FACULDADE DE ADMINISTRAÇÃO E NEGÓCIOS DE SERGIPE

SERGIO RICARDO GOMES SILVA

CIBERCRIME - A EFICIÊNCIA DA LEGISLAÇÃO BRASILEIRA NO COMBATE AO CRIME DE INTERNET

ARACAJU

2018.2

SERGIO RICARDO GOMES SILVA

CIBERCRIME - A EFICIÊNCIA DA LEGISLAÇÃO BRASILEIRA NO COMBATE AO CRIME DE INTERNET

Trabalho de Conclusão de Curso apresentado como pré-requisito parcial de aprovação na disciplina TCC II do Curso de Bacharelado em Direito da Faculdade de Administração e Negócios de Sergipe - FANESE.

Orientador: Prof. Me. Marcelo de Macedo Schimmelpfeng

ARACAJU

2018.2

AGRADECIMENTOS

Agradeço em primeiro lugar a DEUS, por me dar forças a concluir este trabalho, aos meus pais Antonio Menezes Silva e Edilde Gomes Silva, a minha esposa Liene Santos Oliveira e Silva, aos meus filhos Sergio Ricardo Gomes Silva Junior, Ana Luiza Gomes Silva e Larissa Sofia Gomes Silva.

Ao meu orientador Marcelo de Macedo Schimmelpfeng, que foi de grande ajuda na conclusão deste TCC.

E também ao corpo docente da FANESE e seus funcionários.

S586e SILVA, Sérgio Ricardo Gomes.

A Eficiência Da Legislação Brasileira No Combate Ao Crime De Internet / Sérgio Ricardo Gomes Silva; Aracaju, 2018. 56 f.

Monografia (Graduação) – Faculdade de Administração e Negócios de Sergipe. Coordenação de Direito.

Orientador: Prof. Me. Marcelo de Macedo Schimmelpfeng

1. Crime 2. Internet 3. Proteção 4. Marco Civil I. Título.

CDU 343.232(813.7)

Elaborada pela Bibliotecária Lícia de Oliveira CRB-5/1255

SÉRGIO RICARDO GOMES SILVA

CIBERCRIME - A EFICIÊNCIA DA LEGISLAÇÃO BRASILEIRA NO COMBATE AO CRIME DE INTERNET

Monografia apresentada à banca examinadora da FANESE como exigência parcial para a obtenção do título de Bacharel em Direito.

Aracaju, 06 / 12 / 2018.

BANCA EXAMINADORA

Prof. Me. Marcelo Macedo Schimmelpfeng
Faculdade de administração e Negócios de Sergipe

Prof. Dr. Cleverton Barros Lima
Faculdade de administração e Negócios de Sergipe

Prof. Esp. Carlos Augusto Lima Neto
Faculdade de administração e Negócios de Sergipe

RESUMO

A internet, local de convergência de muitos serviços, incluindo bancários, estudantis e outros, proporciona uma interação do usuário com diversos setores de serviços sem que para isso tenha que se deslocar para uma agência física. A praticidade é de fato um chamariz para a utilização da rede, pois se o individuo tem uma conta a pagar, não precisa ir ao banco, bastando utilizar o aplicativo oferecido pela instituição para pagar o seu debito. Além disso pode fazer diversas transações financeiras sem sair de casa. Mas a praticidade traz um perigo junto a ela, o crime cibernético, no qual o usuário pode ter sua senha capturada por terceiros mal intencionados e estes podem acessar a sua conta e fazer transações sem o seu consentimento. Neste contexto o marco civil foi elaborado, para oferecer normas para que a internet no Brasil fosse regulamentada e que a navegação se torne segura.

Palavras-chave: crime, internet, proteção,marco civil.

ABSTRACT

The internet, where many services converge, including banking, students and others, provides a user interaction with several service sectors without having to go to a physical agency. Practicality is in fact a gimmick for the use of the network, because if the individual has an account to pay, he does not have to go to the bank, simply using the application offered by the institution to pay its debit. In addition you can make several financial transactions without leaving home. But practicality carries a danger alongside it, cyber crime, in which the user can have their password captured by malicious third parties and they can access your account and make transactions without your consent. In this context, the civilian framework was developed to provide standards for Internet regulation in Brazil and for safe navigation.

Keywords: crime. Internet. government,civilian framework.

SUMÁRIO

ROL DE ABREVIATURAS E SIGLAS

IBGE – Instituto Brasileiro de Geografia e Estatística

IP – Protocolo de Internet

MPF – Ministério Publico Federal

ONU – Organização das Nações Unidas

PL – Projeto Lei

W.W.W – Rede mundial de computadores

1 INTRODUÇÃO

A globalização trouxe avanços e descobertas tecnológicas que diminuíram as distâncias entre as pessoas, as informações, o lazer, estudos e etc. Mas essa mudança de comportamento aconteceu de uma maneira radical, onde é mais frequente a comunicação ser feita utilizando-se de equipamentos eletrônicos conectados à internet. Até mesmo culturas diferentes passaram a se inserir em nosso meio, com isso podemos interagir com elas através da rede mundial de computadores.

Diante disso, os meios para o acesso à internet são cada vez mais amplos, onde podemos acessá-la não somente pelos computadores, mas também por celulares, tablets, e até mesmo através de um simples relógio, dentre outros equipamentos disponíveis. Com essas novas relações sociais, que passaram a surgir, o Direito busca se adequar à nova realidade: com o surgimento da internet, os crimes tipificados pelo Código Penal passaram a ser praticados também virtualmente, assim como surgiram novas modalidades de crimes, denominados cibernéticos, que carecem de uma legislação específica para a punição dos responsáveis pelo delito. Cabe salientar que existem outros países que apresentam grande avanço legislativo na definição do que seja crime de internet e em seu combate.

No Brasil, muito foi discutido sobre uma legislação específica para uso da internet segura, porém, nada de concreto surgiu devido à falta de infraestrutura para investigar e punir tais crimes, além da deficiência da legislação especifica a ser utilizada no combate a esses crimes. Nos Estados Unidos e na União Europeia esta regulamentação foi feita há pelo menos duas décadas. Portugal, por exemplo, apresenta a Lei de Criminalidade Informática desde 1991, estando muito à frente do Brasil, que teve seu primeiro projeto de lei relevante sobre o tema apenas no ano de 1999 – O PL 84/99- e somente no ano de 2012 aprovada a lei 12.737, que tipifica o crime de invasão de dispositivos informáticos no Brasil.

A lei supracitada foi aprovada às pressas pelo Congresso Nacional, sensibilizado com a repercussão dada ao tema após a situação ocorrida contra uma famosa atriz de televisão, que teve fotos íntimas furtadas de seu computador pessoal. Porém, ainda existe um hiato sobre o que deve ser considerado crime cibernético e como podemos combatê-lo.

Porque não aproveitar a experiência de locais que já é comum o lidar com o crime informático? Copiar o que funciona e aplicar no nosso país, tornando a vida de quem acessa a internet menos perigosa.

Outro ponto importante a ser considerado é que o Brasil não ratificou tratados internacionais sobre o cibercrime, deixando o país fora de uma importante forma de combater estes crimes, a cooperação internacional, ficando isolado no combate a um crime que não respeita fronteiras, pois o infrator residente em outra localidade estrangeira pode cometer uma infração contra uma vitima que reside em solo pátrio.

O presente trabalho objetiva apresentar os crimes cibernéticos no Brasil, como também mostrar um panorama dos crimes de internet consumados no município de Aracaju, no ano de 2017. Será apresentada, também, a evolução do direito digital, desde o surgimento do computador; os crimes praticados frequentemente através da rede; com isso, demonstrar-se-á como o ordenamento jurídico pátrio, e o de outros países, tratam desses crimes.

No Brasil foi aprovado o marco civil,que visa normatizar o uso da internet no país, tornando o que era terra sem lei , em local com regras, apesar destas serem objeto de diversas discussões , das quais se destaca a falta de definição de quais dados são protegidos,alem da necessidade de que as empresas possuam data centers em solo nacional.

O presente trabalho objetiva responder a questão tão importante colocada: o marco civil é suficiente para que haja um combate efetivo ao crime cibernético?

O primeiro capitulo aborda o desenvolvimento do computador, parte essencial da internet, já que esta é descrita como a rede mundial de computadores, mostrando a evolução das maquinas ate a criação da rede em si, abordando também os princípios de governança para a utilização da net.

No segundo capitulo é tratado o tema crime,observando como se chegou a

atual conceituação do crime em si, pois para que sejam elaboradas leis sobre o assunto há de se definir uma delimitação conceitual o que é crime.

O quarto capitulo procura definir o crime realizado na ou por meio da internet, o chamado cibercrime.

No quinto é feito um panorama da legislação vigente em outros países, mostrando que estes já possuem um arcabouço de normas, que efetivamente serve de base para o combate do cibercrime.

O sexto nos apresenta o Marco Civil.

O sétimo elenca a atuação da delegacia especializada em crimes virtuais na capital do estado de Sergipe, Aracaju. Abordando como é combatido este tipo de crime na nossa cidade.

E por fim, há a conclusão sobre a questão principal, que nos traz a resposta ao principal questionamento: se o marco civil é uma ferramenta capaz de fazer frente ao crime virtual.

O tema é de relevante interesse pois aborda um tema que preocupa a maioria dos usuários, e não poderia ser diferente, pois a cada dia a internet se coloca em nossas vidas de modo permanente e com o passar do tempo a rede vai se afirmando como uma via na qual, transações bancarias, comunicações,estudo e muitas outras trafegam através dela, fazendo com que a necessidade de normas e leis se torne crucial,pois todas as utilizações da internet precisam de segurança para que não gerem um passivo negativo.

Para elaboração deste trabalho foi utilizada a pesquisa bibliográfica,como também a entrevista semiestruturada.

2– COMPUTADOR E INTERNET: CONCEITOS E PRECEDENTES HISTORICOS

2.1 – História e Desenvolvimento do Computador

Fabrízio Rosa (2006) em sua obra “Crimes de Informática”, afirma ser impossível se falar sobre internet, crimes de internet e informática sem antes discorrer um pouco sobre o computador, essa inovação tecnológica que mudou o conceito de informação e que se transformou em um instrumento básico na vida do homem.

Segundo o dicionário brasileiro palavra “computador” vem do verbo “computar” que, por sua vez, significa “calcular”, colocando no pé da letra temos seu significado como aquele ou aquilo que calcula baseado em valores digitais; calculador, calculista”. Sendo assim, podemos pensar que a criação de computadores começa na idade antiga, já que a relação de contar já intrigava os homens. Muitos povos da antiguidade utilizavam um aparelho chamado ábaco para realização dos cálculos no dia a dia, que era um instrumento composto de varetas ou barras e pequenas bolas, utilizado para contar e calcular. O mais antigo data de aproximadamente 3.500 a. C., no Vale entre os rios Tigres e Eufrates (Egito).

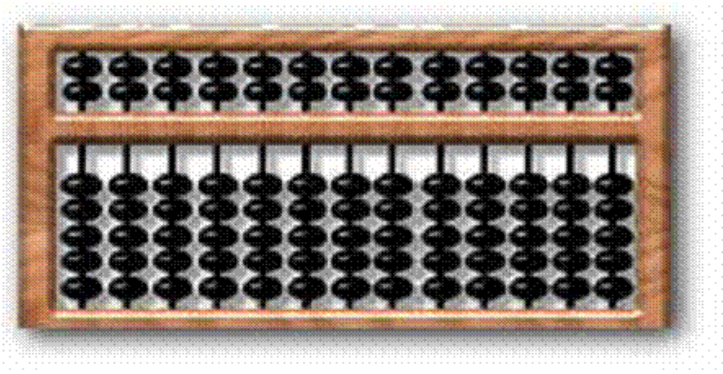

Figura 1: Abaco Chinês

Segundo Cléuzio Fonseca Filho *(2007)*, o homem com os passar dos anos foi aperfeiçoando e desenvolvendo novas máquinas e ferramentas para tornar as atividades diárias mais simples. Podemos deduzir que o computador nasceu dessa ideia, de facilitar as tarefas que eram realizadas num longo espaço de tempo,

passaram a ser realizadas quase de maneira instantânea.

Com essa busca constante, o matemático inglês Charles Babbage no ano de 1830 inventou a Maquina Analítica, que a primórdio tinha intenção de construir um aparelho inteligente, com múltiplos propósitos, capaz de simular o raciocínio humano. Dessa invenção de Babbage, conseguiu-se definir os conceitos básicos do que seria computador, tais como memória, programação, sequencia. Infelizmente essa a máquina não saiu do protótipo, demorou um século para que surgissem avanços tecnológicos necessários pra essa criação.

Na década de 1940 surgem os primeiros os computadores que se utilizavam de simples algoritmos para a entrega de resultados complexos de cálculos. Essa primeira geração foi desenvolvida principalmente após o final da Segunda Guerra Mundial. Em 1946 os físicos norte-americanos John Eckert e John Mauchly criaram o computador ENIAC (Electrical Numerical Integrator and Calculator). Uma revolução tecnológica na época. Uma máquina onde maioria das operações eram realizadas sem a necessidade de movimentar peças de forma manual, mas sim pela entrada de dados no painel de controle. Cada operação podia ser acessada através de configurações-padrão de chaves e switches.

As dimensões desta máquina são muito grandes, com aproximadamente 25 metros de comprimento por 5,50 metros de altura. O seu peso total era de 30 toneladas. Esse valor representa algo como um andar inteiro de um prédio.

Ainda de acordo com Cléuzio Fonseca Filho (2007) *a* segunda geração de computadores teve como marca a chegada dos transistores em 1948, tendo como destaque o Univac 1101, um equipamento de 12 metros de comprimento e 6,1 metros de largura que usava 2.700 tubos a vácuo para seus circuitos lógicos. Neste período também surgem os chamados periféricos de saída, tais como as impressoras, as fitas magnéticas, os discos para armazenamento, etc.

Em 1967 surgi no mercado o IBM 360/91 (terceira geração do computador), que já trabalhava com dispositivos de entrada e saída modernos para a época, como discos e fitas de armazenamento, além da possibilidade de imprimir todos os resultados em papel. Este computador foi um dos primeiros a permitir programação da CPU por microcódigo, ou seja, as operações usadas por um processador qualquer poderiam ser gravadas através de softwares, sem a necessidade do projetar todo o circuito de forma manual.

Com o avanço da tecnologia os computadores têm seu tamanho reduzido, e nessa conhecida com quarta geração, surgiram os computadores pessoais e em 1975 é lançado o Altair 8800, que revolucionou tudo o que era conhecido como computador até aquela época. Com um tamanho que cabia facilmente em uma mesa e um formato retangular, também era muito mais rápido que os computadores anteriores. O projeto usava o processador 8080 da Intel, fato que propiciou todo esse desempenho. Bill Gates, e o jovem programador, Paul Allen, que juntos desenvolveram uma versão da linguagem "Basic" para o Altair. Pouco tempo depois, a dupla resolveu mudar o rumo de suas carreiras e criar uma empresa chamada Microsoft.

Vendo o sucesso do Altair 8800, em 1976, outra dupla de jovens, Steve Jobs e Steve Wozniak, sentiram que ainda faltava algo no projeto: apesar de suas funcionalidades, este computador não era fácil de ser utilizado por pessoas comuns, na visão de Steve Jobs um computador deveria representar de maneira gráfica o seu funcionamento, ao contrário de luzes que acendiam e apagavam. E foi ai que surgiu o Aplle I, considerado o primeiro computador pessoal.

Desde então, o computador vem sofrendo várias alterações, atualizações e modificações; o seu tamanho diminuem e a sua velocidade e capacidade de processamento de dados aumentam. Surgem os softwares integrados e a partir da virada do milênio, começam a surgir os computadores de mão. Ou seja, os smartphones, iPod, iPad e tablets, que incluem conexão móvel com navegação na web.

Figura 3: FONTE: HISTÓRIA..., 2017, disponível em: <https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/>

2.2 - O Surgimento da Internet e Sua Finalidade

A internet está presente no dia a dia como uma nova realidade, que para alguns já se naturalizou, pode ser definida como sendo um conjunto de facilidades de comunicação e conectividade. internet é uma rede de computadores que interconecta centenas de milhões de dispositivos de computação ao redor do mundo. (KUROSE/ROSS,2013.p.75)

> É uma sociedade cooperativa que forma uma comunidade virtual,estendendo-se de um extremo ao outro do globo. Como tal, a Internet é um portal para o espaço cibernético, que abrange um universo virtual de ideias e informações em que nós entramos sempre que lemos um livro ou usamos um computador. (ROSA, 2006, p. 35).

Criada com uma tecnologia iniciada na década de 60, a base da Internet que utiliza-se hoje vem da ARPANet (1969 – *Advanced Research Project Agency Network*) criada com objetivos militares, em que se pretendeu gerar uma infraestrutura de rede de computadores que não fosse interrompida: os servidores estavam espalhados geograficamente, o que garantiria a continuidade do fluxo de informações no caso de destruição (por exemplo: bombas) de um nó de rede. Passando por uma rede acadêmica, desde então a internet só aprimorou (CORNACCHIONE,2012,p 101)

Os trabalhos desenvolvidos no MIT, no Rand Institute e no NPL foram os alicerces do que hoje é a internet. Mas a internet tem uma longa historia de atitudes do tipo “construir e demonstrar”, que também data do inicio da década de 1960. J.C.R.Licklider (DEC, 1990) e Lawrence Roberts, ambos colegas de Kleinrock no MIT, foram adiante e lideraram o programa de ciência de computadores na ARPA (Advanced Reserch Project Agency- Agência de Projetos de Pesquisa Avançada), nos Estados Unidos, Roberts publicou um plano geral para a ARPA-net publica de hoje. Em 1969, foi instalado o primeiro computador na UCLA (Universidade da Califórnia em Los Angeles). Em 1972 a ARPA-net foi apresentada publicamente.(KUROSE/ROSS,2013,p.45). Segundo o artigo do jornalista Leonardo Werner Silva, publicado em 12 de agosto de 2001, pela folha de são paulo, “apartir de 1982 o uso da ARPANET, tornou-se maior no âmbito acadêmico. Inicialmente o uso era restrito a EUA, mas se expandiu para outros países, como Holanda,Dinamarca e Suécia, Desde então, começou a ser utilizado o nome de internet.” Por quase vinte anos, o uso da rede ficou confinado aos meios acadêmicos e científicos. Só sendo permitido a utilização comercial nos Estados Unidos, em 1987. No ano de 1992, surgiram as primeiras empresas fornecedoras de acesso a internet no mesmo pais. No mesmo ano, o CERN- Laboratório Europeu de Física de Partícula criou a World Wide Web, que permitiu o acesso de informações a qualquer usuário da internet.

No Brasil, a conexão de computadores por uma rede somente era possível para fins estatais, assim as Universidades Federais do Rio Grande do Sul e do Rio de Janeiro estavam conectadas a rede, desde 1989.A FAPESPE(Fundação de Amparo à Pesquisa de São Paulo) conectou-se um ano após. Em 1991, a

comunidade acadêmica brasileira conseguiu, através do Ministério da Ciência e Tecnologia, acesso a redes de pesquisas internacionais. Porem, em maio de 1995, a rede foi aberta para fins comerciais, Onde nesse ano foi realizada a primeira transmissão a longa distância entre os estados, e finalmente ficando a cargo da iniciativa privada a exploração dos serviços. No mesmo ano, foi criado o Comitê Gestor da Internet no Brasil (CGI.br), com a finalidade de coordenar e integrar todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. (ROSA, 2006, p. 36). Hoje, para conectar seu computador, o usuário paga os serviços de um provedor de acesso ou tem conexão direta.

Segundo o Pesquisa Nacional por Amostra de Domicílios Contínua (Pnad), divulgada pelo Instituto Brasileiro de Geografia e Estatística (IBGE), que segundo com o seu o levantamento, em 2016 a internet estava presente em 63,6% dos lares e em 94,8% deles havia celulares sendo usados para se conectar à rede.

Pode se afirmar que o fenômeno Internet difere dos outros meios de comunicação conhecidos até agora, haja vista que a postura do receptor no rádio e na televisão é meramente passiva, enquanto em relação à Internet o receptor participa selecionando e emitindo informações.

Há várias maneiras de trocar e obter informações através da Internet, dentre as quais: World Wide Web (www), mecanismos de busca, e-mail (correio eletrônico), peer-to-peer, IRC (Internet Relay Chat), VoIP (voz sobre IP), listas de discussão, bate-papos e mensagens instantâneas. A própria rede, por sua vez, é acessada através de diversos meios, caracterizando o típico exemplo de convergência tecnológica, da facilitação no processo de troca de comunicação. A Internet está presente em computadores, celulares, palms, e diferentes aparelhos multifuncionais.

2.3 Princípios para a governança e uso da internet

Mundialmente, a gestão da internet iniciou-se no âmbito militar, visto que a rede era uma ferramenta estratégica de segurança nacional para o governo norte-americano, precursor na temática. Com o desenvolvimento da web, especialmente após a criação do www, houve a gradativa desvinculação com o Estado, caminhando-se para uma gestão encabeçada pela sociedade civil, como aduz Oppermann (2013)

A partir de 1990 a internet deixa de ser uma ferramenta do setor de ensino e passar ser utilizada no setor privado. Segundo LUCERO (2011) os usuários, técnicos e acadêmicos passaram a preocupar-se e focava-se na colaboração para que se construíssem padrões técnicos robustos que não interferissem no desenvolvimento da rede. Não se pode afirmar que nesse período não havia regulamentação, sendo mais adequado colocar como uma auto-regulamentação, na qual os próprios usuários censuravam condutas abusivas entre si, dificilmente extrapolando esse âmbito. Todavia, o crescimento vertiginoso da Internet comercial na metade da década de 90 e os problemas decorrentes da amplitude dessa rede, despontaram o interesse majoritário na regulação da Internet, ou seja, na criação mais formal de mecanismos de governança.

Etimologicamente, “governança” advém do termo grego kyvernao e do latim gubernare que significam guiar, pilotar, dirigir. Para começar, é preciso entender o que seria governança, pois não se confunde com governo no sentido Estado, mas sim a gestão, gerência, administração da estrutura e processos da Internet. Portanto, deve-se entender Governança da Internet como a Administração da Rede Mundial entre Computadores. (LUCERO ,2011)

No entanto a governança da internet envolve a gestão de endereços de IPs, nomes de domínio, protocolos de envio e recebimento de arquivos. Todavia, ela não se limita a essas questões. De acordo com o relatório do Grupo de Trabalho em Governança da Internet das Nações Unidas, a governança da internet pode ser conceituada como:

> o desenvolvimento e a aplicação, por governos, pelo setor privado e pela sociedade civil – em seus respectivos papéis – de princípios, normas, regras e procedimentos de tomada de decisão, bem como de ações programáticas, que devem determinar a evolução e o uso da Interne.(ONU,2015,n.p.)

Percebe-se, pelo conceito da ONU, que existe um componente normativo e programático indissociável do termo. Canabarro (2012) cita, ainda, o caráter político da governança da internet, que não pode ser subestimado. Destarte, há múltiplos interesses estatais e sociais em jogo, que despertam debates acerca da segurança da rede, da privacidade, da liberdade de expressão, do conflito entre informação e proteção de direitos intelectuais, da proteção de dados pessoais e do próprio acesso à rede de forma efetivamente democrática.

No Brasil, Comitê Gestor da Internet no Brasil (CGI.br) foi criado pela Portaria Interministerial nº 147, de 31 de maio de 1995, e foi alterada pelo Decreto Presidencial nº 4.829, de 3 de setembro de 2003, para coordenar e integrar todas as iniciativas de serviços da Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Formado por membros do governo, do setor empresarial, do terceiro setor e da comunidade acadêmica, o CGI.br representa um modelo de governança na Internet pioneiro, no que diz respeito à efetivação da participação da sociedade, nas decisões envolvendo a implantação, administração e uso da rede. (CGIBr,2009,n.p.)

Patrícia (2015, p. 22) cita Corrêa (2002, p. 17-18): “O Comitê Gestor Internet do Brasil é o maior exemplo da tendência mundial a tornar a Grande Rede algo desvinculado do Poder Público, incentivando a participação da sociedade civil na formulação de diretrizes básicas para o desenvolvimento organizado.”

> O Comitê Gestor da Internet no Brasil – CGI.br, reunido em sua 3ª reunião ordinária de 2009 na sede do NIC.br na Cidade de São Paulo/SP, decide aprovar a seguinte Resolução: CGI.br/RES/2009/003/P- PRINCÍPIOS PARA A GOVERNANÇA E

USO DA INTERNET NO BRASIL. Considerando a necessidade de embasar e orientar suas ações e decisões, segundo princípios fundamentais, o CGI.br resolve aprovar os seguintes princípios para internet no Brasil:

1. Liberdade, privacidade e direitos humanos - O uso da internet deve guiar-se pelos princípios de liberdade de expressão, de privacidade do indivíduo e de respeito aos direitos humanos, reconhecendo-os como fundamentais para a preservação de uma sociedade justa e democrática.
2. Governança democrática e colaborativa - A governança da internet deve ser exercida de forma transparente, multilateral e democrática, com a participação dos vários setores da sociedade, preservando e estimulando o seu caráter de criação coletiva.
3. Universalidade - O acesso à internet deve ser universal para que ela seja um meio para o desenvolvimento social e humano, contribuindo para a construção de uma sociedade inclusiva e não discriminatória em benefício de todos.
4. Diversidade - A diversidade cultural deve ser respeitada e preservada e sua expressão deve ser estimulada, sem a imposição de crenças, costumes ou valores.
5. Inovação - A governança da internet deve promover a contínua evolução e ampla difusão de novas tecnologias e modelos de uso e acesso.
6. Neutralidade da rede - Filtragem ou privilégios de tráfego devem respeitar apenas critérios técnicos e éticos, não sendo admissíveis motivos políticos, comerciais, religiosos, culturais, ou qualquer outra forma de discriminação ou favorecimento.
7. Inimputabilidade da rede - O combate a ilícitos na rede deve atingir os responsáveis finais e não os meios de acesso e transporte, sempre preservando os princípios maiores de defesa da liberdade, da privacidade e do respeito aos direitos humanos.
8. Funcionalidade, segurança e estabilidade - A estabilidade, a segurança e a funcionalidade globais da rede devem ser preservadas de forma ativa através de medidas técnicas compatíveis com os padrões internacionais e estímulo ao uso das boas práticas.
9. Padronização e interoperabilidade - A internet deve basear-se em

padrões abertos que permitam a interoperabilidade e a participação de todos em seu desenvolvimento.

10. Ambiente legal e regulatório - O ambiente legal e regulatório deve preservar a dinâmica da internet como espaço de colaboração.(CGI/BR,2009,n.p.)

3 – CRIME

3.1 – Conceito

O conceito de crime no Brasil, não é definido legalmente, deixando para a doutrina essa definição. Há um critério de distinção, na Lei de Introdução ao Código Penal, do que seja crime e contravenção penal, mas no que consta no artigo 1 desta lei, não é possível encontrar os elementos que levem ao conceito de infração penal.
A doutrina desenvolveu com o tempo, o conceito de crime, sendo que surgiram diversas teorias para explicar esse conceito.(GRECO,2017). Assim acabou tendo que ficar a cargo dos doutrinadores tentarem nos passar uma definição exata do que seria crime, dentre muitos temos Celso Delmanto, que acabou se destacando um pouco com o seu conceito, onde o mesmo diz que crime é “a violação de um bem jurídico penalmente protegido”. (DE PAULA,2018)

O decreto lei 3.914/41, traz uma definição, ainda que incompleta segundo alguns autores, do que é crime:

> Art 1º Considera-se crime a infração penal que a lei comina pena de reclusão ou de detenção, quer isoladamente, quer alternativa ou cumulativamente com a pena de multa; contravenção, a infração penal a que a lei comina, isoladamente, pena de prisão simples ou de multa, ou ambas, alternativa ou cumulativamente

Welzel apud Rogério Greco p59 cita: “A tipicidade, a antijuridicidade e a culpabilidade são três elementos que convertem uma ação em um delito. A culpabilidade – a responsabilidade pessoal por um fato antijurídico – pressupõe a antijuridicidade do fato, do mesmo modo que a antijuridicidade, por sua vez, tem de estar concretizada em tipos legais. A tipicidade, a antijuridicidade e a culpabilidade estão relacionadas logicamente de tal modo que cada elemento posterior do delito pressupõe o anterior

O conceito clássico de delito, elaborado por Von Liszt e Beling, diz que uma ação que produz uma modificação no mundo exterior, vinculado por um nexo de

casualidade,ou seja neste modelo estavam presentes o aspecto objetivo(tipicidade e antijuricidade) e o aspecto subjetivo(culpabilidade).(BITENCOURT,2012, p.582).

Von Liszt e Beling elaboraram o conceito clássico de delito, representado por um movimento corporal (ação), produzindo uma modificação no mundo exterior (resultado). Uma estrutura simples, clara e também didática, fundamentava-se num conceito de ação eminentemente naturalístico, que vinculava a conduta a o resultado através do nexo de causalidade. Essa concepção clássica do delito mantinha em partes absolutamente distintas o aspecto objetivo, representado pela tipicidade e antijuridicidade, e o aspecto subjetivo, representado pela culpabilidade. Aliás, como afirmava Welzel, na 2ª edição do Tratadode Liszt (1884) foi desenvolvida pela primeira vez, claramente, a separação entre a antijuridicidade e a culpabilidade, de acordo com os critérios objetivos e subjetivos . (BITENCOURT,2012, p.582).

3.2 Conceito formal e material de crime

Há duas conceituações, no que diz respeito a crime:

a) formal; é a definição em que crime é toda ação humana que não é permitida pela lei penal.

b) material. Nesta, define que crime é toda ação humana lesiva de um interesse capaz de lesar os fatores de existência, de conservação e de desenvolvimento da sociedade.

Esses conceitos não conseguiram definir com precisão o conceito de crime. Conforme os ensinamentos de Bettiol, “duas concepções opostas se embatem entre si com a finalidade de conceituar o crime: uma, de caráter formal, outra, de caráter substancial. A primeira atém-se ao crime sub especie iuris, no sentido de considerar o crime ‘todo o fato humano, proibido pela lei penal’. A segunda, por sua vez, supera este formalismo considerando o crime ‘todo o fato humano lesivo de um interesse capaz de comprometer as condições de existência, de conservação e de desenvolvimento da sociedade’.”

Sob o aspecto formal, crime seria toda conduta que atentasse, que colidisse frontalmente contra a lei penal editada pelo Estado. Considerando-se seu aspecto material, conceituamos o crime como aquela conduta que viola os bens jurídicos

mais importantes. Na verdade, os conceitos formal e material não traduzem com precisão o que seja crime.

3.3 Conceito analítico de crime

O conceito analítico do crime tem por definição a analise dos elementos que compõem a infração penal, permitindo depois desta analise chegar a conclusão se uma ação é crime ou não.

O conceito analítico do crime procura, como sua própria denominação sugere, analisar os elementos ou características que integram a infração penal, permitindo ao intérprete, após sua averiguação, concluir ou não pela sua prática. Assis Toledo, discorrendo sobre o tema, esclarece que, “substancialmente, o crime é um fato humano que lesa ou expõe a perigo bens jurídicos (jurídico- -penais) protegidos. Essa definição é, porém, insuficiente para a dogmática penal, que necessita de outra mais analítica, apta a pôr à mostra os aspectos essenciais ou os elementos estruturais do conceito de crime. E dentre as várias definições analíticas que têm sido propostas por importantes penalistas, parece-nos mais aceitável a que considera as três notas fundamentais do fato- -crime, a saber: ação típica (tipicidade), ilícita ou antijurídica (ilicitude) e culpável (culpabilidade). O crime, nessa concepção que adotamos, é, pois, ação típica, ilícita e culpável.”(GRECO,2017)

4 - CRIMES CIBERNÉTICOS

4.1 - Conceitos

Os crimes cibernéticos recebem muitas denominações. Spencer Toth (2015, p 55) fala que a expressão crimes de informática não é usada de maneira uniforme pela doutrina, que apresenta outras nomenclaturas para o mesmo estudo, então podemos encontrar denominações como: crimes da era da informática, crimes mediante computador, crimes cibernéticos, crimes eletrônicos, crimes tecnológicos, crimes digitais, crimes high-tech, crimes virtuais e etc..

4.2 - Condutas Danosas Através da Internet ,Rede ou Ciberespaço.

Apesar dos benefícios trazidos pela internet, que se mostraram uma importante ferramenta para a difusão da informação no âmbito mundial, vieram também com esse desenvolvimento algumas condutas danosas para usuários dos meios virtuais. Esses eventos passaram a ser conhecidos como crimes cibernéticos, os quais se incorporaram ao elenco de delitos contemplados pelo código penal.

Essa nova modalidade criminal ainda esta sendo analisada e estudada com a finalidade de se criar mecanismos legais que melhor se adequem ao combate destes crimes. Enquanto isso o aparato policial procura elucidar esses delitos com os meios que possuem atualmente, o que tem evitado maior dano por parte destes delinquentes.

Mas a população tem que fazer a sua parte, não esperando que o legislativo, a policia ou “as autoridades” resolvam a questão, procurando a sua proteção individual e com isso virar estatística destes crimes.
Entre estas novas formas de ataque no mundo virtual, podemos destacar algumas:

- Vírus de Computador

Um vírus de computador , é um código de computador que pode se replicar pela modificação de outros arquivos e programas para inserir código para replicação posterior. Essa característica singular é o que diferencia o vírus de outros tipos de ataques cibernéticos. Outra característica discriminante é que o vírus para se replicar necessita de assistência do usuário, como compartilhar uma unidade USB ou clicar em um anexo de e-mail. O vírus pode realizar algumas tarefas maliciosas ,como destruir arquivos importantes ou roubar senhas. (GOODRICH/TAMASSIA,2012,p.177). Segundo Ferreira e Araújo,em sua obra intitulada Política de segurança da informação – Guia Pratico para a Elaboração e implementação esse é um dos principais problemas de segurança da informação .O vírus é um programa ou código que se duplica; o vírus pode não fazer nada, a não ser, propagar-se e deixar o programa infectado funcionar normalmente. Mas, depois de se propagar silenciosamente por um período, ele pode exibir mensagens ou pregar peças.(FERREIRA/ARAÚJO, p. 92).

- Ransomware

Ransomware é um tipo de código malicioso que torna inacessíveis os dados contidos em um equipamento, como regra utilizando criptografia, e que exige pagamento de resgate,em inglês “ransom”, para restabelecer o acesso ao usuário.O pagamento do resgate geralmente é feito via bitcoins.(CERT,2011,n.p.)

- Cavalo de Troia

Um cavalo de troia é um programa utilitário que realiza um trabalho melhor do que um programa padrão existente, como exibir de forma bonita as pastas e arquivos de um sistema de arquivos, ao mesmo tempo em que está realizando uma tarefa maliciosa secreta.(GOODRICH;TAMASSIA ,2012,p.185).

- Vermes de Computadores

Um verme de computador é um programa malicioso que espalha cópias de si mesmo sem a necessidade de se injetar em outros programas, e, geralmente, sem interação humana.(GOODRICH;TAMASSIA,2012, p.197).os vermes são responsáveis por consumir muito recursos devido a grande quantidade de copias de si mesmo que costumam propagar e com isso afetando o desempenho da rede e de computadores.(CERT.br,2011,n.p.)

- Rootkits

Um rootkit é um tipo especialmente furtivo de malaware. Geralmente alteram utilitários do sistema ou do próprio sistema operacional para evitar detecção.(GOODRICH;TAMASSIA,2012, p. 192).

- Ataques de dia zero

O ataque do dia zero é um ataque que explora uma vulnerabilidade previamente desconhecida, mesmo pelos projetistas de software que criaram o sistema contendo essa brecha. O nome vem da ideia de um temporizador especifico que inicia sua contagem no momento em que os projetistas descobrem uma falha em seu programa e o dia em que publicam uma correção para ela.(G00DRICH;TAMASSIA,2012, p.196).

- Botnets

É o controle de uma rede de computadores, que é usada para roubar informações, como número de cartão de credito, e utilizá-las para cometer crimes. Essas redes são chamadas de redes parasitas(botnets) e o controlador desta rede é chamado de controlador de parasitas(bot header).(GOODRICH;TAMASSIA,2012, p.196-197))
Bot é um programa que dispõe de mecanismos de comunicação com o invasor que permitem que ele seja controlado remotamente. Possui processo de infecção e propagação similar ao do *worm*, ou seja, é capaz de se propagar automaticamente,

explorando vulnerabilidades existentes em programas instalados em computadores.(CERT,2011,n.p.).

- Adware

O ADWARE é uma forma de programa de invasão de privacidade que exibe anúncios na tela de um usuário sem o seu consentimento. (GOODRICH;TAMASSIA,2012, p.199)

- Spyware

O spyware é um programa de invasão de privacidade que é instalado no computador de um usuário sem o seu consentimento e que coleta informação sobre o mesmo, sobre seu computador ou sobre o uso de seu computador, sem o seu consentimento.(GOODRICH;TAMASSIA ,2012,p.200).

4.3 - Pornografia Infantil

A internet tem como característica a facilidade de acesso, sendo que essa tem abrangência todas as faixas de idade, sendo assim há facilidade as crianças a terem acesso a páginas que propiciam aos criminosos contato com crianças, onde antes o contato entre criminoso e vitima eram feitas possivelmente em pessoa, hoje podem ser feitas virtualmente, facilitando as ações dos criminosos.sobre isso:

Qualquer pessoa, em qualquer lugar do mundo, desde que conectada à rede mundial de computadores-internet, o mais poderoso meio de comunicação da atualidade-,poderá acessar o conteúdo de páginas publicadas por um criminoso. E é cada vez mais precoce o uso , pelas crianças e adolescentes, da rede, sendo certo que elas estão muito expostas ao assédio de criminosos. (MORGADO ,2012, p.11)

O Brasil é um dos quatro maiores polos de divulgação de pornografia infantil do mundo, concorrendo com os Estados Unidos, Coreia do Sul e Rússia, segundo a ONG Rainbow Phone. Nesse quadro assustador, a Internet é um facilitador do contato entre criminosos, permitindo sua organização em comunidades e troca de informações, fotos e vídeos(.MORGADO,2012 n.p.)

Portanto, se um crime cibernético ocorreu no Brasil, estará sujeito à jurisdição brasileira, sendo dever do Estado investigar e reprimir as condutas delituosas praticadas e fazer cumprir as decisões emanadas de juiz brasileiro para a efetiva apuração do delito, sem a necessidade de cooperação internacional para o cumprimento da decisão. (MPF, 2018,p.g. 36)

5 - LEGISLAÇÃO INTERNACIONAL EM RELAÇÃO AOS CRIMES CIBERNÉTICOS.

Yury Fedotov (2018),chefe do Escritório das Nações Unidas sobre Drogas e Crime cita um estudo recente estimou o custo global dos cibercrimes em 600 bilhões de dólares.

Assim sendo um valor exorbitante que não sendo combatido este tipo de crime tende a aumentar, gerando prejuízo cada vez maior para as nações que são vitimas deste crime.

5.1 – Convenção de Budapeste.

A convenção de Budapeste (ETS 185), é um meio eficaz para o combate aos crimes de internet, criado pela comunidade europeia, em 23/11/2001 ,Trinta países fizeram adesão ao Tratado de prevenção e combate aos crimes praticados na rede mundial ou com o uso do computador. A Convenção tem como objetivo obter a cooperação de todos os signatários para que adotem medidas legislativas em seus países, assim como o ações preventivas e repressivas no combate as infrações e ofensas praticadas na rede, e com o uso desta como instrumento.(KAMINSKI,2001,n.p.)

O tratado tem como diretrizes:

> (Titulo 1) Ofensas contra a confidencialidade, integridade e disponibilidade de dados de computador e sistemas: acesso ilegal (no todo ou em parte sem autorização), interceptação ilegal (por meios técnicos, incluindo emissões eletromagnéticas); interferência nos dados (dano, obliteração, deterioração, alteração ou supressão de dados); interferência em sistemas (distúrbios sérios no funcionamento); abuso de dispositivos (incluindo programas de

computador, senhas, códigos e dispositivos de acesso);

(Título 2) Ofensas relacionadas a computadores: falsificação (utilização de dados falsos como se verdadeiros fossem, estejam inteligíveis ou não) e fraude (ocasionando perda de propriedade para outrem);

(Título 3) Ofensas relacionadas ao conteúdo: pornografia infantil (produzir, oferecer, tornar disponível, distribuir, transmitir, angariar, ter em posse);

(Título 4) Ofensas relacionadas à infração da propriedade intelectual (observando-se a Convenção de Berna, versão de Paris e o Tratado sobre Direitos Autorais da Organização Mundial da Propriedade Intelectual - OMPI ou WIPO);

(Título 5) Responsabilidade subsidiária e sanções: esforço e auxílio ou colaboração; responsabilização corporativa (crimes cometidos por pessoas jurídicas em seu próprio benefício ou de pessoa natural, utilizando-se de poderes de representação, procuração ou controle); sanções e critérios (persuasivos, proporcionais e dissuasivos, incluindo a pena de privação da liberdade, bem como penas pecuniárias).(KAMINSKI,2001,n.p.)

6- MARCO CIVIL

6.1 - Princípios fundamentais do Marco Civil da Internet

Neutralidade da rede

Não permite que provedores conexão cobrem valores diferentes dos usuários com base no que acessa. Isso significa que a empresa não pode oferecer uma assinatura mais em conta para prover acesso a e-mail e redes sociais e outro de maior valor para acesso total a rede mundial.estando a rede neutra, os provedores somente podem cobrar pela velocidade com a qual o usuário se conecta; com a mesma velocidade para todos os sites e o usuário pode escolher por qual quer acessar.(PORTAL FIOCRUZ,2011,n.p.)

Liberdade de expressão

Enseja que todos os usuários tenham igual direito de passar informações e opiniões na internet. Com isso, o que for colocado na rede só pode ser retirado com permissão de quem o criou ou com ordem judicial e os provedores de acesso e de serviços não tem que responder pelo que os usuários colocam na rede. (PORTAL FIOCRUZ, 2011, n.p.)

Privacidade

Implica que provedores e sites não tem permissão para usar informações de quem acessa com fins comerciais, mas têm que manter armazenados esses dados no prazo mínimo de seis meses. Esse princípio também obriga empresas estrangeiras a submeterem-se às leis do nosso país de segurança à informação, mesmo que os centros de armazenamentos de dados (datacenters) estejam baseados fora do país. (PORTAL FIOCRUZ, 2011, n.p.)

O Marco Civil é a forma para que exista a neutralidade da própria rede, em que não permita que empresas possa utilizar modelos que propiciem só o próprio lucro sem observar a forma livre do usuário utilizar a internet. O MC tem como foco a neutralidade,tendo em vista a proteção dos princípios da rede, de forma que a rede se mantenha livre e aberta.A neutralidade tratado no marco civil é a do acesso à

Internet, tanto para o usuário como para quem promove a infraestrutura da rede, atuando no roteamento e encaminhamento de pacotes na internet. De forma que, a neutralidade pretende impedir que o usuário tenha total acesso aos conteúdos colocados na rede. Existem locais na rede que são bloqueados, como sites de segurança, alguns governos, impedem o acesso a seus domínios. De forma que o que se tem acesso é o que é permitido, sendo considerada a rede possível, não a rede ideal em que todos tem acesso ilimitado a todos conteúdos. O que se tem como objetivo é que esta redá permitida seja de acesso aberto a todos os usuário, sem filtros e bloqueios, negando a possibilidade de empresas só tornarem possível que o individuo vejam o que elas permitem. (GETSCHKO,2015,n.p.)

> ‘”Todo ser humano tem direito à liberdade de opinião e expressão; este direito inclui a liberdade de, sem interferência, ter opiniões e de procurar, receber e transmitir informações e ideias por quaisquer meios e independentemente de fronteiras.” ‘
>
> (DECLARAÇAO UNIVERSAL DOS DIREITOS HUMANOS,1948**)**

No ano de 2009, o Comitê Gestor da Internet no Brasil (CGI.br) ,entidade civil sem fins lucrativos coordenador das iniciativas de serviços relacionados à internet no nosso país, criou um documento que passou por varias consultas e audiências públicas. A partir dos debates, tem origem o projeto de lei 2126/11, que chegou ao Congresso Nacional em 2011. Os principais pontos geradores de discussões são a privacidade, a neutralidade da rede, a liberdade de expressão, a instalação de servidores no nosso país e deveres sob competência do governo.O Marco Civil da Internet tem como objetivo principal propiciar segurança jurídica aos usuários da rede, sejam eles internautas, empresas, provedores e Administração Pública. Ainda que até hoje não houvesse um específico instrumento regulatório da internet no Brasil, há muitos anos a jurisprudência vem sendo construída de forma aleatória e, muitas vezes, contraditória. A nova lei, portanto, define fundamentos, princípios, objetivos e direitos na utilização da internet, além de criar normas de caráter processual para a proteção destes direitos. Sendo assim, estabelece-se um marco

legal que certamente uniformizará entendimentos ainda controversos nos tribunais do Brasil. Outro objetivo evidente da nova norma é garantir os direitos à liberdade de expressão e privacidade dos usuários..(PEREIRA,2014,n.p.)

O Marco Civil está dividido em cinco partes..O primeiro capítulo trata basicamente dos fundamentos e princípios do uso da rede no Brasil. Os mais importantes fundamentos, que também podem ser entendidos como pressupostos da utilização da internet, são a liberdade de expressão, os direitos humanos e a cidadania, a livre iniciativa e a defesa do consumidor.Dentre os princípios – normas de caráter mais genérico que norteiam a aplicação dos direitos ali previstos – encontram-se novamente a liberdade de expressão, a privacidade e a livre iniciativa, além da neutralidade, estabilidade e funcionalidade da rede. A Lei ainda afirma que o uso da internet tem por finalidade promover o amplo direito de acesso à rede, às informações e conhecimentos nela difundidos, a inovação e difusão tecnológicas e a adesão a padrões tecnológicos “abertos”.O segundo capítulo estabelece que são direitos e garantias dos usuários a inviolabilidade da intimidade, da vida privada, do sigilo do fluxo de informações e comunicações, a manutenção da qualidade de conexão contratada, a clareza de informações e cláusulas nos contratos de prestações de serviços e políticas de uso da web, tratando como nulas quaisquer cláusulas que ofendam esses direitos.O capítulo terceiro trata da neutralidade da rede. Afirmando que os provedores de serviços da internet não podem cobrar preços diversos a depender da forma que o usuário utiliza a rede mundial, não permite que exista uma obrigação de pagar um valor para ler emails e outro diferenciado para utilizar o facebook. Dispõe, ainda, que a guarda dos registros de conexão, de acesso a aplicações de internet, de dados pessoais e de comunicações privadas devem respeitar a intimidade, vida privada, honra e imagem das partes envolvidas. Ou seja, os provedores não podem vasculhar, nem disponibilizar a terceiros os registros deixados pelo usuário em seu acesso à rede, salvo por ordem judicial. Todo aquele que não obedecer tais normas está sujeito a penalidades que vão desde advertência até a proibição do direito de exercer suas atividades..(PEREIRA,2014,n.p.)

.A lei tende a pacificar bastante a jurisprudência brasileira, ao estabelecer que o provedor somente será responsabilizado se, por ordem judicial, deixar providenciar que se torne indisponível o conteúdo ofensivo ou, em se tratando de conteúdo de

âmbito sexual, o usuário atingido solicitar, por meio de notificação, que este conteúdo seja bloqueado e o provedor não cumprir a solicitação.O quarto capítulo formata diretrizes que determinam o papel da União, Estados, Distrito Federal e Municípios no desenvolvimento da internet. Para tanto, determina que sejam estabelecidos mecanismos de governança eletrônica transparentes e que permitam a participação da sociedade. Disposições claramente voltadas à ganhos na eficiência, celeridade e comunicação entre as várias tecnologias de diferentes estratos de governo, bem como de um caminho mais ágil de acesso pela sociedade aos serviços disponibilizados pelo governo.O último capítulo prevê que o usuário tem a liberdade de utilizar programas que facilitem o controle de acesso de seus filhos menores de idade a conteúdos proibidos, desde que observados os princípios do Marco Civil e do Estatuto da Criança e do Adolescente..(PEREIRA,2014,n.p.)

Depois da aprovação do Marco Civil da Internet, varias propostas foram lançadas no intuito de complementar o texto desta lei, em parte devido ao prazo dilatado entre apresentação e aprovação, já que a tecnologia avança muito rápido e quando o projeto foi apresentado, não havia como prever quais tipos de ferramentas novas iriam surgir, criando assim a necessidade de atualização do alcance da lei.Sobre isso:

> É nesse universo que estão englobadas 58 propostas para alterar o MCI – e elas não param de surgir. O leque é amplo: há tentativas de legislar sobre o bloqueio de aplicativos como o Whatsapp, o limite para franquia de dados, a privacidade na rede, entre outros.
>
> "É muito significativo que uma lei aprovada em 2014, e que só foi regulamentada em 2016, tenha uma quantidade expressiva de projetos de lei que busquem modificá-la", avalia Bioni.
>
> Esses projetos estão diretamente ligados às discussões travadas pela sociedade civil. Por isso, os picos de proposição de novos projetos vieram em momentos críticos, como os episódios do jogo conhecido como "Baleia Azul", ou os incidentes de bloqueio do WhatsApp em todo o país.
>
> Em alguns temas, as propostas dos parlamentares não têm caráter punitivo. Todos os 21 projetos que tratam de limites para franquia de dados, por exemplo, foram categorizados como "não-punitivos". Mas quando o assunto é liberdade de expressão, o Congresso parece mais disposto a encará-la como uma questão de polícia.

> Estes projetos tratam, em suma, da colisão entre a liberdade de expressão e os direitos de imagem e honra – tocando no chamado “direito ao esquecimento”. Em sua maioria, pretendem alterar a maneira como os conteúdos de postagens de redes sociais e websites devem ser removidos ou desindexados dos buscadores, além de prever punição para quem ofensores. (PÁDUA, 2018, n.p.).

No dia 14 de agosto de 2018, o Presidente Michel Temer sancionou o Projeto de Lei nº 53, que traz normas sobre a proteção e o tratamento de dados pessoais que pássara a vigorar apartir de fevereiro de 2020, traz novos conceitos que fixam tutelas jurídicas anteriores e servem como complementação para regras do Marco Civil da Internet. Considera-se dado pessoal qualquer informação relacionada à pessoa natural identificada ou identificável. Sendo assim, dado pessoal é qualquer dado que possibilite o reconhecimento de um individuo.Os chamados dados sensíveis, são os dados pessoais que trazem a preferência religiosa, partidária, sexual, política, filosófica, dados sobre a origem étnica e racial, e são inclusos também os dados genéticos e biométricos.Estes dados em particular, tem seu tratamento vedado, mas se houver consentimento do sujeito em questão, o tratamento pode ser realizado.(SANTOS,2018,n.p.).

O tratamento de dados é conceituado como toda operação realizada com dados pessoais, incluindo as que se prestam a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação e/ou controle da informação, modificação, comunicação, transferência, difusão ou extração. Existem requisitos necessários para o tratamento de dados, sendo o primeiro o consentimento informado do titular dos dados, tendo que ser expresso o aceite para que haja o uso da informação em operação especifica.No artigo 8º, está explicito que o consentimento pode ser dado por escrito ou por outro meio que demonstre a manifestação de vontade do titular.Há de se destacar que o responsável pelo uso dos dados tem que colocar de forma clara, como os dados vão ser utilizados e o proprietário das informações tem o direito de desistir deste uso. O principio da adequação esta incluso neste processo, no que diz respeito a utilização dos dados

tem que estar em harmonia com o procedimento a que se destina.Outro principio presente é o da necessidade, no qual não cabe a coleta de dados que não são necessários ao processo descrito.A segurança no tratamento de dados é um dos principais norteadores a serem seguidos no que tange ao uso dos dados, uma vez que se não for observado será imposto ao infrator penas e/ou multas.A não discriminação é outro aspecto presente no texto da lei, sendo permitido o uso dos dados para fins lícitos, vedado a utilização para processos ilícitos ou abusivos.(SANTOS,2018,n.p.).

Os agentes responsáveis pelo tratamento de dados são definidos como: o responsável, pessoa natural ou jurídica, de direto público ou privado, encarregada de emitir as deliberações sobre o processo ;operador ,que tem as atribuições de agir de acordo com o que foi normatizado pelo responsável e o encarregado, com a tarefa de receber reclamações dos envolvidos no processo e tomar as devidas providencias. Estão sujeitos a sanções de acordo com o papel que possuem no tratamento dos dados. As sanções vão da advertência, da publicização do fato indo até a multa no valor a 2% do faturamento da pessoa jurídica ou grupo executante no Brasil, calculados com base no total numérico do último exercício financeiro, eliminando os tributos, sendo limitada ao montante de R$ 50.000.000.00 (cinquenta milhões de reais) por cada infração. As empresas que tem atuação no Brasil, mas tem sede no exterior, serão acionadas apartir de sua base no território pátrio.(SANTOS,2018,n.p.).

Observa-se que com a aprovação desta lei sobre tratamento de dados, que antes havia um vácuo no marco civil, mas atualmente, pelo menos em parte, o Brasil conta com mais alguns balizadores para a utilização segura da internet.

7- PANORAMA DOS CRIMES CIBERNÉTICOS NO MUNICÍPIO DE ARACAJU

A cidade de Aracaju pertence ao menor estado do Brasil, Sergipe, mas, o fato de ser pequeno, não significa que o usuário de internet está sujeito a um numero menor de crimes. Segundo a titular da delegacia especializada em crimes virtuais, na cidade de Aracaju ocorrem várias modalidades de delitos informáticos,segundo o CEACRIM a maioria das ocorrências é de estelionato com 31,em depois vem o difamação com 20, injuria com 16 e ameaça com 11. – cometidos através das redes sociais e do whatsApp, nos quais ela observa ser frequente a desculpa dos indivíduos que praticam estas condutas delituosas de que estavam com raiva no momento de praticar a ação de injuria, calunia ou difamação, ou que só replicaram o conteúdo que receberam, pensando que esta ação não teria consequências negativas, pois não foi o autor do comentário. Mas quem repassa esses comentários que difamam terceiros também incorre em crime e também responde por isso

Como se trata de um tipo de criminalidade ainda relativamente recente, é preciso que o pessoal dos departamentos investigativos sejam adequadamente treinados para lidar melhor cm os crimes informáticos. Desse modo, a titular da delegacia especializada informou, que estava previsto o início, em outubro de 2017, de um curso, na ACADEPOL – Academia de polícia do Estado de Sergipe, para preparar servidores de todas as unidades policiais do estado, a fim de estarem capacitados para investigar esse tipo de crime, cujo trabalho até então estava a cargo, somente, da delegacia especializada, o que, doravante, após a conclusão desse treinamento, deverá ser, também atribuição das demais delegacias.

Ela destaca que os indivíduos tem um papel na prevenção dos crimes de internet, o da prevenção, com a utilização de antivirus, evitar clicar em anúncios que aparecem durante a navegação na internet, não mandar fotos intimas ou dados pessoais a terceiros, principalmente os que conhecer por meio de chats ou bate papo informáticos, utilizar senha nos telefones portáteis e também nos programas de comunicação como whatsapp, evitar utilizar wifi público e só conectar ao banco para fazer transações em wifi particular ou com a internet paga do smartfone.

O uso de senha nos smartfones é uma forma de se proteger, mesmo se o telefone for subtraído, pois o individuo que tem a posse do mesmo, precisa de meios

tecnológicos para burlar a senha e ter acesso aos dados da vítima, dando assim tempo hábil para que a vitima do delito possa bloquear o telefone junto com a operadora, para evitar o uso de seus dados e de sua linha.

ESTADO DE SERGIPE
SECRETARIA DE ESTADO DA SEGURANÇA PÚBLICA
SUPERINTENDÊNCIA DE POLÍCIA CIVIL
COORDENADORIA DE ESTATÍSTICA E ANÁLISE CRIMINAL – CEACrim

SOLICITAÇÃO: 22000.001421/2017-35

OCORRÊNCIAS REGISTRADAS NA DELEGACIA DE REPRESSAO A CRIMES CIBERNETICOS

2017

JAN A AGO

FONTE: SSP/PC/SE - BO ONLINE

OBS.: TODOS OS DADOS ESTÃO SUJEITOS A ALTERAÇÕES

OCORRÊNCIAS CRIMINAIS	2017
ESTELIONATO	31
DIFAMACAO	20
INJURIA	16
AMEACA	11
CALUNIA	9
FALSA IDENTIDADE	5
InvasAo de dispositivo informAtico - Art. 154-A	4
EXTORSAO	4
FURTO QUALIFICADO	4
VIOLACAO DE CORRESPONDENCIA	1
LEI 8.069/90 - DIVULGAR PORNOGRAFIA COM CRIANCA/ADOLESCENTE	1
LEI 3.688/41 - ART. 42 PERTURBACAO DO TRAB OU SOSSEGO ALHEIO	1
INJURIA QUALIFICADA	1
INTERRUPCAO/PERTURBACAO DE SERVICO TELEGRAFICO/TELEFONE	1
FALSIFICACAO DE DOCUMENTO PUBLICO	1
FALSIFICACAO DE DOCUMENTO PARTICULAR	1

Sidney Santos Teles
Escrivão da Polícia Civil
Diretor do Ceacrim

CONCLUSÃO

Observa-se que a internet é uma nova ferramenta tecnológica, com muitos atrativos e potenciais nas mais diversas áreas, como a saúde,comunicação,financeiras,entre outras. Mas como tudo que o ser humano cria, tem utilização positiva e também o inverso.

No caso da internet, um dos usos positivos está na comunicação, na qual em tempo real um individuo se comunica com outro a longa distancia, incluindo até imagens, mas esta mesma comunicação pode ser mal utilizada, onde as imagens compartilhadas podem ser utilizados como meio de chantagem, conseguindo assim, o criminoso, vantagem financeira.

Chega-se a conclusão que cuidados com uso da rede são imprescindíveis, pois se não evita que crimes ocorram, os torna mais difíceis de serem aplicados.

Além da ação preventiva, existe a necessidade de uma legislação que seja mais abrangente, que possa alcançar os crimes cibernéticos, punindo os responsáveis por perpetrarem esses atos, pois a policia tem agido dentro da lei atualmente existente, mas em alguns crimes não estão bem tipificados, o que dificulta a ação de repressão a destes delitos.

Com a aprovação do marco civil da internet a regulamentação da internet no Brasil começa a dar os primeiros passos no intuito de normatizar o uso da rede em território pátrio. Entretanto esse é só o primeiro passo, insuficiente para tornar a navegação segura para os usuários, necessitando que outras normas sejam colocadas para que no caso de uma infração ser cometida, se possa ter as ferramentas para a justa punição dos que a cometeram. Outro ponto de avanço é a lei de tratamento de dados, que define o que são dados, seu uso e a proibição do uso destes. Mais um degrau da escada foi alcançado, pois a definição de uma lei que alcance os crimes de internet tem que necessariamente ter as definições do que deve ser protegido, o que não faz parte do marco civil,tornando de suma importância editar normas especificas em descrições do que é permitido ou não fazer na internet.encontra-se em discussão uma nova lei que pretende punir quem faz o uso de “fake news”,ou seja noticias falsas, ação tão disseminada nos dias de hoje na rede,que faz com que o cidadão desavisado ao se depara com uma noticia destas, no mínimo a ficar em pânico, quando não tomar atitudes indevidas e exageradas em relação a fato tão grotescos que vem sendo mostrados a estes.

Enfim não podemos interromper a marcha inevitável do progresso tecnológico nem, tampouco, conter o avanço da globalização, mas é plenamente possível, utilizando-se de mecanismos preventivos adequados, sobretudo cuidando com mais atenção e zelo de nossa privacidade, evitando, assim maior exposição nas redes sociais, a fim de nos proteger, principalmente, da parte sombria e criminosa, que, inevitavelmente tenta invadir nossas vidas com a chegada de nova tecnologia.

REFERÊNCIAS

Atuando para deter o cibercrime. ONUBR. 2018. Disponível em: https://nacoesunidas.org/artigo-atuando-para-deter-o-cibercrime/.>. Acesso em: 10 de out. de 2018.

BITENCOURT, Cezar Roberto. **Tratado de direito penal: parte geral**, 17ª ed. Rev. E atual. São Paulo: Saraiva 2012.

Bloqueio de sites e aplicativos que incentivem ações criminosas está na pauta da CCT. Senado noticias. 2018.Disponível em :< https://www12.senado.leg.br/noticias/materias/2018/08/02/bloqueio-de-sites-e-aplicativos-que-incentivem-acoes-criminosas-esta-na-pauta-da-cct > .acesso em: 21 de out de 2018.

BRASIL,DECRETO-LEI Nº 3.914, DE 9 DE DEZEMBRO DE 1941.Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del3914.htm.> Acesso em:07 de out de 2018.

BRASIL. DECRETO-LEI No 2.848, DE 7 DE DEZEMBRO DE 1940.Disponível em:< código penal http://www.planalto.gov.br/ccivil_03/Decreto-Lei/Del2848.htm >. acesso em:04 de out. de 2018.

BRASIL. Lei Nº 12.965, DE 23 DE ABRIL DE 2014. .Marco Civil. Disponível em:<http://www.planalto.gov.br/ccivil_03/_ato20112014/2014/lei/l12965.htm> Acesso em: 03 out. 2018.

BRASIL. Ministério Público Federal. Câmara de Coordenação e Revisão, 2.**Crimes cibernéticos** / 2ª Câmara de Coordenação e Revisão, Criminal. – Brasília: MPF, 2018.Crimes Cibernéticos - MPF - Vol 3 – 2018.Disponível em: http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes. Acesso em: 01 out. 2018.

CAPETAS, Bruno. **Após marco civil, crescem projetos de lei sobre internet.** revista exame,são Paulo,8 de out. 2016, disponível em < https://exame.abril.com.br/tecnologia/apos-marco-civil-crescem-projetos-de-lei-sobre-internet/ > acesso em: de out. de 2018.

Cartilha de Segurança para Internet - CERT.br. Disponível em: <http://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf>. Acesso em :10 de out de 2018.

CASTELLS, M. (2001), Edição brasileira 2003. **A galáxia da Internet: Reflexões sobre a internet, os negócios e a sociedade**. Rio de Janeiro: Jorge Zahar Editor Ltda.

Computadores. Porto Alegre: Bookman, 2012.
CORNACCHIONE JR.; Edgard B. **Informática aplicada às áreas de contabilidade, administração e economia.** 4. Ed. São Paulo: Atlas, 2012.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet.** 5º ed., São Paulo: Editora Saraiva.

COSTA,Thábata Filizola .**Comentários sobre a governança da Internet no Brasil e o papel do CGI** . Disponível em : < https://thabatafc.jusbrasil.com.br/artigos/387963979/comentarios-sobre-a-governanca-da-internet-no-brasil-e-o-papel-do-cgi?ref=topic_feed > . Acesso em 11 out. 2018.

DECLARAÇÃO UNIVERSAL DOS DIREITOS HUMANOS. Assembleia Geral das Nações Unidas em Paris. 10 dez. 1948. Disponível em: <https://nacoesunidas.org/direitoshumanos/declaracao/ >. Acesso em: 15 out. 2018.

FEDOTOV, Yury. **Atuando para deter o cibercrime**. Disponível em <https://nacoesunidas.org/artigo-atuando-para-deter-o-cibercrime/> acesso em 10 out. 2018

FONSECA FILHO, Cléuzio, **História da computação** [recurso eletrônico] : O Caminho do Pensamento e da Tecnologia – Porto Alegre : EDIPUCRS, 2007.

Fórum de Governança da Internet : **relatórios dos dez primeiros anos do IGF /** Núcleo de Informação e Coordenação do Ponto BR . Disponível em: <https://www.cgi.br/publicacoes/indice/livros/>. Acesso em :10 de out de 2018.

GETSCHKO, Demi,**Reflexões gerais sobre a neutralidade da rede**.Disponível em<http://observatoriodainternet.br/post/reflexoes-gerais-sobre neutralidade>Acesso em : 7 out de 2018.

GOODRICH, Michael T.; TAMASSIA, Roberto. **Introdução à Segurança de**
GRECO, Rogério - **Código Penal Comentado** – 2017 11ediçao editora impetus. Niterói RJ
https://www12.senado.leg.br/noticias/materias/2011/06/08/os-dez-principios-para-a-internet

IBGE - Instituto Brasileiro de Geografia e Estatística**. Pesquisa nacional por amostra de domicílios: Acesso à internet e à televisão e posse de telefone móvel celular para uso pessoal 2016**. Rio de Janeiro; 2018.

KAMINSKI, Omar. **Conheça o Tratado Internacional contra crimes na Internet**.

2001. Disponível em < https://www.conjur.com.br/2001-nov-24/convencao_lanca_tratado_internacional_cibercrimes > . Acesso em de out. de 2018.

KUROSE, James F.; ROSS, Keith W. **Redes de computadores e a Internet: uma abordagem top-down.** 5. ed. São Paulo: Pearson, 2010. 614 p.

MPF. **Em conferência internacional, MPF defende cooperação como forma de combater o cibercrime**. Disponível em:http://www.mpf.mp.br/pgr/noticias-pgr/em-conferencia-internacional-mpf-defende-cooperacao-como-forma-de-combater-o-cibercrime acesso em 13 out. 2018.

OLIVEIRA, Neide Cardoso de. **Educação digital, Ministério Público e as escolas.** Disponível em :https://politica.estadao.com.br/blogs/fausto-macedo/educacao-digital-ministerio-publico-e-as-escolas/. Acesso em: 11 de out. de 2018.

PÁDUA,Luciano.**Parlamentares contra a liberdade de expressão.**Disponível em ;< https://nic.br/noticia/na-midia/parlamentares-contra-a-liberdade-de-expressao/ > . Acesso em: 10 out. 2018.

PEREIRA,Gabriel Senra da Cunha. **Marco Civil da Internet: o que você precisa saber.** Disponível em: < http://cunhapereira.adv.br/marco-civil-internet/ > . Acesso em: 16 out. 2018.

Princípios fundamentais do Marco Civil da Internet. Disponível em :< https://portal.fiocruz.br/documento/principios-fundamentais-do-marco-civil-da-internet > . Acesso em: out 2018

ROSA, Fabrízio. **Crimes de informática.** 2 ed., Campinas: Editora Bookseller, 2006.

SANTOS, Renata.**Sancionada lei de proteção de dados quais as mudanças?** Disponível em < https://renatasantoss.jusbrasil.com.br/artigos/612587703/sancionada-lei-de-protecao-de-dados-pessoais-quais-as-mudancas?ref=topic_feed > acesso em: 21 de out de 2018.

VIANA, André de Paula. **Crimes virtuais e a necessidade de uma legislação especifica.** 2017. Disponível em :http://www.egov.ufsc.br/portal/conteudo/crimes-virtuais-e-necessidade-de-uma-legisla%C3%A7%C3%A3o-especifica . Acesso em: 07 de out. de 2018.

ANEXOS

ENTREVISTA

Com o objetivo principal de conhecer a realidade dos crimes cibernéticos cometidos no Estado de Sergipe, suas características, os cuidados preventivos necessários visando a proteger as pessoas, para não se tornarem vítimas desse tipo de delito, bem como o excelente e proveitoso trabalho da polícia sergipana no sentido de coibir a criminalidade virtual, foi realizada a presente entrevista, com a titular da delegacia especializada no combate aos crimes informáticos.

Não é demais reconhecer o grande empenho dos nossos organismos policiais, especialmente a Polícia Civil do Estado de Sergipe, conjuntamente com as de outros estados da Federação e a Polícia Federal, que, com o seu apurado preparo técnico, apesar dessa modalidade de crime ser ainda muito nova, tem elucidado um grande número de delitos, além de alertar a população para que não facilite a sua ocorrência, através de excessiva exposição nas redes sociais.

Por oportuno, agradecemos à titular da delegacia especializada pela gentileza de nos ter recebido em seu gabinete e haver concedido esta importante entrevista, contendo muitas informações bastante esclarecedoras, a respeito do tema deste trabalho, sem as quais dificilmente se teria uma ideia mais aprofundada sobre a prática, investigação e elucidação dos crimes informáticos.

Qual a área de abrangência da delegacia?

A nossa abrangência aqui, além de Aracaju, estende-se a algumas cidades circunvizinhas, que são consideradas pelos regulamentos internos como integrantes da coordenadoria da capital, como, por exemplo, Itaporanga d´Ajuda, São Cristóvão, Nossa Senhora do Socorro, Laranjeiras. Essas cidades fazem parte da coordenadoria da capital e nós temos abrangência sobre elas.

Aqui, na capital, quais são os principais crimes?

O maior volume é de crimes contra a honra – injúria, calúnia, difamação, ameaças, cometidos através de redes sociais, de whatsApp. E, também, um dos grandes carros chefe é o estelionato, a invasão de contas, tudo através da internet, do uso de site de compras. Por meio de portaria interna, os crimes de maior

potencial ofensivo, como injúria, calúnia, difamação, quando cometidos pela internet são considerados crimes cibernéticos próprios. Desse modo, há os próprios e impróprios; os próprios são crimes cibernéticos propriamente ditos, que só podem ser praticados pela internet, e os crimes cibernéticos impróprios, que são cometidos por meio de carta, um telefonema, uma palavra ou até mesmo pela internet; esses crimes, quando praticados pela internet são considerados crimes cibernéticos impróprios; então, tratando-se de crimes de menor potencial ofensivo, ainda que cometidos pela internet, são apurados por outras delegacias. Agora em outubro (2017), está previsto o início de um curso, na ACADEPOL – Academia de Polícia do Estado de Sergipe, para preparar servidores de todas as unidades policiais do Estado, a fim de estarem aptos a investigar esse tipo de crime, que antes estava a cargo, somente, da delegacia especializada, o que deixou de ser. A internet é um meio comum para se praticar crimes, não é mais um meio especializado; a maioria dos crimes está deixando de ser praticada pelos meios comuns para ser cometida pela internet, então, todas as unidades precisam ter servidores habilitados para esse tipo de investigação; assim, esses crimes de menor potencial ofensivo são encaminhados às delegacias metropolitanas, enquanto a delegacia especializada apura os crimes de estelionato, mediante fraudes acima de dez salários mínimos, bem como apuramos, também, os crimes de internet próprios, como, por exemplo, uma invasão de um site, que é um crime cibernético próprio, que ficam, aqui, na delegacia. No ano passado (2016), foi editada uma portaria modificando um pouco essas atribuições; além disso, essa especializada dá apoio às investigações realizadas por outras unidades, quando elas recorrem a essa especializada.

Agora, particularmente, com respeito ao ataque a instituições, a senhora teria como observar quantos são partidos daqui ou vindos de fora?

Depende, há muitos casos que são de fora, na sua maioria, são de fora, pelo menos os que nós investigamos. Estou aqui há um ano e meio, e o que nós investigamos, até então, partiram de fora, mas há casos que estão localizados aqui; nesses casos, há uma... Mas você está falando sobre quais crimes, estelionatos?

Mais focados em instituições, como o INSS – Instituto Nacional do Seguro Social?

Em regra, esses são de fora, aí a gente precisa manter um contato com as instituições dos outros estados, a vítima e, daí, se dá início à investigação; muitas vezes, para fazer a identificação, contamos com a colaboração da polícia de outros estados para fazer diligências, identificar etc.

E, no caso, em termo de quantidade, os crimes contra a honra são a maioria?

R–São injúria, difamação, crimes contra a honra e estelionato, esses são os grandes números. Se você quiser pode solicitar números oficiais. Como é um trabalho de pesquisa acadêmica, você pode fundamentar e solicitar junto ao CEACRIM – Coordenadoria de Estatística e Análise Criminal, que é o centro de estudos e análises criminais, que vai poder lhe dizer, em termos de estatística, entendeu?, quantos crimes conta a honra, o total de crimes etc., eles compilam todos os dados, boletins de ocorrência de todo o estado; se você quiser somente os da capital, ou do interior, ou, ainda, do estado todo, enfim, é só procurar o CEACRIM.

No geral, quando a apuração de um crime chega aqui, vamos colocar, por exemplo, uma injúria, daí, para achar o autor, é fácil chegar?

Não é complicado, é um pouco diferente; há algum tempo, a polícia trabalhava mais com prova testemunhal e pericial, hoje, nós temos a prova técnica, que é importante nos crimes cibernéticos. Em regra, tem que se ouvir a vítima, colher as provas materiais; se isso se dá por meio de rede social, então, faz-se a prova documental, pede-se uma autorização judicial e chega-se a uma ordem judicial; a partir daí, nós juntamos os dados e, no início, a investigação está em curso. Na maioria das vezes, consegue-se chegar à autoria; é um pouco mais demorado, porque o trâmite é de certa forma mais burocrático: é preciso pegar uma autorização judicial, a fim de que o provedor forneça os dados, aí, essas informações são analisadas. À medida que seja preciso pedir autorização complementar, nós solicitamos novamente, então, existe um trâmite, digamos, assim, burocrático maior, mas não é impeditivo, na hora da elucidação de um crime, na maioria dos casos, chegamos à autoria.

Eu estava pesquisando: o individuo entra, consegue mascarar, não entra pela internet normal, mas pelo Thor?

É Thor, deep web, mas, mesmo assim, nesses casos, existem formas de se chegar, agora, no ponto do crime; nós nunca temos uma elucidação de cem por cento e nem um caso, nem um crime, que é apurado normalmente pela polícia, é, seja roubo, seja homicídio, seja tráfico de drogas, não se consegue uma elucidação de cem por cento, mas os índices de elucidação são altos.

Agora, vamos falar sobre a vítima, o que dá para fazer de proteção, antivírus, antispywere, nem isso é seguro, frewall?

Então, nós vamos precisar orientar as pessoas, como trabalhamos muito com estelionato, no sentido de ter cuidado com o acesso; o pessoal está navegando e, de repente, surge uma oferta de um produto, aí, a pessoa vai e clica naquele link, que, às vezes, leva até o nome de uma loja, digamos, uma loja de compras, como Lojas Americanas, o Extra, só que o link lhe direciona para um site que não é o das Americanas, não é o do Extra; nós estamos comprando um produto e não estamos, pois, na verdade, estamos sendo vítimas de um golpe, entendeu? Então, nós pedimos para que as pessoas sempre que forem, por exemplo, fazer uma compra, digitar o endereçamento eletrônico da loja, evitar acessar anúncios que são direcionados para o seu computador, evitar fazer transações bancárias com Wi-Fi público, ou outros tipos de acessos que, por exemplo, às vezes, as pessoas utilizam uma senha única para tudo; aí, chegam a um restaurante, aeroporto, e usam o Wi-Ffi, que é uma porta de entrada, devendo evitar, para maior segurança, esse tipo de acesso. O celular é um dos ambientes mais seguros para você fazer uma transação bancária, e até mais seguro que um computador normal, a não ser se você estiver com a sua internet ou com o seu W-Fi particular, por que, se estiver com o w-fi público, está dando uma brecha... Nomeia o Wi-Fi como se fosse o Wi-Fi da empresa, como vou saber? Assim, deve-se evitar fazer transações, acessando e-mail com Wi-Fi público, tirar uma foto etc. Agora, se precisa digitar alguma coisa, via internet, utilize uma senha sempre com sua internet particular, privada. Outra questão que nós orientamos é a respeito das senhas: trocar as senhas com

frequência, não ter uma senha para tudo. Você tem um Facebook, uma conta no Facebook, tem um e-mail de recuperação, caso precise, no caso de esquecer sua senha, aí, a senha do e-mail de recuperação é igual à senha do seu perfil do Facebook, que dizer se a pessoa hakear o seu perfil, automaticamente ela haqueou o seu e-mail. Isso acontece, porque é a mesma senha, entretanto, se você colocar a senha diferente, por exemplo, você vê que seu Facebook foi haqueado, então, solicita uma alteração de senha, que vai para um e-mail que não está haqueado, e consegue acessar sua nova senha. Há alguns casos em que o e-mail foi haqueado, cuja senha é igual, em que você perdeu o acesso, tanto da conta do Facebook, quanto do e-mail. As pessoas usam data de nascimento e aí fica fácil, coloca a senha fácil para lembrar, então, é melhor ela estar em um lugar seguro, na casa dela. Outra coisa, também, é você ter uma conta no Facebook, e resolve entrar no Instagram, então, vincula sua conta no Instagram ao Facebook, ou vai participar, por exemplo, de um aplicativo de compras, aí ele pergunta: quer entrar pelo Facebook ou pelo Instagram? Em regra, você responde sim, que é para não ter que preencher tudo e realizar um novo cadastro. Se você tiver uma dessas contas haqueada, que dá acesso a tudo, é algo a ser evitado; são pequenos cuidados que as vítimas devem ter, desconfiando de tudo, inclusive de propostas muito interessantes. Temos aqui inúmeros casos de fraudes aplicadas pelo olx, esses sites de venda, que veiculam anúncios de produtos, aí, a pessoa vê um celular que custa três mil reais, de repente, está sendo anunciado por mil e quinhentos reais, acha que está fazenda um excelente negócio e, na verdade, não está; aí, vai, faz o depósito na conta, que não está no nome da pessoa, com possibilidade de ser vítima de fraude. Você tem que verificar, antes, a procedência, porque, depois que fizer o depósito e constatar que não recebeu o produto, vai verificar na internet qual é a classificação dos vendedores, sites etc., tendo a informação de que aquilo ali era fraude. Por que não checaram antes? Nos crimes comuns, nós sempre orientamos a vítima: uma mulher deve evitar andar sozinha, em local ermo e à noite; que as pessoas evitem estar falando ao celular no meio da rua; são cuidados para que as pessoas não se tornem uma vítima potencial, mesmo na internet, no caso, de um crime cibernético. Ao acessar todos os tipos de links que são encaminhados, neles, pode existir um programa malicioso, que é a entrada, justamente, a partir daquele software, por exemplo, você recebe um link no grupo do qual faz parte – acesse aqui, como se fosse uma notícia, então você acessa ali, então, permitiu a instalação de um

software malicioso, através do qual todos os dados do seu celular serão capturados e transmitidos para outro dispositivo. Existe a dupla verificação no whatsApp: você tem senha no whatsApp – é muito interessante –, porque, às vezes, a pessoa pegou o seu celular e conseguiu haquear sua senha, não necessariamente, vai conseguir ter acesso a sua conta do whatsApp, mas, se você coloca a senha do celular igual à do whatsapp, para facilitar – as pessoas dizem que têm tantas senhas para decorar e, aí, fazem uma só para tudo; o correto seria usar duas, três, criar um certo padrão, para que variem um pouco uma das outras, mas variem, e para facilitar a lembrança, usar, por exemplo, mudar uma letra a cada senha, senão vira alvo dos hackers; usar frases, como “vou sair daqui” ou “não vou sair daqui”, alguma variação simples, para que você consiga lembrar a sua senha, mas para quem estiver haqueando, vai ser difícil, sai da lógica.

Sobre colocar tudo no Facebook?

Não recomendamos. Em nossas palestras, pedimos que se tenha muita cautela em relação à exposição; existe uma cultura, hoje em dia, que o meio cibernético criou, que chamam de stalker, o perseguidor, através da qual estamos atraindo o perseguidor para a nossa vida; as vezes, não são perseguidores totalmente do mal, pessoas que querem nos fazer mal, mas as que passam a querer saber da nossa vida, com quem andamos, onde vamos, o que comemos, e isso traz consequências negativas. No mesmo jeito que podem começar a estalkear você, porque acham que sua vida é curiosa, as pessoas informam qual academia que frequentam, qual o horário da academia etc.

Sobre comentários na internet?

Comentamos, nas nossas palestras, o seguinte: não fale na internet o que você não falaria pessoalmente, porque as pessoas acham que a internet é um meio, é uma terra sem lei; lá, eu estou escondido atrás do computador, aí, eu posso xingar, posso dizer que vou bater nas pessoas, que as pessoas merecem ser linchadas, que eu posso, digamos assim, praticar injúrias racistas, que são muito comuns, preconceito, porque estou sob o manto da internet. A nossa constituição permite a liberdade de expressão, mas proíbe o anonimato, então, quando se publica alguma

coisa na internet, há alguma responsabilidade por aquilo. Nós já tivemos casos em que as pessoas foram indiciadas por prática criminosa, porque discordaram da atitude de alguém na internet; falaram da vida de alguém, uma pessoa pública, um dono de uma escola, um político e, aí, foram na rede social para dizer que essa pessoa merecia ser linchada, que essa pessoa é um mau caráter, porque teve essa opinião, e essas pessoas foram responsabilizadas, ao serem chamadas aqui para prestar esclarecimentos, ocasião em que justificam que não fizeram com essa intenção, ah, eu fiz esse comentário porque todo mundo estava comentando, todo mundo que comentou foi responsabilizado, cada um na medida do seu comentário; mas, precisamos ter essa dimensão, por exemplo, divulgação de fake news (notícias falsas), em que as pessoas recebem uma notícia pelo whatsApp, do seu grupo, muitas delas até inicialmente bem intencionadas, acham que estão fazendo um favor, mas, se tivermos o cuidado de colocar no Google, já vai ter meio caminho andado para saber que aquilo ali é uma fake news, e, aí, muitas vezes, temos casos, por exemplo, de traficante que manda foto, estuprador que manda foto, já houve linchamento aqui no Brasil por conta disso; portanto, temos de ter muito cuidado, porque, aí, as pessoas dizem assim: eu não sabia que era fake news, isso não tira a responsabilidade delas, porque se você não sabia que a origem é positiva ou negativa, não divulgue, você só pode divulgar aquilo que sabe a origem, uma vez que está se responsabilizando por aquilo que divulgou, então, no mínimo, cheque antes se realmente é verdadeira, as vezes, há um número de telefone, um disque denúncia, liga para o número para saber se é verdade, se existe, se aquela pessoa realmente praticou um crime, porque senão você esta cometendo um crime, ao divulgar uma notícia, por exemplo, dizendo que aquela pessoa é um estuprador, quando não é, então você está cometendo um crime, de calúnia ou difamação, podendo ser responsabilizado criminalmente, aquilo ali pode ter uma consequência. Nós já tivemos muitos casos aqui, em que um vizinho brigou om outro e, aí, para se vingar, pegou a foto do desafeto e fez uma fake news, dizendo que ele era o traficante do bairro. Entendeu, através desse exemplo, só que essa pessoa fez a notícia, criou a notícia, responde por ela, e todo mundo que recebeu aquela notícia e que repassou também responde, porque vai haver uma responsabilidade por esse ato. No mínimo, verifique antes o conteúdo da notícia, se você tiver interesse em repostar aquilo ali, assim, vai saber em que terreno está pisando.

E, no whatsApp, tem como identificar quem iniciou a rede de postagens?

Tem, sim, pelos contatos, pois fica registrado o número do telefone de quem postou, e, aí, nos vamos rasteando.

Fazendo uma observação sobre a internet, por se tratar de uma tecnologia nova, com a qual as pessoas ainda não estão acostumadas, e que, em uma conversa, se colocam opiniões e o assunto acaba aí, mas a internet postou lá, gerando repercussões.

Exatamente, ainda sobre essa questão de cuidados, essa coisa de que não faça na internet o que você não faria pessoalmente, por exemplo, as pessoas começam a se comunicar com alguém através de um aplicativo, Mensager, Facebook, de repente, mandam fotos, vídeos para eu não sei quem é, eu presumo, mas, realmente, eu não sei; nós temos quadrilhas especializadas, quadrilhas internacionais, especializadas só nisso, realizam contato com as pessoas, ganham a confiança delas, depois fazem com que elas encaminhem vídeos, imagens, nudes, após o que passam a extorquir essas pessoas. Olha, vou mandar para os seus contatos, para a sua família, para a sua esposa, para o seu marido, para os seus filhos, se você não me der tanto, são quadrilhas internacionais, quadrilhas da África do Sul, da China, de diversos lugares do mundo, especializadas nisso; temos vítimas, aqui, em Sergipe, dessas quadrilhas, porque as pessoas não têm os cuidados que normalmente teriam, por exemplo, você chamaria para dentro de sua casa alguém que acabou de conhecer? Mandaria fotos suas, nudes, para um sujeito que você se sentou com ele no bar, ou para uma mulher que acabou de conhecer? Precisamos estar atentos, qualquer pessoa pode ser vítima de um estelionato, e uma das características do estelionato é o convencimento, um poder de convencimento muito forte, eles são bem articulados na fala, nas vestimentas, são sempre pessoas bem vestidas, bem educadas, então, não achamos que o estelionato vai chegar para você de forma truculenta, não, porque, se ele não tivesse essa habilidade, simplesmente, lhe assaltava, não dava um golpe, então, é importante ter cuidados, porque, se fica atento, você já vai desconfiando, epa, tem algo errado aqui! Por que essa pessoa está me pedindo isso? Até com casais, nós orientamos, não mandem nudes, até brincamos, façam nudes ao vivo, é mais

interessante, porque, se faz no celular, ao tirar fotos de sua esposa e de sua namorada, ah, é só para mim, o relacionamento pode acabar, é um fato, mas, ainda que o relacionamento nunca acabe, você vai vender aquele aparelho, formata o aparelho e acha que está salvo, não está. Você, que está fazendo uma pesquisa sobre isso, já deve ter visto que é possível resgatar conversas de um aparelho, então, às vezes, vende, acha que está a salvo e a pessoa vem e faz um procedimento que reseta e recupera as informações. Nós temos vários casos em que as pessoas são extorquidas por causa de imagens íntimas que estavam no seu aparelho; não foi porque eu terminei um relacionamento e a pessoa sacaneou e divulgou, não. Temos um caso de uma pessoa que foi vítima de um roubo, botaram a arma na cabeça e levaram o celular, pronto, conseguiram desbloquear e no telefone havia imagens íntimas – tecnologia nova e as pessoas estão preparadas. Exatamente, alguns cuidados que devemos ter na nossa vida cotidiana e não nos habituamos, ainda, a ter, no ambiente virtual, em regra, o mesmo tipo de comportamento. Assim, não deixamos que uma pessoa desconhecida entre na nossa casa, mas aceitamos, no nosso perfil do Facebook, um desconhecido como amigo, uma pessoa que vimos uma vez, ou, então, que é amigo de um amigo nosso; não sabemos nem quem é, aí, ela pede para ser seu e você aceita, daí, ela está vendo suas fotos, quem são seus familiares, onde você está; desse modo, as pessoas não têm os cuidados da vida real na vida virtual, então, vamos ter que começar a agir com esse tipo de consciência.

Aqui, já aconteceu algum conflito com a área federal em virtude dos crimes estarem próximos?

É muito comum ocorrer o conflito de atribuições, mas não se trata, verdadeiramente, de conflito, pois quando se pega casos em que começa a investigação e, aí, no início, identificamos que é uma atribuição da Polícia Federal, então, encaminhamos para eles; há casos em que eles recebem a notícia, verificam que não é atribuição deles e encaminham para nós. Então, existe, é comum porque há casos que transitam na linha tênue entre atribuição da Polícia Civil e atribuição da Polícia Federal, mas, digamos, assim, constituem conflitos de atribuições que são dirimidos com muita facilidade, não têm nenhum tipo de estresse ou dissabor sobre isso não, é feito de uma forma muito natural.

Agora, fale um pouco sobre deep web.

A maioria das pessoas não sabe, nem que existe, essa internet negra, esse submundo da internet, e, infelizmente, diante dessa realidade, até a polícia tem encontrado dificuldade nessa modalidade de internet, que é mais difícil que na internet natural, na verdade, toda criminalidade é difícil de ser combatida, senão não existiriam índices de criminalidade tão altos, e a internet e a criminalidade na internet é relativamente nova, e é um ponto, digamos, assim, a ser explorado em matéria de investigação. Infelizmente, a polícia ainda tem muita dificuldade de acessar a internet, mas nada é intransponível; assim, ao longo da história, temos conseguido deslocar as barreiras que vêm surgindo, à medida que elas aparecem, então, ainda é um ponto novo para a polícia, policiais, no âmbito acadêmico. Você vê que estamos na faculdade e o material é difícil, por exemplo, não há conteúdo expressivo sobre cibercrime, porque é tudo muito novo, a legislação também o é, e não acompanha o seu desenvolvimento, é escassa; precisamos da colaboração do legislativo para ajudar, porque são pontos que ainda precisam ser trabalhados.