVJB1t5C_2019-2-28-16-36-0.pdf>. Acesso em: 05 out. 2022.

ORRIGO, G. M. A. e FILGUEIRA, M. H. B. (2015). CRIMES CIBERNÉTICOS: UMA ABORDAGEM JURÍDICA SOBRE OS CRIMES REALIZADOS NO ÂMBITO VIRTUAL. Disponível em: <http://intertemas.toledoprudente.edu.br/index.php/ETIC/article/view/5000/4854>. Acesso em: 05 out. 2022.