CRIMES DIGITAIS E O DIREITO PENAL

Marciel Abadio da SILVA[1]
Paulo Henrique Faria SILVA[2]
André Luiz Duarte PIMENTEL[3]

RESUMO

A era digital chegou com força total e trouxe inúmeras mudanças. Os seus benefícios são incalculáveis, mas também trouxe muitos problemas, como a prática de crimes virtuais por exemplo. Nesta ótica, a presente pesquisa foi desenvolvida com o propósito de esclarecer temas importantes como, a chegada da era digital, a legislação aplicada atualmente no Brasil e internacionalmente, visto que a internet faz conexão global. Sendo assim, de nada adianta um trabalho interno do país para coibir tais práticas, se não houver um conjunto de esforços externos em prol de resolver o mesmo problema.

PALAVRAS-CHAVE: Internet, Era Digital, Crimes Virtuais.

ABSTRACT

The digital age came with full force and brought numerous changes. Its benefits are incalculable, but also brought many problems, such as the practice of virtual crimes for example. In this perspective, the present research was developed with the purpose of clarifying important topics such as the arrival of the digital age, the legislation currently applied in Brazil and internationally, since the internet makes a global connection. Therefore, there is no point in domestic work to curb such practices if there is no set of external efforts to solve the same problem.

KEYWORDS: Internet, Digital Age, Virtual Crimes.

[1] Aluno do Curso de Direito da Faculdade Santa Rita de Cassia- UNIFASC
[2] Aluno do Curso de Direito da Faculdade Santa Rita de Cassia- UNIFASC
[3] Professor do Curso de Direito da Faculdade Santa Rita de Cassia- UNIFASC

1 INTRODUÇÃO

A era digital chegou, trazendo uma infinidade de coisas úteis para vida das pessoas, possibilitando resolver problemas que antes eram impossíveis sem essa tecnologia, encurtando distâncias, atravessando fronteiras e conectando o mundo.

Conforme o tempo passa, essas tecnologias estão se tornando cada vez mais necessárias para que as pessoas possam ter uma melhor qualidade de vida, isso sob um prisma bastante holístico, envolvendo o bem-estar físico, psicológico, social, cultural, financeiro e de mobilidade.

O conforto de realizar tarefas sem sair de casa, como: pagar contas, fazer transações bancárias, participar de reuniões em videoconferência, praticar jogos online, namorar, fazer cursos, aprender de tudo, entre outras inúmeras possibilidades de utilização, aperfeiçoamento e desenvolvimento através da internet.

Entretanto, em meio a tantos benefícios, também trouxe muita coisa ruim, como por exemplo: a possibilidade de cometimento de diversos crimes por parte de pessoas mal intencionadas, que estão sempre a espera de uma oportunidade para tirar proveito de pessoas inocentes.

Diante desta situação, em que o direito dos usuários da internet é violado, surge então, a obrigação por parte do Estado de promover uma tutela jurisdicional adequada, que garanta a integridade física e moral destes indivíduos. Com a elaboração de leis que sejam realmente efetivas, de forma que os praticantes de crimes virtuais possam ser punidos regularmente, como um meio de garantir a ordem social e inibir incidência de novos crimes.

Este artigo, tem como finalidade fazer uma explanação sobre como o Direito Penal atua para resolver estas questões em busca de proteger os usuários da rede mundial de computadores (internet), que também pode ser acessada por telefones, smartfones, tablets e televisões digitais.

O primeiro tópico conterá uma explanação sobre a chegada do computador no mundo e sua evolução ao longo do tempo.

O segundo tópico tem por sequência, trazer à baila como o Direito Penal tem olhado para esta questão em prol de resolver este problema, o esforço internacional para combater esses crimes virtuais no mundo todo, e quais são os meios de se proteger contra esses crimes,

quais praticas devem ser adotadas pelos usuários para tentar dirimir estas condutas a fim de se esquivar desses criminosos.

2 O INICIO DA ERA DIGITAL

2.1 CRIAÇÃO E EVOLUÇÃO DO COMPUTADOR

Em toda a trajetória humana na terra, de acordo com livros e relatos, é possível perceber que o homem já demonstrava a necessidade de uma máquina que realizasse tarefas de forma automatizada. A raça humana está em constante evolução, e para uma melhor qualidade de vida em sociedade, percebia-se uma necessidade também de melhorar a forma de comunicação entre os povos, o computador foi a solução para essas duas necessidades, realizar tarefas e facilitar a comunicação conjuntamente com a internet. (Goulart, Ilídio, 2013).

A palavra Computador surgiu no século XIX, significa: pessoa com função de fazer contas e resolver problemas com número. (Goulart, Ilídio, 2013).

Neste percurso será detalhado o processo evolutivo dos computadores separados por um marco especial, a era antes de Steve Jobs e a era após Steves Jobs.

De acordo com (Goulart, Ilídio, 2013), computador teve vários inventores, um deles, o Alemão Wilhelm Schickard, que em 1623 construiu a primeira máquina de calcular, capaz de fazer cálculos de adição e subtração.

Outro inventor foi Blaise Pascal, de naturalidade francesa, em 1642, criou uma máquina com 6 rodas dentadas que calculavam sobre uma base de 0 a 9, a qual teve o nome de La Pascaline, essa máquina conseguia fazer somas de valores não maiores que 999999 e foi usada por duzentos anos. (Goulart, Ilídio, 2013).

Deve ser destacada a invenção de Charles Babbage, que em 1834,criou uma máquina com a capacidade de entrada de dados por meio de cartões perfurados, que conseguia fazer a resolução de polinômios. Foi ele o responsável pelo projeto de máquina analítica que posteriormente veio a ser a base usada para os computadores, tinha entrada, processamento e saída de dados. Esta máquina só não foi construída por que na época o criador sofreu com

limitações tecnológicas que tornaram o processo impossível de acontecer. (GOULART; ILÍDIO, 2013).

Já Herman Hollerith um americano no ano de 1880, inventou uma máquina para realizar as operações de recenseamento nos Estados Unidos da América. Essa máquina era capaz de realizar a leitura de cartões perfurados, possuía um contador acionado por impulsos elétricos.

Foi na Segunda Guerra Mundial entre os anos 1939 a 1945 que ocorreram os maiores avanços tecnológicos, foram criados os computadores para criar e decifrar códigos. Máquina criada com fins militares para dar apoio na guerra em curso.

A partir de então, foram aperfeiçoando até chegar na máquina ENIGMA, que teve sua primeira versão fabricada em 1926, projetada pelos Nazistas, ela era capaz de projetar códigos que mudavam a cada mensagem, mas foram quebrados em 1993, quando o inglês Alan Turing concluiu a Teoria da computabilidade criando a Máquina de Turing, que trabalhava com formalismo matemático para a criação de algorítimos. Foi usada no Bletchley Park (Centro de decodificação britânica), essa máquina foi criada para decifrar os códigos Alemães. (GOULART; ILÍDIO, 2013).

Em1942 o inglês Thommy Flowers inventou o Colossus, primeiro computador eletrônico programável, era capaz de decifrar códigos criptografados utilizando as mesmas idéias de Turing. (GOULART; ILÍDIO, 2013).

Neste sentido, quem definiu a arquitetura dos computadores que é usada até os dias atuais foi Von Neumann, com a criação de um computador binário 0 e 1.

Já o primeiro computador pessoal apareceu em 1981, foi chamado de IBM 5051 PC. Esperava-se que esse modelo alcançasse uma vende de mil unidades, e vendeu um milhão.

Após, o próximo e um dos maiores inovadores da era digital foi o senhor Steve Jobs, que em 1977 criou o primeiro computador da Apple, o Apple II, mas o primeiro que contagiou o mundo foi criado em 1984, o Macintosh, que foi também o primeiro a trazer interface gráfica e mouse (GOULART; ILÍDIO, 2013).

Na era Steve Jobs, as coisas começaram a mudar, ele tinha o conhecimento de que as pessoas não tinham certeza daquilo que queriam.

Ele conseguiu um grau tão grande de aprimoramento e perfeição em suas obras, que fez com que o mundo inteiro quisesse os seus computadores, sua forma de pensar era diferente da maioria das pessoas. Em seu trabalho ele procurava agir da seguinte forma:

Segundo Steve Jobs (1985), quando você é um carpinteiro fazendo uma cômoda linda, você não vai colocar um sarrafo no fundo do móvel, mesmo que ele fique voltado para a

parede e ninguém possa ver. Você sabe que está lá, então você vai usar um pedaço de madeira bonito no fundo. Você faz isso para dormir bem à noite. A estética e a qualidade têm de ser levadas até o último detalhe.

O que o visionário Steve Jobs fez para melhorar a informática, foi maior do que qualquer outro grande nome desta indústria, como Bill Gates, Steve Wozniak ou Adam Osborne. O Apple II, de 1977, mudou o padrão de computador doméstico e foi para muitas pessoas a porta de entrada no mundo digital. Um homem que pensava além do seu tempo, verdadeiro gênio, Steve Jobs trouxe a máxima simplicidade para facilitar o entendimento do computador por parte dos usuários, no seu modo de pensar, o uso do computador tinha de ser fácil, teve uma expressão sua que ficou bastante conhecida: "user friendly" (facil de usar).

3. O DIREITO PENAL E O COMBATE AOS CRIMES VISTUAIS.

3.1 LEI PENAL NO COMBATE AOS CRIMES VIRTUAIS

O Código Penal possui em seu corpo dois artigos específicos para crimes digitais que são: artigos 154-A e 298 que dizem o seguinte:

> Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput. [...]Art. 298- Falsificar, no todo ou em parte, documento particular ou alterar documento particular verdadeiro: Pena- reclusão, de um a cinco anos, e multa. Falsificação de cartão. Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (BRASIL, 1940, p. 34, 65).

Também é utilizado na proteção e combate aos crimes virtuais duas leis especiais publicadas em 2012. Uma delas é a Lei dos Crimes Cibernéticos (Lei 12.737/2012) conhecida como Lei Carolina Dieckmann.

Este evento aconteceu em uma ocasião na qual uma atriz famosa nacionalmente teve seu e-mail pessoal invadido por "Crackers" (pessoas que usam seus conhecimentos em informática para praticar crimes), que roubaram 36 fotos intimas da mesma. Após entraram em contato e pediram dez mil reais para não publicarem as fotos. Fato este que, causou grande comoção nacional fazendo com que fosse votada e sancionada esta lei de forma rápida.

A segunda é a Lei 12.735/12 que determina a instalação de delegacias especializadas para o combate de crimes digitais.

Fora estas leis, temos o Marco Civil da Internet (Lei 12.965/2014), que dispõe sobre os direitos e deveres dos usuários da internet, ou seja, os internautas. A lei protege os dados pessoais e a privacidade dos usuários. Sendo assim, uma possível quebra de dados e informações pessoais particulares só é possível mediante ordem judicial.

3.2 COMPETÊNCIA E LUGAR DO CRIME INFORMÁTICO

Quando se fala em competência e lugar do crime, ou seja, a questão da territorialidade, é possível encontrar amparo nos Códigos Penal e Processo Penal do Brasil, cabendo ressaltar, que o tema é bastante controverso.

Definir a territorialidade: significa dizer qual o juiz será competente para processar e julgar determinado crime cibernético.

O Direito Penal brasileiro é inerente ao território nacional, sendo assim, o que ocorre além dos limites territoriais do país, carece de uma revisão nos acordos entre os países que possam estar envolvidos na realização do crime.

Salienta-se que, sendo o crime informático praticado contra bens da União, a competência será da Justiça Federal. Conforme preceitua o artigo 109 incisos IV e V da Constituição Federal de 1988.

No Código Penal Brasileiro, a parte da norma que trata desta questão da competência está elencada nos artigos: 5, 6 e 7:

> **Territorialidade**: Art. 5º - Aplica-se a lei brasileira, sem prejuízo de convenções, tratados e regras de direito internacional, ao crime cometido no território nacional.
> § 1º - Para os efeitos penais, consideram-se como extensão do território nacional as embarcações e aeronaves brasileiras, de natureza pública ou a serviço do governo brasileiro onde quer que se encontrem, bem como as aeronaves e as embarcações brasileiras, mercantes ou de propriedade privada, que se achem, respectivamente, no espaço aéreo correspondente ou em alto-mar.
> § 2º - É também aplicável a lei brasileira aos crimes praticados a bordo de aeronaves ou embarcações estrangeiras de propriedade privada, achando-se aquelas em pouso no território nacional ou em vôo no espaço aéreo correspondente, e estas em porto ou mar territorial do Brasil.
> **Lugar do crime**: Art. 6º - Considera-se praticado o crime no lugar em que ocorreu a ação ou omissão, no todo ou em parte, bem como onde se produziu ou deveria produzir-se o resultado.
> **Extraterritorialidade:** Art. 7º - Ficam sujeitos à lei brasileira, embora cometidos no estrangeiro:

> I - os crimes:
> a) contra a vida ou a liberdade do Presidente da República;
> b) contra o patrimônio ou a fé pública da União, do Distrito Federal, de Estado, de Território, de Município, de empresa pública, sociedade de economia mista, autarquia ou fundação instituída pelo Poder Público:
> c) contra a administração pública, por quem está a seu serviço;
> d) de genocídio, quando o agente for brasileiro ou domiciliado no Brasil.(BRASIL, 1940, p. 1-2).

De acordo com o artigo 6º do Código Penal, em relação ao lugar do cometimento do crime, a teoria adotada foi a da Ubiquidade, que diz que, o lugar do crime, é o local onde ocorreu a ação ou omissão, no todo ou em parte, bem como onde produziu ou deveria produzir o resultado.

Cabe ressaltar o que diz artigo 70 § 2º do Código de Processo Penal:

> Art. 70. A competência será, de regra, determinada pelo lugar em que se consumar a infração, ou, no caso de tentativa, pelo lugar em que for praticado o último ato de execução.
> § 2º Quando o último ato de execução for praticado fora do território nacional, será competente o juiz do lugar em que o crime, embora parcialmente, tenha produzido ou devia produzir seu resultado. (BRASIL, 1941, p. 9).

Também existe uma corrente que defende que a teoria a ser adotada é algo semelhante a da atividade, na qual o local do crime é aquele em que o agente praticou o delito. Ainda, em contraponto, outra corrente, acredita que, o lugar do crime deve ser aquele em que se encontra o autor.

Em consonância com os ensinamentos dos autores, (VALIN, 2000, p. 117 apud JESUS e MILAGRE, 2016, p. 61).

> Para casos relacionados à internet, deveria ser adotado algo semelhante à teoria da atividade que, como visto, determina como sendo o local do crime aquele em que o agente praticou o delito. Pensamento contrário é defendido por Valin, que acredita ser a melhor solução considerar-se como local do crime aquele em que está o autor das infrações, pois o referido país teria melhores condições de aplicar eventual pena, sem necessidade de discussão sobre extradição, no máximo se discutiria o cumprimento dos efeitos cíveis da condenação no sentido de retirar da rede o material publicado, o que talvez possa gerar a necessidade de um novo processo em país distinto ao da condenação.

3.3 ESFORÇO INTERNACIONAL PARA COMBATER TAIS PRÁTICAS

A evolução da tecnologia informática conectou o mundo em uma grande teia, onde qualquer pessoa tem acesso a todos os conteúdos, sem a necessidade de estarem em algum lugar físico. Entretanto, o local em que foi praticado o delito, é de grande importância para que a justiça possa determinar qual juízo será competente para julgar o litígio.

É bastante usual que indivíduos busquem praticar crimes por meio de hospedagens na internet em sistemas do exterior. Sendo assim, para uma possível investigação por parte do Brasil, carecerá de uma cooperação internacional. O que acaba não sendo uma tarefa simples, visto que muitos provedores costumam alegar que não estão sujeitos às leis brasileiras.

Neste sentido, fica evidente que a cooperação internacional é fundamental para o combate aos crimes informáticos.

Na Europa oito países mais industrializados criaram um grupo de cooperação chamado de "Rede 8x7", que foi extendida para outros países como o Brasil por exemplo, e também está acessível para autoridades policiais.

O que acontece na realidade é que para uma autoridade conseguir dados inerentes a usuários de serviços hospedados no exterior, o jeito mais usado é a carta rogatória que é bastante lenta, isso levando em conta que no Brasil não se pode produzir provas ilícitas. Também existe uma forma de cooperação chamada de "auxílio direto", porém, cada país que decide a sua forma de cooperação no auxílio direto.

Segue então uma explanação exclarecedora sobre este assunto dos autores: (JESUS e MILAGRE, 2016, p.195).

> Deste modo, a cooperação internacional ainda é um desafio para a eficácia do combate ao crime eletrônico. Os provedores, como "portas" de entrada e saída da internet, são os primeiros a ter a possibilidade de apurar dados de usuários que sejam seus clients. Não bastasse, no que tange a provimento de aplicações e serviços, é notório que os serviços mais utilizados no brasil pertencem a grandes provedores de conteúdo com sede no exterior (alguns, sequer com filiais físicas no Brasil).
> Neste contexto, em defesas envolvendo processos de quebras de sigilo de seus usuários, no Brasil, quase sempre argumentam que não estão sujeitos à jurisdição brsileira, apresentando inclusive a "lei do país sede". Muito embora tal argumentação seja desconsiderada peo judiciário na grande maioria dos casos, ainda preocupa a questão do provedor no exterior que não tem filial no Brasil. Nestes casos, é importante que a cooperação internacional efetivamente se desenvolva.

Fica assim, evidente que, esta necessária cooperação internacional ainda caminha a passos lentos, não podendo afirmar que de fato está sendo fácil resolver problemas que envolvem crimes internacionais, ou até mesmo crimes cometidos por brasileiros em vítimas

dentro do país, mas pelo fato de não estarem usando sistemas com hospedagem no Brasil, acaba por dificultar este rastreamento e a consequente solução do caso.

Nesta douta, é necessário que exista um esforço global ainda maior no sentido de combater esses referidos crimes e consequentemente garantir uma possível navegação com segurança para os usuários desta ferramenta que vem se tornando cada vez mais importante na vida das pessoas de todo o mundo.

3.4 MEIOS DE SE PROTEGER CONTRA OS CRIMES VIRTUAIS

No Brasil e no mundo, diariamente pessoas são vítimas de ofensas nas redes sociais, outras recebem cobrança de compra que nunca fizeram, milhares de pessoas tem suas contas roubadas, também sofrem com a compra de produtos pela internet que nunca chegam. Hoje, infelizmente a internet não é um ambiente cem por cento seguro. É de suma importância que os usuários da rede estejam a par dos riscos que estão correndo para que possam conseguir se proteger de maneira adequada.

Foi de olho nesta questão, que vários órgãos do governo juntamente com organismos privados passaram a se dedicar na criação de ações que objetivam a utilização ética da internet, para que mais pessoas possam aproveitar o que é oferecido de bom pela rede.

Uma destas ações é a criação de cartilhas com várias dicas para um uso seguro da internet.

Em relação a proteção do computador, é indicado que o usuário possua instalado na máquina um software que atue contra possíveis ameaças virtuais os chamados antivírus, é obrigatório que todo computador possua pelo menos um antivírus na defesa desta máquina.

Conforme explica Cassanti

> Estudo indica que 16% dos computadores no Brasil não possuem software contra ameaças virtuais instalado, o que os torna mais vulneráveis a invasões de atacantes e a vírus.
> Os dados são de um levantamento divulgado pela companhia de segurança digital McAfee. Foram analisados cerca de 28 milhões de computadores por mês em 24 países diferentes durante o ano passado.
> O antivírus é obrigatório em qualquer computador. Um bom antivírus é capaz de identificar e eliminar phishing, spyware, rootkit e deve ter ainda sistemas para verificar vírus em e-mails, mensageiros e programas de trocas de arquivos P2P. Esses programas estão sempre à procura de novas ameaças que se disseminam na web, por isso existem atualizações diárias que mantêm a segurança (CASSANTI, 2014, p.65).

Uma das formas de tomar de se proteger, é mantendo o sistema operacional e os demais programas utilizados sempre atualizados, em cada atualização que é feita, os criadores aprimoram esses sistemas para uma melhor utilização, e também atualizam a questão da segurança dos mesmos. O melhor é que estes programas e sistemas sejam originais.

Outro ponto importante para a segurança do usuário é o Firewall, a maioria dos sistemas operacionais possui, é um programa que controla os acessos ao computador impedindo a transmissão ou recepção de acessos indesejados. Para navegar com segurança pela rede é necessário possuir um computador bem configurado, visto que os atacantes procuram por vulnerabilidades dos usuários.

É também indicado que o usuário, ao criar e-mails ou contas bancárias que elabore senhas difíceis e que consiga efetuar mudanças periódicas nas mesmas como forma de dificultar o deciframento.

De acordo com o que esclarece Cassanti,

> Um estudo divulgado pela empresa de segurança SplashData criou uma lista das senhas mais fracas utilizadas pelos usuários de computadores. A mais usada é a própria palavra *password* (senha em inglês), seguida por 123456 e 12345678. Logo depois aparecem senhas como abc123 e qwerty (a sequência das seis primeiras teclas alfabéticas de qualquer teclado). Na lista ainda é possível encontrar as sequências numéricas 111111, 123123 e o nome Jesus. (CASSANTI, 2014, p. 69).

É recomendado que seja evitado as senhas mais simples, ou nomes de parentes de datas de aniversário, Especialistas aconselham a não criar senhas com menos de 6 carácteres.

Ao criar uma senha, procure uma mais longa, utilize uma frase que só você saiba o sentido. Coloque números misturados com símbolos, para tornar a sua frase indecifrável. Use também letras maiúsculas e minúsculas. Tenha uma senha diferente para cada serviço.

Não coloque perguntas de segurança. São poucas as respostas para a pergunta: qual sua cor favorita? os malfeitores podem descobrir estas respostas com facilidade e roubar seus dados e mudar até mesmo a senha do usuário, bloqueando o acesso do mesmo em seu próprio cadastro ou conta.

É necessário tomar cuidado ao realizar compras pela internet, para tanto, recomenda-se que o usuário leia a política de privacidade do site, confira se o CNPJ tem registro em órgão competente quando for o caso, guardar os e-mails recebidos da loja e os e-mails enviados pelo comprador, e se possível, verificar se no cadastro o site pede informações em excesso.

Pesquisas revelam que é crescente o número de golpes pela internet, isso se dá pelo fato de que é fácil imitar um site da internet, criar sites falsos e assim conseguir efetuar vendas de produtos que não existem.

Quando se fala em operações bancárias, é necessário também um grande cuidado, pois essas transações proporcionam rapidez, conforto e praticidade, entretanto, sem os cuidados necessários é bastante perigoso.

Para garantir segurança nas operações bancárias, as instituições financeiras gastam muito dinheiro implantando tecnologias que consigam combater esses ataques malignos pela rede.

Conforme salienta Cassanti,

> de acordo com a Febraban, 24% de todas as transações bancárias são feitas atualmente pela internet, o que demanda um investimento, pelos bancos, de US$ 9,2 bilhões por ano no combate aos crimes virtuais. O setor é o que mais investe em tecnologia de segurança, que inclui sistemas de segurança física e virtual, como cartões com chip, tokens de geração de senhas, softwares de proteção de máquinas de usuários e identificação biométrica dos clientes.
>
> Mesmo com todo esse investimento em tecnologia, as fraudes eletrônicas causaram um prejuízo de aproximadamente R$ 1,4 bilhão aos bancos brasileiros em 2012. E foi o comportamento do cliente o principal fator de ocorrência de fraudes eletrônicas bancárias, principalmente nas transações por cartões e pela internet (CASSANTI, 2014, p. 74).

Para realizar as operações bancárias com segurança é necessário seguir alguns passos:

Antes de instalar algum aplicativo ou software de segurança solicitado pelo banco, observe se quem enviou a mensagem foi realmente o banco.

Não acesse sua conta em computadores públicos, ou maquinas que não sejam conhecidas.

Quando clicar em algum link na página do banco, certifique-se de que é realmente vinculado ao banco.

Quando acessar a conta do banco, digite a senha de forma errada, se na primeira vez, acusar o erro, significa que está no site certo.

Os principais bancos do Brasil usam um domínio terminado em "**b.br**", confirme na barra de endereços da página. No tocante ao combate a essas praticas criminosas, existem diversos procedimentos a serem adotados de acordo com o "Roteiro de Atuação da Ministério Público Federal" publicado no site do MPF em 2013, que é um roteiro de uso exclusivo das autoridades da justiça do Brasil, como a Polícia Federal, Polícia Civil, Procuradores, juízes e Promotores da esfera Federal. Entretanto, existe um esforço para que ocorra uma

disseminação do conhecimento deste roteiro entre os leitores em geral em prol de uma conscientização sobre como se proteger de ataques digitais.

Este roteiro ensina formas de se proteger e aborda diversas formas para essa transmissão de conhecimento, como por exemplo, a utilização de acontecimentos reais de crimes e a forma de combatê-los. Possui temas como: Principais técnicas utilizadas para ocultação do crime e de seu autor, também fala sobre a legislação aplicada.

Após estudos e análises, é possível perceber que existem muitas possibilidades de se aprender como fazer uma navegação segura pela internet, partindo do princípio de que a própria internet é uma fonte inesgotável de conhecimento, o usuário pode buscar nela as melhores maneiras de se proteger e de como agir para não ser uma preza fácil, seja por meio de vídeos explicativos, cursos, ou até mesmo sites e livros disponibilizados na rede.

4 CONSIDERAÇÕES FINAIS

No presente trabalho, objetivou-se mostrar a evolução do computador ao longo dos anos, buscou-se também explicar quais são os crimes digitais mais comuns no intuito de informar os leitores para que eles não venham a cair em ciladas existentes no dia a dia do mundo virtual, tendo partido do princípio de que é crescente o número de crimes nesta área, e é também crescente o número de pessoas inexperientes que estão aderindo ao uso da internet.

Os crimes digitais estão cada vez mais evoluídos, ficando assim cada vez mais fácil alcançar novas vítimas, que poderão vir a cair em golpes financeiros, compra de produtos que não existem, pagando contas que não devem e inúmeros outros delitos.

Só quem passou por isso sabe a dor que é perder dinheiro, o sossego e ser obrigado a superar problemas que poderiam ser evitados, se houvesse um esforço maior por parte das grandes empresas de internet, conjuntamente com esforços governamentais em busca pela segurança dos usuários, o que na prática ainda deixa muito a desejar.

5 REFERÊNCIAS

A evolução da Internet: **uma perspectiva histórica - página pessoal de ...** <www.belins.eng.br/ac01/papers/aslegis48_art01_hist_internet.pdf>. Acesso em: 10 fev. 2019.

A História do Computador - UFSJ <https://ufsj.edu.br/portal2-repositorio/File/prof.../A_historia_do_computador.pdf> Acesso em: 9 fev. 2019.

BRASIL. **DECRETO-LEI Nº 2848 DE 7 DE DEZEMBRO DE 1940.** Código Penal. Disponível em: <http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848compilado.htm>. Acesso em: 10 maio 2019.

BRASIL. **DECRETO-LEI Nº 3689 DE 3 DE OUTUBRO DE 1941.** Código de Processo Penal. Disponível em: < http://www.planalto.gov.br/ccivil_03/decreto-lei/del3689.htm> . Acesso em: 10 maio 2019.

Brasil. Ministério Público Federal. Câmara de Coordenação e Revisão**,** 2. **ROTEIRO DE ATUAÇÃO: crimes cibernéticos.** 2 ed. rev. - Brasília: MPF/2ªCCR, 2013. Disponível em: < http://www.mpf.mp.br/atuacao-tematica/ccr2/publicacoes/roteiro-atuacoes/docs-cartilhas/crimes-ciberneticos>. Acesso em: 16/02/2019.

Brasil tem 116 milhões de pessoas conectadas à internet, diz IBGE ... <https://g1.globo.com/.../brasil-tem-116-milhoes-de-pessoas-conectadas-a-internet-diz-i...> Acesso em 11 fev. 2019.

CASSANTI, Moisés de Oliveira. **CRIMES VIRTUAIS, VÍTIMAS REAIS.** Ed. Brasport. Rio de Janeiro, RJ, 2014.

Crimes digitais: quais são, quais leis os definem e como denunciar (25 de junho de 2018). **Justificando**. Disponível em:<www.justificando.com/.../crimes-digitais-quais-sao-quais-leis-os-definem-e-como-den...> Acesso em: 20 abr. 2019.

DANI, Marília Gabriela Silva; Oliveira, Luiz Gustavo Caratti de. OS CRIMES VIRTUAIS E A IMPUNIDADE REAL. **ÂMBITO JURÍDICO.** 2011. Disponível em: <http://www.ambitojuridico.com.br/site/index.php?n_link=revista_artigos_leitura&artigo_id=9963> Acesso em: 19 fev. 2019.

DIANA, Daniela. HISTÓRIA E EVOLUÇÃO DOS COMPUTADORES. **Toda Matéria.** Disponível em: <https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/>. Acesso em: 10 fev. 2019.

DULLIUS, Aladio Anastacio; HIPLLER, Aldair. "Dos Crimes Praticados em Ambientes Virtuais". **Portal de e-governo, inclusão digital e sociedade do conhecimento – eGov**. Disponível em: <http://www.egov.ufsc.br/portal/conteudo/dos-crimes-praticados-em-ambientes-virtuais> Acesso em:27 fev 2019.

Crimes virtuais: que leis existem?**. E-DOU.** 2016 Disponível em: <https://edou.com.br/2016/08/crimes-virtuais-que-leis-existem/> Acesso em: 21 fev. 2019.

GOMES, Helton Simões. INTERNET CHEGA PELA 1ª VEZ A MAIS DE 50% DAS CASAS NO BRASIL, MOSTRA IBGE. **G1.** Disponível em: <http://g1.globo.com/tecnologia/noticia/2016/04/internet-chega-pela1-vez-mais-de-50-das-casas-no-brasil-mostra-ibge.html> Acesso em: 22 fev.2019.

GOULART; ILÍDIO. **A História do Computador.** Slide apresentado à Universidade Federal de São João Del-Rei – UFSJ. Disponível em: <https://ufsj.edu.br/portal2-repositorio/File/prof.../A_historia_do_computador.pdf> . Acesso em: 9 fev. 2019.

HISTÓRIA e desenvolvimento do computador. Disponível em: <https://www.todamateria.com.br/historia-e-evolucao-dos-computadores/>. Acesso em: 10 fev. 2019.

JESUS, Damasio de; Milagre, José Antônio. **Manual de crimes informáticos**. São Paulo: Saraiva, 2016.

RUTHERORD, Mikhail. CRIMES NA INTERNET: falta de normatização, dificuldades na regulamentação e entendimentos sobre o assunto. **JusBrasil.** 2015. Disponível em: <https://mikhail.jusbrasil.com.br/artigos/234313175/crimes-na-internet-falta-denormatizacao-dificuldades-na-regulamentacao-e-entendimentos-sobre-o-assunto> Acesso em: 16/02/2019.

SCHMIDT, Guilherme. CRIMES CIBERNÉTICOS. **JusBrasil.** 2014. Disponível em: <http://gschmidtadv.jusbrasil.com.br/artigos/149726370/crimes-ciberneticos> Acesso em: 14 fev 2019.

TROYACK, Leandra. MACINTOSH: 30 anos de revolução e evolução. **Código Fonte.** 2014. Disponível em: <https://www.codigofonte.com.br/artigos/macintosh-30-anos-de-revolucao-e-evolucao>. Acesso em: 15 fev. 2019.

UMA CONTRIBUIÇÃO REVOLUCIONÁRIA - **Economia - Estadão** <https://economia.estadao.com.br/.../geral,uma-contribuicao-revolucionaria-imp-,7817...> Acesso em 10 fev. 2019.