Centro Universitário de Brasília Instituto CEUB de Pesquisa e Desenvolvimento - ICPD

JORGE LUIZ VIEIRA DA SILVA FILHO

PROPRIEDADE DE BENS DE CONSUMO VIRTUAIS: CRIMES E LEGISLAÇÃO

Brasília
2017

JORGE LUIZ VIEIRA DA SILVA FILHO

PROPRIEDADE DE BENS DE CONSUMO VIRTUAIS: CRIMES E LEGISLAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* na área de Rede de Computadores, com ênfase em Segurança.

Orientador: Profº Rafael Sarres, Msc

Brasília

2017

JORGE LUIZ VIEIRA DA SILVA FILHO

PROPRIEDADE DE BENS DE CONSUMO VIRTUAIS: CRIMES E LEGISLAÇÃO

Trabalho apresentado ao Centro Universitário de Brasília (UniCEUB/ICPD) como pré-requisito para a obtenção de Certificado de Conclusão de Curso de Pós-graduação *Lato Sensu* na área de Rede de Computadores, com ênfase em Segurança.

Orientador: Profº Rafael Sarres, Msc

Brasília, 10 de abril de 2017.

Banca Examinadora

_____

Prof.º. Gilberto de Oliveira Netto, MA

_____

Prof.º. Drª Gilson Ciarallo

Simples como uma criança... e profundo como um filosofo... Severo como um juiz... e carinhoso como uma mãe... terrível como a tempestade... e meigo como a luz do sol... Este é o exemplo a ser seguido... o trabalho a ser imitado... a lição a ser aprendida...pois o preceito é uma lâmpada, e a instrução a luz.

AGRADECIMENTO (S)

Gostaria de agradecer àqueles que me deram força e incentivo durante toda a minha caminhada até aqui. Mas, primeiramente, a minha querida mãezinha, mulher batalhadora e de fé. Pois se cheguei onde estou, foi por causa dela. A minha namorada, Caroline Faiad, por todo apoio e suporte.

— Deus quer... O Homem Sonha... A Obra Nasce... ‖

—Por mares nunca antes navegados... navegar é preciso... viver... viver não é preciso‖

Camões

RESUMO

Esse trabalho apresenta um estudo sobre o que é propriedade de bens de consumo virtuais e como os usuários interagem com esses bens na Internet, analisando como o mundo começou a se preocupar com a segurança na Internet e a proteger os usuários de cibercrimes. A pesquisa baseou-se no levantamento de dados históricos sobre a construção da legislação mundial sobre crimes virtuais relacionados à Internet, buscando conceitos técnicos herdados de escolas especializadas na rede mundial de computadores que surgiu no seu crescimento, bem como na análise sobre o surgimento do ordenamento jurídico brasileiro na segurança da informação, confrontando opiniões de alguns pesquisadores analisando os prós e contras da implementação da legislação no Brasil. Também foram analisadas as vulnerabilidades mais comuns na Internet, pesquisando as formas mais utilizadas por criminosos, isto é, para cometer crimes virtuais, foram apresentadas técnicas simples para proteção dos dados na Internet, com o objetivo de auxiliar aqueles que desejam se resguardar no perigoso mundo online. Por fim, faz-se uma análise de alguns crimes cibernéticos no mundo e no Brasil, de como aconteceram e foram solucionados e ainda como são assistidos pela população brasileira e mundial.

Palavras-chave: Bens Virtuais. Cibercrime. *Online*.

ABSTRACT

This paper presents a study on what is virtual consumer goods property and how its users interact with such goods on the Internet, analyzing how the world has begun to worry about Internet safety and to protect users from cybercrime. The research is based on the collection of historical data about the construction of the worldwide legislation on virtual crimes related to the internet. We search for technical concepts inherited from specialized schools in the worldwide computer network that appeared in its growth, as well as in the analysis on the emergence of the Brazilian legal system in information security, confronting the opinions of some researchers that analyzed the pros and cons of the implementation of such legislation in Brazil. The most common vulnerabilities on the Internet were also analyzed, researching the forms most used by criminals (to commit cybercrimes). As a result, we presented simple techniques for data protection on the internet, with the aim of helping those who wish to safeguard themselves in the dangerous online world. Finally, an analysis of some cybercrimes worldwide and in Brazil is made, looking for how did they happen and how were they solved and still how have they been assisted by the Brazilian and worldwide population.

Key words: Virtual Goods. cyber crime. *online*;

LISTA DE FIGURAS

SUMÁRIO

INTRODUÇÃO

A cada dia que passa cresce o número de usuários na rede mundial de computadores, estimulados por novas tecnologias e a procura de ativos digitais, cujo intuito é terem acesso a conhecimentos, socializar com outras pessoas e utilizar da praticidade com fins bancários e comerciais.

Esse processo facilita o acesso dos usuários a recursos *online*, melhorando o seu desempenho com os bens que podem aumentar a sua produção virtual, como: textos, vídeos, áudios, jogos eletrônicos e moedas digitais. Sem contar o acesso ao mercado eletrônico com a praticidade de compras *online* de qualquer lugar do mundo.

Essas práticas carregam a crença, presente na maioria dos usuários, de estarem seguros dentro do ambiente virtual, ou seja, livre de qualquer tipo de ameaça física ou mesmo, livre de outro indivíduo capaz de subtrair seus bens de consumidor dos produtos e plataformas citadas.

Porém, esse ambiente não é completamente seguro. Assim como no mundo externo existem pessoas mal-intencionadas. Por exemplo, em uma guilda (grupo) de um jogo eletrônico, um dos membros se aproveita de seu alto cargo rouba os cofres e sai do grupo, deixando a guilda sem o ouro pelo qual tantos batalharam. Outro caso é quando acontece um acordo entre dois usuários, ao pagar ao outro usuário a compra de um determinado item (fotos, texto, áudios, vídeos e moedas), um terceiro de má fé se aproveita da oportunidade e furta o item ou arquivo comprado deixando a outra parte desamparada com a perda, que era importante fruto de investimento.

Esse contexto traz novas questões relacionadas à propriedade de bens virtuais dentro de ambientes digitais, como por exemplo: garantir os direitos dos usuários, e o mais importante, se a legislação e o poder judiciário estão preparados para lidar com tais crimes.

Como os profissionais da área de segurança da informação junto com os três poderes governamentais têm agido em relação a esses bens virtuais e quais são os possíveis avanços que ainda podem promover?

Assim, neste trabalho são apresentadas definições sobre o que são bens reais e virtuais através da legislação aplicável, analisando o comportamento de doutrinas no estudo de casos correlacionados, analisando seu funcionamento e explorando a legislação relacionada a bens de consumo virtuais.

Propõe-se, ainda, a análise de como os usuários podem se proteger, evitando ataques virtuais aos seus bens digitais através do estudo de casos. Serão explicados, passo a passo, como ocorreram e como poderiam ser evitados, pesquisar vulnerabilidades e possíveis ataques, bem como buscar ferramentas e soluções já implementadas com a função de prover maior segurança.

Espera-se demonstrar a importância da realização de pesquisas na área, pois pouco se tem discutido sobre esse aspecto até o presente momento em nosso país. Atualmente, poucos possuem conhecimento de como se resguardar juridicamente dos perigos citados. Onde os juristas possuem dúvida e dificuldade de como podem e devem atuar em casos similares.

Este trabalho foi dividido em cinco capítulos. No primeiro capítulo, apresentamos os conceitos de bens reais e bens virtuais segundo a legislação brasileira. São apresentados os conceitos e paradigmas de cada um, realidades pertinentes ao contexto deste estudo. No segundo capítulo é feita uma

contextualização da legislação. Onde essa legislação começou a se preocupar em relação ao ambiente virtual, relacionado aos bens de consumo virtuais. No terceiro capítulo é feita uma análise de alguns casos de crimes virtuais relacionados com ativos digitais, verificando como os mesmos foram finalizados. No quarto capítulo são abordados os procedimentos de segurança para bens virtuais, analisando suas vulnerabilidades e seu papel no serviço ao usuário. No quinto capitulo será apresentado dicas é informações para que os usuários possam se resguardar e se proteger em ambientes virtuais. No sexto capitulo o objetivo é dar as devidas conclusões sobre o estudo desenvolvido nesse trabalho.

BENS DE CONSUMO REAIS E BENS DE CONSUMO VIRTUAIS.

Neste capítulo são apresentados os conceitos de bens virtuais e bens reais, através de doutrinadores estrangeiros e brasileiros, além da legislação nacional sobre o assunto. Como o objeto desse estudo é a propriedade de bens de consumo virtuais, são discutidos apenas as características e especificações relevantes aos bens digitais.

1.1 Bens reais

Bens sempre foram objetos de disputa em diversas civilizações em toda a história da humanidade, mas afinal de contas, o que são bens?

Os “bens”, plural da palavra “bem”, vem do latim *ben*e. Esta palavra possui três formas de ser contextualizada: bens filosóficos, bens econômicos e bens jurídicos, porém, o foco se dará em apenas duas definições: bem econômico e bem jurídico.

Segundo Paulo Nunes (2016), economista pela Universidade Nova de Lisboa, bens econômicos são recursos materiais ou imateriais, que quando utilizado ou consumido, satisfazem uma necessidade concreta sentida pelo homem. Uma refeição é um bem porque satisfaz uma necessidade concreta quando consumida. Da mesma forma, o trigo é também um bem na medida em que satisfaz uma necessidade concreta quando utilizado como matéria-prima na produção de farinha.

Neste trabalho abordamos sobre os bens de consumo e, segundo Thais Pacievitch (2017) da InfoEscola, o mesmo é uma das classificações de bens

econômicos. Então bens de consumo são patrimônios que possuem o objetivo de satisfazer as necessidades de dispêndio das pessoas, com o efeito de agradar a consumação das pessoas, destinados a finalidade de consumir. São propriedades ou objetos que só podem ser utilizados para o consumo, não podendo ser utilizados na criação de outras posses. O que o torna diferente dos bens intermediários, que são utilizados no processo de produção para serem transformados em bens finais, ou dos bens de capitais, que são as máquinas utilizadas pelas indústrias.

Existem os bens de consumo duráveis, semiduráveis e não duráveis. Os duráveis são aqueles bens que podem ser utilizados mais de uma vez, em um longo período de tempo, como um *smartphone* ou um computador. Os não duráveis são aqueles que devem ser consumidos imediatamente, como alimentos e afins. Os semiduráveis são os que se desgastam mais facilmente com o tempo, como roupas e outros acessórios de vestuário.

Segundo o Código Civil Brasileiro (Lei nº 10.406, de 10 de janeiro de 2002), e doutrinadores da central jurídica, bens são aqueles objetos que podem servir a uma relação jurídica. Para que um bem seja um objeto jurídico é necessário que ele possua algumas características:

- Idoneidade para satisfazer um interesse econômico;
- Gestão econômica autônoma;
- Subordinação jurídica ao titular;

Sendo assim, dentro do Código Civil Brasileiro (Lei nº 10.406, de 10 de janeiro de 2002) ainda existem dispositivos específicos que a legislação brasileira não contempla, por considerar distinção de pouca importância pratica, já que esses dispositivos trabalham em conjunto com os que a lei já especifica. Para um melhor entendimento desses dispositivos serão citadas explicações de doutrinadores da

central jurídica (Dos Bens...) correlacionados com o Código Civil Brasileiro, portanto, os bens jurídicos são agrupados em classes que assim ficam:

- ***Bens corpóreos:*** São os bens que possuem existência material, como uma casa, um terreno, um livro etc.
- ***Bens incorpóreos:*** São os bens que não possuem existência tangível e são relativos aos direitos que as pessoas físicas ou jurídicas têm sobre as coisas, sobre os produtos de seu intelecto ou com outra pessoa, apresentando valor econômico, tais como os direitos reais, obrigacionais e autorais.
- ***Bens fungíveis:*** São os bens móveis que podem ser substituídos por outros de mesma espécie, qualidade e quantidade. Por exemplo, dinheiro, roupa e gado.
- ***Bens infungíveis:*** São os insubstituíveis, pois são únicos. Exemplos: escultura e quadro de arte famoso. É importante destacar que um bem fungível poderá rapidamente se tornar infungível em determinada situação. Por exemplo, como foi dito, o dinheiro é um bem fungível, mas se o indivíduo for um colecionador ele se tornará infungível, pois o mesmo irá considera-lo único.
- ***Bens consumíveis:*** São os que se destroem assim que vão sendo usados (alimentos em geral).
- ***Bens inconsumíveis:*** São os de natureza durável, como um livro.
- ***Bens divisíveis:*** São aqueles que podem ser fracionados em porções reais. Por exemplo, terreno e barra de ouro.

- ***Bens indivisíveis:*** São aqueles que não podem ser repartidos, caso contrário, o bem perderá o seu valor econômico. Por exemplo animal, navio e relógio.
- ***Bens singulares:*** São as que, embora reunidas, se consideram de per si, independentemente das demais, consideradas em sua individualidade. Por exemplo, um boi, um carro, mesmo fazendo parte de outra coisa maior (boiada, concessionaria), podem ser vendidos separadamente.
- ***Bens coletivos:*** São constituídos por vários bens singulares, considerados em conjunto, formando um todo único, que passa a ter individualidade própria, distinta de seus objetos componentes, que conservam sua autonomia funcional. Por exemplo, uma biblioteca, que não seria uma se tivesse apenas um livro.
- ***Bens móveis:*** São todos os bens que podem ser transportados, deslocados sem prejuízo em sua estrutura, por movimento próprio ou removidos por força alheia. Exemplos: livros, eletrodomésticos, celulares, dentre outros. Podem ser classificados *em*:

  - Bens móveis por natureza: São os *bens corpóreos* que podem ser removidos sem danos, por força própria ou alheia. Por exemplo, os animais, os materiais de construção ou materiais provenientes da demolição de algum prédio.

  - ***Bens móveis por antecipação***: São *bens imóveis* incorporados ao solo, mas que a vontade humana mobiliza em função da finalidade econômica. Por exemplo, as árvores cortadas para a produção de um determinado produto.

  - ***Bens móveis por determinação de lei:*** São os direitos reais sobre objetos móveis e as ações correspondentes, as energias com valor econômico,

direitos pessoais patrimoniais e suas ações, os direitos de obrigação e as ações respectivas. Exemplos: o Direito autoral sobre um objeto móvel, ou seja, todos relacionados com a produção intelectual, como patentes, desenho industrial, obras artísticas, etc.

- ***Bens imóveis:*** São os bens que não podem ser transportados sem alteração ou danos em sua estrutura. Precisam ter uma escritura e um registro em cartório. Exemplos: Apartamento, Casa, Sitio etc. Podem ser classificados *em*:

  - Bens imóveis por sua natureza: Abrange o solo com sua superfície, os seus acessórios e adjacências naturais, compreendendo as árvores é por acessão física industrial ou artificial que são aquelas adquiridas por meio do trabalho humano e incorporadas ao solo, como as plantações e as construções.

  - Bens imóveis por acessão intelectual**:** São todas as coisas móveis que o proprietário do imóvel mantiver, intencionalmente, empregadas em sua exploração industrial, decoração ou comodidade. Por exemplo, objetos de decoração e máquinas.

  - Bens imóveis por determinação legal: São direitos que não podem ser móveis ou imóveis, mas para fins de segurança jurídica o legislador considera como imóvel. Exemplo: penhor agrícola, apólices da dívida pública dentre outros.

- ***Bem principal:*** São os que existem em si e por si, abstrata ou concretamente, independentes de outros. Por exemplo, um terreno.

- ***Bens acessórios:*** São aqueles cuja existência supõe a existência do principal para existir. Por exemplo, as plantações que precisam de um

terreno. Os acessórios, por sua vez, dos artigos 95 a 97 do Código Civil Brasileiro (Lei nº 10.406, de 10 de janeiro de 2002), classificam se em:

- *Frutos:* Aqueles produzidos em um período, sendo que se retirados, não afetarão o valor da coisa.

- *Produtos:* Aqueles que são extraídos de algo, diminuindo a sua quantidade.

- *Benfeitorias:* Podem ser necessárias, quando feitas para conservação (obras, pagamento de impostos dentre outros). Uteis quando servem para otimizar o uso de algo (adubação) voluntárias, utilizadas para fins de beleza, como jardins e fontes.

- **Bens públicos:** São os que pertencem a pessoas jurídicas de direito público, politicas, à união, aos Estados e aos Municípios.

  - Bens públicos *de uso comum do povo:* São os que, embora pertencentes as pessoas jurídicas de direito público interno, podem ser utilizados, sem restrição, e gratuitamente, por todos, sem a necessidade de qualquer permissão especial. Por exemplo, praia, ruas e praças.

  - Bens públicos *de uso especial:* São utilizados pelo próprio poder público, construindo-se por imóveis aplicados ao serviço ou estabelecimento federal, estadual ou municipal, como prédios onde funcionam tribunais, escolas públicas, secretarias, ministérios, etc. São os que têm uma destinação especial. Por exemplo, escolas públicas e quárteis.

  - Bens públicos *dominicais:* São os que compõe o patrimônio da União, dos Estados ou dos Municípios ou DF, como objeto do direito pessoal ou real dessas pessoas. Abrangem bens móveis ou imóveis. Por exemplo, terrenos que fazem parte dos órgãos públicos e constituem seu patrimônio.

- **Bens particulares:** São os que pertencem a pessoas naturais ou jurídicas de direito privado.
- **Bens que estão fora do comércio:** Os bens alienáveis, disponíveis ou no comércio, são os que se encontram livres de quaisquer restrições que impossibilitem sua transferência ou apropriação. Portanto, podem passar, gratuita ou onerosamente, de um patrimônio a outro, quer por sua natureza, quer por disposição legal, que permite, por exemplo, a venda de bem público. Os bens inalienáveis ou fora do comércio são os que não podem ser transferidos de um acervo patrimonial a outro ou insuscetíveis de apropriação.

Consideram-se nesta classificação o valor econômico, sua mobilidade, sua abundância, sua forma, dentre outras inúmeras características que se criam em decorrência de seu interesse ou finalidade.

Até então, sabemos que todo e qualquer objeto que possua valor econômico é considerado um bem. Porém, vimos que para o direito é necessário haver uma disputa ou um interesse entre sujeitos para ser qualificado dentro de uma relação jurídica, sendo que existem bens não econômicos.

Entretanto, vale ressaltar que o fato de um bem se enquadrar em uma determinada categoria não significa que ele não se enquadre em outra, podendo um único bem pertencer a diversas categorias ao mesmo tempo. Por exemplo, um carro pode ser considerado um bem corpóreo, móvel, particular dentre outros, ao mesmo tempo.

Sendo assim, no decorrer deste trabalho focaremos nos bens de consumo. Porém, estamos cientes de que determinados bens podem ser classificados em mais de uma categoria classificatória.

1.2 Bens de consumo virtuais

Bens virtuais assim como os bens reais, para a economia, são recursos que possuem um valor econômico com a finalidade de satisfazer o consumo das pessoas. Porém, o que difere os dois é o fato de que nos bens de consumo virtuais, esses recursos são objetos não físicos, comprados para utilização de forma digital em redes sociais, jogos online e smartphones. Não possuem valor intrínseco (valor real de alguma coisa) e, por definição, são intangíveis.

Emenreciano (2003, p.77, apud Wikens; Ferreira, 2008, p.xx) conceitua bens digitais da seguinte forma:

> Os bens digitais, conceituados, constituem conjuntos organizados de instruções, na forma de linguagem de sobre nível (O computador opera as instruções transmitidas em linguagem de baixo nível, que é a linguagem capaz de ser interpretada pela máquina. As linguagens são de alto ou de baixo nível conforme sua maior ou menor proximidade com a linguagem humana), armazenados em forma digital, podendo ser interpretados por computadores e por outros dispositivos assemelhados que produzam funcionalidades predeterminadas. Possuem diferenças especificas tais como sua existência não-tangível de forma direta pelos sentidos humanos e seu transito, por ambientes de rede teleinformática, uma vez que não se encontram aderidos a

> suporte físico. [...]. Feitas essas considerações, pode-se afirmar que os bens digitais constituem **software sem suporte tangível (grifo nosso)**, sendo aplicadas todas as normas em que a referida definição seja encontrada. Vale ressaltar que a intangibilidade dos bens digitais refere-se aos sentidos humanos, podendo existir uma forma de existência corpórea qualquer. [...] Todos os bens digitais fornecidos pela rede imitam o objeto físico, real, material ou produzem os mesmos efeitos em nossos sentidos. Dentro dos mais diversos **programas de computador (grifo nosso)**, que cumprem este papel, podem-se enumerar: as fotografias digitais, a música transferida por meio digital, os livros eletrônicos, as enciclopédias multimídias, os jogos, os desenhos técnicos, os mapas eletrônicos, as pinturas em museus virtuais, entre outros.

Na maioria dos casos, os bens virtuais estão ligados na customização de personagens em ambientes digitais, redes sociais e em alguns momentos em blogs e smartphones, segundo Rodrigues (2016). Os patrimônios virtuais podem ser divididos de três formas:

- **Estéticos**: utilizado simplesmente para customização do ambiente virtual, de forma estética, para ter direito a novas personalizações em seus perfis ou avatar (personagem), não modificando o *ranking* e sim a forma como é visto perante os outros usuários. Exemplo são os *skins* (roupas para personagens de jogo), avatares, papéis de paredes, dentre outros.
- **Essenciais:** essenciais: Item ou bem, o qual é necessário para a evolução de um personagem em um jogo *online* ou para a evolução dentro de um *ranking* em outros ambientes virtuais. Exemplos são as chaves para entrar em determinados lugares dentro de jogos.

- **Facilitadores:** ajuda na passagem evolutiva de um personagem em um jogo online, ou para evolução dentro de um *ranking* em outros ambientes virtuais, de forma que seu uso não é necessário ou obrigatório para se ter a evolução pretendida. Por exemplo, comprar itens que destacarão o perfil do usuário, e impulsioná-lo ao topo frente ao perfil de outros usuários, ou alguma espécie de item que vai fortalecer o personagem em algum jogo, fazendo o mesmo ficar mais forte.

Vimos que um usuário, ou jogador, podem obter tais bens virtuais no decorrer da evolução do personagem, na realização de tarefas específicas, objetivos, ou na compra de tais itens em uma loja virtual conforme exemplo na figura 1, analisando um catálogo de produtos virtuais no mercado de bens virtuais.

Figura 1. Loja Virtual.

Fonte: Wolrd Of Warcraft - Blizzard , 2017.

O mercado de bens virtuais é um mercado ainda muito novo, não tendo mais que 20 anos. Empresas de diversos segmentos iniciaram a exploração desse setor, trazendo lojas virtuais com uma visão futurista.

No decorrer do tempo, o mercado de bens virtuais alcançou as redes sociais e jogos eletrônicos. Esses segmentos vendem ou oferecem um desafio para que os usuários customizem seus perfis e personagens, colocando-os no topo da lista.

Um bem virtual, para que seja atrativo aos consumidores, precisa ter um equilíbrio entre a escassez e o curso de determinado bem. O bem precisa ser relevante no contexto em que são oferecidos, como um recurso que permita a compra de tempo em um jogo onde o tempo é fundamental para o cumprimento de tarefas.

Bens de consumo virtual não são só itens de jogos online, ou artifícios para customizar perfis em redes sociais, como vimos anteriormente, também são a compra de jogos eletrônicos em mídias digitais, compra de tempo de jogo para poder continuar jogando, itens, como armadura, armas em um jogo, filmes digitais dentre muitos outros, que tentaremos abordar no decorrer do trabalho.

O mercado de compra e venda de bens de consumo virtual cresceu muito nos últimos anos, em todo o mundo, como lembra Sophia Mind (2017), pesquisadora do universo consumidor feminino. A Coreia do Sul e a China apresentaram um crescimento explosivo em 2009, naquele ano possuindo uma estimativa de um faturamento na casa dos bilhões de dólares, somente com jogos online. Sendo que no Brasil foi apurado, por ela mesma, que 93% das usuárias Brasileiras de internet costumavam utilizar algum tipo de mídia social. Alavancando o mercado de mídias digitais.

O dinheiro virtual, conhecido por muitos como o dinheiro do futuro, é a moeda que pode ser usada no mundo virtual. Cabe informar que o *bitcoin*, a mais famosa, tem como um de seus cernes a facilitação de compra e transações entre bens físicos e também virtuais. O *bitcoin* possui cotação própria e varia como uma ação na bolsa de valores.

Referem-se como “dinheiro virtual” as moedas que circulam em diferentes aplicativos e que vinculam um valor financeiro simbólico que é usufruído tanto no ambiente virtual como no real.

2 BENS DE CONSUMO NA ERA DIGITAL

As pessoas, com o decorrer dos últimos anos, estão cada vez mais conectadas a uma única rede, que chamamos de *Internet.* A Internet é um universo que se conectada com uma diversidade enorme de pessoas de todas as partes do mundo. Automaticamente essa conexão interpessoal, causa uma individualização decorrido por uma gama altíssima de escolhas.

Na era digital uma das formas de caracterizar a informação é pelo seu caráter de riqueza inesgotável. Para a indústria tradicional o bem de consumo é indivisível. Uma vez fabricado, um determinado produto acaba se tornando quase impossível de ser copiado com perfeição. O que é bem diferente na indústria da informação, onde as propriedades são produzidas uma única vez, e copiadas com perfeição sempre que necessário. Como é o caso dos *softwares*, que são replicados por diversas vezes até chegar ao seu consumo, nunca vindo o original a mão do consumidor. Isso traz uma grande variedade de possibilidades, pois assim como a indústria da informação te envia uma cópia do produto, o próprio consumidor ou usuário pode replicar o produto e repassar para outros usuários quantas vezes quiser, muitas das vezes de forma ilegal, trazendo diversos desafios para a legislação.

2.1 O mundo preocupado com a era virtual.

Em um mundo em que todas as pessoas podem estar conectadas como nunca antes visto na história, a uma única rede, comunicar-se a todo momento, acarreta em diversas complexidades. O comportamento do mercado, hoje, afeta a

todos em uma velocidade incrível, o que antes em uma crise financeira na Europa, acarretaria consequências no mundo, demoraria meses para alcançar e surtir efeito em todos os países. Com os adventos da tecnologia, hoje tal crise surtiria um efeito imediato em todos os países.

Essa complexidade abordada demonstra o que enfrentamos em diversos setores da sociedade. Todos esses avanços beneficiam a interatividade entre as pessoas em todo o planeta, através de jogos *online*, redes sociais, música e movimentos sociais e tecnológicos.

Este mercado procura atender toda essa gama de consumidores 24 horas por dia sete dias na semana em qualquer lugar do mundo. Uma empresa do Vale do Silício que está pronta para interagir com uma pessoa em Manaus, claro corre alguns riscos.

Outra complexidade do mercado da informação está na territorialidade ou jurisdição. José Aires (2000), em seu artigo sobre o assunto, cita que a internet por não possuir territórios, acaba facilitando os crimes virtuais, e dificultando a forma como tais crimes serão julgados.

A partir dessas complexidades, percebemos que, empresas, governos, instituições e principalmente as pessoas, possuem uma grande dependência da rede mundial de computadores. Hoje quase tudo está conectado à *Internet,* trazendo uma grande visibilidade para o mundo, mas também trazendo os riscos à segurança da informação, como sabotagens por *hacker*, hacketivismo e etc. Além disso, trazendo outros tipos de riscos como a concorrência desleal.

Sendo assim junto com uma melhora para a sociedade, vem um grande crescimento da criminalidade. Os criminosos, muita das vezes, aprendem sobre as novas tecnologias antes de todo mundo, já com o pensamento de transformar aquilo

e uma nova forma de lucro ilícito, atentando contra propriedades intelectuais, marcas, patentes, entre outras.

2.2 Direito Digital e o Marco Civil da Internet

Os primeiros debates acerca da regulamentação da internet começaram logo nos meados da década de 90. De início, se teve a concepção a partir da Escola da Independência do Ciberespaço de John Perry Barlow, de que o Estado não deveria interferir nos acontecimentos dentro da rede mundial de computadores, transformando a *Internet* em uma terra sem lei. Como trata a Declaração da Independência do Ciberespaço apresentado em Davos na Suíça:

> Governo do mundo Industrial, aborrecidos gigantes de carne e de aço, eu venho do Ciberespaço, a nova morada da mente. Em nome do futuro, peço que vocês, do passado, nos deixem em paz. Vocês não são bem-vindos entre nós. Vocês não têm soberania onde nós reunimos. Não temos governo eleito, tampouco é provável que venhamos a ter; então dirijo-me a vocês com a mesma autoridade com a qual a própria liberdade sempre fala. Declaro que o espaço social global que estamos construindo é naturalmente independente das tiranias que vocês buscam nos impor. Vocês não têm direito moral de nos governar; tampouco possuem qualquer método de aplicação de leis que tenhamos algum motivo real para temer. (Declaração da Independência do Ciberespaço de John Perry Barllow, 1996).

Em relação a todos estes acontecimentos tecnológicos, foi surgindo aos poucos à escola do direito do ciberespaço, inspirada na síntese de que o direito só poderia ser aplicado dentro do limite territorial selecionado em determinadas fronteiras. Com esse pensamento, considerando que as normas até então em vigor foram criadas para uma sociedade com fronteiras territoriais firmemente delimitadas, isso representa dificuldades para regulamentar as novidades da internet, cujas características são essenciais a liberdade, o direito de ir e vir e acesso a qualquer informação. A escola descaracterizou as normas vigentes, defendendo a impossibilidade de usá-las no ordenamento jurídico dentro da internet.

Ainda na década de 90, o direito internacional considerava a Internet um “território internacional”, pregando que era um lugar sem fronteiras, com o intuito de facilitar as mais diversas formas de comunicação entre pessoas de qualquer lugar do mundo em qualquer distância, e a qualquer momento.

Nesse pensamento já havia a iniciativa de utilizar legislações já existentes para a regulamentação da Internet, fazendo adaptações para o uso relacionado à Internet, a fim de vincular as atitudes dos habitantes das nações signatárias, quando estivessem na rede mundial de computadores. Assim, a escola de Arquitetura de Redes está cada vez mais ganhando espaço em todo o planeta.

A escola de arquitetura de redes, idealizada por Lawrence Lessing, apud Pinheiro (2016), defendia a filtragem feita por determinados países para limitar a atuação do usuário de comum acordo com as leis vigentes e os interesses dos representantes de dada nação. Exemplo disso foram às restrições de uso, na Europa, de determinadas redes sociais. As mesmas eram utilizadas para o

agendamento de manifestações. Lawrence Lessing cita três modalidades de regulamentação para a Internet: leis, normas sociais e mercado.

A partir dos estudos de José Aires (2000), alguns ordenamentos jurídicos no mundo, analisaram o objeto ou objetivo. Entende-se que se o produto do processo estiver em servidores de um determinado país, será julgado pelas leis dele, mas em alguns Estados, tal pensamento não foi aceito, por exemplo, no Estado da Califórnia nos Estados Unidos, que reside dois dos maiores provedores de Internet do mundo.

Recentemente os provedores de Internet da Califórnia acabam de se eximir dos crimes na Internet. Mesmo se os criminosos usem os sítios da Califórnia para fazer os crimes, os responsáveis não deverão ser julgados na Califórnia, pois deve-se analisar o princípio do crime, o que o levou a acontecer, não a localidade dele, e sim a nacionalidade do criminoso. Na lei brasileira é adotado o princípio da territorialidade. Se o crime foi cometido por um brasileiro dentro do seu território, contra um americano, o Brasil também estaria apto a julgar, assim como os Estados Unidos.

> A Internet recebeu o status de Direito fundamental, pela ONU. No Brasil, foi criado um projeto de emenda constitucional, para que a Internet seja considerada um meio pelo qual os cidadãos podem exercer os seus direitos de liberdade de expressão. A Internet se tornou indispensável para as pessoas, sendo que a administração pública possui diversos serviços *online*.

Segundo Patrícia Peck Pinheiro (2016), foi criado um modelo doutrinador para julgar tais avanços tecnológicos, que afetam diretamente ou indiretamente as relações sociais.

No caso, o direito digital que usa muito do direito costumeiro, que por sua vez, utiliza o histórico de decisões de casos concretos como subsídios legais para uma

ação judicial. Ou seja, utiliza de casos anteriores através do costume de uma sociedade, com o intuito de dar soluções rápidas aos conflitos.

Um dos métodos empregados pelo direito digital de Patrícia Peck Pinheiro (2016) são as normas digitais. Estas devem ser publicadas na página inicial de um sítio, com os princípios gerais da empresa. São os termos de uso, que devem estar claros, com toda a sua norma padrão para determinada atuação, estando o produto ou o serviço jurisdicionados as leis do país. Usa-se então, da publicidade das regras, possibilitando assim um maior conhecimento do público, o que consequentemente aumenta a sua eficácia. Assim, auxilia o usuário em relação ao conhecimento de normas, sejam das empresas ou do ordenamento jurídico que a mesma segue.

Existem convenções para determinadas normas, podemos citar a lei modelo da *United Nations Commission on International Trade La*w (Uncitral), para o comércio eletrônico com guia para aplicação, produzido pela primeira vez em 1996, atualizando-se em 1998. Esse documento é referência mundial, e todos os países devem fundamentar-se nele ao regulamentar o comércio eletrônico em seu território. Também existe a cartilha sobre o comércio eletrônico e propriedade intelectual, publicado pela *WIPO/OWPI*, que aborda questões como jurisdição e legislação aplicável, entre outras, relativas ao comércio eletrônico.

Com a velocidade dos avanços tecnológicos é muito difícil legislar sobre a Internet, principalmente no Brasil, segundo Patrícia Peck Pinheiro (2016). Para uma lei ser regulamentada é necessário um grande período de tempo para o estudo dos legisladores até a promulgação dela. Acaba que o ordenamento jurídico, no sentido tecnológico na Internet como objeto de lei, por muitas vezes já está ultrapassado ou modificado, não sendo mais cabível aquela legislação continuar em vigor.

Se a lei não se encaixar com o objeto, o consumidor por sua vez, não a obedecerá, assim, entra no princípio de que se vários indivíduos deixem de se comportar segundo a norma, com o tempo a mesma perderá a sua validade. Por conta disso, mesmo sendo criada da forma mais genérica possível, acaba se tornando obsoleta rapidamente. Assim, o direito digital prega que as leis devem ser mais flexíveis. Algo que o ordenamento brasileiro seria complexo, sabendo que ele é um ordenamento codificado como base predominante, o que dificulta na tomada de decisão sendo que pelo teor deve ser tomada com mais rapidez.

O direito digital traz consigo a característica da uniformidade, onde se usa do pensamento que uma decisão a favor de um determinado cliente contra uma empresa deve ser usado para generalizar outras empresas. Ou seja, as demais empresas devem se adequar a decisão de acordo como o caso analisado é decidido, quando semelhante. Por exemplo, se uma empresa como a *Blizzard* for condenada por algum processo, as outras empresas do mesmo ramo devem ficar cientes do acontecido e se adaptar, acaso aconteça um processo semelhante contra qualquer outra empresa, A decisão será analisada comparando os processos anteriores com um princípio genérico.

Outra característica que o direito digital prega é a notoriedade. As decisões devem sempre se tornar públicas, para que sejam transparentes, assim diminuindo a obsolescência de decisões. Com isso, países como o Brasil, seguindo tal doutrina, devem tomar por bases questões que começaram a ser discutidas a pelo menos cinco anos, um tempo que pode ser fatal em uma época de velozes transformações.

A Prova é outra característica importantíssima para a correta aplicação do direito no mundo digital. Um exemplo é uma empresa de jogos eletrônicos, onde sem prévio aviso modifica a lista de itens (armas, roupas, armaduras e etc.) do jogador,

retirando um determinado item sem aviso, indagando não ser dele. Não cabe ao jogador que se sentiu lesado provar qualquer coisa perante a justiça, mas a empresa acusada provar.

No Brasil, a partir do ano de 1998, começou-se a debater a necessidade de regulamentação específica para preencher algumas lacunas que já se conseguiam vislumbrar, em razão dos avanços tecnológicos no mundo, e a grande utilização de sua população. A partir daí, adotamos a teoria da aplicabilidade do Direito Vigente, denominada como uma corrente tradicionalista, defendendo a aplicabilidade do Direito vigente ao que se passa na Internet, defendendo a não separação do “mundo real” do “mundo eletrônico”. Dessa forma, as diferenças são reconhecidas em termo de aplicabilidade da lei entre o que se passa na Internet e no ambiente físico, mas sim, utilizar-se das previsões legislativas já existentes como princípios próximos para julgar determinados acontecimentos, a partir do que a lei já implica adaptando-o ao novo mundo tecnológico.

Em 2012, a atriz brasileira Carolina Dieckmann, teve 36 fotos íntimas furtadas de seu computador pessoal, a atriz foi chantageada para que suas fotos não fossem inseridas na *Internet*, mas se recusou a pagar e fez o registro da ocorrência. Logo, o caso da atriz se tornou um escândalo nacional.

Coincidentemente, já havia um projeto de regulamentação em tramitação na Câmara dos Deputados. O acontecimento fez com que os deputados, em tempo recorde (um ano), colocassem em vigor a Lei nº 12.737/ 2012 com o intuito de tipificar os crimes cibernéticos, ou seja, colocando os tipos de crimes e suas penas. Em razão do caso acontecido com a atriz, apelidaram tal ato com o seu nome, Lei Carolina Dieckmann. (Lei nº 12.737/2012).

Um ano depois da promulgação da lei Carolina Dieckmann (Lei nº 12.737/2012), promulgou-se a Lei nº 12.965/2014, conhecida como Marco Civil da *Internet*, que regulamenta a relação Civil das pessoas. No início, estipulou a privacidade e a proteção dos dados pessoais como princípio fundamental. Hoje, não existe no Marco Civil da *Internet* código específico para dados pessoais. Utilizam-se previsões sobre o assunto em outros ordenamentos nacionais como:

- **Lei geral de Telecomunicações** –Apenas na execução de sua atividade, a prestadora poderá valer-se de informações relativas à utilização individual do serviço pelo usuário. $1 A Divulgação das informações individuais dependerá da anuência expressa e especifica do usuário. $2 A prestadora poderá divulgar a terceiros informações agregadas sobre o uso de seus serviços, desde que eles não permitam a identificação, direta ou indireta, do usuário, ou a violação de sua intimidade. (Lei nº 9.472/1997, Art. 72.).
- **Código de Defesa do Consumidor** – O consumidor, sem prejuízo do disposto no artigo 86, terá acesso às informações existentes em cadastros, fichas, registros e dados pessoais e de consumo arquivados sobre ele, bem como sobre as suas respectivas fontes. $1 Os cadastros e dados de consumidores devem ser objetivos, claros, verdadeiros e em linguagem de fácil compreensão, não podendo conter informações negativas referentes a períodos superior a cinco anos. $2 A Abertura de Cadastro, ficha, registro e dados pessoais e de consumo deverá ser comunicada por escrito ao consumidor, quando não solicitada por ele. (Lei nº 8.078/1990, Art. 43).

- **Lei de Acesso a informação** – Para os efeitos desta lei, considera-se: I – Informação: Dados, processados ou não, que podem ser utilizados para produção e transmissão de conhecimento, contidos em qualquer meio, suporte ou formato. (Lei nº 12.527/2011, Art. 4)
- **Lei da Organização Criminosa** – O delegado de polícia e o Ministério público terão acesso, independentemente de autorização judicial, apenas aos dados cadastrais do investigado que informem exclusivamente a qualificação pessoal, a filiação e o endereço mantidos pela justiça eleitoral, empresas telefônicas, instituições financeiras, provedores de Internet e administradoras de cartão de crédito. (Lei nº 12.850/2013, Art. 15).

Dentro do ordenamento jurídico do Marco Civil da *Internet*, existem princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Sendo construído a partir de consulta pública, de forma participativa.

Depois do Marco Civil da *Internet* (Lei nº 12.965/2014), o ato de invadir dispositivo alheio, conectado ou não a rede de computadores, mediante violação de segurança com o fim de obter informações sem autorização, gera uma pena de detenção de três meses a um ano e multa, agravando a pena se causar prejuízo econômico para três meses a um ano e quatro meses. Se houver roubo de conteúdo de comunicações privadas, como e-mail, a pena aumenta para seis meses a dois anos e multa e se as informações roubadas forem divulgadas e comercializadas a pena sobe de oito meses a três anos e quatro meses de reclusão. Porém, se invadirem o equipamento informático de uma pessoa que não estiver com qualquer tipo de mecanismo de segurança, não é considerado crime. O Marco civil da *Internet*

ainda prevê: privacidade dos usuários, privacidade das comunicações e liberdade de expressão.

Sendo assim, pelo fato de os bens digitais serem intangíveis no comércio eletrônico, isto é, pela *Internet*, são equiparados aos programas de computador. A legislação enxerga as propriedades virtuais dentro do regimento jurídico do Direito autoral, por conta disso julga todos os bens digitais como propriedades intelectuais, a partir da Lei nº 9.609/98, que trata da proteção da propriedade intelectual do programa de computador, e a Lei nº9.610/98 que consolida as regras relativas aos direitos autorais. Usando a Lei Carolina Dieckmann. (Lei nº 12.737/2012) é o Marco Civil da *Internet* (Lei nº 12.965/2014), somente em aspectos pertinentes a privacidade e liberdade de expressão.

3 ANÁLISE DE CRIMES VIRTUAIS.

Diariamente existe um crime virtual com bens digitais envolvidos sendo julgados no mundo, cada país possui a sua legislação, porém na maioria as penas acabam sendo brandas. Sendo que esse tipo de crime muita das vezes ou passa despercebido ou a pena não passa de 1 a 5 anos de detenção.

O simples fato de utilizar um Torrent ou um *software* para *download* de forma gratuita sem os meios legais, em determinados países já é o suficiente para ser registrado como um crime. Quando os videogames chegaram ao Brasil, foi uma febre, jogos piratas eram mais acessíveis que os originais. Segundo estudo feito pela Federação do Comércio do Estado do Rio de Janeiro (Fecomércio-RJ, 2010) em parceria com o instituto Ipsos (empresa de pesquisas e inteligência de mercado), a pesquisa chegou à conclusão de que 43% dos brasileiros, que abusavam do consumo de produtos piratas, se manteve entre 2007 a 2010, aumentando o número de produtos adquiridos, incluídos jogos eletrônicos, CDs de música e DVDs de Filmes. Aproximadamente do fim da primeira década dos anos 2000, grandes empresas começaram a tomar medidas em relação à pirataria, dificultaram a cópia das mídias dos jogos eletrônicos a partir, do lançamento do *Blu-ray* em meados de 2010, e ofereceram serviços exclusivos em ambientes *online*, para que assim fosse necessário o uso da mídia original e uma autenticação para jogar.

A partir de agora analizaremos alguns crimes que marcaram o mundo e o Brasil. Alguns dos quais tiveram um fecho exemplar, outros que não foram solucionadas da maneira devida.

3.1 Crimes virtuais em Jogos Virtuais

Em 2013, uma quadrilha de *crackers* chineses foi condenada a dois anos de prisão por roubar 11.500 contas de *Word of Warcraft*, Jogo online de *MMORPG* (*Massively Multiplayer Online Game* – Jogos Online para Multijogadores), da produtora de jogos eletrônicos Blizzard, lançado em 2004. Eles foram condenados por venderem no mercado negro itens virtuais (como roupas, armas e habilidades), transformando em um negócio extremamente lucrativo.

A quadrilha era liderada por um chinês chamado Chen, que trabalhava em um espaço improvisado no qual as operações ilegais eram realizadas. No início, eles compravam as informações de *Login* por cerca de US$1,00 por conta, para depois receber, em média, US$ 3,00 com a venda dos itens e do ouro presentes em cada uma.

Com o tempo, a quadrilha aprendeu a roubar as informações por conta própria, o que permitiu a abertura de um local de operações próprio e a contratação de ajudantes. De acordo com as investigações que levaram os criminosos à prisão, a quadrilha de Chen lucrou com a venda de itens das 11.500 contas roubadas em torno de US$ 10,800 (cerca de R$ 25.000).

Em agosto do mesmo ano, os membros da quadrilha receberam a sentença de pagar a multa de US$ 1.000 cada um e pena de um ano e meio de prisão, Chen foi condenado a dois anos de prisão, além de pagamento de uma multa de US$8.000.

A polícia chinesa chegou a quadrilha através de denúncias feitas por jogadores do jogo *World of Warcraft*. A China é um dos países mais preocupados com o cibercrime no mundo, tendo muitas vezes lançado projetos de censura para

dificultar tais crimes. Essa preocupação vem pelo fato de que o país sempre esteve entre os que sofrem um maior número de casos de crimes virtuais.

Também foi na China, o caso controverso em que um presídio feminino de *Heilongjiang*, na cidade de Harbin no norte da China, ficou famoso por suas torturas denunciadas na web. Presidiárias eram obrigadas a passar 12 horas por dia jogando *World of Warcraft*. As detentas jogavam para ganhar créditos (como novos personagens, roupas, armas, habilidades e moedas do jogo), que posteriormente eram revendidos na *Internet*. Rendiam por volta de R$ 900,00 diários aos administradores da cadeia. O valor não é alto, mas plausível, a prática de revender créditos obtidos em jogos se chama "*Gold Farm*", e movimenta mais de US$ 1,2 Bilhões na China. Ação considerada ilegal na plataforma do jogo, mas que nunca a empresa obteve êxito em obter auxílio das autoridades chinesas.

Mas não é só na China que crimes são cometidos por causa de jogos virtuais. Em 2007, antes da lei Carolina Dieckmann (12.737/2012) e do Marco Civil da *Internet* (12.965/2014), uma quadrilha de São Paulo após sequestrar um jogador de Gumbound fazendo ele de refém por quase cinco horas. DuduMagik foi obrigado a transferir os mais de 500 mil pontos que tinha para a conta de um dos sequestradores, que pretendiam revendê-los na Internet por R$15.000. Porém esse caso foi ao mais extremo, pois a quadrinha antes tinha tentado *hackear* a conta do usuário, como não conseguiu resolveram realizar o sequestro para obter os bens virtuais.

Muitos dos crimes que acontecem em jogos eletrônicos acabam passando em branco, mesmo que desde de 2014, segundo a EBC (Empresa Brasil de Comunicação, 2015), a denúncia de tais crimes tem crescido, os próprios jogadores ainda preferem deixar de lado e não denunciar ou alguns órgãos públicos brasileiros

simplesmente ignoram. Por conta disso, as empresas detentoras da administração dos jogos online acabam tendo que fiscalizar, criando uma legislação interna dentro do jogo para resguardar e proteger o jogador, e a si mesmo.

Para combater crimes online, tais empresas investigam o comportamento inadequado de certos jogadores, e aplica as penas necessárias, sendo cada vez mais duras. A Blizzard, por exemplo, expulsou um clã acusado de praticar pedofilia e corrupção de menores em *World of Warcraft*. Segundo alguns competidores, os membros do clã Abhorrent Taboo promoviam “atos obscenos” durante o jogo, tanto nos textos de bate papo quanto no comportamento dos avatares. Já a Riot Games, responsável pelo *League of Legends*, baniu 13 jogadores brasileiros que praticaram atividades consideradas ilegais. Segundo comunicado da empresa, os competidores estavam sendo pagos por outros para melhorar suas contas.

Será que tais produtoras possuem o direito de simplesmente, sem legislação cabível, punir tais jogadores? Muitas vezes um jogador ao ser banido de um jogo fica sem entender o real motivo pela qual foi banido, sendo assim, não possuindo a condição de defesa. Por conta disso diversos casos vão para a justiça. Como um caso de 2013, no estado do Rio grande do Sul, onde um jogador de um jogo online foi banido do jogo, acusado de tumultuar o fórum quebrando as regras do jogo, por ter reclamado alguns serviços. O *Player* foi condenado pela empresa administradora ao banimento do jogo, por conta disso o jogador entrou na justiça, alegando abusividade da empresa ao bani-la do jogo, e conseguiu uma liminar, onde a sua conta fosse somente suspensa por um tempo determinado com posterior reativação da conta é condenando a produtora a pagar uma indenização por danos morais, já que pelo entendimento do juiz julgador do processo, as leis da produtora não estão acima das leis brasileiras, e a produtora não podia punir de forma definitiva a

jogadora (Recurso Cível Nº 71004351888, Relator: Alexandre de Souza Costa Pacheco, Julgado em 04/09/2013).

3.2 Crimes Virtuais em outros ambientes digitais

Uma empresa de segurança da informação chamada Sophos, acredita que os usuários são descuidados demais ao fornecer dados pessoais. Para provar isso criou um perfil de um sapo de plástico e convidaram 200 desconhecidos para serem seus amigos no FaceBook. Quase metade aproveitou a oportunidade de compartilhar suas informações pessoais com o sapo Freddie. O nome completo, a lista de amigos, informação sobre educação e não parava, como vimos no capítulo anterior, a base para um ataque são as informações. Dados adquiridos com esse experimento, seriam o suficiente para um ataque de engenharia social a algum usuário dessa forma facilitaria muito a vida de um criminoso cibernético.

Diante deste acontecimento é fácil perceber que o principal problema é o fato das pessoas não entenderem que suas informações são particulares por um motivo, a privacidade. Depois que as informações estão na *Internet* não existe uma forma de retira-las por sua totalidade, ficam lá para sempre, sem controle algum.

Acontece o tempo inteiro, *Crackers* e fraudadores roubam a identidade dos outros para conquistar suas propriedades virtuais. E isso acontece cada vez mais nas mídias sociais. É um fato na história do ser humano.

Em 2009 na cidade de Seattle, Estados Unidos, Bryan Rutberg teve seu perfil no Facebook roubado por um cracker profissional. Sua filha tinha acabado de fazer o dever de casa, e resolveu entrar no Facebook lá viu que o status de seu pai dizia que ele precisava de ajuda, o criminoso invadiu é roubou o perfil de Bryan. Em poucos

minutos, o cracker, entrou em contato com todos os seus amigos, dizendo que Bryan estava com problemas, dizia que tinha sido assaltado em Londres, sabia o nome de sua esposa pois estava na sua lista de familiares. Em pouco tempo o *Cracker* conseguiu alguém para mandar dinheiro ao amigo necessitado. Benny, um amigo antigo de Rutberg, se pronunciou e enviou quatro parcelas de uma quantia não declarada ao Reino Unido e alguém com o nome do Bryan recebeu o valor. Neste caso a intenção do criminoso era usar do perfil do usuário, no caso Bryan Rutberg, para acessar outras pessoas e conseguir fundos monetários, mas se o criminoso quisesse poderia, a partir do perfil de Bryan acessar de seus contatos e roubar os seus perfis ou seus itens ou bens virtuais que ali existisse. A empresa, o Facebook se pronunciou dizendo que esse tipo de crime só acontece em 1% dos seus usuários que naquela época era em torno de 250 milhões de usuários. Então 1% é 2,5 Milhões de usuários São muitas pessoas que tiveram os perfis roubados ou conhecem pessoas com perfis roubados. O criminoso desse caso conseguiu fugir com a quantia e o caso foi arquivado.

Esse golpe de pedir ajuda tem suas origens há séculos, no reinado de Elizabeth I. Naquela época as vítimas davam dinheiro para soltar ingleses presos nas masmorras espanholas. É conhecido como o golpe do prisioneiro espanhol. E 400 anos depois seus descendentes tecnológicos chegaram a Internet.

Esse tipo de crime, acontece com todo o tipo de pessoa, de diversas formas e com intuitos diferentes. Com um intuito diferente do caso anterior, uma estudante brasileira do estado do Rio de Janeiro, caiu em um golpe parecido, mas com proporções sociais. Aos 11 anos, uma estudante do ensino fundamental viu seu mundo desmoronar, depois que em 2014 enviou uma foto íntima a um rapaz, de 16 anos que tinha o intuito de denegrir a imagem da garota na Internet, por meio do

Facebook. Logo a imagem foi compartilhada nas redes sociais. Moradora de Casimiro de Abreu, interior do Rio de Janeiro, com 30 mil habitantes a 140 km da capital. A garota teve que mudar de escola e foi proibida pelos pais de usar computadores. O inseparável celular que carrega no bolso agora serve apenas para escutar músicas e não tem chip de nenhuma operadora. O drama enfrentado pela família da garota, é cada vez mais comum. O garoto de 16 anos foi procurado pela polícia, mas como se trata de um menor de idade o mesmo somente teve uma medida socioeducativa.

A cada minuto, 54 pessoas são vítimas de crimes cibernéticos, como os citados, no Brasil, segundo a multinacional Symantec, empresa de segurança na Internet. O mundo virtual é campo fértil para pedófilos e também para *hackers* que limpam contas bancárias e devassam arquivos pessoais na web, em busca de algo que possa ser usado para extorquir o usuário, ou para meios ilícitos de se obter vantagens.

Uma forma de se obter vantagens na *Internet* é a facilidade de se obter recursos digitais na rede como, filmes, músicas dentre outros, ferindo os direitos autorais. Exemplo disso foi o caso do What.CD, um rastreador de *Torrent* de música que foi retirado do ar por autoridades francesas após quase uma década de atividades. Todos os 12 servidores operados pelo What.CD foram apreendidos, neles continham cerca de 3 milhões de *Torrents*. A música, um dos bens virtuais mais pirateados do mundo, e disponibilizada de forma ilegal na Internet desde o início da própria rede mundial de computadores. O diferencial do What.CD era que os usuários podiam além de conseguir músicas que não eram mais comercializadas, podiam também organizar seus arquivos por ano, gênero e uma série de parâmetros, o que faziam ser uma espécie de Wikipédia para músicas. O What.CD estava na mira

da polícia francesa desde o final de 2015 e era considerado a fonte mais importante de pirataria de músicas. A acusação é de que o site gerou mais de 40 milhões de euros em prejuízo para os produtores de músicas representados pelo órgão.

Outros tipos de crimes são os relacionados com as moedas digitais ou moedas virtuais ou criptomoedas que muito das vezes são consideradas objetos de crimes e não o motivo do crime em si. Muitos desses criminosos ao fazer uma chantagem ou o pagamento por um serviço, solicitam que sejam pagos por moedas digitais, pela praticidade e a dificuldade de rastreamento. Mas nem mesmo as criptomoedas pelos motivos citados deixaram de ser alvos.

Como em Londres, onde a corretora Bitfinex anunciou que 119.756 mil bitcoins foram roubados dos computadores da empresa, que tem sede em Hong Kong. A notícia sobre o sumiço que se aproxima dos R$ 260 milhões fez com que o valor da moeda virtual caísse drasticamente. Em reais, o *bitcoin* despencou do patamar de R$ 2.200 por 1 *bitcoin* no fim da semana para R$ 1.800 por 1 *bitcoin* em agosto de 2016. A corretora anunciou que depois de uma auditoria de segurança, foi encontrado uma falha de segurança nos computadores e decidiu suspender todas as negociações com a moeda virtual, sejam ordens de compra, venda ou saque dos clientes. Até o presente momento não foi divulgado mais informações sobre o caso que ainda se encontra em investigação.

Outro caso foi, em 2014 outra corretora asiática já tinha passado por um roubo de bitcoins a partir de um ataque virtual. A japonesa Mt. Gox sofreu um roubo de quase US$ 500 milhões e acabou fechando as portas. As investigações foram arquivadas depois do fechamento da empresa.

4 PROCEDIMENTOS DE SEGURANÇA PARA BENS VIRTUAIS.

Todos os dias na televisão ou na própria *Internet* são observados casos de ataques virtuais, pessoas que tiveram seus perfis de redes sociais ou jogos *online*, fotos e vídeos íntimos e quantias monetárias furtadas na rede mundial de computadores. Assim como no dia a dia, onde temos que nos precaver para evitar furtos, temos que estar prevenidos na Internet para evitar tais crimes, mas como nos precaver na Internet, como evitar que os famosos "*crackers*" efetuem tais crimes contra os bens virtuais dos usuários?

Iniciou-se um novo ciclo na era digital, a maioria dos dispositivos eletrônicos como o *smartphones* e *notebooks* já saem de fábrica com mecanismos de segurança, como o leitor biométrico, justamente para incentivar o usuário a sempre manter o seu equipamento seguro. Empresas como a Intel já produzem *softwares* como o *true key* que organizam seus *logins* de acesso de determinados sistemas, para que assim facilite a vida do usuário e o deixe mais seguro.

O Brasil em 2015 ficou em quinto lugar no mundo em fraudes digitais em uma pesquisa feita pela *Trend Micro Incorpora*ted (Empresa especializada em segurança na nuvem), tendo em seu histórico o ranking mundial de *hackers* e crimes virtuais em 2002 onde liderou e conquistou o título de maior laboratório de cibercrime em todo o mundo. Segundo um levantamento feito pela mi2g (*Intelligence Unit*) empresa de consultoria de riscos digitais baseada em Londres, e em 2013 o quarto lugar em vítimas de crimes virtuais, em estudo realizado pela RSA *Anti-Fraud Command Center* (AFCC) divisão de segurança da EMC2 *Corporatio*n.

Gravamos a nossa vida, interagimos com os outros e, sem pensar duas vezes, compartilhamos nossas experiências na *Internet*. É uma versão moderna da

necessidade primitiva, mas todo o compartilhamento tem um risco pessoal. Para algumas pessoas a vida real já não importa mais. O que importa é a vida virtual, o que pensam e o que falam sobre elas nas redes sociais e o que fazem o que elas são. Como uma máscara, uma pessoa onde quando se está em sociedade você usa para não parecer antissocial ou desconectado do mundo usado no dia a dia, na convivência das pessoas, mas quando se conecta a Internet, retira-se esta máscara e torna-se outra pessoa, começa a se mostrar e buscar o anonimato para defender o que acredita sem medo de retaliação e atacar o que não gosta imaginando estar seguro.

O homem hoje, na frente do computador age como os homens das cavernas nessa revolução tecnológica. Erros comuns são cometidos nesses novos tempos, o que muitas das vezes são aproveitados em prol do benefício de um criminoso. Um mundo onde as pessoas só interagiam com outras da mesma cidade, agora interagem com povos de várias partes do mundo, o que fazem delas, com o sentimento de conforto na Internet. Essa zona de conforto ao se utilizar a rede mundial de computadores, acaba levando o usuário a ser vítima de crimes virtuais, que alguma das vezes por simples descuido ou falta de conhecimento, pode conter consequências gravíssimas.

4.1 Vulnerabilidades de bens de consumo virtuais e possíveis ataques.

As redes sociais são como um jogo *multiplayer* de RPG, no qual o objetivo é colecionar “amigos”. Em resumo, a mídia social mudou as relações entre as pessoas com consequências futuras imprevisíveis.

Nesses ambientes virtuais se colocam o máximo de informações possíveis, desde nome, telefone, e-mail, fotos, vídeos e o registro de acontecimentos importantes no dia a dia do usuário. Quanto mais informações se colocam, maior o *status* do usuário, fazendo com que o mesmo seja seguido pelo maior número de pessoas. Pessoas essas que podem estar com boas e más intenções.

Os criminosos precisam de informações para atacar uma vítima, é muito difícil um criminoso atacar uma vítima sem dados básicos de como a abordar, os lugares que ela frequenta e que tipo de bens que ele pode conseguir dela. Informação na Internet é um dos bens mais valiosos, com ela muita coisa pode ser feita.

Nos jogos eletrônicos de ambiente virtual *multiplayer*, os RPGs, não é muito diferente, informações como o horário que o jogador entra, o nível que o jogador está, os tipos de bens que ele possui, os amigos dele, e quanto ele possui na carteira de criptomoedas, são dados suficientes para que um "*Cracker*" use para conseguir se aproveitar de um momento despercebido do jogador e aplicar-lhe um golpe.

Existem diversos tipos de ataques utilizados por criminosos, Paulo Brito (2015) classifica os mais utilizados.

Nos ataques de browser o criminoso se aproveita diretamente do usuário, usando técnicas de engenharia social e *phishing* (Técnica utilizada para "pescar" informações na Internet a partir da suplantação de identidade por parte do criminoso, exemplo um e-mail onde diz ser de um banco solicitando alguns dados do usuário). Os crackers percebem a desatenção de um usuário, para que assim encontre uma brecha para invadir um dispositivo ou um perfil em um ambiente virtual.

O ataque mais usado é o do *browse*r pois como visto, nele o atacante se aproveita do usuário que é considerado o elo mais fraco, mas não deixam de usar os outros ataques para este fim. Usam destes ataques muito das vezes para o roubo de

perfis em ambientes virtuais e dados bancários, para que assim se passem pelo usuário ou façam saques diretos em suas contas bancarias ou suas carteiras digitais. Tais golpes algumas das vezes podem chegar a ser bilionários.

Um exemplo de ataque de browser é detalhado a seguir. O *cracker* utilizando técnicas de *phishing* é engenharia social, enviaria ao usuário alvo, e-mails ou links oferecendo algum serviço gratuito ou dizendo que o alvo ganhou algum prêmio. O usuário, ao receber mensagens referentes a produtos gratuitos ou prêmios, na inocência cadastra seus dados e envia ao criminoso, que por sua vez, dependendo dos dados recebidos, usa-os para ou invadir as contas do usuário ou fazer transações bancários.

Dentro dos ataques evasivos os *crackers* procuram inserir *malware*s (qualquer tipo de software malicioso que tenta infectar um dispositivo) com o intuito de explorar os dispositivos, desviando a ameaça da inspeção ou encobrindo sua existência, usando técnicas evasivas.

Já um crime a bens virtuais utilizando o ataque evasivo, o criminoso disponibilizaria na Internet ou diretamente ao usuário um programa contendo malwares, de forma que ao acessar o dispositivo do usuário os Malwares infectam todo o equipamento é ajuda o criminoso a encontrar brechas para uma invasão futura.

Os ataques furtivos disfarçam a sua intenção até atingirem a meta, que é o roubo de dados e o desvio de dinheiro. Meses de pesquisa dão aos atacantes um conhecimento profundo do alvo. Os criminosos contam ainda com o grande volume de dados a serem analisados, para passarem despercebidos entre tantos alertas dos dispositivos. Quando a ameaça é descoberta, o roubo já aconteceu.

O ataque furtivo é um dos mais bem elaborados, pois o atacante fica por um longo período de tempo, vigiando o usuário alvo, analisando a sua rotina, procurando brechas para a realização do crime. Sendo assim, no momento do ataque estando mais bem planejadas, as chances de o plano funcionar como o previsto são maiores que os outros.

O *SSL* (*Secure Socket Layer*, padrão global em tecnologia de segurança, desenvolvido pela Netscape, que cria um canal criptografado entre um servidor web e um navegador (browser) para garantir que todos os dados transmitidos sejam sigilosos e seguros) permite novos caminhos para os criminosos virtuais, já que possui uma ligação com a criptografia. Os *crackers* se escondem no tráfego criptografado, pois sabem que muitas das vezes o usuário não possui ferramentas adequadas para inspecioná-lo. Usar os canais criptografados já disponíveis dentro de uma rede é uma ótima maneira para ocultar as ameaças das ferramentas de detecção. À medida que outras plataformas, como a nuvem é as mídias sociais abraçam a criptografia, mais lugares os *crackers* terão para se esconder.

Com o ataque de *SSL* o criminoso simplesmente se esconderia e esperaria o melhor momento para o ataque, sendo que este seria mais interessante se utilizado em conjunto com algum dos outros, tendo uma melhor eficácia.

Os criminosos usam todos esses tipos de ataques, para conquistar os seus objetivos. A ideia é conseguir o máximo de opções para a realização do crime, para que assim escolham a que for mais fácil e seguro de se alcançar o resultado desejado.

Com o acesso aos dados dos usuários, os criminosos podem também acessar os perfis destes utilizadores em redes sociais ou em outros ambientes virtuais. A partir do roubo de perfis digitais, o *Cracker* poderá tentar fazer novos golpes contra

outras pessoas que possuem alguma espécie de ligação com a conta roubada, dando brechas para outros crimes, não só os ligados a bens virtuais.

5 Como proteger seus bens de consumo virtuais.

Dentro da Internet, não existe um local completamente seguro, porém o homem busca diminuir ao máximo todas essas vulnerabilidades existentes, trabalhando com diversas condições de proteção à informação.

Segundo a ISO/IEC 27002:2005(2005), a informação é um conjunto de dados que representa um ponto de vista. Um dado processado é o que gera uma informação, não tendo valor antes de ser verificado. A partir daí ele passa a ser considerado uma informação, que pode gerar entendimento e conhecimento. Portanto, pode-se entender que o conhecimento produzido é o resultado do processamento de dados.

Ainda, segundo a ISO/IEC 27002:2005, a informação é um ativo que como qualquer outro, é importante e essencial para as pessoas, e deve ser adequadamente protegida. A definição de ativo compreende ao conjunto de bens e direitos de uma entidade. Entretanto, atualmente, um conceito mais amplo tem sido adotado, para se referir ao ativo como tudo aquilo que possui valor para o usuário. Segundo Dantas (2011, p.21) a informação ocupa um papel de destaque no ambiente das organizações empresariais, e também adquire um potencial de valorização para as empresas e para as pessoas, passando a ser considerado o seu principal ativo.

A informação é encarada, atualmente, como um dos recursos mais importantes, contribuindo decisivamente para uma maior ou menor competitividade.

Para a ISO/IEC 27002:2005 (ISO/IEC 27002:2005, 2005, p. x):

> A informação pode existir em diversas formas. Ela pode ser impressa ou escrita em papel, armazenada eletronicamente, transmitida pelo correio ou por meios eletrônicos, apresentada em filmes ou falada em conversas.

Seja qual for a forma em que a informação é apresentada ou o meio pelo qual é compartilhada ou armazenada, ela é importante. Como resultado deste significante aumento da interconectividade, a informação está agora exposta a um crescente número e a uma grande variedade de ameaças e vulnerabilidades.

Para a ABNT NBR ISO/IEC 17799:2005 (2005, p.ix):

> Segurança da informação é a proteção da informação de vários tipos de ameaças para garantir a continuidade do negócio, minimizar o risco ao negócio, maximizar o retorno sobre os investimentos e as oportunidades de negócio informação pode existir em diversas formas.

A informação é um ativo que deve ser protegido e cuidado por meio de regras e procedimentos, do mesmo modo que protegemos nossos recursos financeiros e patrimoniais.

A Segurança da Informação é a proteção contra o uso ou acesso não-autorizado à informação, enquanto a integridade e a confidencialidade dessas informações são preservadas. Ela possui três pilares que orientam, sendo esses:

- **Disponibilidade:** É a forma de garantia, onde pode-se contar com a disponibilidade da informação, para que todos os usuários autorizados tenham acesso do que serão disponibilizadas.
- **Integridade:** O fundamento que trata da proteção de dados, buscando que não haja violação ou modificação. A forma de assegurar que da

forma como foram salvas, as informações estarão disponibilizadas, sem alterações.

- **Confidencialidade:** Interligada a confiabilidade, onde o sigilo das informações, estabelecendo níveis de acesso a informações determinadas, à usuários autorizados, restringindo e disponibilizando dados pertinentes a cada um, respeitando os níveis hierárquicos e as políticas de segurança adotados.

Essa norma possui uma seção introdutória sobre o processo de avaliação e tratamento de riscos e está dividida em onze seções específicas, que são: política de segurança da informação; organização da segurança da informação; gestão de ativos; segurança em recursos humanos; segurança física e do ambiente; gestão das operações e comunicações; controle de acesso; aquisição, desenvolvimento e manutenção de sistemas de informação; gestão de incidentes de segurança da informação; gestão da continuidade do negócio, e conformidade. Essas seções totalizam trinta e nove categorias principais de segurança, e cada categoria contém um objetivo de controle e um ou mais controles que podem ser aplicados, bem como algumas diretrizes e informações adicionais para a sua implementação. Para Fontes e Araujo (2008), o sistema de gestão de segurança da informação é o resultado da sua aplicação planejada, diretrizes, políticas, procedimentos, modelos e outras medidas administrativas que, de forma conjunta, definem como são reduzidos os riscos para a segurança da informação.

Segundo Fontes (2008), a principal razão em classificar as informações, é de que elas não possuem o mesmo grau de confidencialidade, ou então as pessoas podem ter interpretações diferentes sobre o nível de confidencialidade da informação. Para poder classificar uma informação, é importante saber quais as consequências

que ela trará para o usuário, caso seja divulgada, alterada ou eliminada sem autorização. Somente através da interação com as pessoas diretamente responsáveis pela informação, que será possível estabelecer estas consequências e criar graus apropriados de classificação.

Segundo Campos (2007), a ameaça pode ser considerada um agente externo ao ativo de informação, pois se aproveita de suas vulnerabilidades para quebrar os princípios básicos da informação, a confidencialidade, integridade ou disponibilidade. Atualmente, o mundo apresenta-se bastante inseguro, onde as pessoas devem estar sempre atentas para as ameaças aos seus bens, que, se concretizadas poderão causar grandes perdas, e consequentemente danos financeiros. As ameaças podem ser:

- **Naturais**: são aquelas que se originam de fenômenos da natureza.
- **Involuntárias**: são as que resultam de ações desprovidas de intenção para causar algum dano.
- **Intencionais**: são aquelas deliberadas, que objetivam causar danos, tais como hackers.

A NBR ISO/IEC 27002:2005 define a vulnerabilidade como uma fragilidade de um ativo ou grupo de ativos que pode ser explorada por uma ou mais ameaças. Segundo Campos (2007), vulnerabilidade são as fraquezas presentes nos ativos, que podem ser exploradas, seja ela intencionalmente ou não, resultando assim na quebra de um ou mais princípios da segurança da informação. Ao terem sido identificadas as vulnerabilidades ou os pontos fracos, serão possíveis dimensionar os riscos aos quais o ambiente está exposto e assim definir medidas de segurança apropriada para sua correção.

Com relação a segurança, os riscos são compreendidos como condições que criam ou aumentam o potencial de danos e perdas. É medido pela possibilidade de um evento vir a acontecer e produzir perdas. Para evitar possíveis perdas de informações, que dependendo do seu grau de sigilo, poderá causar danos irreparáveis a uma pessoa. A norma NBR ISO 27002(2005) nos oferece uma métrica, em que o risco pode ser calculado pela seguinte formula:

RISCO = (Ameaça) x (Vulnerabilidade) x (Valor do Risco).

Na Segurança da Informação, existem mecanismos de segurança que são medidas que visam controlar o acesso às informações de forma física e lógica. Enquanto os controles físicos limitam o contato direto que um usuário pode ter com a informação e toda a estrutura que a envolve, os controles lógicos trabalham pela integridade da informação de modo que ela não seja acessada e manipulada. Os controles físicos e lógicos tratam da segurança de diversos recursos, como código-fonte de aplicativos, arquivos de senha, base de dados, registros de usuários e, por fim, limita o acesso às ferramentas que permitem editar arquivos e programas.

São esses mecanismos que promovem essas qualidades e benefícios da Segurança da Informação aos ambientes corporativos. Alguns desses mecanismos são:

- **Criptografia:** Meio de conversão de dados em um formato do qual seja quase impossível decifrá-lo. Uma das formas seguras para armazenar os dados e impedir completamente a interpretação das informações, sendo convertido ao estado inteligível quando uma chave (senha) é inserida.

- **Assinatura digital:** É a garantia da integridade dos dados armazenados, por meio de criptografia, tendo seu acesso sendo em alguns casos irrestrito e seu conteúdo não pode ser alterado.
- **Certificação**: Forma de atestar e autenticar um arquivo, garantindo que o mesmo, seja válido.
- **Honeyspot**: Um software, que age comumente como um antivírus em tempo real, onde suas funcionalidades incluem a proteção dos dados contra invasores, tentativas de aplicações maliciosas e fora do comum ao sistema. O que diferencia de um antivírus, é que ao invés de manter o sistema em quarentena, o honeyspot cria uma sequência falsa de informações, fazendo com que o invasor acredite que está tendo acesso as informações verdadeiras.

Dentre os tipos de vulnerabilidades, a Segurança da Informação promove a proteção de seus dados indicando um estado de fraqueza, que pode se abordar tanto ao comportamento do indivíduo, como objetos, situações ou ideias. Dentre as citadas, pode-se exemplificar o software, pois não é incomum apresentar erros e falhas que possibilitem a violação de dados. Existem ainda, algumas outras vulnerabilidades das quais a Segurança da Informação é capaz de coibir.

As vulnerabilidades de hardware, assim como acima citado, softwares, podem apresentar sinais de defeitos de fabricação, comprometendo a confidencialidade ou a integridade de seus dados.

As vulnerabilidades de armazenamento, são os dispositivos ou mídias de armazenamento ou gravação de dados.

As vulnerabilidades humanas, assim como seu nome, são riscos corridos pelas próprias pessoas, independentemente de suas intenções. Ao tentar violar as informações contidas em um documento de forma acidental, normalmente são causados devida à plena falta de preparo por parte do usuário, que pode cometer equívocos durante uma consulta ou simplesmente não seguir os procedimentos de

segurança. Ou ainda, quando informações são extraídas de forma ilegítima, por não haver meios de segurança adequados.

Para que a cultura dos usuários seja mudada em relação à segurança da informação, é fundamental que eles estejam preparados para a mudança, por meio de avisos, palestras de conscientização, elaboração de guias rápidos de consulta e treinamento direcionado.

Hoje no mercado existem diversas empresas que estão se preocupando com a falta de segurança da informação e como ela está afetando os seus usuários. Empresas como a Apple, Samsung e a Intel, veem fazendo investimentos em tecnologias para facilitar e auxiliar o usuário na forma como ele protege as suas informações.

A Intel criou o Intel Authenticate, uma solução de autenticação de vários fatores, aprimorada por hardware. Ele protege o ponto de extremidade, proteção de segurança fora do sistema operacional para reduzir o risco de violação de dados. Fatores de autenticação, as políticas de segurança de TI e as decisões de autenticação são criptografadas no hardware. As credenciais do usuário gerenciadas pela Intel Authenticate são protegidas no hardware e nunca estão expostas ao software. Está ferramenta de início traz recursos de biometria, e autenticação através de outros aparelhos, porém, promete trazer autenticação através de gestos, íris e pela voz.

A Samsung desenvolveu um ambiente de segurança para Android chamado Knox, que tem como objetivo principal solucionar os problemas de segurança enfrentados diariamente. Tal aplicativo permite que os usuários façam uso de dispositivos pessoais em qualquer rede. O Knox é um aplicativo descrito como uma solução de segurança, abrange desde hardware ao nível de aplicativos para Android, porém, como principal atrativo do Knox é a forma de participação de equipamentos pessoais para uso profissional e o dia a dia de seus usuários. Na versão 2.8 utilizada nos aparelhos Samsung Galaxy S8 garante a defesa ininterrupta dos dados pessoais.

Já a Apple utiliza o recurso Chaves do iCloud para guardar senhas de seus usuários, quando o usuário criar uma senha exclusiva, o recurso Chaves do iCloud vai lembrar essa senha para ele, guardando as suas combinações de nome de usuário e

senha e sincroniza com os dispositivos que escolhido — Mac, iPhone, iPad e iPod touch. Quando o usuário entrar em um site, Chaves do iCloud preenche as informações de login para acessar suas contas e pode preencher os dados de seu cartão de crédito quando fizer compras online.

Tanto em redes sociais, jogos online e moedas digitais dentre outros serviços que nos trazem bens virtuais, é necessário preocupar-se com os dados que deixamos nestas plataformas e em outras. As informações mal protegidas podem levar um indivíduo a obter acesso ou a conhecimentos sobre o usuário.

Existem algumas aplicações de software projetadas como meios de proteção e segurança para resguardar os dados e o funcionamento de sistemas informáticos caseiros e empresariais de outras aplicações conhecidas comumente como vírus ou malware que tem a função de alterar, perturbar ou destruir o correto desempenho dos computadores. Muitos atacantes, utilizam desses tipos de aplicações (vírus) para invadir os dispositivos e assim efetuar o roubo das informações ou dos bens.

Um programa de proteção de vírus, tem um funcionamento comum, que com frequência compara o código de cada arquivo que revisa com uma base de dados de códigos de vírus já conhecidos, e desta maneira, pode determinar se trata de um elemento prejudicial para o sistema. Também pode reconhecer o comportamento ou padrão de conduta típica de um vírus. Os antivírus podem registrar tanto os arquivos encontrados dentro do sistema como aqueles que procuram ingressar ou interagir com o mesmo.

Um antivírus pode ser complementado por outros aplicativos de segurança, como firewalls ou antispywares que cumprem funções auxiliares para evitar a entrada de intrusos. Alguns dos programas de proteção, agregam funcionalidades e trabalham como firewall e antispyware para facilitar o uso do usuário.

Assim, serão listados os principais métodos e formas para o auxílio na proteção destes dados.

- **Antivírus:** primeira ferramenta necessária dentro de um computador para o usuário se proteger. É possível encontrar bons softwares de proteção, os pagos que existem no mercado ainda são superiores. Com o antivírus começamos a impedir que o criminoso envie vírus para danificar o dispositivo e deixa-lo mais frágil a um ataque.
- ***Firewall*:** ele trabalha em conjunto com o antivírus. Uma vez que ele é o responsável em monitora o tráfego de entrada e saída e tomar a decisão se permiti ou bloqueia tráfegos específicos de acordo com um conjunto definido de regras de segurança. Uma vez dentro (quando o firewall falha) o programa invasor ainda tem que enfrentar o antivírus que fará o que for possível para elimina-lo.
- ***Antispyware*:** eles são responsáveis em executar varreduras no computador com o objetivo de tentar eliminar do sistema spywares (programas que recolhem informações dos usuários, sobre os seus costumes na Internet e transmite a uma entidade externa na Internet, sem o seu conhecimento).
- **Atualizações:** manter as atualizações do sistema operacional (*Windows*, Mac OS, IOS, Android dentre outros) sempre em dia. Estas atualizações muito das vezes são para corrigir falhas no sistema, e se o mesmo não estiver atualizado, o criminoso que tiver conhecimento destas vulnerabilidades poderá realizar um ataque sendo mais facilmente alcançado o seu sucesso, o crime em si.

- **Links ou Sites desconhecidos:** procure acessar somente sites de sua confiança verificando sempre o certificado digital do mesmo, para não correr o risco de ser uma página clonada. Sites de compras online dentre outros serviços, busque não utilizar aqueles que não conheça, veja sempre indicações de amigos próximos e se possível olhe outras formas de pagamento que não deixe gravado no site informações de seu cartão de credito, mesmo com a praticidade pode acarretar riscos
- **Cadastros:** como visto em um dos exemplos, uma das formas de um criminoso roubar os bens virtuais e a partir do envio de um e-mail a vítima, solicitando o cadastro para algum serviço inovador ou algum prêmio, ao cadastrar, a vítima envia informações de extrema importância para o criminoso facilitando o ataque. Procure evitar o envio de dados importantes e pessoais por e-mail, nunca envie senhas de suas contas pessoais ou de trabalho e números de cartões de credito com suas senhas. Se não participou de algum concurso para ganhar um prêmio, a probabilidade de ter ganhado tende a zero.
- **Senhas:** procure usar senhas diferentes em todos os serviços que obtiver na Internet, uma para a rede social, uma para o jogo online, uma para o *e- mail* e para todas as contas que tiver, sempre uma para cada. Pois mesmo que o criminoso descubra a senha da sua rede social, ele não vai conseguir o acesso a outros serviços online, e o caso de se não conseguir proteger uma conta, pelo menos as outras estarão. E por recomendações procure sempre trocar a senha de tempos em tempos, para que assim dificulte o acesso indesejado.
- **Backup**: A ISO/IEC 27002 (2005) recomenda que o backup dos sistemas seja armazenado em outro local, o mais longe possível do

> ambiente atual, como em outro prédio. Um dos maiores erros cometidos em questão de segurança de backup, foi o atentado de 11 de setembro, onde foram derrubadas as torres gêmeas nos EUA, onde empresas localizadas na torre A tinham backups na torre B, e empresas da torre B tinham backup na torre A, depois da queda das duas torres, várias empresas simplesmente sumiram, deixando de existir, um erro que poderia ser controlado caso o backup estivesse localizado em outro lado da cidade. É evidente que o procedimento de backup é um dos recursos mais efetivos para assegurar a continuidade das operações em caso de paralisação na ocorrência de um sinistro.

Nas redes sociais, procurar sempre manter as suas informações no privado assim, quando o criminoso for acessar na rede social o seu perfil, ele não terá informações como o seu e-mail, dentre outros dados pessoais. Procurar indicar aos amigos que façam o mesmo, pois assim, somente pessoas daquele círculo de amizades poderão ter acesso, pois hoje por mais que o seu perfil seja privado para acesso somente de seus amigos, se um amigo postar uma foto ou uma informação sobre vocês de forma publica, o criminoso a partir dela pode efetuar um ataque aos dois. Algumas redes sociais possuem a opção de grupos, ou seja, o usuário poderá postar informações relacionadas a um grupo de pessoas sem que o outro grupo de pessoas tenha acesso às informações, sendo assim as vezes não é interessante que o grupo de amigos da faculdade tenham acesso a fotos do grupo do ensino médio

Ao levar o seu equipamento ao conserto, procure sempre fazer um backup, uma cópia de segurança das informações que estão no equipamento depois apague todos os seus arquivos pessoais que estão em sua máquina e saia de todas os perfis que possua no computador. Não é seguro que terceiros tenham acesso aos seus

dados, podendo o técnico acabar salvando para si tais arquivos, sem o seu consentimento, é um risco.

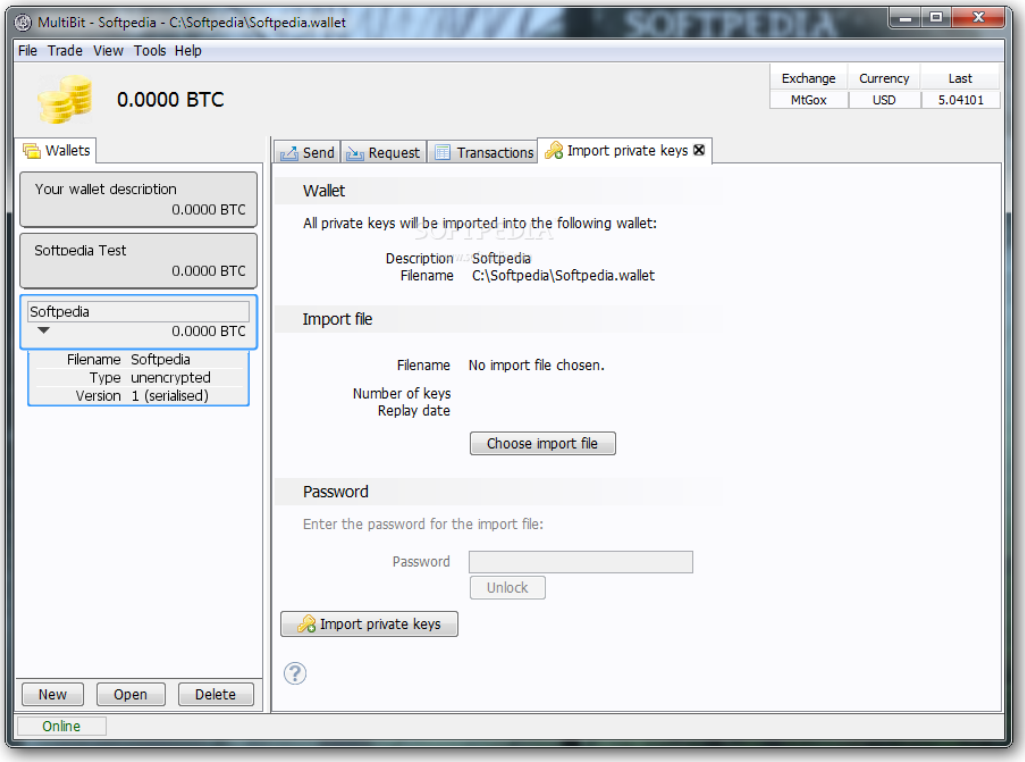
5.1 Moedas Digitais.

Com o surgimento das moedas digitais, despertou-se o interesse de diversas instituições, governos e criminosos neste tipo de bem virtual. Tudo se transformou em uma corrida: as instituições para que estejam aptas a trabalhar e lucrar nesse mercado, os governos para que possam ter o controle e legislar e os criminosos para se aproveitar, tirar vantagem e roubar dos usuários.

Pelo pensamento de João Victor Rozzati Longhi e Cristiano Medeiros de Castro (2014), a uma linha tênue entre o dinheiro existente no mundo real e aqueles que existem no mundo virtual, em questão da função e de sua aquisição. Percebe-se que ambos os valores dados de maneira a valorizar um objeto, facilitando assim a movimentação de mercadorias. Nos mundos virtuais a função é a mesma, contudo os valores dos objetos são totalmente arbitrados pelo proprietário. A moeda virtual e a moeda real têm uma conexão, visto ser possível a compra de moedas pagando por elas em dinheiro vivo.

De forma geral, as criptomoedas são compostas por uma carteira (ou wallet) – programa que implementa os algoritmos criptográficos, carteira essa exemplificada na figura 2. As carteiras possuem um par de “senhas criptográficas”, chamadas de endereço e chave privada, que compõem a base da criptografia da *Wallet.* Com o endereço é possível enviar e receber criptomoedas. A perda da chave privada acarreta na perda de todo o conteúdo da carteira, por isso se aconselha a fazer “backup” constantemente.

Figura 2. Carteira (Wallet).



Fonte: Carteira de Bitcoin – Imã de Bitcoin , 2017.

É mais seguro que dentro destas carteiras sejam depositados somente valores pequenos, que possam vir a ser utilizados no dia a dia. O dinheiro digital que não for utilizado diariamente ficará seguro se guardado em outros meios, de preferência que sejam de difícil acesso, para que assim fiquem mais protegidos.

Uma carteira *offline*, também conhecida como *Cold Storage* (armazenamento frio), provê o mais alto nível de segurança para a sua conta. Trata-se de armazenar uma carteira em local protegido que não está ligado à rede. Quando feito corretamente, pode oferecer uma boa proteção contra vulnerabilidades de computadores. Usando uma carteira offline em conjunto com backups e criptografia é também uma boa prática (BITCOIN, 2017).

Existem algumas empresas no mercado, especializadas em proteção de carteiras, é um pouco arriscado confiar fundos monetários digitais a uma empresa terceirizada, mas com as devidas precauções, é possível manter seu dinheiro digital seguro. Um diferencial é que algumas já estão provendo serviços como cartões de débito, onde se retira as quantias que estão na carteira.

Outra forma de proteção é a utilização de carteiras físicas, que são dispositivos feitos para proteger sua conta. Funciona basicamente assim, conecta-se o equipamento ao computador, será pedido uma senha é se sua conta já estiver cadastrada o dispositivo mostrará informações sobre a mesma, ao terminar de usar é só o retirar e pronto, sua conta estará a salva nesse aparelho.

Se mesmo utilizando todas estas formas para se resguardar e se proteger na Internet, você for vítima de um crime online, procure a delegacia mais próxima e faça um boletim de ocorrência, para que assim, as autoridades legais possam ter o registro e em eventuais acontecimentos chegar até o criminoso.

CONCLUSÃO

O estudo sobre propriedade de bens de consumo virtuais permitiu compreender como as pessoas estão desprotegidas na rede mundial de computadores. Durante este estudo, percorremos os conceitos, as legislações internacionais e brasileiras, e paradigmas de cibercrimes pertinentes e correlacionados ao assunto, explorando suas características, funcionalidades e peculiaridades. Com um embasamento teórico formado, partimos para o estudo do direito digital e a visão sobre os bens digitais. Foram apontadas as aplicações do direito digital sobre os bens virtuais mais conhecidas pelo mundo e seus modos de operações. Para aprofundar a pesquisa, foi estudado quando o mundo começou a se preocupar com o cibercrime e como o mesmo chegou até os bens digitais e seu consumismo.

No que se refere à Segurança da Informação, apesar de existir tipificação no ordenamento jurídico brasileiro, ele não provê proteção total contra-ataques, sendo que uma das falhas é se o usuário não tiver alguma forma de segurança em seu dispositivo, mesmo sendo atacado não será considerado crime. Fica a cargo do usuário a adoção de medidas de segurança em seu dispositivo e seus bens virtuais, com um ordenamento jurídico lento e fraco para crimes virtuais. Para a comunicação na Internet é sugerido o uso de softwares para proteção e alguns cuidados para com o acesso e o download em determinados tipos de sites.

Ao dedicar um item de um capítulo ao estudo sobre a análise de cibercrimes envolvendo bens virtuais, pode-se concluir que entre as diversas

formas de proteção e prevenção existentes os criminosos ainda encontram brechas para fazer com que o usuário acabe caindo em golpes, ainda que bem orientado. Contudo, nem todos os golpes na qual os usuários são enganados, a culpa por sua totalidade é deles, tendo, as empresas administradoras uma parcela da culpa pela forma como protegem as informações básicas dos seus usuários. Por exemplo, no caso de redes sociais que vendem informações de seus utilizadores. Assim, as redes sociais da mesma forma que melhoram a vida social das pessoas, encontrando novas amizades, amizades perdidas ou familiares que há tempos não se viam, tais mídias sociais também podem acabar com a vida social de indivíduos, ofendendo a imagem de algum individuo ou o simples fato da obtenção de informações desse usuário. Esse é o novo paradigma tecnológico, em que as pessoas devem se adaptar a nova forma de se comunicarem e agirem, se reeducando e estando aptas a entender que o que se fala ou posta na Internet não pode ser mais retirado da *Internet*.

Focando na legislação brasileira, o uso da *Internet* já se tornou um direito de todos, pois o país já conta com leis que garantam isso. Basta o brasileiro saber lidar com a liberdade que possui e com as vulnerabilidades em sua volta, ao proteger seus bens virtuais.

Foram apresentados, também, os tipos de cibercrimes mais realizados no mundo, e no Brasil. Foi visto que com eles é possível destruir grandes corporações e desmantelar famílias.

Por isso, como trabalho futuro, proponho que seja desenvolvido um estudo mais especifico sobre a relação das pessoas com o mercado de compras online e especificando a segurança das criptomoedas, e que seja feito uma pesquisa voltada para estes assuntos. Focando, assim, na interação saudável

dos usuários com o consumismo na rede mundial de computadores, abordando as principais tecnologias para proteger as moedas virtuais, relacionando o mercado digital com as criptomoedas, e detalhando os riscos dessa interação diária, e até mesmo realizando um estudo de caso, por desempenhar um papel importante na evolução da sociedade e no acesso à *Internet*.

REFERÊNCIAS

AGÊNCIA BRASIL. **Brasileiros compram produtos piratas, indica pesquisa da Fecomércio-RJ**. 2010. Disponível em: <http://extra.globo.com/noticias/brasil/brasileiros-compram-mais-produtos-piratas-indica-pesquisa-da-fecomercio-rj-725133.html>. Acesso em: 2 abri. 2017.

AIRES, José. **Direito, Sociedade e Informática:** Limites e perspectivas da vida digital. Florianopolis: Fundação Boiteux, 2000.

ABNT - ASSOCIAÇÃO BRASILEIRA DE NORMAS TÉCNICAS.ABNT NBR ISO/IEC 27002 – Tecnologia da informação – técnicas de segurança – Código de pratica para gestão de segurança da informação. ABNT, 2005.Acessado em 20 de out. 2017

BARLOW, John Perry. A Declaration of the Independence of Cyberspace. 1996. Disponível em: <https://www.eff.org/cyberspace-independence>. Acesso em 10 abri. 2017.

BITCOIN. **Protegendo sua Carteira**.2017 Disponível em: <https://bitcoin.org/pt_BR/proteja-sua-carteira>. Acesso em 29 mar. 2017.

BRASIL Congresso Nacional, Câmara dos Deputados. **Marco Civil da Internet.** 2.ed. Brasília: Livraria Câmara, 2015.

BRASIL. **Lei Nº 8.078**, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. Diário Oficial da república Federativa do Brasil. Brasília, DF, 11 set. 1990. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/l8078.htm >. Acesso em: 28 mar. 2017.

BRASIL. **Lei Nº 9.472**, de 16 de julho de 1997. Dispõe sobre a organização dos servidores de telecomunicações, a criação e funcionamento de um órgão regulador e outros aspectos institucionais, nos termos da Emenda Constitucional nº8, de 1995. Diário Oficial da república Federativa do Brasil. Brasília, DF, 16 jul. 1997. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/L9472.htm >. Acesso em: 28 mar. 2017.

BRASIL. **Lei nº. 9.609**, de 19 de fevereiro de 1998. Dispõe sobre a proteção da propriedade intelectual de programa de computador, sua comercialização no País, e dá outras providências. Diário Oficial da república Federativa do Brasil. Brasília, DF, 19 fev. 1998. Disponível em:< http://www.planalto.gov.br/ccivil/Leis/L9609.htm >. Acesso em: 28 mar. 2017.

BRASIL. **Lei nº. 9.610**, de 19 de fevereiro de 1998. Altera, atualiza e consolida a legislação sobre direitos autorais e dá outras providências. Diário Oficial da república Federativa do Brasil. Brasília, DF, 19 fev. 1998. Disponível em: <http://www.planalto.gov.br/CCIVIL/Leis/L9610.htm>. Acesso em: 28 mar. 2017.

BRASIL. **Lei Nº 10.406**, de 10 de janeiro de 2002. Código Civil. Diário Oficial da república Federativa do Brasil. Brasília, DF, 10 jan. 2002. Disponível em: < http://www.planalto.gov.br/ccivil_03/leis/2002/L10406.htm>. Acesso em: 28 mar. 2017.

BRASIL. **Lei Nº 12.527**, de 18 de novembro de 2011. Regula o acesso a informações previsto no inciso XXXIII do art. 5º, no inciso II do § 3º do art. 37 e no § 2º do art. 216 da Constituição Federal; altera a Lei nº 8.112 de 11 de dezembro de 1990; revoga a Lei nº.11.111, de 5 de maio de 2005, e dispositivos da Lei nº 8.159, de 8 de janeiro de 1991; e dá outras providências. Diário Oficial da república Federativa do Brasil. Brasília, DF, 18 nov. 2011. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2011/lei/l12527.htm >. Acesso em: 28 mar. 2017.

BRASIL. **Lei Nº 12.737**, de 30 de novembro de 2012. Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº2.848, de 7 de dezembro de

1940 – Código Penal; e dá outras providências. Diário Oficial da república Federativa do Brasil. Brasília, DF, 30 nov. 2012. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em: 28 mar. 2017.

BRASIL. **Lei Nº 12.965**, de 30 de novembro de 2014. Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil. Diário Oficial da república Federativa do Brasil. Brasília, DF, 23 abr. 2014. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em: 28 mar. 2017.

BRASIL. **Lei Nº 12.850**, de 2 de agosto de 2013. Define organizações criminosas e dispõe sobre a investigação criminal, os meios de obtenção da prova, infrações penais correlatas e o procedimento criminal; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 (Código Penal); revoga a lei nº 9.034, de 3 de maio de 1995; e dá outras providências. Diário Oficial da república Federativa do Brasil. Brasília, DF, 2 ago. 2013. Disponível em: < http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2013/lei/l12850.htm >. Acesso em: 28 mar. 2017.

BRITO, Paulo. **Os Ataques Hackers mais comuns**. 2015. Disponível em: < http://www.cibersecurity.com.br/os-ataques-hackers-mais-comuns/>. Acesso em: 20 jan. 2017.

CENTRAL JURÍDICA. **Dos Bens**. Disponível em: < http://www.centraljuridica.com/doutrina/58/direito_civil/dos_bens.html >. Acesso em: 28 mar. 2017.

CAMPOS, A. **Sistemas De Segurança da informação**. 2 eds. Florianópolis: Visual Books, 2007.

CRESPO, Marcelo Xavier de Freitas. **Crimes Digitais.** 1.ed. São Paulo, Saraiva, 2011.

DANTAS, M. **Segurança da Informação : Uma Abordagem focada em gestão de riscos.** 1 ed. Olinda: Livro rápido, 2011.

FONTES, E. **Praticando a Segurança da Informação**. Rio de Janeiro: Brasport, 2008.

FREITAS, F; ARAUJO, M. **Políticas de Segurança da Informação: Guia prático para elaboração e implementação.** 2ed. Rio de Janeiro: Ciência Moderna LTDA, 2008

GNT, **Vítimas do Facebook**, 2012. Disponível em: <https://www.youtube.com/watch?v=taYESjyhMjY>. Acesso em: 20 mar. 2017.

JALIL, Daniela Schaun. **Direitos autorais sobre a música na Internet**. 2003.Disponível em: <http://www2.uol.com.br/direitoautoral/artigo0804b.htm/>. Acesso em: 20 nov. 2016.

LEITE, George Salomão; LEMOS, Ronaldo. **Marco Civil da Internet.** 1.ed. Brasília: Atlas, 2014.

LONGHI, João. Vitor; CASTRO, Cristiano Medeiros. **O Direito do consumidor no comércio eletrônico dos jogos "MMORPG" e Jogos sociais (FREEMIUNS).** 2014. Disponível em: <http://www.publicadireito.com.br/artigos/?cod=6b3829244a3cb6ef>.Acesso em: 20 ago. 2016.

MACIEL, Camila. **Cresce o número de denúncias de crimes virtuais em 2014**.

2015 disponível em: < http://www.ebc.com.br/noticias/2015/02/cresce-numero-de-denuncias-de-crimes-na-Internet-em-2014>. Acesso em: 29 mar. 2017.

MIND, Sophia, **Bens Virtuais**. Disponível em:< http://www.sophiamind.com/wp-content/uploads/SophiaMind_Bens-Virtuais_Brasil1.pdf>. Acesso em: 28 mar. 2017.

NUNES, Paulo. **Bem**, 2016. Disponível em:<http://knoow.net/cienceconempr/economia/bem/>. Acesso em: 28 mar. 2017.

PACIEVITCH, Thais. **Bens de Consumo**, 2017. Disponível em:<http://www.infoescola.com/economia/bens-de-consumo/>. Acesso em: 28 mar. 2017.

PINHEIRO, Patrícia Peck. **Direito Digital Aplicado 2.0**. 2.ed São Paulo: Saraiva, 2016.

REBS, Rebeca. **Lugares de apropriação em social games**. 2012. Disponível em: <http://www.rebs.com.br/?tag=bens-virtuais>. Acesso em: 20 ago. 2016.

REVA, João Gustavo, **Hacker de World of Warcraft é sentenciado a dois anos de prisão na China**, 2013, disponível em:<https://www.tecmundo.com.br/video-game-e-jogos/48621-hacker-de-world-of-warcraft-e-sentenciado-a-dois-anos-de-prisao-na-china.htm>. Acesso em: 10 de dez. 2016.

RODRIGUES, J.C. ***Brincando de deus - Criação de Mundos Virtuais e Experiências de Imersão Digitais***. Rio de Janeiro: Marsupial. pp. 58 a 62. 2016.

TRUZZI, Gisele. Redes **sociais e segurança da informação**. 2015.Disponível em: <http://www.cnasi.com.br/redes-sociais-e-seguranca-da-informacao/>. Acesso em: 20 nov.2016.

WIKENS, Érica Elisa Dani; FERREIRA, Luiz Felipe. Aspectos Conceituais da tributação de bens digitais. **Revista Catarinense de Ciência Contábil**, Florianópolis, v.7, n.21, p.71 – 84, ago. / nov. 2008.

GLOSSARIO

Internet: rede de computadores dispersos por todo o planeta que trocam dados e mensagens utilizando um protocolo comum, unindo usuários particulares, entidades de pesquisa, órgãos culturais, institutos militares, bibliotecas e empresas de toda envergadura.

Sitio: Site em português, local na Internet identificado por um nome de domínio, constituído por uma ou mais páginas de hipertexto, que podem conter textos, gráficos e informações em multimídia.

Online: é um anglicismo advindo do uso da Internet, sendo "em linha" sua tradução literal, pouco usada no português. Partir da palavra em inglês "fishing", que significa "pescando".

Browser: navegador.

Download: ato de fazer cópia de uma informação, ger. de um arquivo, que se encontra num computador remoto.

Backup: cópia de segurança.

Cibercrime: Crime cibernético

Ciberespaço: espaço das comunicações por redes de computação

Hacker: ou ciberpirata, pessoa com profundos conhecimentos de informática que eventualmente os utiliza para violar sistemas ou exercer outras atividades ilegais, pirata eletrônico.

Hacktivismo: uma junção de hack e activismo, é normalmente entendido como escrever código fonte, ou até mesmo manipular bits, para promover ideologia política - promovendo expressão política, liberdade de expressão, direitos humanos, ou informação ética.

Hackear: Ato praticado na violação de sistema ou exercício de outras atividades ilegais relacionadas à Internet.

Cracker: perito em informática que usa seus conhecimentos para violar sistemas ou redes de computadores.

Phishing: é uma técnica de fraude online, utilizada por criminosos no mundo da informática para roubar senhas de banco e demais informações pessoais, usando-as de maneira fraudulenta. A expressão phishing (pronuncia-se "fichin") surgiu a surgiu a partir da palavra em inglês "fishing", que significa "pescando".

Software: conjunto de componentes lógicos de um computador ou sistema de processamento de dados; programa, rotina ou conjunto de instruções que controlam o funcionamento de um computador; suporte lógico.

Malware: é a combinação das palavras inglesas malicious e software, ou seja, programas maliciosos. São programas e comandos feitos para diferentes propósitos:

apenas infiltrar um computador ou sistema, causar danos e apagar dados, roubar informações, divulgar serviços

Spyware: é um software espião de computador, que tem o objetivo de observar e roubar informações pessoais do usuário que utiliza o PC em que o programa está instalado, retransmitindo-as para uma fonte externa na internet, sem o conhecimento ou consentimento do usuário.

Bitcoin: Moeda digital

Login: é um termo em inglês usado no âmbito da informática, um neologismo que significa ter acesso a uma conta de e-mail, computador, celular ou outro serviço fornecido por um sistema informático. Esta palavra é formada pela junção de log e in. Em inglês log pode ser uma espécie de registro e in significa dentro.

True Key: é o modo mais fácil e seguro de acessar seu mundo digital. É um aplicativo que pode ser instalado em todos os seus dispositivos para eliminar a confusão das senhas.

Status: condição (de alguém ou de algo) aos olhos do grupo humano em que vive.

Player: *Player* é uma palavra inglesa que significa “tocador” ou “jogador”, em português. Deriva do verbo “*to play*” que significa “jogar”, “tocar”, “brincar”, “se divertir” e se emprega em diversas situações relacionadas.

Multiplayer: Jogos multijogador, também conhecidos como jogos multiplayer, são jogos que permitem que vários jogadores participem simultaneamente de uma mesma partida.

Avatar: Personagem de jogos

Skins: Acessório usado em jogos

Honeyspot: trata-se de um software que age como um antivírus em tempo real, cuja função é proteger os dados de invasores, aplicações maliciosas e estranhas ao sistema.