FACULDADES SÃO JOSÉ
CURSO DE DIREITO

BRUNO DA SILVA PATO E JEFFERSON LUIZ DE SOUZA VIANNA

PROFESSOR-ORIENTADOR: GLÁUCIO CASTELO BRANCO

CRIMES VIRTUAIS

Rio de Janeiro

2018

CRIMES VIRTUAIS

VIRTUAL CRIMES

BRUNO DA SILVA PATO E JEFFERSON LUIZ DE SOUZA VIANNA
Professor orientado: Gláucio Castelo Branco

RESUMO

Os objetivos do trabalho são mostrar a evolução histórica desde o surgimento dos crimes virtuais e analisar os seus conceitos, juntamente com os novos institutos do Direito digital. Tendo como objetivo geral buscar verificar as formas de se analisar um crime virtual, a busca de sua autoria, suas peculiaridades e sua evolução histórica. O presente artigo visa estudar os principais crimes que são cometidos via internet e mostrar a importância de que estes tenham tipificação legal específica, pois a falta dela que é encontrada hodiernamente no ordenamento jurídico brasileiro faz-se gerar uma lacuna legislativa que encoraja a continuidade da prática delitiva, tornando assim difícil a punição daqueles que se aproveitam dessa falta de previsão legal.

Palavras-chave: crimes, conceito, digital.

ABSTRACT

The objectives of the work are to show the historical evolution since the emergence of virtual crimes and analyze their concepts, along with the new institutes of digital law. Its main objective is to verify the ways of analyzing a virtual crime, the search for its authorship, its peculiarities and its historical evolution. This article aims to study the main crimes that are committed via the Internet and show the importance of having specific legal classification, since the lack of it that is currently found in the Brazilian legal system creates a legislative gap that encourages the continuity of practice delirium, thus making it difficult to punish those who take advantage of this lack of legal foresight.

Key-words: Crime, Concept, Digital.

INTRODUÇÃO:

Nos dias de hoje, o mundo é considerado predominantemente digital. Não há mais como negar que a Internet faz parte essencial do dia a dia da sociedade, no entanto, não obstante todos os seus benefícios, há também, como custo, a prática crescente de ilícitos no meio digital.

Além do aumento do número de usuários, outro ponto que influi para a grande quantidade de crimes praticados na Internet, é a sensação de impunidade

que ainda existe. Tal sensação ocorre, uma vez que, devido à ausência de legislação adequada, a determinação da autoria, a competência de julgamento, as provas, as perícias e até mesmo a execução das penas, se mostram prejudicadas e ineficientes.

Com essas novas relações sociais que passaram a surgir nesta era digital, entre várias culturas diferentes é que o Direito deve se moldar e se adequar a nova realidade devendo caminhar junto com os avanços dessas tecnologias para que desta forma não deixe a sociedade digital à mercê da criminalidade.

Diante da relevância desse tema, o presente trabalho compromete-se com a análise desse dinâmico ramo do Direito, denominado Direito Digital, e suas repercussões no Direito Penal e Processual Penal Brasileiro.

Portanto, este trabalho foi elaborado para tentar buscar responder as grandes problemáticas, a saber:

“- Quais os principais crimes praticados na internet?;

- Como o ordenamento jurídico pátrio e o de outros países tratam sobre os crimes perpetuados na internet?;

- O que já vem sendo feito no nosso ordenamento jurídico par abranger os crimes virtuais?”

2. DOS CRIMES VIRTUAIS

2.1 Conceito

Os crimes virtuais são, assim como os crimes comuns, condutas típicas, antijurídicas e culpáveis, porém praticadas contra ou com a utilização dos sistemas da informática.

Para a ONU, “crime de computador é qualquer comportamento ilegal,

aético, ou não autorizado envolvendo processamento automático de dados e, ou transmissão de dados".

Nos dias atuais, a conceituação permanece a mesma. Segundo o qual, delito eletrônico, em sentido amplo, deve ser entendido como qualquer conduta criminógena ou criminal cuja realização haja o emprego da tecnologia como método, meio ou fim, e, em um sentido estrito, qualquer ato ilícito penal em que os computadores, suas técnicas e funções desempenham um papel como método, meio e fim.

2.2 Classificação

Embora existam as divergências doutrinárias quanto à classificação dos crimes virtuais, o presente trabalho adotará a sistematização defendida por Ivette Senise Ferreira e Vicente Greco Filho, que divide os crimes digitais em crimes próprios e impróprios, por ser menos complexa que as demais existentes na doutrina, todavia, mais plausível de ser adotada dada sua particular popularidade acadêmica e social. Vicente Greco Filho assim o explica:

> *"Focalizando-se a Internet, há dois pontos de vista a considerar: crimes ou ações que merecem incriminação praticados por meio da Internet e crimes ou ações que merecem incriminação praticados contra a Internet, enquanto bem jurídico autônomo. Quanto ao primeiro, cabe observar que os tipos penais, no que concerne à sua estrutura, podem ser crimes de resultado de conduta livre, crimes de resultado de conduta vinculada, crimes de mera conduta ou formais (sem querer discutir se existe distinção entre estes) e crimes de conduta com fim*

> *específico, sem prejuízo da inclusão eventual de elementos normativos. Nos crimes de resultado de conduta livre, à lei importa apenas o evento modificador da natureza, com, por exemplo, o homicídio. O crime, no caso, é provocador o resultado morte, qualquer que tenha sido o meio ou a ação que o causou.*

Há de se ressaltar ainda que, segundo Ivette Senise Ferreira, sistema de informática ou o computador é um instrumento como tantos outros, tal qual armas de fogo, explosivos, etc., utilizados por criminosos para facilitar o cometimento de um delito. Cabe ao Estado tutelar as novas modalidades e lesões aos diversos bens e interesses que surgiram com a crescente informatização das atividades individuais e coletivas desenvolvidas na sociedade.

Essa informatização colocou novos instrumentos e meios nas mãos dos criminosos e propiciou a formação de uma nova criminalidade específica da informática cujo alcance ainda não foi corretamente avaliado.

2.3 – OS CRIMES MAIS PRATICADOS NA INTERNET

As redes sociais, tendo como base um meio comum e acessível a todos, contam com milhares de usuários em todo o planeta. Há também quem não faz uso das famosas redes, porém, acessa a internet para outros serviços, como transações bancárias, compras online, entre outros.

Duas leis que tipificam os crimes na internet foram sancionadas em 2012, alterando o Código Penal e instituindo penas para crimes como invasão de computadores, disseminação de vírus ou códigos para roubo de senhas, o uso de

dados de cartões de crédito e de débito sem autorização do titular.

A primeira delas é a Lei dos Crimes Cibernéticos (12.737/2012), conhecida como Lei Carolina Dieckmann, que tipifica atos como invadir computadores, violar dados de usuários ou "derrubar" sites. Apesar de ganhar espaço na mídia com o caso da atriz, o texto já era reivindicado pelo sistema financeiro diante do grande volume de golpes e roubos de senhas pela internet.

Os crimes menos graves, como “invasão de dispositivo informático”, podem ser punidos com prisão de três meses a um ano e multa. Condutas mais danosas, como obter, pela invasão, conteúdo de “comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas” podem ter pena de seis meses a dois anos de prisão, além de multa.

O mesmo ocorre se o delito envolver a divulgação, comercialização ou transmissão a terceiros, por meio de venda ou repasse gratuito, do material obtido com a invasão da privacidade. Nesse caso, a pena poderá ser aumentada em um a dois terços. Já a Lei 12.735/12 tipifica condutas realizadas mediante uso de sistema eletrônico, digitais ou similares que sejam praticadas contra sistemas informatizados. Essa é a lei que determina a instalação de delegacias especializadas.

Sendo assim, fica evidenciada com mais clareza a prática de tais delitos, onde os mais comuns e cometidos com mais freqüência são a ameaça *(art. 147)*, a calúnia *(art.138)*, a difamação *(art. 139)*, a injúria *(art. 140)* e o crime de falsa identidade *(art.307),* todos do Código Penal Brasileiro.

2.4 MARCO CIVIL

O Marco Civil da Internet (Lei 12.965/2014) foi sancionado em 2014 e regula os direitos e deveres dos internautas. Ele protege os dados pessoais e a privacidade dos usuários.

Até o ano 2012, não existia nenhuma lei para punir os crimes cibernéticos próprios, existindo somente legislação acerca dos crimes cibernéticos impróprios. Contudo, em decorrência de alguns episódios, como os DDoS - *Distributed Denial of Service* (ataques distribuídos de negação de serviço) a sites do governo e a divulgação de fotos íntimas da atriz Carolina Dieckmann, duas leis foram sancionadas com maior urgência, sanando algumas das várias deficiências existentes no ordenamento em relação a essa matéria, quais sejam, a Lei 12.735/201215, conhecida popularmente como “Lei Azeredo”, e a Lei 12.737/201216, conhecida como “Lei Carolina Dieckmann”.

Em 2014, foi sancionada pela ex-presidente Dilma Rousseff, a Lei 12.965/2014, oficialmente chamada de Marco Civil da Internet17, que por sua vez, regula a mesma no Brasil estabelecendo princípios, garantias, direitos e deveres para o seu uso, para os usuários e também para o próprio Estado. Além dessas legislações supracitadas, que serão tratadas de forma mais abundante, ainda tem-se a Lei nº 11.829/2008, que combate a pornografia infantil na internet; a Lei nº 9.609/1998, que trata da proteção da propriedade intelectual do programa de computador; a Lei nº 9.983/2000, que tipificou os crimes relacionados ao acesso indevido a sistemas informatizados da Administração Pública; a Lei nº 9.296/1996 disciplinou a interceptação de comunicação telemática ou informática; e a Lei nº 12.034/2009, que delimita os direitos e deveres dentro da rede mundial, durante as campanhas eleitorais.

Desta forma, somente mediante ordem judicial pode haver quebra de dados e informações particulares existentes em sites ou redes sociais.

Uma das grandes inovações diz respeito a retirada de conteúdos do ar. Antes de sua entrada em vigor, não havia uma regra clara sobre este procedimento. A partir de então, a retirada de conteúdos do ar só será feita mediante ordem judicial, com exceção dos casos de “pornografia de vingança”.

Pessoas vítimas de violações da intimidade podem solicitar a retirada de

conteúdo, de forma direta, aos sites ou serviços que hospedem este conteúdo.

2.5 DA COMPETÊNCIA JURÍDICA

O Marco Civil da Internet também determinou que os Juizados Especiais são os responsáveis pela decisão sobre a ilegalidade ou não dos conteúdos. Isto se aplica aos casos de ofensa à honra ou injúria, que serão tratados da mesma forma como ocorre fora da rede mundial de computadores.

A fixação da competência independe do local do provedor de acesso ao mundo virtual, sendo considerado o lugar da consumação do delito, nos termos do artigo 70 do Código de Processo Penal. Já nos casos de crimes como violação de privacidade ou atos que atinjam bens, interesse ou serviço da União ou de suas empresas autárquicas ou públicas, a competência é da Justiça Federal, assim como crimes previstos em convenções internacionais (tráfico, tortura, moeda falsa e outros).

2.6 DAS PREVENÇÕES PARA EVITAR TAIS DELITOS

Dois em cada três internautas já foram vítimas de crimes virtuais no mundo. O dado é do relatório de *cibercrime* de 2018 da Norton, linha de antivírus da empresa de soluções de segurança virtual Symantec. De acordo com o levantamento, o custo do *cibercrime* é estimado em R$ 220 bilhões e atinge cerca de 556 milhões de pessoas todos os anos. E o Brasil está no topo dessa lista, com um prejuízo anual estimado em R$ 16 bilhões.

Desde seu surgimento, os vírus de computador evoluíram. “Com a

popularização dos *smartphones* e do comércio eletrônico, novas ameaças ganharam espaço entre os internautas", afirma Gerson Rolim, presidente da Câmara Brasileira de Comércio Eletrônico. Dois terços dos usuários não usam dispositivo de segurança, o que os expõe a vírus ou a programas mal-intencionados também conhecidos como *malware*.

Boas práticas podem reduzir significativamente os ataques virtuais, porém, a maioria dos usuários da rede mundial de computadores se descuida e facilita o acesso dos *hackers.* Dentre outras práticas, vale ressaltar a importância da certificação de que há um programa de proteção instalado, assim como a cautela ao realizar transações bancárias através de *smartphones* ou em conexões sem segurança, manter atualizados os aplicativos existentes no computador, etc.

CONSIDERAÇÕES FINAIS

As novas tecnologias da informação, especialmente a Internet, impulsionaram (e continuam impulsionando) o processo de globalização econômica e cultural. Essas mudanças trouxeram novos paradigmas para a sociedade pós-moderna e os sistemas que a organizam e regulam, como o Direito.

Novas modalidades criminosas surgiram, uma vez que o ambiente virtual alimenta no ser humano a sensação de liberdade ao separar as pessoas por uma interface e proporcionar o anonimato.

Assim, a partir das observações efetuadas ao longo deste trabalho, constatou-se que a criminalidade informática não foi responsável somente pelo aparecimento de novas condutas ilícitas praticadas com o auxílio de um computador, mas também possibilitou a violação de bens jurídicos até então não atingidos com a prática dos delitos já previstos no ordenamento jurídico brasileiro.

Ainda que existam algumas normas que tratem da matéria, pode-se afirmar

que o Brasil, quando comparado a outros países, ainda está em processo de crescimento no que tange o combate aos crimes cibernéticos.

Constata-se que a inovação jurídica e a deficiência da persecução penal abordadas nesse trabalho requerem muito mais que atualizações e regulamentações de novas leis no ordenamento jurídico brasileiro, pois o ritmo de evolução tecnológica será sempre mais veloz que o da atividade legislativa.

Grande parte da eficácia legal necessária para tentar suprir a deficiência legislativa interna de um país, exige uma colaboração internacional, ou seja, necessita de um tratamento adicional de múltiplos ordenamentos jurídicos, seja em sede de Tratados ou Convenções Internacionais, ou em outra fórmula legal ainda a ser inventada.

Enquanto os países tratarem do tema apenas dentro de suas realidades, a comunidade de usuários da Internet ainda ficará carente de soluções mais adequadas para proteger sua privacidade e garantir segurança no ambiente digital, uma vez que o isolamento do pensamento jurídico não se adequa à nova realidade digital da sociedade.

Depreende-se desse trabalho não só a exigibilidade de criatividade por parte do operador do direito, o qual deve deixar de ser um mero burocrata para se tornar um estrategista, como também a indispensabilidade de acompanhamento de todo profissional, seja ele da área jurídica, técnica ou administrativa, à evolução do Direito Digital, em razão de sua volatilidade.

Finalmente, com essa pesquisa, conclui-se que a sociedade digital está evoluindo muito rápido e o Direito deve acompanhar esta mudança, aprimorar-se, renovar seus institutos e criar novos capazes de continuar garantindo a segurança jurídica das relações sociais, sob pena de ficar obsoleto. Isso pode estimular a prática da “justiça com as próprias mãos” e todas as mazelas associadas ao uso arbitrário das próprias razões e ao desequilíbrio gerado pelo poder desmedido das grandes corporações que são proprietárias dos recursos que permitem a

realização da vida digital.

Por fim, cabe ressaltar que o presente estudo não tem a finalidade de exaurir a matéria dos crimes cibernéticos e sim discutir a relevância do tema para o ramo do Direito, através das suas repercussões. Mesmo porque a criatividade humana é ilimitada e não se conseguiria exaurir neste trabalho todos os aspectos jurídicos que a tecnologia pode possuir.

REFERÊNCIAS

BRASIL. Código Penal. **Decreto-Lei nº 2.848**, de 7 de dezembro de 1940.

BRASIL. **Constituição Federal de 1988**. Promulgada em 05 de outubro de 1988. Disponível em <http:/planalto.gov.com.br/ccivil03/constutuicao.htm>.

BRASIL. **Lei Ordinária nº 12.735,** de 30 de novembro de 2012. Altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei no 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei no 7.716, de 5 de

janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

BRASIL. **Lei Ordinária nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei no 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

BRASIL. **Lei Ordinária nº 12.965**, de 23 de abril de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. **Cartilha de Segurança para Internet: Ransomware.**

CONVENÇÃO SOBRE O CIBERCRIME. Aberta para assinatura em Budapeste, Hungria, em 22 de novembro de 2001.

CERT.BR, Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança No Brasil. **Recomendações para Melhorar o Cenário de Ataques Distribuídos de Negação de Serviço (DDoS).**

FERREIRA, Ivette Senise. **A Criminalidade Informática. Direito & Internet – Aspetos Jurídicos Relevantes.** Editora Edipro, 2011.

GRECO FILHO, Vicente. **Algumas observações sobre o direito penal e a internet. Boletim do IBCCrim.** São Paulo. Ed. Esp., ano 8, n. 95, out. 2000.

Marco civil da internet entra em vigor. Disponível em http://cultturadigital.com.br/marcocivil-entra-em-vigor/.

MPF, Ministério Público Federal. Combate aos Crimes Cibernéticos. Disponível em http.//mpf.mp.br/-atuacao-tematica-combate-de-crime/.

PIAUHYLINO, Luiz. **Projeto de Lei nº 84, de 1999.** Dispõe sobre os crimes

cometidos na área de informática, suas penalidades e dá outras providências.

PINHEIRO, Patricia Peck. **Direito digital**. 6. ed. rev., atual. e ampl. São Paulo: Saraiva, 2018.

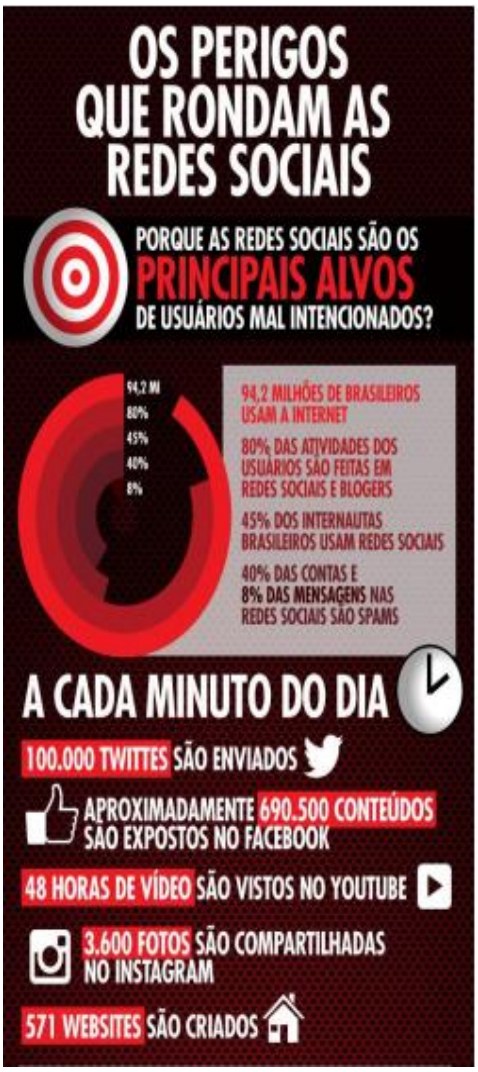
ROSSINI, Augusto Eduardo de Souza. **Informática, telemática e direito penal**. São Paulo: Memória Jurídica, 2017.

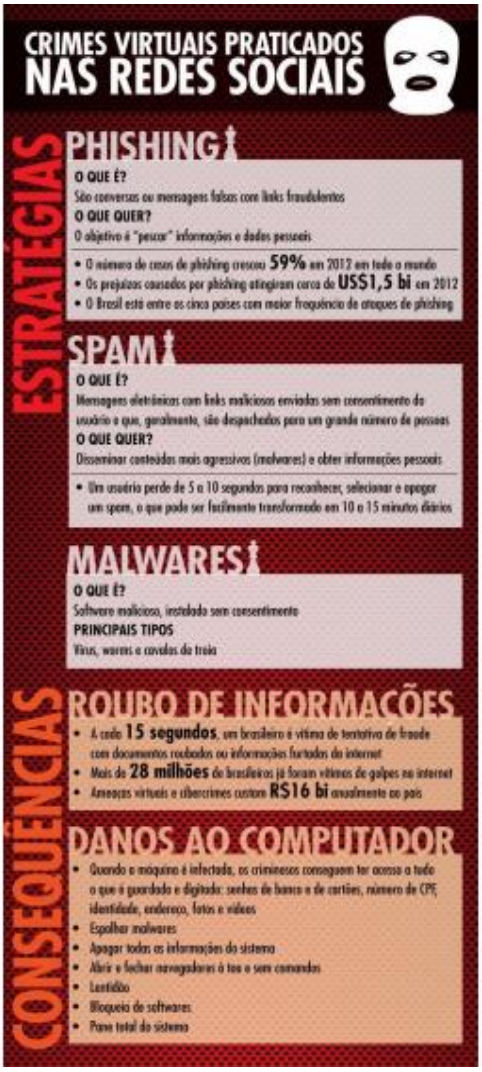
TEIXEIRA, Paulo; Erundina, Luiza; D'ávila, Manuela; Arruda, João; Neto, Brizola; José, Emiliano. **Projeto de Lei nº 2793, de 2011.**

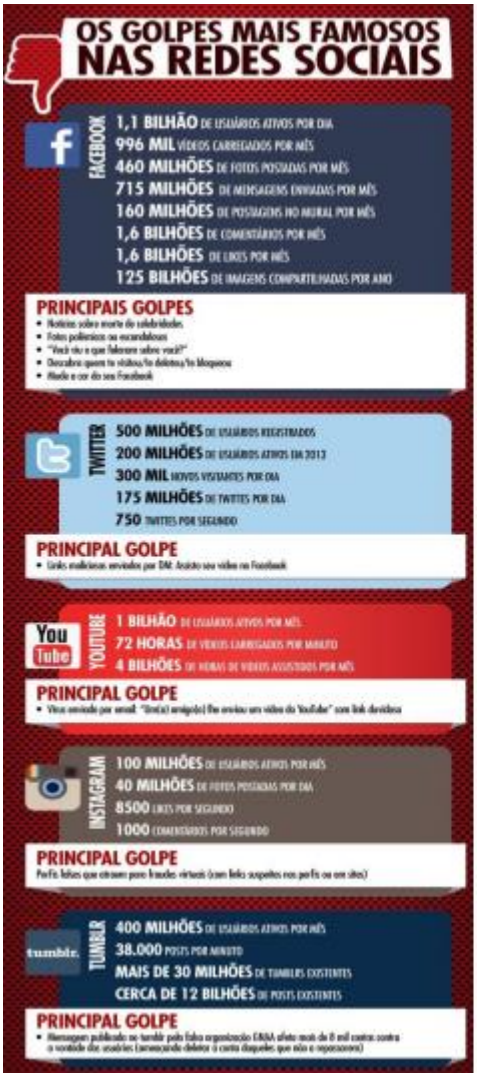
PINHEIRO, Patrícia Peck; HAIKAL, Victor Auilo. **A nova lei de crimes digitais. 2013.**

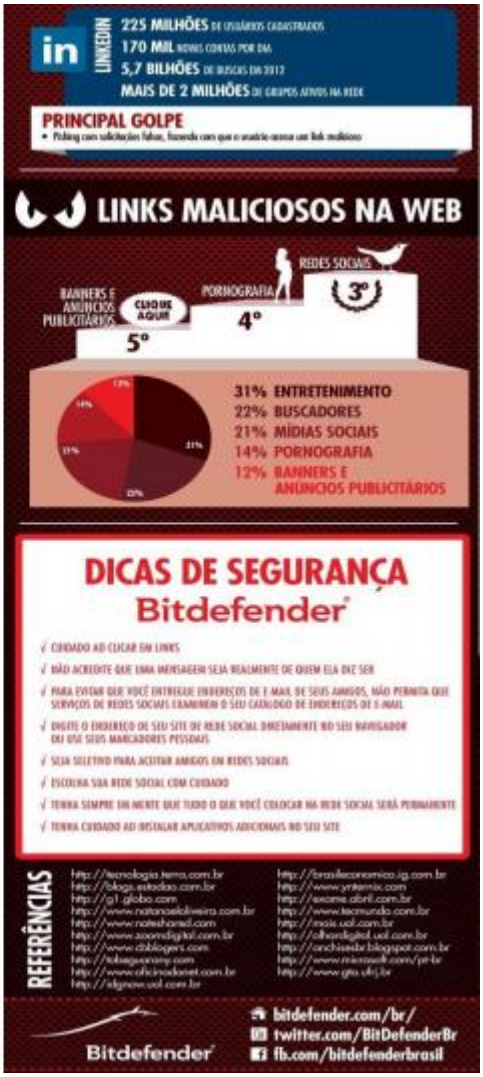
APÊNDICES E ANEXOS

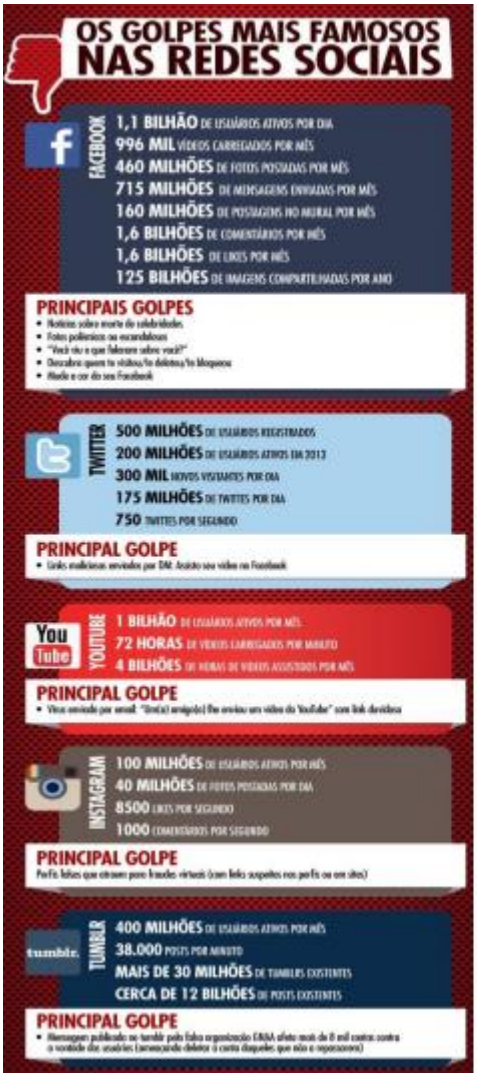
Na figura N° 1 podemos notar o porquê das redes sociais serem as mais procuradas pelos malfeitores, o texto fala em "minutos" e não em horas e muito menos em dias. Na figura N° 2, logo após as palavras "*Phishing*", "*Spam*" e "*Malwares*", podemos notar que há uma peça de xadrez, o Rei, que quer dizer cheque mate na figura N° 3 podemos ver os golpes mais aplicados em determinadas páginas na rede social já na figura N°4 veremos alguns links maliciosos e como se prevenir.

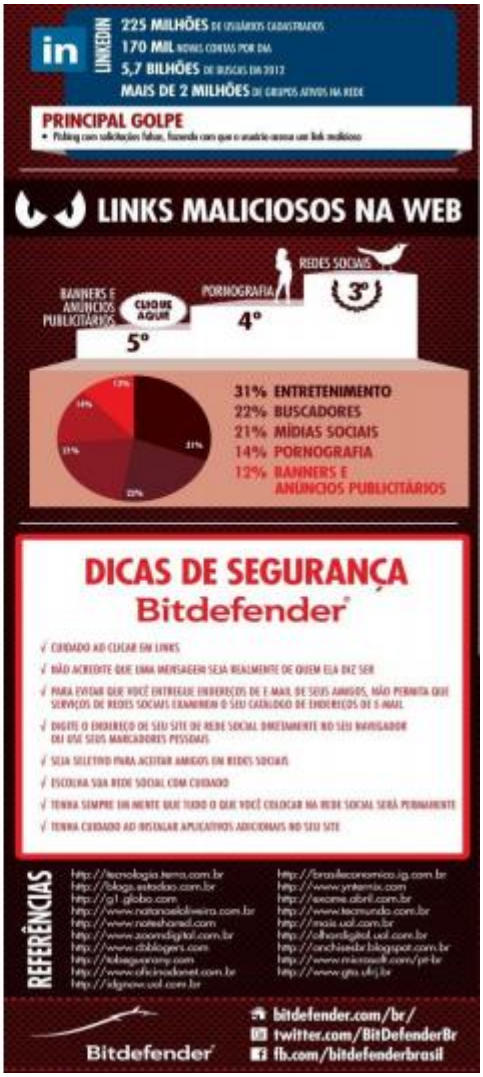

OS PERIGOS QUE RONDAM AS REDES SOCIAIS
PORQUE AS REDES SOCIAIS SÃO OS PRINCIPAIS ALVOS DE USUÁRIOS MAL INTENCIONADOS?
94,2 MI
80%
45%
40%
8%
94,2 MILHÕES DE BRASILEIROS USAM A INTERNET
80% DAS ATIVIDADES DOS USUÁRIOS SÃO FEITAS EM REDES SOCIAIS E BLOGERS
45% DOS INTERNAUTAS BRASILEIROS USAM REDES SOCIAIS
40% DAS CONTAS E 8% DAS MENSAGENS NAS REDES SOCIAIS SÃO SPAMS
A CADA MINUTO DO DIA
100.000 TWITTES SÃO ENVIADOS
APROXIMADAMENTE 690.500 CONTEÚDOS SÃO EXPOSTOS NO FACEBOOK
48 HORAS DE VÍDEO SÃO VISTOS NO YOUTUBE
3.600 FOTOS SÃO COMPARTILHADAS NO INSTAGRAM
571 WEBSITES SÃO CRIADOS

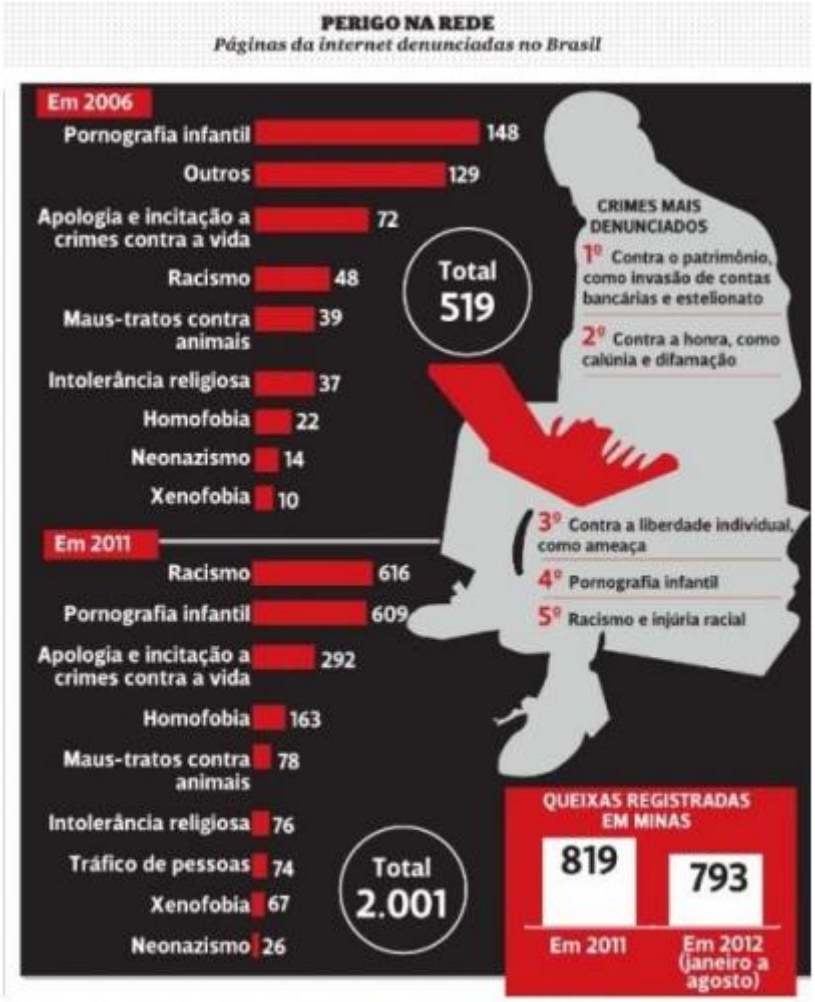

CRIMES VIRTUAIS PRATICADOS NAS REDES SOCIAIS
ESTRATÉGIAS
PHISHING
O QUE É?
São conversas ou mensagens falsas com links fraudulentos
O QUE QUER?
O objetivo é "pescar" informações e dados pessoais
• O número de casos de phishing cresceu 59% em 2012 em todo o mundo
• Os prejuízos causados por phishing atingiram cerca de US$1,5 bi em 2012
• O Brasil está entre os cinco países com maior frequência de ataques de phishing
SPAM
O QUE É?
Mensagens eletrônicas com links maliciosos enviadas sem consentimento do usuário e que, geralmente, são despachados para um grande número de pessoas
O QUE QUER?
Disseminar conteúdos mais agressivos (malwares) e obter informações pessoais
• Um usuário perde de 5 a 10 segundos para reconhecer, selecionar e apagar um spam, o que pode ser facilmente transformado em 10 a 15 minutos diários
MALWARES
O QUE É?
Software malicioso, instalado sem consentimento
PRINCIPAIS TIPOS
Vírus, worms e cavalos de troia
CONSEQUÊNCIAS
ROUBO DE INFORMAÇÕES
• A cada 15 segundos, um brasileiro é vítima de tentativa de fraude com documentos roubados ou informações furtadas da internet
• Mais de 28 milhões de brasileiros já foram vítimas de golpes na internet
• Ameaças virtuais e cibercrimes custam R$16 bi anualmente ao país
DANOS AO COMPUTADOR
• Quando a máquina é infectada, os criminosos conseguem ter acesso a tudo o que é guardado e digitado: senhas de banco e de cartões, número de CPF, identidade, endereço, fotos e vídeos
• Espalhar malwares
• Apagar todas as informações do sistema
• Abrir e fechar navegadores à toa e sem comandos
• Lentidão
• Bloqueio de softwares
• Pane total do sistema


OS GOLPES MAIS FAMOSOS NAS REDES SOCIAIS
FACEBOOK
1,1 BILHÃO DE USUÁRIOS ATIVOS POR DIA
996 MIL VÍDEOS CARREGADOS POR MÊS
460 MILHÕES DE FOTOS POSTADAS POR MÊS
715 MILHÕES DE MENSAGENS ENVIADAS POR MÊS
160 MILHÕES DE POSTAGENS NO MURAL POR MÊS
1,6 BILHÕES DE COMENTÁRIOS POR MÊS
1,6 BILHÕES DE LIKES POR MÊS
125 BILHÕES DE IMAGENS COMPARTILHADAS POR ANO
PRINCIPAIS GOLPES
Notícias sobre morte de celebridades
Fotos polêmicas ou escandalosas
"Você viu o que falaram sobre você?"
Descubra quem te visitou/te deletou/te bloqueou
Mude a cor do seu Facebook
TWITTER
500 MILHÕES DE USUÁRIOS REGISTRADOS
200 MILHÕES DE USUÁRIOS ATIVOS EM 2013
300 MIL NOVOS VISITANTES POR DIA
175 MILHÕES DE TWITTES POR DIA
750 TWITTES POR SEGUNDO
PRINCIPAL GOLPE
Links maliciosos enviados por DM: Assista seu vídeo no Facebook
YOUTUBE
1 BILHÃO DE USUÁRIOS ATIVOS POR MÊS
72 HORAS DE VÍDEOS CARREGADOS POR MINUTO
4 BILHÕES DE HORAS DE VÍDEOS ASSISTIDOS POR MÊS
PRINCIPAL GOLPE
Vírus enviado por email: "Fulano(a) amigo(a) lhe enviou um vídeo do YouTube" com link duvidoso
INSTAGRAM
100 MILHÕES DE USUÁRIOS ATIVOS POR MÊS
40 MILHÕES DE FOTOS POSTADAS POR DIA
8500 LIKES POR SEGUNDO
1000 COMENTÁRIOS POR SEGUNDO
PRINCIPAL GOLPE
Perfis falsos que atraem para fraudes virtuais (com links suspeitos nos perfis ou em sites)
TUMBLR
400 MILHÕES DE USUÁRIOS ATIVOS POR MÊS
38.000 POSTS POR MINUTO
MAIS DE 30 MILHÕES DE TUMBLRS EXISTENTES
CERCA DE 12 BILHÕES DE POSTS EXISTENTES
PRINCIPAL GOLPE
Mensagem publicada no tumblr pela falsa organização ENISA alerta mais de 8 mil contra o vereador diz: usuários (ameaçando deletar a conta daqueles que não o repercutirem)


LINKEDIN
225 MILHÕES DE USUÁRIOS CADASTRADOS
170 MIL NOVAS CONTAS POR DIA
5,7 BILHÕES DE BUSCAS EM 2013
MAIS DE 2 MILHÕES DE GRUPOS ATIVOS NA REDE
PRINCIPAL GOLPE
Phishing com solicitações falsas, fazendo com que o usuário acesse um link malicioso
LINKS MALICIOSOS NA WEB
BANNERS E ANÚNCIOS PUBLICITÁRIOS
CLIQUE AQUI
5º
PORNOGRAFIA
4º
REDES SOCIAIS
3º
31% ENTRETENIMENTO
22% BUSCADORES
21% MÍDIAS SOCIAIS
14% PORNOGRAFIA
12% BANNERS E ANÚNCIOS PUBLICITÁRIOS
DICAS DE SEGURANÇA
Bitdefender
√ CUIDADO AO CLICAR EM LINKS
√ NÃO ACREDITE QUE UMA MENSAGEM SEJA REALMENTE DE QUEM ELA DIZ SER
√ PARA EVITAR QUE VOCÊ ENTREGUE ENDEREÇOS DE E-MAIL DE SEUS AMIGOS, NÃO PERMITA QUE SERVIÇOS DE REDES SOCIAIS EXAMINEM O SEU CADERNO DE ENDEREÇOS DE E-MAIL
√ DIGITE O ENDEREÇO DE SEU SITE DE REDE SOCIAL DIRETAMENTE NO SEU NAVEGADOR OU USE SEUS MARCADORES PESSOAIS
√ SEJA SELETIVO PARA ACEITAR AMIGOS EM REDES SOCIAIS
√ ESCOLHA SUA REDE SOCIAL COM CUIDADO
√ TENHA SEMPRE EM MENTE QUE TUDO O QUE VOCÊ COLOCAR NA REDE SOCIAL SERÁ PERMANENTE
√ TENHA CUIDADO AO INSTALAR APLICATIVOS ADICIONAIS NO SEU SITE
REFERÊNCIAS
http://tecnologia.terra.com.br
http://blogs.estadao.com.br
http://g1.globo.com
http://www.natanaelsilveira.com.br
http://www.noteshared.com
http://www.zoomdigital.com.br
http://www.dbblogers.com
http://tobeguronny.com
http://www.oficinadanet.com.br
http://edgnow.uol.com.br
http://brasileconomico.ig.com.br
http://www.ynternix.com
http://exame.abril.com.br
http://www.tecmundo.com.br
http://mais.uol.com.br
http://olhardigital.uol.com.br
http://anchisesbr.blogspot.com.br
http://www.microsoft.com/pt-br
http://www.gta.ufrj.br
Bitdefender
bitdefender.com/br/
twitter.com/BitDefenderBr
fb.com/bitdefenderbrasil


OS GOLPES MAIS FAMOSOS NAS REDES SOCIAIS
FACEBOOK
1,1 BILHÃO DE USUÁRIOS ATIVOS POR DIA
996 MIL VÍDEOS CARREGADOS POR MÊS
460 MILHÕES DE FOTOS POSTADAS POR MÊS
715 MILHÕES DE MENSAGENS ENVIADAS POR MÊS
160 MILHÕES DE POSTAGENS NO MURAL POR MÊS
1,6 BILHÕES DE COMENTÁRIOS POR MÊS
1,6 BILHÕES DE LIKES POR MÊS
125 BILHÕES DE IMAGENS COMPARTILHADAS POR ANO
PRINCIPAIS GOLPES
Notícias sobre morte de celebridades
Fotos polêmicas ou escandalosas
"Você viu o que falaram sobre você?"
Descubra quem te visitou/te deletou/te bloqueou
Mude a cor do seu Facebook
TWITTER
500 MILHÕES DE USUÁRIOS REGISTRADOS
200 MILHÕES DE USUÁRIOS ATIVOS EM 2013
300 MIL NOVOS VISITANTES POR DIA
175 MILHÕES DE TWITTES POR DIA
750 TWITTES POR SEGUNDO
PRINCIPAL GOLPE
Links maliciosos enviados por DM: Assista seu vídeo no Facebook
YOUTUBE
1 BILHÃO DE USUÁRIOS ATIVOS POR MÊS
72 HORAS DE VÍDEOS CARREGADOS POR MINUTO
4 BILHÕES DE HORAS DE VÍDEOS ASSISTIDOS POR MÊS
PRINCIPAL GOLPE
Vírus enviado por email: "Fulano(a) amigo(a) lhe enviou um vídeo do YouTube" com link duvidoso
INSTAGRAM
100 MILHÕES DE USUÁRIOS ATIVOS POR MÊS
40 MILHÕES DE FOTOS POSTADAS POR DIA
8500 LIKES POR SEGUNDO
1000 COMENTÁRIOS POR SEGUNDO
PRINCIPAL GOLPE
Perfis falsos que atraem para fraudes virtuais (com links suspeitos nos perfis ou em sites)
TUMBLR
400 MILHÕES DE USUÁRIOS ATIVOS POR MÊS
38.000 POSTS POR MINUTO
MAIS DE 30 MILHÕES DE TUMBLRS EXISTENTES
CERCA DE 12 BILHÕES DE POSTS EXISTENTES
PRINCIPAL GOLPE
Mensagem publicada no tumblr pela falsa organização ENISA alerta mais de 8 mil contra o vereador diz: usuários (ameaçando deletar a conta daqueles que não o repercutirem)


LINKEDIN
225 MILHÕES DE USUÁRIOS CADASTRADOS
170 MIL NOVAS CONTAS POR DIA
5,7 BILHÕES DE BUSCAS EM 2013
MAIS DE 2 MILHÕES DE GRUPOS ATIVOS NA REDE
PRINCIPAL GOLPE
Phishing com solicitações falsas, fazendo com que o usuário acesse um link malicioso
LINKS MALICIOSOS NA WEB
BANNERS E ANÚNCIOS PUBLICITÁRIOS
5º
CLIQUE AQUI
PORNOGRAFIA
4º
REDES SOCIAIS
3º
31% ENTRETENIMENTO
22% BUSCADORES
21% MÍDIAS SOCIAIS
14% PORNOGRAFIA
12% BANNERS E ANÚNCIOS PUBLICITÁRIOS
DICAS DE SEGURANÇA
Bitdefender
√ CUIDADO AO CLICAR EM LINKS
√ NÃO ACREDITE QUE UMA MENSAGEM SEJA REALMENTE DE QUEM ELA DIZ SER
√ PARA EVITAR QUE VOCÊ ENTREGUE ENDEREÇOS DE E-MAIL DE SEUS AMIGOS, NÃO PERMITA QUE SERVIÇOS DE REDES SOCIAIS EXAMINEM O SEU CADERNO DE ENDEREÇOS DE E-MAIL
√ DIGITE O ENDEREÇO DE SEU SITE DE REDE SOCIAL DIRETAMENTE NO SEU NAVEGADOR OU USE SEUS MARCADORES PESSOAIS
√ SEJA SELETIVO PARA ACEITAR AMIGOS EM REDES SOCIAIS
√ ESCOLHA SUA REDE SOCIAL COM CUIDADO
√ TENHA SEMPRE EM MENTE QUE TUDO O QUE VOCÊ COLOCAR NA REDE SOCIAL SERÁ PERMANENTE
√ TENHA CUIDADO AO INSTALAR APLICATIVOS ADICIONAIS NO SEU SITE
REFERÊNCIAS
http://tecnologia.terra.com.br
http://blogs.estadao.com.br
http://g1.globo.com
http://www.natanaelsilveira.com.br
http://www.noteshared.com
http://www.zoomdigital.com.br
http://www.dbblogers.com
http://tobeguronny.com
http://www.oficinadanet.com.br
http://edgnow.uol.com.br
http://brasileconomico.ig.com.br
http://www.ynternix.com
http://exame.abril.com.br
http://www.tecmundo.com.br
http://mais.uol.com.br
http://olhardigital.uol.com.br
http://anchisesbr.blogspot.com.br
http://www.microsoft.com/pt-br
http://www.gta.ufrj.br
Bitdefender
bitdefender.com/br/
twitter.com/BitDefenderBr
fb.com/bitdefenderbrasil



FONTES: Safer Brasil e Polícia Civil de Minas

FIGURA nº 11