A IMPORTÂNCIA DA PRESERVAÇÃO DA EVIDÊNCIA DIGITAL NOS CRIMES CIBERNÉTICOS

Elias CHAQUIAN FILHO[1]; Sara Luize Oliveira DUARTE[2]; Liluyoud Cury de LACERDA[2]

1. Faculdade de Ciências Administrativas e Tecnologia, Porto Velho – RO, Brasil.
2. Centro Universitário São Lucas, Porto Velho – RO, Brasil
*Autor Correspondente: liluyoud@saolucas.edu.br

Recebido em: 05 de julho de 2018 - **Aceito em:** 05 de novembro de 2018

RESUMO: Tendo em vista que os crimes cibernéticos têm aumentado a cada ano, pesquisa-se o motivo porque isso ocorre, a fim de indicar as formas de preservação da prova para a vítima. Para tanto, é necessário definir os crimes, os atores, os danos e pessoas afetadas e as formas de preservação. Realiza-se uma pesquisa quantitativa do crescimento dos crimes correlacionada com o aumento dos aparelhos conectados na internet. Diante disso, verifica-se que os crimes cibernéticos crescerão de forma exponencial, e as vítimas terão que preservar a prova para posterior responsabilização dos infratores, demonstrando os tipos de preservação mais adequados para a vítima realizar, o que impõe a constatação de que as pessoas precisam ser mais informadas acerca dos tipos de preservação de prova.

Palavras-Chave: Crime cibernético. Crescimento. Vítima. Prova. Forma de preservação.

INTRODUÇÃO

US$ 142,00 (cento e quarenta e dois dólares)! Esse foi o custo médio sofrido pelas mais de 978 milhões de vítimas de crime cibernético em 2017[1].

E esses números que só tendem a aumentar. A questão é que as pessoas estão cada vez mais dependentes da internet e da tecnologia para melhorar suas vidas. Não existe instituição financeira ou grandes empresas sem banco de dados e um departamento de tecnologia de informação. O comércio, o governo e o judiciário caminham para se tornarem eletrônicos.

Vivemos cada vez mais conectados, seja para comprar alguma coisa, jogar online, estudar, participar de redes sociais, conversarem, ter relacionamentos, fazer negócios ou investimentos ou somente desestressar. E aqui reside o problema.

Nesse ambiente virtual, comumente chamado de ciberespaço, as fronteiras são quebradas, existindo interação entre milhões de pessoas, em qualquer lugar e em qualquer momento. Aqui também se forma a cibercultura, que é a complexa junção do conhecimento, artes, costumes, técnicas, hábitos formas e modos de pensar adquiridas pelas pessoas ao fazer parte do ambiente virtual.

[1] Disponível em: http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf . Acesso em: 13 maio 2018.

Contudo, o ciberespaço não é só um lugar de coisas boas. As pessoas podem ser vítimas de crimes na internet. Nunca estivemos tão conectados e ao mesmo tempo tão vulneráveis. E é fato que grande parcela da população sofrerá prejuízos de ataques virtuais nos próximos anos. E no Brasil, conforme recentes estatísticas, o prejuízo causado pelo crime virtual está em um crescimento exponencial.

O crime cibernético se vale do anonimato, dos ataques em larga escala e o alcance global. Esses fatores estimulam os criminosos a migrarem seus delitos para o no mundo virtual.

Com todos esses fatos, levanta-se uma questão interessante. Mesmo com todas as campanhas, sites e matérias, informando os internautas como se prevenir de crimes cibernéticos, cada vez mais milhões de pessoas são prejudicadas pela atividade dos cibercriminosos.

Essa questão se desdobra em duas indagações. A primeira é porque o cibercrime cresce no Brasil e no mundo? A segunda, o que fazer depois de ser vítima de um crime virtual? Qual o procedimento que a pessoa deve realizar para preservar a evidência dos delitos cibernéticos, já que o ambiente virtual é dinâmico, volátil e mutável.

O propósito deste trabalho é analisar as variáveis que envolvem o aumento do crime cibernético e demonstrar formas de preservar a evidência para futura salvaguarda da vítima. Para tanto e dado a enorme gama de crimes possíveis de serem praticados na internet, será explanado acerca de algumas das formas que podem ser utilizadas pela vítima para criar uma prova robusta do prejuízo sofrido.

Neste artigo, o procedimento metodológico utilizado foi feito em duas etapas para nortear o método de trabalho. Na primeira, foi realizada uma coleta de informações em sites e livros acerca dos conceitos primários de crime cibernético, prova e preservação da prova, abrangidos pelo artigo. Em seguida foi feito uma pesquisa explicativa, analisando os dados quantitativos coletados em sites de estatísticas e de proteção aos crimes virtuais, de forma a compreender o crescimento do cibercrime no mundo e no Brasil.

Esse resultado quantitativo do crescimento dos crimes virtuais no mundo apresenta uma discussão interessante, mostrando as perdas que as vítimas sofreram, e nos aponta para uma projeção no horizonte do que possivelmente acontecerá no futuro: A ocorrência crescente do cibercrime e perdas trilionárias para as pessoas e empresas.

Com base nessas variáveis, se procura nortear o internauta sobre o que fazer quando for vítima de um crime virtual.

No referencial teórico será contextualizada a nossa sociedade tecnológica, com ênfase no ciberespaço e cibercultura, com uma breve explanação do cibercrime, com seu conceito, classificação, e principais tipos, sujeito ativo e vítima desses crimes.

Após, serão analisadas as estatísticas colhidas para demonstra a escala do problema do crime cibernético no mundo e no Brasil, de forma a traçar uma análise entre o aumento dos aparelhos conectados a rede mundial e o aumento dos crimes virtuais.

Em seguida, será feita uma breve abordagem sobre prova em um processo normal, com sua conceituação, finalidade e objetivo, e no capítulo posterior aborda-se a evidência em um crime virtual, ressaltando a necessidade da preservação da prova, pois os dados digitais podem ser facilmente forjados. Por fim, procura-se definir algumas das formas de preservação da prova com ênfase na ata notarial, importante instrumento ao alcance da vítima. Com análise de um caso específico.

Por fim, conclui-se sobre a necessidade de aumentar a informação acerca da preservação da prova digital quando ocorrerem os crimes, permitindo que a vítima possa buscar a reparação ou ajudar a prender o criminoso.

REFERENCIAL TEÓRICO

CIBERESPAÇO E CIBERCULTURA

Antes de se falar sobre o crescimento dos crimes cibernéticos, vamos falar sobre o local onde ocorrem esses delitos – **O ciberespaço**. Essa palavra surgiu em 1982, com Willian Gibson, escritor norte-americano, que a utilizou em seu livro de ficção científica, *Neuromancer*, lançado em 1984. Esse livro descreve uma realidade formada por um conjunto de tecnologias tão arraigadas na sociedade que termina por modificar o comportamento e os princípios dos usuários que nela estão conectados.

Sua definição é interessante e cada dia torna-se mais atual.

> **A descrição de Gibson do ciberespaço consistia em uma realidade virtual totalmente imersiva através da qual os usuários de redes de computadores de todo o mundo podiam se comunicar e interagir entre si.** Isso é essencialmente o que ocorreu através da invenção da Internet e da *World Wide Web*, embora essas plataformas tecnológicas diferem e também sejam diferentes do ciberespaço, sendo mais duas dimensões e contendo menos dos aspectos científicos cúbicos da realidade virtual. Logo após a comercialização da Internet em 1988, os jogos on-line e as

> redes sociais suportadas por subscrições, como a America Online e a *Compuserve*, tornaram-se fóruns para que as pessoas se comunicassem e colaborassem em conjunto, ou o que é comumente referido como "no ciberespaço". Como a Internet de O início de 1990s tornou-se efetivamente o que agora é conhecido como *World Wide Web*, ou simplesmente "a Web" ou "a rede", novas capacidades e complexidades surgiram. Essas realidades eletrônicas combinam tecnologia com percepções cognitivas de lugares onde as pessoas podem interagir." (MACQQUADE, 2009, p. 52) – grifo não original.

O ciberespaço guarda similitude com o espaço real, organizado e povoado, não sendo fixo e estático, mas dinâmico e mutável, recebendo atualizações constantes, em virtude da relação entre as pessoas, documentos, máquinas e também da evolução destas. Isso ocorre devido às suas características peculiares, conforme define Crespo (2011, p. 46-47):

> a) Capacidade de Processar, guardar e circular, de forma automatizada e em tempo real, grandes quantidades de informações em formato digital dos mais variados (fotos, filmes, sons). Isso é facilitado pela própria estrutura descentralizada e não hierarquizada da internet que inviabiliza a existência de órgão de controle da informação circulante e, como consectário lógico, torna praticamente impossível supervisionar a qualidade e o volume de informações;
> b) O número enorme de usuários, a frequência com que acessam, a liberdade que têm para enviar, transferir, difundir e acessar informações de modo que os internautas passam a ser potenciais vítimas, mas também potenciais sujeitos ativos de delitos;
> c) As próprias características físicas, técnicas e lógicas da TIC, que podem ser acessadas de forma ilegítima, tendo seu conteúdo alterado. Consegue-se acesso a arquivos das mais distintas naturezas e aos mais variados programas de computador;
> d) A enorme potencialidade de multiplicação de ações ilícitas. Isso decorre da própria estrutura das TIC, como mencionado acima. A criação de fóruns de debates, páginas na internet, comunidades de relacionamento etc., podem facilitar a prática de delitos, podendo ainda, dar maior repercussão a eles, como nas ofensas contra a honra, por exemplo.

Com base nessas características, verifica-se o aumento progressivo da utilização da tecnologia, que nos leva a viver em duas realidades existenciais. A nossa vida física e a virtual. Ambas coexistindo interligadas.

Essa tecnologia aliada com a sociedade pós-moderna cria a chamada cibercultura, que é "o conjunto de técnicas (materiais e intelectuais), de práticas, de atitudes, de modos de pensamento e de valores que se desenvolvem juntamente com o crescimento do ciberespaço" (LÉVY, 1999, p. 17).

É nessa realidade que os crimes virtuais acontecem, dadas as facilidades existentes, nas quais os criminosos virtuais encontram dados desguarnecidos e potenciais vítimas.

CRIMES CIBERNÉTICOS

Definir crime cibernético, ou cibercrime, é uma questão complicada. O motivo é devido o ciberespaço ser um lugar em que se cometem delitos que já existem no nosso ordenamento jurídico, mas também onde se cometem condutas atípicas, que podem, porém, ser potencialmente danosas, sendo incontáveis as ações ilícitas que podem ser praticadas pela internet, mas que afetam o mundo real.

A nomenclatura é extremamente variada, com divergências entre os autores, que procuram dar sua definição. As denominações variam, dentre elas cibercrime, crimes cibernéticos, crimes de computador, crimes tecnológicos, crimes digitais, delito informático, crimes por meio de informática, fraude informática, dentre inúmeros outros.

Crespo (2011, p. 48) narra que no início dos anos 80, a doutrina espanhola utilizava o termo "delitos informáticos" para os crimes praticados com tecnologia, sendo uma tradução do termo *computer crimes* que era usado pelo Departamento de Justiça norte-americano na seção "computer crime and intellectual property section"[2]. E continua, citando Maria Helena Junqueira Reis, a qual diz que no Brasil, existem oito possíveis denominações:

> (a) computer crimes (aduz que o crime não é "do computador, mas do agente"); (b) abuso de computador (detectar o que sejam abusos dependeria de amadurecimento do campo ético-informático); (c) crime de computação (há crimes próprios – puros – e os impróprios, sendo que esta denominação leva em conta apenas a primeira categoria); (d) criminalidade mediante computadores (mesma crítica feita ao termo anterior); (e) delito informático (mais comum em países de língua espanhola, é feito pensando-se no objeto jurídico tutelado proteção da informação – mas nem sempre esse será o foco da proteção); (f) fraude informática (nem todos os delitos praticados com o auxílio da tecnologia são fraudulentos); (g) delinquência econômica (há crimes sem motivo econômico) e; (h) computerkriminalistät (conceito mais amplo e que talvez fosse mais adequado).

A empresa de segurança Norton Symantec define crime cibernético como:

> Todo crime que é executado online ou principalmente online. Isso pode incluir desde os roubos de identidade e outras violações de segurança mencionadas acima a crimes do tipo "pornografia de vingança", "cyberstalking", assédio, bullying e até mesmo exploração sexual infantil[3].

Em 2001, na Convenção sobre o Cibercrime, em Budapeste, em seu preâmbulo, definiu tais atos como aqueles "praticados contra a confidencialidade, integridade e

[2] "Seção de Crimes de Computador e propriedade intelectual", disponível em: https://www.justice.gov/criminal-ccips. Acesso em: 11 jun. 2018.
[3] Disponível em: https://br.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html. Acesso em: 03 jun.2018.

disponibilidade de sistemas informáticos, de redes e dados informáticos, bem como a utilização fraudulenta desses sistemas, redes e dados"[4].

Qual a definição capaz de alcançar todo o espectro de ações que podem ser praticadas no ciberespaço?

O mais perto que podemos chegar de um conceito completo sobre crime cibernético, é o citado por Rossini (2004, apud BARRETO & BRASIL, 2016, p. 16), ao definir que "delito informático como a conduta típica e ilícita, constitutiva de crime ou contravenção, dolosa ou culposa, comissiva ou omissiva, praticada por pessoa física ou jurídica, com o uso da informática, em ambiente de rede ou fora dele [...]".

Esse conceito abrange o máximo possível de situações que causam um resultado lesivo a um bem tutelado conforme nosso direito.

CLASSIFICAÇÃO DOS CRIMES CIBERNÉTICOS

Os cibercrimes podem ser classificados em puros (ou próprios) e impuros (ou impróprios). Os puros são aqueles cujos bens jurídicos atingidos são os sistemas informatizados ou os dados. Eles são o alvo do crime em si. Já os impuros ou impróprios, são aqueles delitos que podem ser realizados normalmente no mundo real sem precisar da tecnologia. Todavia, o criminoso utiliza-se do manto da obscuridade do mundo virtual para praticar a conduta de forma a produzir um resultado lesivo para a vítima.

Crespo (2011, p. 63), classifica os crimes cibernéticos em:

> [...] todas as condutas praticadas contra bem jurídicos informáticos (sistemas, dados) são delitos de risco informático ou próprios, ao passo que aquelas outras condutas que se dirigirem contra bens jurídicos tradicionais (não relativos à tecnologia) são crimes digitais impróprios.

A lista dos crimes é extensa, e só a título de citação, temos como exemplo de crimes próprios, a invasão de dispositivo informático, dano, inserção de dados falsos em sistema de informações e modificação ou alteração não autorizada de sistema de informações.

Já o exemplo de crimes impróprios, temos os crimes de calúnia, difamação, injúria, ameaça, furto mediante fraude, estelionato, pornografia infantil (pedofilia on-line), racismo,

[4] Disponível em: http://www.mpf.mp.br/atuacao-tematica/sci/normas-e-legislacao/legislacao/legislacoes-pertinentes-do-brasil/docs_legislacao/convencao_cibercrime.pdf . Acesso em: 29 jul. 2018.

xenofobia e intolerância religiosa, apologia e incitação a crimes contra a vida, pornografia de revanche dentre inúmeras outras.

SUJEITO ATIVO DOS CRIMES CIBERNÉTICOS

Esqueçam os estereótipos aqui. O lugar comum, eternizado pelos filmes, no qual o cibercriminoso é um cara novo, inteligente, habilidoso, com conhecimentos excepcionais de informática e sem trato social não mais se aplica na atualidade.

Hoje em dia qualquer pessoa pode ser o sujeito ativo de um crime cibernético, em virtude da quantidade de informações oferecidas sobre qualquer coisa na internet. Barreto e Brasil (2016, p. 22) afirmam que:

> Qualquer um pode vir a ser criminoso especializado, até porque a própria internet ensina as técnicas dos mais diversos crimes, indo desde a captura de senhas e identidades às grandes fraudes em sistemas, passando por tráfico de drogas e de armas, contratação de assassinos profissionais, divulgação e prática de pornografia infantojuvenil, etc.

Uma diferença interessante talvez seja com relação às categorias de crimes digitais citadas anteriormentes. Para cometer os crimes cibernéticos próprios, o criminoso depende de uma expertise na área da informática. Esses crimes serão cometidos por hackers, justamente por ser preciso um maior grau de técnica para praticar a conduta. Já no caso dos crimes digitais impróprios, que nada mais são do que crimes comuns praticados com a utilização de computadores (ameaças, furtos, extorsões, cyberbulling etc), o criminoso não necessita de possuir conhecimentos técnicos especiais.

Trazendo para a realidade do Brasil, verifica-se que o cibercriminoso brasileiro é um dos mais ativos e criativos do mundo. Assolini (2015)[5], em seu artigo publicado no site https://securelist.com/ intitulado "Beaches, carnivals and cybercrime: a look inside the Brazilian underground" aponta o submundo criminoso brasileiro possui alguns dos autores mais criativos, e assim como seus colegas de crime da China e Rússia, procuram focar seus ataques cibernéticos no próprio país, ou seja, os cibercrimosos do Brasil procuram atacar brasileiros, pois seus ataques são projetados para refletir sites do cenário nacional, além de acharem aqui um público-alvo bem expressivo, com mais de 100 milhões de internautas, 141

[5] Disponível em https://securelist.com/beaches-carnivals-and-cybercrime-a-look-inside-the-brazilian-underground/72652/. Acesso em 06 jun. 2018.

milhões de eleitores e mais de 50 milhões de pessoas que utilizam serviços de banco disponibilizado na web todo dia.

SUJEITO PASSIVO DOS CRIMES CIBERNÉTICOS

Conceituar o sujeito passivo dos crimes cibernéticos é de extrema importância nesse trabalho, porque seu número vem aumentando. Basta uma pessoa ter um celular ou computador conectado que já se torna uma vítima em potencial.

Para tanto, devemos definir bem o conceito de vítima e a mais importante definição pode ser retirada da Resolução 40/34, de 29 de novembro de 1985 da Assembléia Geral da ONU, que esclarece:

> Entendem-se por "vítimas" as pessoas que, individual ou coletivamente, tenham sofrido um prejuízo, nomeadamente um atentado à sua integridade física ou mental, um sofrimento de ordem moral, uma perda material, ou um grave atentado aos seus direitos fundamentais, como conseqüência de atos ou de omissões violadores das leis penais em vigor num Estado membro, incluindo as que proíbem o abuso de poder.[6]

Brito (2013, p. 88) em seu livro Direito Penal Informático afirma que:

> As vítimas em potencial que somos todos nós – devem exercer o seu papel de vigilância na rede, cuidando principalmente da integridade das suas informações pessoais. Algumas pessoas ainda acreditam que é possível, nos dias de hoje, ganhar um milhão de dólares por e-mail de uma pessoa desconhecida.
> Portanto, qualquer pessoa, física ou jurídica, individual ou coletiva, que esteja ligada, através de um computador, a uma rede de computadores com ou sem conexão a internet tem grandes chances de se tornar vítima de um crime informático caso nao tome os devidos cuidados.
> Ressaltamos o papel individual de vigilância na rede, pois há registros de que grande parte dos delitos informáticos hoje só é possivel graças à participação efetiva e direta da vitima. Como falamos, algumas pessoas. iludidas com a oferta de prêmios ou vantagens fáceis de serem adquiridas, acabam fornecendo informações pessoais, como dados bancários e de cartões de crédito, dificultando corn isso o trabalho de quem luta pela redução desse tipo de delinquência.
> Albert Einstein afirmou que apenas duas coisas são infinitas: O Universo e a estupidez humana, mas não tinha certeza se isso era verdadeiro em relação ao primeiro. E a afirmação só vem se comprovando com o sucesso da Engenharia Social somada a utilização das novas tecnologias da informação.

[6] Texto original: "Victims" means persons who, individually or collectively, have suffered harm, including physical or mental injury, emotional suffering, economic loss or substantial impairment of their fundamental rights, through acts or omissions that are in violation of criminal laws operative within Member States, including those laws proscribing criminal abuse of power. Disponível em: http://www.un.org/documents/ga/res/40/a40r034.htm. Acesso em 02 jun. 2018.

Analisando esse conceito, conclui-se que todas as pessoas que tiverem acesso a internet podem ser vítimas do cibercrime.

Para termos uma noção do quanto isso representa em números no Brasil, só a título exemplificativo, em 2016, o IBGE registrou que "Das 179,4 milhões de pessoas com 10 anos ou mais, 64,7% utilizaram a Internet pelo menos uma vez nos 90 dias que antecederam à data de entrevista nos domicílios pesquisados ao longo do último trimestre de 2016"[7].

Essas pessoas totalizam 116,07 milhões, com acesso a rede mundial de computadores e serviços online. Cada uma delas é uma vítima em potencial, algo muito atrativo no mundo do crime virtual.

ANÁLISE DO CRESCIMENTO DOS CRIMES CIBERNÉTICOS NO MUNDO E NO BRASIL

O mercado do crime virtual causa prejuízos de bilhões de dólares anuais às pessoas e empresas, e a cada ano que passa, esses danos continuam crescendo, conforme os relatórios das empresas de segurança.

Ao ponderar sobre essa variável do crescimento do cibercrime, observa-se que aumentou de forma exponencial.

Em 2015, o Relatório do Norton Cybersecurity Insights Report[8] aponta que 594 milhões de pessoas foram afetadas pelo cibercrime globalmente, com US$ 150 bilhões de prejuízo. No Brasil, o prejuízo foi de R$ 45 Bilhões (que dá aproximadamente US$ 13,51 bilhões de dólares, utilizando-se uma média do dólar a R$ 3,331).

Já em 2016, conforme o relatório de segurança da Norton Cyber Security, 21 países foram afetados por cibercrimes, com 689,4 milhões de usuários atingidos, com prejuízo financeiro de aproximadamente US$125,9 bilhões. Só no Brasil, foram 42,4 milhões de usuários, dos 116 milhões que acessam a internet, com US$10,3 bilhões de prejuízos[9].

[7] Disponível em: https://agenciadenoticias.ibge.gov.br/agencia-noticias/2013-agencia-de-noticias/releases/20073-pnad-continua-tic-2016-94-2-das-pessoas-que-utilizaram-a-internet-o-fizeram-para-trocar-mensagens.html. Acesso em 06 jun. 2018
[8] Disponível em: https://us.norton.com/norton-cybersecurity-insights-report-global?inid=hho_norton.com_cybersecurityinsights_hero_seeglobalrpt. Acesso em: 13 mai. 2018.
[9]Disponível em: https://www.symantec.com/content/dam/symantec/br/docs/reports/2016-norton-cyber-security-insights-comparisons-brazil-pt.pdf. Acesso em: 13 mai. 2018.

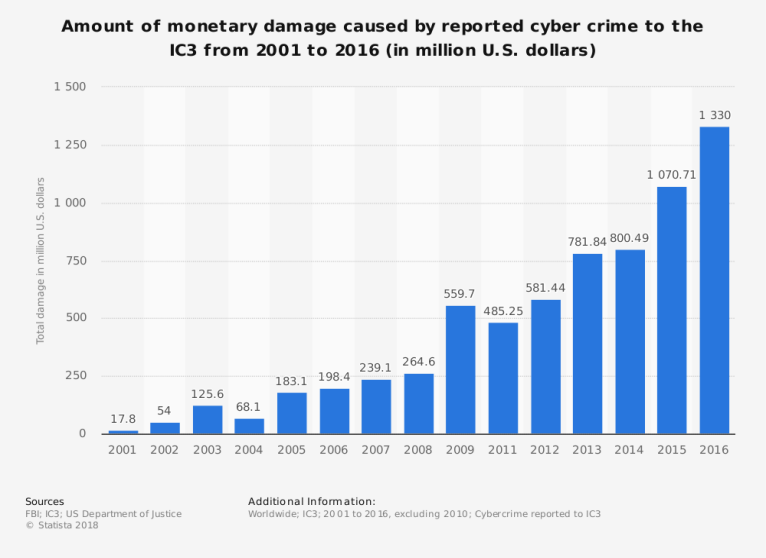
Da mesma forma, no ano de 2017, o Norton Cyber Security Insights Report[10], constatou que aproximadamente 978 milhões de pessoas em 20 países foram afetadas pelo cibercrime, com perdas de 172 bilhões de dólares. No Brasil foram afetadas 62,21 milhões de pessoas, com prejuízos da monta de US$ 22,5 bilhões Ressalte-se que o Brasil ficou em segundo no ranking, de quem mais perdeu com o cibercrime em bilhões de dólares, ficando atrás apenas da China[11].

De 2015 até 2017, houve um aumento de 384 milhões de pessoas afetadas pelo cibercrime, o que dá um crescimento de 64,65% nos usuários atingidos.

Esses dados demonstram que o cibercrime cresce exponencialmente, o que pode ser constatado observando-se outros dados colhidos de sites de segurança.

Por sua vez, o site www.statista.com, analisando a quantidade de danos monetários causados por crimes cibernéticos nos Estados Unidos entre os anos de 2001 e 2016[12] mostra um gráfico alarmante, que demonstra um crescimento exponencial dos prejuízos causados pelos crimes cibernéticos:

Gráfico 1 – Dano causado por cibercrimes de 2001 a 2016

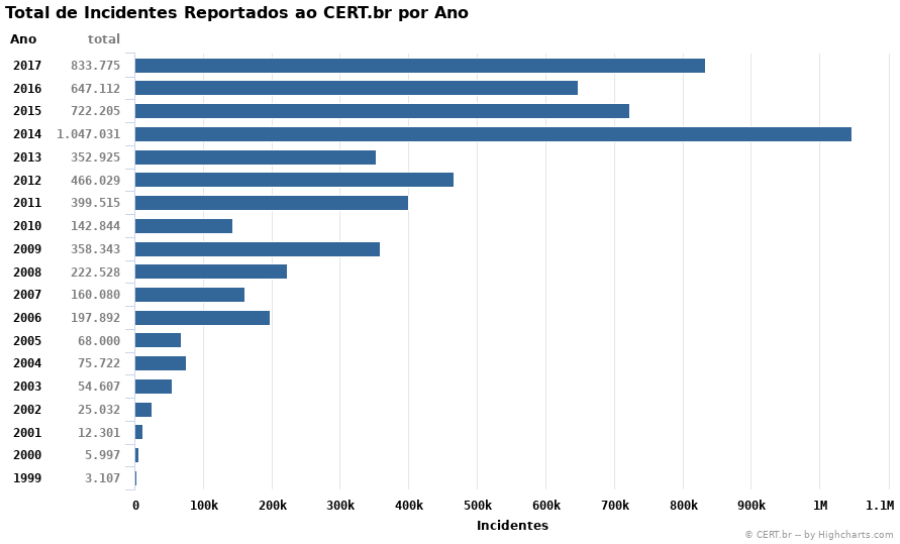


Fonte: Statista.com(2018)

[10] Disponível em: http://now.symassets.com/content/dam/norton/global/pdfs/norton_cybersecurity_insights/NCSIR-global-results-US.pdf. Acesso em: 13 maio 2018.
[11] Disponível em: https://www.statista.com/statistics/799875/countries-with-the-largest-losses-through-cybercrime/ . Acesso em: 03 jun. 2018.
[12] Disponível em: https://www.statista.com/statistics/267132/total-damage-caused-by-by-cyber-crime-in-the-us/ . Acesso em: 13 maio 2018.

Analisando esse crescimento no Brasil, com a utilização dos dados colhidos do site CERT.br, Grupo de Resposta a Incidentes de Segurança para a Internet no Brasil, que é responsável por tratar incidentes de segurança em computadores que envolvam redes conectadas à Internet no Brasil, podemos observar o mesmo crescimento:

Gráfico 2 – Estatísticas dos Incidentes Reportados ao CERT.br



Fonte: CERT.br (2017)

Essa estatística informa apenas os incidentes reportados e não a totalidade. Nela pode-se notar que em 1999 apenas 3.107 incidentes foram reportados, enquanto que em 2017, 833.775 incidentes foram contabilizados, totalizando um aumento de 26.735,37%. Se utilizarmos apenas as variáveis de 2015 e 2017, verifica-se que em 2015 ocorreram 722.205 incidentes, e em 2017 houve 833.775 casos, que significa um aumento de 111.570 usuários atingidos, ou 15,45%.

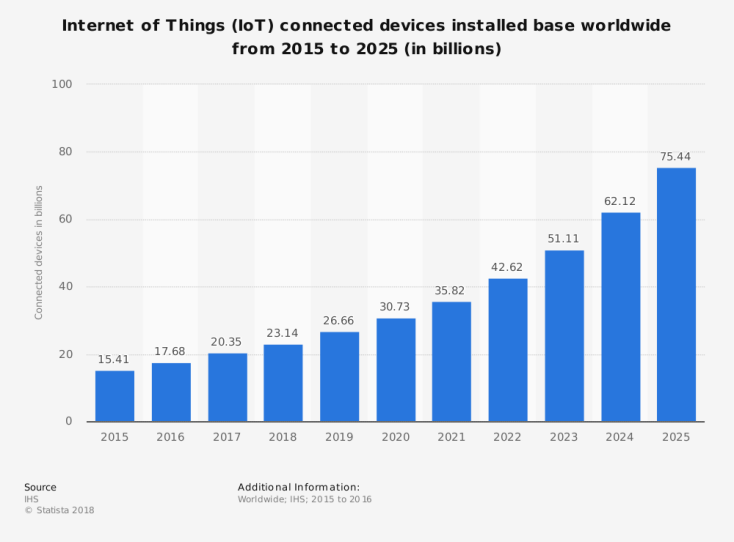
Um dos motivos pode relacionar-se ao aumento do número de aparelhos que cada vez mais se conectam a internet a cada ano.

Analisando a taxa de crescimento de aparelhos conectados, conforme o site www.statista.com pode perceber que em 2015, havia 15,41 bilhões de aparelhos conectados e nesse ano de 2018, a projeção é de que 23,14 bilhões de aparelhos estejam na rede mundial de computadores, ou seja, um aumento de 51,16% da quantidade de aparelhos que estão na rede.

Com a popularização da IoT, temos uma projeção de que até 2025 teremos 75,44 bilhões[13] de aparelhos conectados a internet, um aumento de 389,55% em relação a 2015.

Essa estatística é um resumo das previsões de 2017 para a Internet das Coisas que foi publicado no site da Forbes[14] a saber:

Gráfico 3 – Projeção de aparelhos que estarão conectados de 2015 a 2025.



Fonte: Statista.com

Essa variável demonstra que estaremos mais conectados do que nunca, porém, não demonstra que essas pessoas estão mais seguras.

Ao observar todos esses gráficos, verifica-se que possuem curvas de crescimento parecidas. E o cenário não é otimista. De acordo com o site Cybersecurity Ventures, o cibercrime causará danos na ordem de US$ 6 Trilhões até 2021[15], incluindo nessa previsão, os danos e destruição de dados, furto de dinheiro, perda de produtividade, furto de propriedade intelectual, dados pessoais e financeiros, crimes, interrupção de negócios, custos de investigação forense, restauração e exclusão de dados e sistemas invadidos, além de danos à reputação, sendo tratado como uma das maiores ameaças para cada empresa no mundo e um dos maiores problemas da humanidade.

Portanto, pode-se relacionar o crescimento do número de aparelhos conectados na internet com o crescimento na quantidade de danos causados pelos criminosos na internet, e o

[13] Disponível em: https://www.statista.com/statistics/471264/iot-number-of-connected-devices-worldwide/. Acesso em: 14 de maio de 2018.
[14]Disponível em: https://www.forbes.com/sites/louiscolumbus/2017/12/10/2017-roundup-of-internet-of-things-forecasts/#3aabcc41480e . Acesso em: 14 de maio de 2018.
[15] Disponível em: https://cybersecurityventures.com/hackerpocalypse-original-cybercrime-report-2016/. Acesso em: 13 de maio de 2018.

Brasil está nas primeiras colocações do ranking de perdas. É fato que grande parcela da população sofrerá com isso, e desse conjunto de vítimas, poucas saberão o que fazer para reagir após sofrer um ataque virtual.

TRATAMENTO DA PROVA EM CRIMES CIBERNETICOS

A maioria dos sites de proteção foca sua estratégia na prevenção. Em uma rápida pesquisa no site da Symantec corporation, por exemplo, na página "Como reconhecer e se proteger contra o crime cibernético"[16] pode-se observar que as abordagens são de precaução, e sempre giram em torno do que fazer para se proteger contra o crime cibernético. Usar um antivírus, ter senhas fortes, manter os softwares atualizados, gerenciar configurações de mídias sociais, proteger sua rede doméstica, e se suspeitar que foi vítima, procurar a polícia. E só.

O fato é que mesmo com essas dicas, os sites não explicam o procedimento correto para se fazer DEPOIS que as pessoas forem vítimas de um crime virtual.

A primeira providência que devemos fazer é preservar a prova.

E por quê?

Embora existam inúmeros delitos cibernéticos e ações prejudiciais para as pessoas, e esse artigo procura expor de uma forma genérica as formas de salvaguardar a maioria das provas existentes pela própria vítima do crime, de modo a ajudar os investigadores como conseguir identificar a autoria e chegar a uma condenação do crime.

A primeira coisa que a pessoa atingida deveria fazer, é preservar a prova para poder futuramente responsabilizar o criminoso, seja na esfera cível ou criminal.

Mas como? Primeiro, temos que entender o conceito de prova, para então mostrar as formas de como preservá-la.

Provar significa demonstrar a veracidade ou autenticidade de alguma coisa como sendo verdade. O objetivo da prova é deixar claro para o juiz a realidade de um fato ou acontecimento. E no universo da informática, uma informação é extremamente volátil. Se não conseguirmos preservá-la rapidamente, pode ser modificada ou excluída.

Para Nucci (2015, p. 20), a prova tem três sentidos:

[16] Disponível em: https://br.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html. Acesso em 03 jun. 2018.

> a) como ato: é o processo pelo qual se verifica a exatidão do fato alegado pela parte (ex.: fase da prova); b) como meio: trata-se do instrumento pelo qual se demonstra a verdade de algo (ex.: prova testemunhal); c) como resultado: é o produto extraído da análise dos instrumentos de prova oferecidos, demonstrando a verdade de um fato. Neste último senso, pode dizer o juiz, ao chegar à sentença: "Fez-se prova de que o réu é autor do crime".

Podemos concluir que a finalidade da prova é a comprovação lógica do fato, para gerar na pessoa a que se destina a certeza do que foi alegado. A vítima, ainda mais nesses casos tem que realizar um esforço para extrair o maior número possível de elementos necessários para convencimento do destinatário da prova, seja o delegado ou juiz.

DA EVIDÊNCIA DIGITAL E A IMPORTÂNCIA DE SUA PRESERVAÇÃO

Em um crime comum, praticado no mundo real, podem existir vestígios a serem coletados. Um fio de cabelo, DNA, uma faca deixada no local do crime ensangüentada, uma impressão digital do criminoso. Tudo isso são vestígios a serem coletados e utilizados para se chegar ao autor do crime.

No mundo da informática, contudo, os vestígios são digitais, são bits e bites que podem representar qualquer tipo de informação. Um site criado para denegrir alguém, um e-mail compartilhando pornografia infantil, a invasão de um site governamental, a disseminação de um vírus, a exposição de fotografias íntimas de alguém nas redes sociais, a criação de perfis falsos para prejudicar alguém, o ciberbulling, racismo, dentre outras inúmeras condutas que podem ser praticadas por um cibercriminoso.

É preciso identificar, isolar, coletar e preservar o vestígio cibernético. A correta identificação, o mais rápido possível pode ajudar a identificar o criminoso, pois geralmente, ainda mais no caso do Brasil, pode ser possível identificá-lo.

Eleutério e Machado (2010, p. 16) ao abordarem os vestígios, esclarecem:

> "Crimes sempre deixam vestígios!" – é uma frase dita costumeiramente pelas pessoas. Vestígio, segundo o dicionário Michaelis da Língua Portuguesa, é definido como "1 Sinal deixado pela pisada ou passagem, tanto do homem como de qualquer outro animal; pegada, rasto. 2 Indício ou sinal de coisa que sucedeu, de pessoa que passou. 3 Ratos, resquícios, ruinas. Seguir os vestigios de alguém: fazer o que ele fez ou faz; imitá-lo.". No caso da computação, os vestígios de um crime são digitais, uma vez que toda a informação armazenada dentro desses equipamentos computacionais é composta por bits (números zeros e uns), em uma sequência lógica.

Como dito acima, o crime cibernético pode envolver uma gama muito abrangente de condutas e a vítima de um cibercrime deve tomar algumas precauções, porque a evidência digital possui algumas características peculiares, segundo Barreto e Brasil (2016, p. 31), podendo ser: "volátil, anônima (em princípio), alterável e/ou modificável, bem como pode ser eliminada a qualquer instante". E prosseguem, explicando que:

> A preservação é de grande importância em razão da volatilidade dos dados na internet, podendo estes ser rapidamente manipulados, alterados ou deletados. Nesse ínterim, o usuário responsável pela postagem de conteúdo ofensivo poderá modificar ou excluir o conteúdo, dificultando a individualização da autoria e materialidade delitiva.

Preservar a evidência de crimes virtuais é um dos grandes empecilhos que a investigação se depara. A vítima geralmente não sabe o que fazer, ou demora demais até procurar a delegacia de polícia, que após os trâmites normais de instauração de inquérito, solicitará uma ordem judicial para conseguir os registros de conexão e acesso a aplicação da internet, e isso estamos falando somente em casos que os crimes foram praticados na internet, sem afetar o computador da vítima. O responsável pela investigação muitas vezes se depara com essas barreiras.

Essa prova pericial, até ser feita pelos peritos competentes, pode vir a ser prejudicada pela demora, impossibilitando uma identificação da autoria e posterior condenação. Nesse sentido a vítima pode ajudar a preservar a prova, realizando alguns procedimentos imediatos que ajudariam a investigação, tão logo tome conhecimento do delito.

FORMAS DE PRESERVAÇÃO DA EVIDÊNCIA DIGITAL PELA VÍTIMA

E esses procedimentos que a pessoa prejudicada pode fazer para salvaguardar os dados são simples e ao seu alcance, mas muitas vezes desconhecidos deles, seja por falta de conhecimento ou informação. As possibilidades são as seguintes:

A principal forma é a impressão do site. Essa seria a forma inicial, porém existem outras opções a serem utilizadas para dar mais fidedignidade para a prova que irá apresentar ao Delegado para fortalecer a investigação.

A segunda forma seria a utilização da tecla *print screen*, que gera uma imagem do que estiver aparecendo na tela do computador da vítima. Após, a vítima pode colar essa imagem em um programa de edição de imagens, como no "paint" do Windows, ou em um editor de

textos, como Libre Office, podendo ser feito um relatório acerca dos fatos e entregue ao Delegado para investigar ou advogado para ingressar com a ação cível correspondente contra a pessoa.

Essa forma de preservar a prova não é recomendada. Sua validade jurídica é questionável, pois pode ser facilmente editada nesses mesmos editores de imagens utilizados para gravar o print da tela, além de metadados e dados importantes das páginas serem perdidos.

Nesse sentido, esclarecem Barreto e Brasil (2016, p. 39):

> Quando for utilizada a tecla *printscreen* ou for feito um *screenshot* (foto da tela), copia-se a tela que está aparecendo no terminal, transformando-a em imagem, sem entretanto, salvar os metadados que compõem esse conteúdo, perdendo informações importantes sobre este, como as propriedades de criação, localização geográfica, etc. Além do mais, com qualquer editor de imagens é possível modificar o conteúdo apresentado, eis que fora produzido unilateralmente.
> As redes sociais, por exemplo, possuem uma infinidade de dados nem sempre capazes de serem alcançados apenas com uma simples captura de tela. No Facebook, por exemplo, há diversos metadados associados a uma conta individual que precisam ser salvos de forma correta para que tenha um valor probatório.

Você pode até fazer o *screenshot* da tela, mas deverá ser utilizada em conjunto com outras formas de preservação.

A terceira possibilidade é a utilização do salvamento de cópia da página em arquivos .html, que existe por padrão em todos os navegadores, geralmente está na aba arquivo ou ferramentas e coloca o salvar página como página web completa. Aqui, criam-se dois arquivos, um HTML com o nome da página e uma pasta com os arquivos linkados.

Também não é a melhor prática para preservar uma prova. Aqui o maior problema reside em que os links que fazem parte do arquivo não são salvos, tendo que fazer isso pra cada um dos vínculos que interesse ao procedimento investigativo. Outro grave problema, é que a página HTML salva pode ser editada ou manipulada, por alguém com conhecimento mínimo de linguagem HTML padrão.

A quarta forma é utilizar programas de softwares específicos, que fazem o download de todo o conteúdo da página criminosa inclusive os links. Um desses aplicativos, por exemplo, é o HTTrack Website Copier[17], de fácil uso e extremamente útil. Pode-se gerar uma cópia da webpage criminosa incluindo-se os links vinculados que sejam importantes para comprovar o delito. O próprio software gera um log da gravação feita e um arquivo de índex,

[17] Disponivel em: https://www.httrack.com/page/2/en/index.html. Acesso em 08 jun. 2018.

possibilitando-se gravar tudo em uma mídia não regravável e posteriormente encaminhar o conteúdo para a perícia ou delegado. Uma resalva aqui é no caso dos sites com acesso de login e senha, no qual o HTTrack não pode ser utilizado.

Todas as quatro formas acima narradas, tem um ponto fraco. A simples juntada aos autos de investigação não é suficente para produzir uma prova robusta para uma condenação, pois foram produzidas por parte interessada e de forma unilateral.

Para que tenham integridade e veracidade, é necessário que as pessoas que as produzam tenham fé pública. No caso, um escrivão de polícia poderia certificar a coleta, ou um tabelião do cartório do registro de notas poderia lavrar uma ata notarial, para dar validade a prova.

Portanto, a quinta modalidade é a certidão elaborada por escrivão de polícia ou outro servidor que tenha fé pública. Wendt e Jorge (2012, p. 73), esclarecem acerca da utilização desta forma de preservação da prova:

> [...] O agente policial, na condição de "Escrivão", tem fé pública sobre seus atos e pode, acessando uma página na internet, promover a sua impressão e certificar data e existência. Assim, também pode e deve usar todos os meios disponíveis.
> Nada impede que o Escrivão de Polícia possa, ao certificar a data e a existência de um site e seu conteúdo, utilizar o programa HTTrack Website Copier, ou, caso não tenha condições técnicas de empregar esse programa, para realizar a cópia do site ele possa usar a tecla "´print screen" e colar o texto no conteúdo da certidão, propriciando seu melhor entendimento. Apesar dessa forma de aquisição de indícios não ser recomendável, nas hipóteses em que a referida ação for realizada pelo Escrivão de Polícia, ela pode ser empregada em virtude da presunção de veracidade do conteúdo da certidão. O mesmo pode também ser feito nos casos em que for necessário inserir login e senha, pois nestes casos o referido programa não realiza a cópia do site.
> Cabe salientar que a perspectiva de utilização da certidão do Escrivão de Polícia agrange também qualquer cidadão que deseje comunicar um fato criminoso por intermédio do registro de um boletim de ocorrência. Nestes casos a vítima deve procurar uma Delegacia de Polícia e, após a elaboração do boletim de ocorrência, solicitar que promova a impressão do conteúdo do site ou blog que contenha os fatos criminosos.

Por fim, a última possibilidade de preservação da prova é a ata notarial. Podemos conceituar como o documento escrito, lavrado pelo tabelião, que possui fé pública, para atestar a existência de um fato específico ou situação.

Neste documento, o tabelião não pode emitir nenhum juízo de valor sobre o que está vendo na tela do computador, deve apenas descrever o que observa, sem modificar qualquer conteúdo. É pouco conhecido, mas tem sido utilizado como importante meio de prova.

Barreto e Brasil (2016, p. 42), narram que a ata notarial já foi empregada para "constatação de página na internet, ofensas proferidas em fórum de debate na internet e crime contra a honra publicada em comentário de blog".

A ata notarial comprova inúmeros fatos na internet, dentre eles, podemos citar: o teor de páginas da internet armazenadas no computador telefone celular, constatação de e-mails, aplicativos de comunicação via internet (WhatsApp, Messenger, Viber, Telegram, dentre outros), conteúdos postados no facebook e no twitter e instagram. E não para por ai. As possibilidades são infinitas.

Está prevista no art. 384 do Código de Processo Civil, a saber:

> Art. 384. A existência e o modo de existir de algum fato podem ser atestados ou documentados, a requerimento do interessado, mediante ata lavrada por tabelião.
> Parágrafo único. Dados representados por imagem ou som gravados em arquivos eletrônicos poderão constar da ata notarial.

Note-se que até mesmo dados representados por imagens ou sons podem se representados na ata notarial.

Pode ser utilizada para inúmeros casos, dos quais cito alguns exemplos retirados do site do 26º Cartório de Notas de Brasília[18]:

> **Atas de internet:** prova o conteúdo divulgado em páginas da internet.
> **Atas de mídia social (Facebook, Twitter, Youtube etc.):** prova o conteúdo divulgado em redes sociais, microblogs e vídeos.
> **Atas de mensagem eletrônica (e-mail):** prova o conteúdo de mensagens e o IP emissor.
> **Atas de mensagem instantânea (WhatsApp, Skype, Snapchat, SMS, etc.):** prova o conteúdo de mensagens e o número/conta emissora.
> **Atas de diálogo telefônico:** prova o conteúdo do diálogo entre os interlocutores.(negrito do autor)

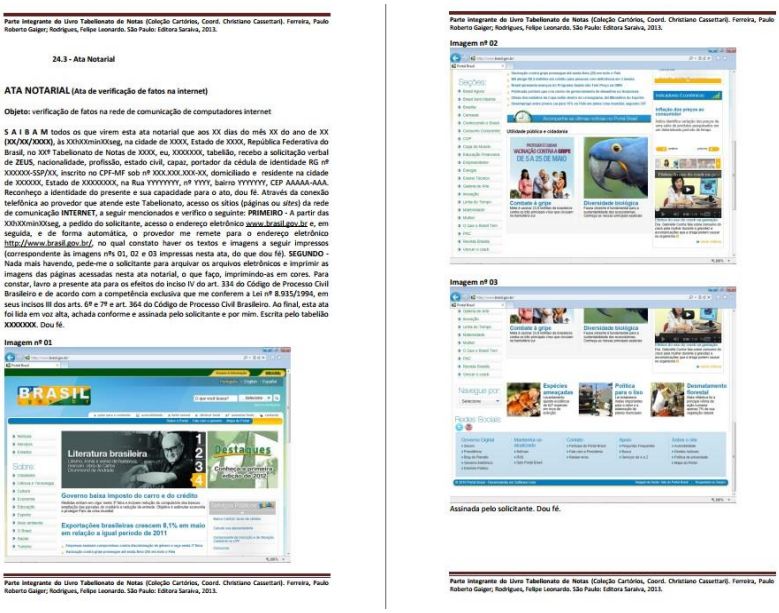
O procedimento é simples. A vítima do crime praticado na internet procura o Cartório de Registro de Notas, com computador, telefone ou acessando o próprio terminal do cartório e solicita que seja feita a ata notarial. Na ata, deverá constar o requerimento da vítima para que o tabelião faça a elaboração da ata, com a indicação do local, hora, dia, mês e ano da realização.

Esse é é um importante instrumento que deve ser amplamente divulgado na sociedade, de modo a se tornar útil e possibilitar o seu uso como importante aliado para resguardar direitos futuros e identificar a autoria de crimes.

[18] Disponível em: https://www.26notas.com.br/servicos/ata-notarial. Acesso em 11 jun. 2018.

Abaixo, um modelo de ata notarial é disponibilizado, para se ter uma noção de como é feita.

Figura 1 – Modelo de Ata Notarial



24.3 - Ata Notarial

ATA NOTARIAL (Ata de verificação de fatos na internet)

Objeto: verificação de fatos na rede de comunicação de computadores internet

S A I B A M todos os que virem esta ata notarial que aos XX dias do mês XX do ano de XX (**XX/XX/XXXX**), às XXhXXminXXseg, na cidade de XXXX, Estado de XXXX, República Federativa do Brasil, no XXº Tabelionato de Notas de XXXX, eu, XXXXXXX, tabelião, recebo a solicitação verbal de **ZEUS**, nacionalidade, profissão, estado civil, capaz, portador da cédula de identidade RG nº XXXXXX-SSP/XX, inscrito no CPF-MF sob nº XXX.XXX.XXX-XX, domiciliado e residente na cidade de XXXXXX, Estado de XXXXXXXX, na Rua YYYYYYYY, nº YYYY, bairro YYYYYYY, CEP AAAAA-AAA. Reconheço a identidade do presente e sua capacidade para o ato, dou fé. Através da conexão telefônica ao provedor que atende este Tabelionato, acesso os sítios (páginas ou sítes) da rede de comunicação **INTERNET**, a seguir mencionados e verifico o seguinte: **PRIMEIRO** - A partir das XXhXXminXXseg, a pedido do solicitante, acesso o endereço eletrônico www.brasil.gov.br e, em seguida, e de forma automática, o provedor me remete para o endereço eletrônico http://www.brasil.gov.br/, no qual constato haver os textos e imagens a seguir impressos (correspondente às imagens nºs 01, 02 e 03 impressas nesta ata, do que dou fé). **SEGUNDO** - Nada mais havendo, pede-me o solicitante para arquivar os arquivos eletrônicos e imprimir as imagens das páginas acessadas nesta ata notarial, o que faço, imprimindo-as em cores. Para constar, lavro a presente ata para os efeitos do inciso IV do art. 334 do Código de Processo Civil Brasileiro e de acordo com a competência exclusiva que me conferem a Lei nº 8.935/1994, em seus incisos III dos arts. 6º e 7º e art. 364 do Código de Processo Civil Brasileiro. Ao final, esta ata foi lida em voz alta, achada conforme e assinada pelo solicitante e por mim. Escrita pelo tabelião XXXXXXX. Dou fé.

Imagem nº 01

Imagem nº 02

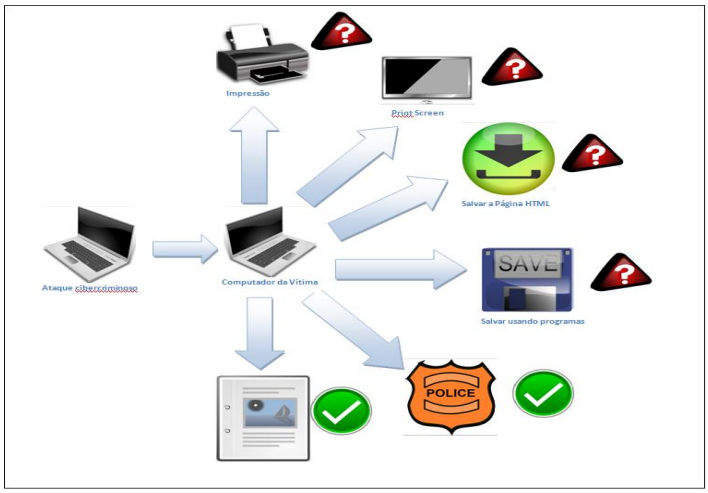
Imagem nº 03

Assinada pelo solicitante. Dou fé.

Fonte: 26º Tabelionato de Notas (2018)[19]

Esses seis meios usuais que o usuário de computador leigo (potencial vítima), pode utilizar para se resguardar de eventuais problemas, bem como para provar a existência e autoria de determinado crime praticado na internet. Para melhor ilustrar esses procedimentos, segue esquema:

Esquema 1 – Procedimentos



Fonte: Própria (2018)

[19] Disponível em: https://www.26notas.com.br/blog/wp-content/uploads/2013/06/Minutas-para-estudo_Livro-Tabelionato-de-Nota s_2013-v2.pdf. Acesso em: 09 jun 2018.

CONSIDERAÇÕES FINAIS

Convergimos cada vez mais para a informatização e virtualização da sociedade, o que nos deixa extremamente vulneráveis. Conforme demonstrado acima, o cibercrime só aumenta com o passar dos anos. E mesmo com todos os gastos feitos pelas empresas e consumidores para se proteger, esses crimes não tendem a diminuir.

Os dados apresentados nesse artigo convalidam a hipótese de que grande parte da população mundial sofrerá com os delitos virtuais. E não saberá como reagir quando for vítima de um cibercrime.

E uma das possíveis respostas para esse problema é a utilização de mecanismos para preservar o fato que aconteceu, antes que desapareça, na volatilidade do mundo virtual. Seis possibilidades foram levantadas: imprimir, tirar print screen da tela, salvar a página, utilizar um software de captura de páginas da web, fazer uma certidão do escrivão de polícia e registrar uma ata notarial.

Dessas possibilidades, as duas que melhor se adequam ao conceito de prova aceita nos tribunais, que são: a certidão do escrivão de polícia e a ata notarial. Instrumento pouco conhecidos das pessoas, mas que estão a sua disposição.

Para que essas duas formas de preservação passassem a ser de conhecimento maior dos internautas, seria necessário que houvesse uma conscientização em massa das pessoas, seja por intermédio da imprensa, das redes sociais, dos sites de opinião, ou até mesmo das empresas de segurança, explicando mais detalhadamente o procedimento de como fazer quando alguém for vítima desses crimes.

Esse estudo realizado não esgota todas as hipóteses sobre o problema do crescimento do cibercrime bem como sobre as formas de reação ao seu prejuízo. Novas pesquisas devem ser realizadas para identificar outros fatores preponderantes no aumento da criminalidade e procurar solucionar da melhor forma.

ABSTRACT: Given that cybercrime has increased each year, the reason for this is investigated in order to indicate ways of preserving the evidence for the victim. To do so, it is necessary to define the crimes, the actors, the damages and people affected and the forms of preservation. A quantitative investigation of the growth of the crimes is carried out correlated with the increase of the devices connected in the Internet. Given this, cyber crimes will grow exponentially, and victims will have to preserve evidence for later accountability of offenders, demonstrating the most appropriate type of preservation for the victim to perform, which makes it clear that people need to be more informed about the types of evidence preservation.

Keywords: Cyber Crime, Growth, Victim, Proof, Preservation Form.

REFERÊNCIAS

ASSOLINI, Fábio. **Beaches, carnivals and cybercrime: a look inside the Brazilian underground. 2015**. Disponível em <https://securelist.com/beaches-carnivals-and-cybercrime-a-look-inside-the-brazilian-underground/72652/>. Acesso em 10 jun. 2018.

BARRETO, Alesandro Gonçalves; BRASIL, Beatriz Silveira. **Manual de Investigação Cibernética à Luz do Marco Civil da Internet**. Rio de Janeiro: BRASPORT, 2016.

BRITO, Auriney. **Direito penal informático**. São Paulo: Saraiva, 2013.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais**. São Paulo: Saraiva, 2011.

ELEUTÉRIO, Pedro Monteiro da Silva; MACHADO, Márcio Pereira. **Desvendando a computação forense**. São Paulo: Novatec Editora, 2010.

FERREIRA, Aurélio Buarque de Holanda. **Novo dicionário Aurélio da língua portuguesa** / Aurélio Buarque de Holanda Ferreira; Coordenação Marina Baird Ferreira, Margarida dos Anjos. – 4. ed. – Curitiba: Ed. Positivo: 2009.

LÉVY, Pierre. **Cibercultura**. São Paulo: Ed. 34, 2010. 3ª ed..

MACQUADE, Samuel C., III, **Encyclopedia of Cybercrime**, Westport, Connecticut – London: Greenwood Press, 2009.

NUCCI, Guilherme de Souza. **Provas no processo penal**. – 4. ed. – Rio de Janeiro: Forense, 2015.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes cibernéticos: ameaças e procedimentos de investigação**. – Rio de Janeiro: Brasport, 2012.