Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GABRIEL RODRIGUES GRANJEIA

DIREITO DIGITAL: A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Assis/SP 2020

Fundação Educacional do Município de Assis
Instituto Municipal de Ensino Superior de Assis
Campus "José Santilli Sobrinho"

GABRIEL RODRIGUES GRANJEIA

DIREITO DIGITAL: A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

Projeto de pesquisa apresentado ao curso de Direito do Instituto Municipal de Ensino Superior de Assis – IMESA e à Fundação Educacional do Município de Assis – FEMA, como requisito parcial à obtenção do Certificado de Conclusão.

Orientando(a): Gabriel Rodrigues Granjeia
Orientador(a): Márcia Valéria Seródio Carbone

Assis/SP
2020

FICHA CATALOGRÁFICA

S586d GRANJEIA, Gabriel Rodrigues.

Direito Digital: a importância da segurança da informação / Gabriel Rodrigues Granjeia. Fundação Educacional do Município de Assis –FEMA – Assis, 2020.

49p.

Trabalho de Conclusão de Curso (Direito). – Fundação Educacional do Município de Assis – FEMA

Orientadora: Dra. Márcia Valéria Seródio Carbone

1.Direito-digital 2.Segurança-informação

CDD341.55251
Biblioteca da FEMA

DIREITO DIGITAL: A IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO

GABRIEL RODRIGUES GRANJEIA

Trabalho de Conclusão de Curso apresentado ao Instituto Municipal de Ensino Superior de Assis, como requisito do Curso de Graduação, avaliado pela seguinte comissão examinadora:

Orientador: Márcia Valéria Seródio Carbone

Examinador: Hilário Vetore Neto

Assis/SP
2020

DEDICATÓRIA

Dedico este trabalho primeiramente a Deus, e a todos que me permitiram ter a oportunidade de estudar, principalmente a minha namorada Ana Rita.

A nova fonte de poder não é o dinheiro nas mãos de poucos, mas informação nas mãos de muitos.

-John Naisbitt

RESUMO

Este trabalho tem como objetivo estudar a importância do Direito Digital e a Segurança da Informação em aspectos sociais e comerciais, levando em consideração a necessidade destes globalmente, além de analisar a evolução e as necessidade do tema na atualidade, objetivando compreender e entender acerca do tema.

Palavras-chave: Direito Digital; Marco Civil da Internet; Segurança da informação.

ABSTRACT

This work aims to study the importance of Digital Law and Information Security in social and commercial aspects, taking into account their need globally, in addition to analyzing the evolution and needs of the topic today, aiming to understand and understand about the topic.

Keywords: Digital Law; Brazilian Civil Rights Internet Framework; Information Security.

LISTA DE ABREVIATURAS E SIGLAS

CERT’BR - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

CGI - Comitê Gestor da Internet no Brasil

CNB - Congresso Nacional Brasileiro

CGI - Comitê Gestor da Internet no Brasil

CNJ - Conselho Nacional de Justiça

EAD - Educação a Distância

ECA - Estatuto da Criança e do Adolescentes

EUA - Estados Unidos da América

IEC - International Organization for Standardization

ISO - Organização Internacional de Normalização

M2M - Máquina entre Máquina

MEC - Ministério da Educação

NIST - Instituto Nacional de Padrões e Tecnologia

ONU - Organização das Nações Unidas

SAJ - Sistema de Automação da Justiça

SPS - Sistemas de Pagamento Seguro

WEF - World Economy Forum

SUMÁRIO

INTRODUÇÃO

O Direito Digital nasce em decorrência das reações entre a ciência do Direito com a Ciência da computação. Neste trabalho, abordaremos o conjunto de regras, formas de aplicações, dados e das relações jurídicas, advindas do mundo digital. Como o efeito da relação entre o direito e a segurança, as informações oriundas no mundo digital passam a exigir a necessidade de se criar o Direito Digital. Há que se aprimorar as práticas legais do conhecimento jurídico conforme as necessidades cada vez mais latentes, como os contratos digitais, certificados, E-commerce etc. Também se percebe que é crescente necessidade de os Operadores do Direito quanto a instrumentos computacionais para racionalizar e aprimorar seus afazeres. Entretanto, há também os pontos negativos. Além das facilidades e regalias, sabemos que tais tecnologias trouxeram um aumento significativo na incidência de crimes cibernéticos, tais como Sniffing, taques de ransomware, espionagem cibernética, esses são alguns exemplos dentro de uma infinidade de possibilidades.

Este estudo tem como objetivo apresentar uma análise da importância do relacionamento do ramo da ciência jurídica, por intermédio do Direito Digital, com o ramo da ciência computacional por meio da Segurança da Informação. Buscando analisar as necessidades sociais e comerciais advindas dessas novas tecnologias do mundo digital, percebe-se o acesso a diferentes métodos de troca de informações de forma tão rápida, fácil e com tamanha grande propagação, que isso acaba trazendo inúmeras responsabilidades. É também sabido que tais ferramentas têm um grande poder para uma infinidade de objetivos, tanto para o bem quanto para o mal. Procuraremos, ainda, apontar alguns dos desafios enfrentados tanto pelo Direito Digital, quanto pela Segurança da Informação diante das necessidades sociais e empresariais.

1. CAPÍTULO – DIREITO DIGITAL

1.1 DO DESENVOLVIMENTO DO DIREITO DIGITAL

Comecemos pela leitura deste fragmento de Patrícia Peck (2016),

> Há pouco mais de quarenta anos, a Internet não passava de um projeto, o termo "globalização" não havia sido cunhado e a transmissão de dados por fibra ótica não existia. Informação era um item caro, pouco acessível e centralizado. O cotidiano do mundo jurídico resumia-se a papéis, burocracia e prazos. Com as mudanças ocorridas desde então, ingressamos na era do tempo real, do deslocamento virtual dos negócios, da quebra de paradigmas. Essa nova era traz transformações em vários segmentos da sociedade — não apenas transformações tecnológicas, mas mudanças de conceitos, métodos de trabalho e estruturas. O Direito também é influenciado por essa nova realidade. A dinâmica da era da informação exige uma mudança mais profunda na própria forma como o Direito é exercido e pensado em sua prática cotidiana.

Inicialmente é importante entendermos que vivemos um momento especial, pois, o profissional de seja qual for sua área de atuação, mas eu diria que principalmente o do Direito, necessariamente precisa se manter atualizado e acompanhando todas as transformações que ocorrem com o desenvolvimento da sociedade. Podemos afirmar sem sombra de dúvidas que a internet tem uma grande responsabilidade por esse momento único de grandes mudanças no aspecto tecnológicos, econômicos e sociais que vivemos.

O Direito Digital consiste na evolução do próprio Direito, abrangendo todos os princípios fundamentais e institutos que estão vigentes e são aplicados até hoje, assim como introduzindo novos institutos e elementos para o pensamento jurídico, em todas as suas áreas (Direito Civil, Direito Autoral, Direito Comercial, Direito Contratual, Direito Econômico, Direito Financeiro, Direito Tributário, Direito Penal, Direito Internacional etc.).

É importante termos em mente que os novos profissionais de Direito são os responsáveis por garantir o direito à privacidade, em especial o que tratado pela segurança da informação, pois ele diz respeito não somente ao direito fundamental da privacidade, mais de todos os direitos inerentes a pessoa humana que são extremamente vulneráveis quando se está tratando do mundo digital, são alguns, a proteção dos direito autoral, do direito de imagem, da propriedade intelectual, dos royalties e é de

conhecimento popular o tamanho dos problemas causados pelos hackers e suas repercussões jurídicas, esses são alguns pontos de uma infinidade, pois quando se trata do mundo digital a quantidade de possibilidades e de pessoas que são afetadas são vertiginosamente maior. Para isso, precisamos entender e estudarmos modos e criar instrumentos capazes de atender as necessidades do Direito Digital.

Segundo Patrícia Peck (2016):

> "A Internet é mais que um simples meio de comunicação eletrônica, formada não apenas por uma rede mundial de computadores, mas, principalmente, por uma rede mundial de Indivíduos. Indivíduos com letra maiúscula, porque estão inseridos em um conceito mais amplo, que abrange uma individualização não só de pessoas físicas como também de empresas, instituições e governos. A Internet elimina definitivamente o conceito de corporação unidimensional, impessoal e massificada. Isso significa profunda mudança na forma como o Direito deve encarar as relações entre esses Indivíduos."

Diante disto, entendemos a importância de refletirmos sobre o desenvolvimento do Direito para saciar as necessidades sociais de nossa pátria no que diz respeito ao tão novo, grande e crescente âmbito digital. Durante a abordagem desse capítulo, teremos como objetivo entender a origem e a necessidade do desenvolvimento do Direito Digital, vendo soluções para atender lacunas em nosso ordenamento jurídico no que diz respeito ao tema.

1.2 EVOLUÇÃO DO DIREITO DIGITAL

Ao se falar do tema Direito Digital no Brasil, deve-se ter em mente que se trata de uma fase inicial e precária se comparada ao nível mundial, visto que em nosso país muito já foi transferido para o meio digital, contudo ainda não temos uma base sólida para tratar do assunto, Segundo Jurista e coordenador de pesquisas do Instituto de Investigaciones Jurídicas Facultad de Derecho y Ciencias Sociales, Universidad Autónoma de Nuevo León Ricardo Cantú Aguillén estes são os graus percorridos pela evolução do Direito Digital (tradução nossa):

1. Tendência inicial ou básica: 1) Pouco avanço e desenvolvimento da computação

jurídico e informático, devido à pouca importância dada ao assunto por professores de Direito de Universidades e por funcionários públicos. 2) Passa a promover a inclusão da disciplina de informação jurídica nos planos de estudos das faculdades de direito, desenvolvimento inicial da doutrina nacional.

2. Tendência crescente ou progressiva: 1) Distinção clara entre computação

direito jurídico e informático (ramos afins, mas totalmente independentes um do outro); a doutrina nacional a esse respeito está começando a se desenvolver firmemente. 2) Direito da Informática como ramo autónomo do Direito (incluído nos planos de estudos das principais Faculdades de Direito do país), separadamente da disciplina de Informação Jurídica; na Europa, recomenda-se reunir as duas disciplinas sob o conceito de “informática e direito”, em virtude de considerar esta definição mais completa.

3. Tendência avançada ou próspera: 1) Destaca a necessidade e a importância de

desenvolver trabalhos legislativos relativos ao direito informático, normas específicas que regulam a sua aplicação; aumento significativo em relação à doutrina e jurisprudência a este respeito (por exemplo, crimes informáticos não tipificados nos códigos penais, etc.). 2) Desenvolvimento e importante consolidação da legislação nacional, doutrina e jurisprudência do direito informático; polêmica de casos práticos nacionais e internacionais no Supremo Tribunal Federal do país.

4. Tendência culminante ou inovadora: 1) Avanços importantes em termos de

desenvolvimento de meta-documentário ou informática jurídica de tomada de decisão; surgimento de centros de pesquisa para a utilização de sistemas especialistas ou inteligência artificial aplicada ao direito; 2) Desenvolvimento de projetos práticos e específicos para o uso de inteligência artificial aplicada ao direito.

Inicialmente devemos levar em consideração a rapidez da evolução do mundo digital, em outros termos, 5 anos quando se trata da seara jurídica é algo extremamente prematuro e inicial, entretanto, quando nós falamos de 5 anos a respeito do mundo digital, é uma mudança e aprimoramento infinitamente maior e vertiginoso. Diante destes fatos, é notório a necessidade de analisar e percebermos que existe a obrigação, tanto dos profissionais do mundo digital, quanto os do mundo do Direito, objetivando preencher evidentes lacunas existentes em nosso ordenamento jurídico a respeito desse assunto e conseguirmos sanar as necessidades jurídicas de forma plena e especifica a cerca deste assunto.

O Direito Digital nasce das relações sociais adversas dentro e fora no meio digital, devido essas mudanças extremamente rápidas em pouco tempo, criam a necessidade de se construir uma área do direito buscando a maior celeridade normativa para atender

as necessidades no que diz respeito a nossa sociedade cada vez mais digital e informatizada.

De acordo com o professor Ricardo Luís Lorenzetti:

> “O surgimento da era digital tem suscitado a necessidade de repensar importantes aspectos relativos à organização social, à democracia, à tecnologia, à privacidade, à liberdade e observa-se que muitos enfoques não apresentam a sofisticação teórica que semelhantes problemas requerem; esterilizam-se obnubilados pela retórica, pela ideologia e pela ingenuidade”.

Neste mesmo sentido Patrícia Peck nos mostrar uma nova visão sobre o papel do profissional do Direito na sociedade digital, onde ele deve deixar de ser um burocrata para se tornar um estrategista. Acredito que a discussão sobre a autonomia do Direito Digital é de relevante valor para nosso ordenamento jurídico e para a segurança jurídica, pois assim teremos normas para fazer frente as inovações advindas a todo momento do mundo digital de diversas formas de contratos e em consequência dos inúmeros atos lesivos oriundos dela, tendo assim uma correta base para aplicação de uma disciplina reguladora.

Assim como é defendido por Maria Fernanda Paci:

> “A informática jurídica ou direito eletrônico é a ciência que estuda a utilização dos elementos físicos eletrônicos, como o computador, no Direito; isto é, a ajuda que este uso presta ao desenvolvimento e aplicação do direito. Em outras palavras, é o instrumental necessário a utilização da informática no Direito. O Direito Eletrônico, digital ou da Informática não se dedica apenas ao estudo do uso dos aparatos da informática como meio auxiliar ao direito, delimitado pela informática jurídica, mas, ao contrário, constitui o conjunto de normas, aplicações, processos, relações jurídicas que surgem como consequência da aplicação e desenvolvimento da informática, isto é, a informática é geral deste ponto de vista e da forma como é regulado pelo direito.
> Portanto entendemos o Direito Eletrônico como, o ramo autônomo atípico da ciência jurídica que congrega as mais variadas normas e instituições jurídicas que almejam regulamentar as relações jurídicas estabelecidas no ambiente virtual.”

1.3 DIREITO DIGITAL X OUTROS RAMOS DO DIREITO

Devido ao fato de o Direito Digital tratar de relações jurídicas de todos os tipos em um ambiente com inúmeros contextos diferentes, entende-se que o Direito Digital é multidisciplinar, quer dizer, sua atuação e influencia é percebida quase que em todos os ramo existentes no meio jurídico, dos quais são refletidos no meio virtual. A respeito do

assunto, o ilustre Alexandre Atheniense (2015, p. 1) leciona sobre os distintos ramos jurídicos que se correlacionam com o Direito Digital:

> O material e o Processual Civil (assinatura digital, responsabilidade civil, invasão da privacidade e destruição de propriedade virtual ou informatizada; provas ilícitas; direitos autorais sobre software e hardware; atividades irregulares no processo; composição judicial por meios eletrônicos), Penal (diferenciação dos crimes de informática puros e impuros; valoração e pena; discussão acerca da tipicidade ou inaplicabilidade de dispositivos velhos em atividades realizadas através de aparelhagem eletrônica), Tributário (tributação de atividades econômicas realizadas no mundo virtual, distinção das atividades, aplicação ou não de certas normas tributárias; incidência tributária territorial; regulamentação e legitimação da informática como uma forma de pagamento, declaração de imposto) e até Trabalhista (nos casos de trabalho realizado à distância através de instrumentos informatizados).

Ainda acerca do assunto, vemos o Direito Digital se comunicando com o Direito Civil no que diz respeito a danos morais por difamação, no Direito Constitucional no que diz respeito a invasão de privacidade por exemplo de documentos pessoais, no tocante ao Código de Defesa do consumidor, podemos falar sobre a manipulação das informações usando os bancos de dados angariadas do consumidor, é notório a ramificação do Direito Digital intrínseca entre grandes outras áreas de nosso ordenamento jurídico. Podemos dizer que o mundo digital trouxe grandes avanços como por exemplo contratos de compra e venda, comodato, empréstimos e inúmeras cláusulas novas, tudo isso mesmo fazendo parte de grandes áreas de nosso ordenamento jurídico precisa ser comtemplado pelo Direito Digital como uma área especializada para tratar dos assuntos do mundo digital.

Em consonância com esse pensamento, Marcelo de Camilo Paiva (2009, p. 26) disciplina:

A. Direitos Humanos – utilização da informática na agilização de processos de milhares de detentos no país, permitindo, assim, julgamentos mais céleres, progressões de regimes automáticas, dentre outras medidas que diminuiriam consideravelmente as injustiças que o Estado tem perpetrado contra vários apenados, os quais, muitas vezes, já cumpriram suas penas, embora continuem no cárcere à espera de uma solução jurisdicional;
B. Propriedade Intelectual - a inter-relação entre o Direito Digital e a propriedade intelectual é primordial e enseja uma série de preocupações por parte dos

estudiosos, advindas de implicações jurídicas provenientes da facilidade de reprodução e utilização da propriedade intelectual, que pode ser violada com um simples toque de comando por intermédio de um computador; a tecnologia digital permite cópias perfeitas, enquanto que a Internet sem fronteiras propicia rápida disseminação das cópias, sem custo de distribuição;

C. Direito Civil – dessa relação tem-se inúmeros pontos de convergência materializados pelo direito contratual e das obrigações; o fenômeno da internet é um movimento social que necessita do amparo jurídico e legal para fins de pacificação dos possíveis conflitos oriundos dos choques de interesses dali decorrentes, dentre os quais, os relativos à contratação por meio eletrônico; outra questão é quanto a jurisdição ou Tribunal competente para se julgar o caso, já que na rede mundial de computadores a existência de espaços virtuais dificulta, senão inviabiliza, a individualização do lugar onde se deu o evento danoso;
D. Direito Comercial - as relações comerciais vêm sofrendo uma série de modificações que tem fundamental importância para a própria sobrevivência ou não da empresa no mercado, o que enseja uma série de problemas jurídicos que necessitam ser dirimidos pelo Direito Comercial, que, no entanto, não está apto a fornecer soluções eficazes para os problemas surgidos; daí a necessidade da correlação entre os dois direitos para fomentar o comércio eletrônico, através da criação de normas reguladoras e de definições legais a respeito do tema, posto que inexistam hoje em termos legislativos no Brasil;
E. Direito Tributário - as atividades realizadas virtualmente têm gerado discussões polêmicas, sendo que as principais giram em torno do comércio eletrônico, mais especificamente sobre se a tributação incide ou não sobre esse tipo de transação e, caso incida, como tributá-la; atualmente os sites não podem ser qualificados como estabelecimentos virtuais, devendo ser considerados meras extensões dos estabelecimentos físicos, por não haver legislação que regule as peculiaridades dos mesmos;
F. Direito do Consumidor – a proteção aos direitos do consumidor deve ser estendida às relações de consumo estabelecidas via internet, o que denota maior evidência e importância para o entrelaçamento entre as duas matérias que devem caminhar juntas, para que a referida relação permaneça pautada pelos princípios do Direito;

G. Direito Eleitoral – com a modernização do processo eleitoral em todo o país os eleitores passaram a exercer seu direito de voto utilizando a evolução tecnológica evidenciada pela urna eletrônica; eleição totalmente informatizada, do início ao fim, do registro do eleitor à totalização dos votos, passando pelo ato de votar; entretanto, essas inovações implicam em questões jurídicas que, por intermédio do Direito Eleitoral, terão que ser adequadas e estudadas com a devida vinculação aos princípios e normas pertinentes do Direito Digital.

Devido ao tamanho dessa interação, é importante dizer que o exposto acima é apenas algumas das áreas jurídicas do qual o Direito Digital se faz presente, havendo muitas outras questões e princípios a serem analisados que tanta importância quanto estas, o que torna nítido o avanço do Direito Digital a cada dia, se interrelacionado com todos os Direitos fixados como fundamentais em nossa Carta Magna e em grande parte de todo o nosso ordenamento jurídico vigente.

1.3 INFORMÁTICA JURÍDICA

São irrefutáveis as grandes mudanças proporcionadas pelo avança da tecnologia da informação no âmbito jurídico. Foram criadas inúmeros Softwares que melhoraram e mudaram muito a vida dos profissionais do Direito, tudo graças as inovações advindas dos computadores e da Internet.

Sobre essas mudanças, o diretor executivo da Softplan, sendo essa a empresa responsável pelo PJE (Processo Judicial eletrônico), da qual é a versão chancelada pelo CNJ (Conselho Nacional de Justiça), com vistas a unificar o ecossistema de processos eletrônicos brasileiros em todas as instâncias do Judiciário. Ilson Stabile, afirma:

> As mudanças atuais são consequência de uma revolução que começou mais ou menos 15 anos atrás. Muita gente vivenciou e ainda lembra do cenário: pilhas de papel, estantes atulhadas de arquivos, dificuldade de comunicação, pouca informação, excesso de burocracia, morosidade. Era a regra não só dentro dos Tribunais, mas em praticamente todas as instituições da Justiça.
>
> A transformação digital não foi apenas a substituição do papel pelo computador. Fosse apenas isso, já representaria uma grande revolução. Com o processo digital,

> a Justiça conseguiu ir além: mudou a mentalidade, e inventou novas formas de trabalhar. Colheu resultados.

A aplicação da informática no meio jurídico se provou de extrema importância, com base nos informativos da Softplan em 2019, os Tribunais de Justiça que adotaram o SAJ(Sistema de Automação da Justiça) economizaram R$ 75 milhões de reais durante 1 ano, somente em relação ao fato de não precisarem confeccionar o processo físico. Apuraram também que economizaram mais de 8 milhões de horas de trabalho ao ano, depois que as distribuições, juntadas e publicações foram automatizadas. Afirmam também que o processo digital conseguiu reduzir o prazo médio de 46 dias para 9 no tempo entre o ajuizamento da ação e o primeiro ato do juiz.

Podemos concluir que a informatização do judiciário trouxe redução a burocracia e morosidade, economia de gastos e sustentabilidade, assim proporcionando um salto na produtividade extremamente positiva, tudo graças a tecnologia.

Neste sentido na época como presidente do Tribunal de Justiça de São Paulo, Jose Renato Nalini, afirmou:

> “A informatização completa do Judiciário estadual é uma medida sem precedentes em todo o mundo e foi tomada porque a obsolescência está correndo atrás de nós, nos mordendo os calcanhares”.
>
> “O processo digital elimina até 70% do tempo hoje empregado para trâmite do processo físico, em papel. Elimina-se autuação, juntada de documentos, transporte dos autos e anotações”
>
> “Há um ganho de 47% na taxa de vazão dos processos, os novos processos têm sua celeridade aumentada em 87%, além do crescimento na produtividade dos magistrados, que chega a 50%”.

1.5 O PROCESSO JUDICIAL ELETRÔNICO

O termo “processo judicial eletrônico” pode ser entendido como, o resultado da informatização do processo judicial físico objetivando uma maior celeridade processual, econômica de recursos e sustentabilidade.

Assim como Aires José Rover melhor conceitua:

> “É o resultado da informatização de um conjunto mínimo e significativo de ações e, por consequência, de documentos organizados e ordenados em uma sequência definida de fluxos de trabalho representando fases processuais, atendendo a

> requisitos de autenticidade, temporalidade e integralidade, eliminando o uso do papel”

Já Pereira define como sendo “É o processo controlado por um sistema de informação, um software especializado, que incorpora saberes da ciência jurídico processual e de diferentes ciências da complexidade: teoria dos sistemas, cibernética, teoria da informação, entre outras”.

O processo judicial eletrônico é um instrumento judicial para sanar os conflitos sociais e buscar a justiça, assim como os processos físicos de antigamente, entretanto da mesma forma, porém, com todos os benefícios provenientes da evolução da tecnologia.

Em minha visão o processo judicial eletrônico é a chave mestra para a informatização da justiça, é a possibilidade de se criar um conjunto de ações ou métodos de controle processual que permita o avanço dessa área para atender à crescente demanda do judiciário Brasileiro, sendo um método revolucionário construído por meio de instruções lógicas. Vale dizer que o método é para aumentar a produtividade do serventuário, otimizando assim suas horas a disposição e não automatizar e gerar desemprego.

CAPÍTULO II – MARCO CIVIL DA INTERNET DO BRASIL

2.1 DO MARCO CIVIL

A Lei do Marco Civil da internet ou Lei Azeredo, trata das inovações que ocorreram no mundo digital, no Direito Digital e principalmente os efeitos na sociedade, tratou também dos efeitos e impactos gerados pela globalização do mercado, tanto nacional quanto internacional.

Seguindo essa mesma linha de pensamento PECK:

> Recentemente em nosso Ordenamento Jurídico uma nova lei, chamada de Marco Civil da Internet, que inaugura uma tendencial mundial de não apenas atualizar as leis existentes sobre as novas questões trazidas pelos avanços tecnológicos e seus impactos nas relações humanas, mas também criar um arcabouço legal de abrangência mais internacional, para que as regras sejam de fato eficazes. E esta nova dimensão do próprio Direito Digital, que está sendo construído em leis nacionais, mas também por meio de Acordos, Convenções e Tratados Internacionais, denomina-se Digital Rights. Ou seja, quais valores todos os ordenamentos jurídicos deveriam resguardar para garantir a proteção do indivíduo nesta Sociedade Digital.

O Marco Civil da internet, introduzido pela Lei nº 12.965/2014, foi idealizada de forma atípica, devido a forma em que foi dada sua criação e discussão, teve uma grande participação da sociedade, por meio de fóruns de discussão pela internet e cessões públicas promovido pelo CNB (Congresso Nacional Brasileiro).

2.2 RESPONSABILIDADE CIVIL PELOS ATOS NO MUNDO DIGITAL

Haikal (2016), o uso da Internet criou um ambiente que resultou no aumento de conflitos, uma vez que os sites são responsáveis pelos comentários publicados pelos seus leitores. No entanto, deve-se saber de antemão como proceder a retirada de conteúdos disponibilizados no ambiente virtual, especialmente, quando for ofensivo.

Um dos temas abordados pela Marco Civil da internet e que gerou muitos debates, foi a responsabilidade civil, por divulgar conteúdos na internet, pois, a lei dispõe de

diversas obrigações aos responsáveis de sites, dentre eles, remover conteúdos denunciado, traz também o dever de indenizar as pessoas vítimas de danos em decorrência de suas divulgações e deverá proteger e guardar os registros das atividades de sua propriedade no mundo digital.

O armazenamento de registros, sendo o nome técnico “logs”, causaram grandes discussões, devido ao fato de a possibilidade das provedoras de internet terem acesso a todo o histórico de navegação dos usuários, e guardarem essas informações de forma interna e sem possibilidade da fiscalização de terceiros.

E caso aconteça qualquer tipo de violação a essas informações sensíveis e sigilosas, não seria possível ter certeza de fato da veracidade das informações fornecidas quando necessárias para o poder judiciário, comprometendo assim a veracidade dos crimes cometidos no mundo digital, tendo assim o direito de defesa prejudicado aqueles que sofreram abuso. Gerando assim, insegurança jurídica e dando uma brecha para possíveis atentados contra a imagem ou reputação de outrem.

2.2.1 RESPONSABILIDADE CIVIL DOS PAIS E RESPONSÁVEIS

A pouco tempo, um adolescente de 16 anos foi detido pela polícia nos EUA após se valer de métodos tecnológicos para alterar suas notas de seu sistema escolar.

Em 2010, também nos EUA, um jornal de respeito publicou uma notícia de uma criança de apenas 9 anos de idade que havia invadiu o sistema escolar de sua escola e alterou as senhas de professores e funcionários. Além de modificar e excluir o conteúdo de classes e atividades virtuais.

Estes casos são importantes para ilustrar a impotência que tem a orientação e na educação das crianças e adolescentes no uso correto e consciente dessas novas tecnologias, dando importância nas implicações legais de suas ações na internet.

Com uma população superior aos 7 bilhões de pessoas no mundo, de acordo com relatórios das Nações Unidas (ONU). É evidente o crescimento vertiginoso dos recursos oriundos do mundo digital pela sociedade, exigindo assim uma transformação na forma de como ver a importância da tecnologia e suas implicações na sociedade.

Nos tempos em que vivemos em nosso mundo cada dia mais tecnológico e conectado, não basta mais ensinarmos aos mais jovens apenas as matérias básicas

fundamentais como física, química ou matemática. É de suma importância também educar esses novos cidadãos do uso das novas tecnologias e como as usar de forma consciente no mundo digital, visto que cada vez mais o mundo está conectado em decorrência da acessibilidade de instrumentos tecnológicos como smartphones, notebooks e tablets.

Contudo, devemos nos lembrar que o dever de educar é da família, escola e da própria sociedade, assim como foi determinado pela Constituição federal em seu artigo 205:

> Art. 205. A educação, direito de todos e dever do Estado e da família, será promovida e incentivada com a colaboração da sociedade, visando ao pleno desenvolvimento da pessoa, seu preparo para o exercício da cidadania e sua qualificação para o trabalho.

E no mesmo sentido pelos artigos 4º e 5º do Estatuto da criança e do adolescente (ECA):

> Art. 4º É dever da família, da comunidade, da sociedade em geral e do poder público assegurar, com absoluta prioridade, a efetivação dos direitos referentes à vida, à saúde, à alimentação, à educação, ao esporte, ao lazer, à profissionalização, à cultura, à dignidade, ao respeito, à liberdade e à convivência familiar e comunitária.
> Art. 5º Nenhuma criança ou adolescente será objeto de qualquer forma de negligência, discriminação, exploração, violência, crueldade e opressão, punido na forma da lei qualquer atentado, por ação ou omissão, aos seus direitos fundamentais.

Endossado pelo Código Civil em seu artigo 1634 I:

> Art. 1.634. Compete a ambos os pais, qualquer que seja a sua situação conjugal, o pleno exercício do poder familiar, que consiste em, quanto aos filhos:
> I - dirigir-lhes a criação e a educação;

Embora as instituições de ensino devam cumprir essa importante missão de ensinar como se comportar e usar de forma consciente o mundo digital e suas tecnologias, os pais e responsáveis não podem simplesmente se abster e querer que as instituições de ensino faça tudo isso sozinhas, é essencial a participação e o esforço de ambos para atingir esse objetivo.

É sabido que muitos dos pais ou responsáveis não estavam ou não estão preparados para aprender sobre o mundo digital, devido ao fato de terem crescidos em um momento em que sequer imaginavam as possibilidades tecnologias atuais. Essas

pessoas são denominadas de imigrantes digitais, termo criado para identificar e ajudar na inclusão digital.

Já essa nova geração da qual já nascem e crescem nos dias atuais com acesso às novas tecnologias digitais e acesso ao mundo digital são denominados nativos digitais.

É possível notar que devido a esse acesso a essas tecnologias serem introduzida bem cedo em suas vidas, elas aprendem a usa-las muito naturalmente, porém, existe o problema na falta de discernimento do que pode ou não ser feito e a falta de conhecimento das condições de seus atos realizados no mundo digital.

Não raras as vezes que nos deparamos com esses jovens sendo vítimas e expostas a conteúdos que são prejudiciais a ales, como conteúdos com cunho violento, ódio, pornografia, ódio, nudez, pedofilia e inúmeros jogos e brincadeiras extremamente perigosas, como por exemplo o recente desafio da Baleia Azul e muitos outros que atingem diretamente a integridade física dessas crianças e adolescentes.

Mas também, essas crianças e adolescentes também fazem o papel de agressores, como disseminar ódio e compartilhar conteúdos criminosos, cyberbullying e infinitos atos ilegais possíveis de serem praticados no mundo digital.

Em nosso País, devido ao estatuto da Criança e do Adolescentes (ECA), é possível esses menores responderem por suas práticas delitivas por meio das medidas socioeducativas, previstas no artigo 112 deste Estatuto.:

> Art. 112. Verificada a prática de ato infracional, a autoridade competente poderá aplicar ao adolescente as seguintes medidas:
> I - advertência;
> II - obrigação de reparar o dano;
> III - prestação de serviços à comunidade;
> IV - liberdade assistida;
> V - inserção em regime de semi-liberdade;
> VI - internação em estabelecimento educacional; VII - qualquer uma das previstas no art. 101, I a VI.
> § 1º A medida aplicada ao adolescente levará em conta a sua capacidade de cumpri-la, as circunstâncias e a gravidade da infração.
> § 2º Em hipótese alguma e sob pretexto algum, será admitida a prestação de trabalho forçado.
> § 3º Os adolescentes portadores de doença ou deficiência mental receberão tratamento individual e especializado, em local adequado às suas condições.

Ainda assim, os pais ou responsáveis podem se responsabilizar por todo o dano causado pelo menor a sua tutela, assim como é previsto pelo artigo 932 do Código Civil I:

> Art. 932. São também responsáveis pela reparação civil:
> I - os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;

O Marco Civil da Internet do Brasil também trouxe determinações legais sobre o assunto, garantindo assim meios para identificar aqueles que cometeram atos ilegais no mundo digital, mesmo que cometidos de forma anônima, e discute também acerca do exercício do controle parental, que discorre sobre o uso dos recursos tecnologias pelos seus menores tutelados, determinando assim a supervisão dos responsáveis no que os menores estão fazendo no mundo digital.

Assim como podemos ver no artigo 29 da Lei nº 12.965 de 23 de abril de 2014 (Marco Civil da Internet do Brasil):

> Art. 29. O usuário terá a opção de livre escolha na utilização de programa de computador em seu terminal para exercício do controle parental de conteúdo entendido por ele como impróprio a seus filhos menores, desde que respeitados os princípios desta Lei e da Lei no 8.069, de 13 de julho de 1990 - Estatuto da Criança e do Adolescente.

Apesar dos riscos na utilização da Internet, é quase impossível e até mesmo inviável afastar-se da tecnologia, que inclusive pode ser uma grande aliada dos pais na difícil tarefa de educar.

Logo, se faz importante a monitoração dos menores tutelados pelos pais e responsáveis, nas atividades praticadas no mundo digital, visando assim a segurança dos mesmo e a prevenção de eventuais responsabilidades civis em decorrência de atos ilícitos praticados no mundo digital.

Portanto, o futuro da sociedade digital dependerá dos princípios e valores educacionais ensinados para os jovens de hoje, garantindo-se cada vez mais o uso seguro, consciente e responsável da Internet.

2.3 DA NEUTRALIDADE NO MUNDO DIGITAL

Trata-se de um assunto amplamente discutido em todo o globo, principalmente nos Estados Unidos (EUA) e na Europa. Nos EUA o foco acerca do assunto é em torno da conexão de banda larga oferecida pelo próprio País aos seus cidadãos, porem essa internet oferecida é controlada e monitorada pelo mesmo, em busca de conteúdo não

autorizado, monitoramento para possíveis ligações com grupos envolvidos em atividades criminosas e terroristas ou até mesmo acesso a tão famigerada Deep Web.

Já na Europa é bem similar ao tratado em nosso País, sendo referente a grande quantidade de dados usados nos serviços de mensagens instantâneas e streaming.

A neutralidade no mundo digital requer muita discussão, pois, envolve um assunto muito importante, o acesso sem limites a informações disponíveis no mundo digital. Sabemos que essa comunicação e esse banco de informação são muito poderosos, podemos citar aqui o caso das eleições do Irã em 2009, primavera árabe em 2010 e os protestos brasileiros em 2013 e mais recente o escândalo da Cambridge Analytica e as manipulações da eleição da qual Donald Trump venceu em 2016. Esse escândalo em particular é o melhor exemplo para entendermos o poder e a importância da neutralidade no mundo digital. Em síntese trata do fato da empresa Cambridge Analytica fomentada por Donald Trump, ter supostamente usado informação de forma indevida cerca de 87 milhões de perfis no Face Book para fazer marketing eleitoral para Donald Trump durante as eleições passadas.

2.4 EDUCAÇÃO, ÉTICA E SEGURANÇA NO MUNDO DIGITAL

Recentemente, principalmente na última década, podemos perceber uma grande evolução no que diz respeito às instituições de ensino como um todo, tanto nas salas de aulas, quanto na organização nas instituições. O mundo digital dado pela conexão com a Internet, junto a inúmeras ferramentas tecnológicas voltadas para a educação, proporcionou grandes mudanças. Também é importante entendermos que, grande parte desse desenvolvimento do ensino está acontecendo dentro de nossas próprias casas.

É possível afirmar que o uso dessas tecnologias são uma boa opção para educação, porém, necessitam de acompanhamento.

A base da educação no mundo digital deveria vir de dentro dos lares, no ambiente familiar, pois é notório a dificuldade do controle de acesso a certos conhecimentos e tecnologias pelas instituições de ensino, porém, muitas das vezes, nem os pais e responsáveis conseguem fazer esse papel. É vertiginoso o crescimento da educação a distância (EAD), pois, o número de vagas ofertadas no ensino superior à distância no Brasil em 2018 superou as do ensino superior presencial pela primeira vez na história. É

o que mostram os dados do Censo de Educação Superior 2018, divulgados hoje pelo MEC (Ministério da Educação).

É de grande importância o estudante ser orientado de como se desenvolver com respeito e discernimento, para poder usufruindo da liberdade que tem em estudar a distância, devendo manter-se responsável com seus deveres e com o professor. Evitando os possíveis as possíveis formas de se prejudicar e prejudicar os outros em decorrência dessa liberdade proporcionada pelo mundo digital.

Segundo Pinheiro (2016):

> Não somente a Instituição de Ensino, mas também os pais, têm o solene dever de educar e corrigir seu filho-aluno (crianças e jovens) acerca do uso seguro, sustentável, ético e legal de ferramentas tecnológicas, no lar, em sala de aula ou no ambiente social, para que deem destinação adequada ao uso e fruição de seus aparelhos tecnológicos ou da escola, bem como o acesso coerente à Internet.

O que se como objetivo aqui, é buscar entender uma forma de se educar e preparar a pessoa para o mundo digital, para crescimento da sociedade, buscando entender os limites éticos e morais do uso dessas novas tecnologias, desenvolvendo formas para que todos entendam e tenha consciência ao se valerem das inovações dessa era digital.

Uma forma de grande importância para prevenir e educar sobre esses possíveis incidentes em ambientes educacionais é criar uma espécie de senso coletivo, moral e ético nas atividades digitais.

É sabido que no momento em que vivemos, as leis não atendem todas as exigências do mundo digital, e acaba sendo necessário intervenção do Poder Judiciário em dadas situações. Portanto, é especialmente importante que as instituições de ensino, criem metodologias para conscientizar a essas pessoas para que usem essas novas tecnologias de forma consciente.

2.5 A UTULIZAÇÃO DA TECNOLOGIA NA EDUCAÇÃO

As inovações tecnológicas revolucionaram a forma em que as pessoas se relacionam, sendo que, qualquer pessoa que tiver acesso a essas tecnologias tem a possibilidade de se comunicar em tempo real com pessoas qualquer pessoa do mundo,

não importando distância, poder aquisitivo ou lugar e hora determinado. Porém, com toda essa liberdade e possibilidades, também vem aspectos negativos, a velha história de que liberdade não é libertinagem, podendo ser caracterizadas desde ofensas simples como injúria, difamação e plágio a crimes graves como apologia ao crime e furto de dados.

(PINHEIRO, 2016)

Segundo Pinheiro e Haikal (2016):

> “jovens nascidos e criados com o rigor de aparatos tecnológicos, impulsionados pela insegurança que existe no mundo real, passam a viver uma vida mais virtual que real, inspirados em eventos visualizados na Internet, com amigos e interações fundamentadas nas redes sociais, devendo ser monitorados e cuidados por seus pais e responsáveis.”

É muito importante essas pessoas serem orientadas, pois, muita das vezes eles não serão apenas as vítimas e sim os infratores, sempre reforçando a ideia de que as instituições de ensino e os pais ou responsáveis devem serrem mais presentes e interativos, buscando ensinar essa nova linguagem do mundo digital, demonstrando que existem regras e limites para o uso dessas tecnologias.

Podemos dizer que os problemas que acontecem no mundo real são muito semelhantes ao que acontecem no mundo digital, tais problemas como assédio, furto, acesso a conteúdo inapropriado, exposição de intimidade indevida etc. Temos que ter em mente que ao termos equipamentos tecnológicos como Smartfones, temos acesso uma câmera de forma muito fácil, logo, é importante saber dos riscos de se obter e divulgar determinados tipos de imagens, sabendo as possíveis repercussões que a o uso indevido disso pode causar, ainda mais quando se fala em divulgação de forma pública no mundo digital.

Um caso emblemático ocorrido no início de 2012 ocorrido com a atriz Brasileiro Carolina Dieckmann, do qual foram publicadas fotos pessoais da atriz sem autorização da mesma, a repercussão foi tamanha que foi aprovada no ano seguinte a lei 12.737/2012, também chamado extra oficialmente de Lei Carolina Dieckmann que alterou o Código Penal para tipificar como infrações uma série de condutas no ambiente digital, principalmente em relação à invasão de computadores, além de estabelecer punições específicas.

Como o esperado, o crescimento vertiginoso do acesso e uso dessas novas tecnologias, trouxeram o aumento dos incidentes em decorrência do mal uso destas,

principalmente devido ao fato da falta de educação das pessoas sobre o mundo digital, o fato de se sentir intocável ou até mesmo anônimo, acaba aumentando a propensão em cometer esses atos ilícitos.

Para contornar tudo isso é importante se investir não somente em infraestrutura e novas tecnologias, mas também em educação, para se construir um ambiente próprio e segura para usufruir das infinitas possibilidades que o mundo digital nos disponibiliza, sendo assim possível criar regras e leis para fixar a importância da ética no mundo digital e buscarmos a liberdade de expressão com responsabilidade.

CAPÍTULO III – SEGURANÇA DA INFORMAÇÃO

3.1 DA IMPORTÂNCIA DA SEGURANÇA DA INFORMAÇÃO.

A questão da segurança é um dos principais temas a serem discutidos e resolvidos não apenas no Direito Digital, mas na sociedade como um todo, uma vez que é uma das barreiras para o maior aproveitamento das novas tecnologias e um limitador para a exploração de seu potencial comercial. A necessidade de segurança nas expectativas da sociedade foi um dos fatores que motivaram a criação do próprio Direito como fenômeno de controle das condutas, e do estado como ente autorizado a praticar o controle dentro de limites permitidos pela própria sociedade por meio das leis, o chamado Estado de Direito. Por isso, é logico imaginar que toda nova tecnologia que possibilite uma nova ferramenta de relacionamento necessite de um estudo mais profundo sobre a sua capacidade em transmitir segurança e ter no Direito um mecanismo que possa garanti-la.

Mesmo que a Internet e as ferramentas tecnológicas, ainda não está claro o que é “certo e errado” para as pessoas de um modo geral. Tais ferramentas devem ser usadas de forma segura e ética, buscando definir políticas e diretrizes de Segurança da Informação o que é mais adequado para proteção no mundo digital, evitando que se corram riscos desnecessários que possam gerar responsabilidade civil e criminal. Mas o que significa informação propriamente dito?

Segundo a International Organization for Standardization (IEC) ou Organização Internacional de Normalização (ISO):

> “A segurança da informação está diretamente relacionada com proteção de um conjunto de informações, no sentido de preservar o valor que possuem para um indivíduo ou uma organização... Na sociedade da informação, a informação é o principal patrimônio da empresa e está sob constante risco, representando a inteligência competitiva dos negócios e é reconhecida como ativo crítico para continuidade operacional e saúde das empresas”.

Dessa forma, é importante destacar que a Informação é importante para a sociedade como um todo, porém, em especial para as Empresas.

A informação É ativo intangível é possível deduzir que esteja sujeita a diversas ameaças, tais como: acesso indevido, furto de informações; fraude eletrônica e

falsificação de identidade; dano aos dados e informações arquivadas; espionagem para obtenção de segredos industriais/comerciais; cópia de programa; violação do direito autoral; interceptação indevida de informação; violação de bases de dados pessoais; uso indevido de marca em Search Engine para gerar trafego; exposição da marca associada a conteúdo ofensivo ou falso.

Diante deste cenário surge a norma ABNT NBR ISO/IEC 27002:2013:

> “estabelecer diretrizes e princípios gerais para iniciar, implementar, manter e melhorar a gestão de segurança da informação em uma organização. Isso também inclui a seleção, a implementação e o gerenciamento de controles, levando em conta os ambientes de risco encontrados na empresa, sendo utilizada para apoiar a implantação do Sistema de Gestão de Segurança da Informação (SGSI) em qualquer tipo de organização, pública ou privada, de pequeno ou grande porte, com ou sem fins lucrativos”.

A segurança da informação é alcançada pela implementação de um conjunto adequado de controles, incluindo políticas, processos, procedimentos, estrutura organizacional e funções de software e hardware”

A principal causa para o vazamento de informações são as próprias ações humanas. Com propriedade, o autor Antônio Everardo Nunes da Silva destaca que a falha humana é o principal motivo para darmos maior atenção à Segurança da Informação. Mesmo dentro do ambiente corporativo, ou até mesmo dentro da própria residência, é necessário ter cautela com os ativos e informações que são suscetíveis de vazamento. Dessa forma, devemos estar cada vez mais atentos e conscientes de que a informação é a moeda mais preciosa na era do conhecimento.

Quanto aos seus objetivos, a Segurança da Informação visa a três pontos:

a) confidencialidade — a informação só deve ser acessada por quem de direito;
b) integridade — evitar que os dados sejam apagados ou alterados sem a devida autorização do proprietário; e
c) disponibilidade — as informações devem sempre estar disponíveis para acesso. Alguns autores defendem o acréscimo de mais dois aspectos: a autenticidade e a legalidade.

A autenticidade é a capacidade de identificar e reconhecer formalmente a identidade dos elementos de uma comunicação eletrônica ou comércio. Já a legalidade

é característica das informações que possuem valor legal dentro de um processo de comunicação, onde todos os ativos estão de acordo com as cláusulas contratuais pactuadas ou a legislação política institucional, nacional ou internacional vigentes.

No que diz respeito aos interesses comerciais e de acordo com as melhores normas do mercado, para realizar um projeto de segurança da informação o primeiro passo é fazer uma análise de risco (qualitativa e quantitativa), de maneira que se possa descobrir quais são suas vulnerabilidades. Em seguida devem ser classificadas as informações de acordo com sua sensibilidade e criticidade, considerando a seguinte divisão pública, privada e confidencial.

É preciso harmonizar uma série de fatores, que vão de aspectos técnicos, no sentido de implementação de softwares e hardwares para segurança da informação, aos aspectos jurídicos, em especial a aplicação de monitoramento que não gere riscos legais de privacidade, ou infrações civil e penal.

Os principais objetivos da criação desse sistema são:

a) adequar o sistema de controles à crescente complexidade;

b) reduzir os riscos de descontinuidade, parcial ou total, da operação;

c) reduzir os riscos de vazamentos de segredos do negócio;

d) reduzir os riscos de fraudes;

e) reduzir os riscos de não cumprimento de obrigações legais;

f) atender às recomendações da auditoria externa;

g) adequar o sistema de gestão de riscos em TI aos padrões de mercado;

h) formalizar papéis e responsabilidades de todos os colaboradores;

i) comunicar formalmente o que é permitido ou proibido em relação à manipulação de informações e uso de sistemas da empresa;

j) informar que o não cumprimento da política poderá gerar punições e até mesmo a demissão por justa causa;

k) servir como diretriz para que todas as áreas da organização revejam seus procedimentos, sistemas, ativos de informação e serviços prestados com o objetivo de tornarem-se conformes à nova política.

É importante compreender que esse sistema visa formar um modelo não só para proteção jurídica das empresas, mas também tendo em vista a crescente dependência da informática, criando padrões para o uso dessas novas tecnológicas proporcionadas pela internet e o mundo digital.

Assim sendo, os principais focos jurídicos da Segurança da Informação são:

a) estar em conformidade com as leis vigentes;

b) proteger a sociedade e a empresa de riscos e contingências legais relacionados ao mau uso da informação, ao uso não autorizado, o vazamento de informação confidencial, danos a terceiros, crime e fraude eletrônica, invasão de privacidade etc.;

c) atender aos preceitos da Constituição Federal, do Código Civil, do Código Penal, da Lei de Direitos Autorais, da Lei de Software (antipirataria), da Consolidação das Leis do Trabalho e outros dispositivos legais nacionais e internacionais;

d) garantir que, na hipótese de investigação de um incidente, a empresa possa usar as provas coletadas, e que, de forma preventiva, possa praticar monitoramento, sem que isso gere riscos legais;

No Brasil existe um órgão especializado para combater e prevenir ataques criminosos no mundo digital, sendo ele um time de resposta a incidentes, são eles responsáveis pela Internet Brasileira, o grupo denominado CERT – BR (Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil), este é mantido pelo Comitê Gestor da Internet no Brasil (CGI), deixando sobe esse grupo a responsabilidade de receber, analisar e responder os incidentes de segurança em computadores, envolvendo redes conectadas a Internet no território nacional.

Considerando o foco tecnológico da Segurança da Informação, entende-se que o Direito Digital deve interpretar de forma clara o conjunto de conceitos técnicos para que possa suportar metodologias que tenham eficiência jurídica. É por isso que devemos estudar como operam, por exemplo, os mecanismos de chaves criptográficas e criptografia assimétrica. Ou seja, é preciso que o advogado tenha um mínimo de conhecimento técnico da matéria para melhor poder aplicar soluções jurídicas adequadas.

No quesito segurança, o sistema de chaves “públicas” e “privadas”, além de garantir o sigilo das transações ocorridas na rede, possibilita a identificação do remetente e do receptor, uma vez que é atribuída ao remetente uma chave privada, de conhecimento exclusivo deste, enquanto o destinatário deverá saber a chave pública, correspondente à chave privada do remetente, que é a única capaz de decodificar a mensagem enviada. Sendo assim, a chave privada funciona como uma assinatura eletrônica.

Há, ainda, outras tecnologias que devem ser compreendidas em sua concepção e funcionamento, como a de Firewall, uma barreira para entrada de invasores no sistema interno de empresas ou domicílios, pois com o crescimento da banda larga e da convergência, fica cada vez mais difícil e caro manter a porta fechada. A convergência aumenta o risco de exposição a Crackers, crimes e fraudes em ambientes eletrônicos, porque possibilita um contato constante de todos com todas as portas. Por isso, vem se tentando utilizar Sistemas de Pagamento Seguro (SPS) e Sistemas de Validação de cartões online (SSL). É necessária uma padronização das chaves de criptografia e a exigência de um compromisso maior das empresas em manter a atualização de seus softwares de segurança com certa periodicidade, para que possamos viver em um ambiente virtual mais seguro.

3.2 DIREITO A PRIVACIDADE E VEDAÇÃO AO ANONIMATO

Quando se fala de segurança da informação, inevitavelmente se cai na discussão de dois pontos conflitantes, privacidade contra anonimato. Sabemos que o direito a privacidade está garantido no rol de direitos fundamentais no artigo 5º, X em nossa Constituição Federal outorgada em 1988:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
>
> X - São invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação;

E também garantido pela Convenção de Estrasburgo de 1981 do qual o Brasil assinou:

> Artigo 1º - Objetivos e finalidades: A presente Convenção destina-se a garantir, no território de cada Parte, a todas as pessoas singulares, seja qual for a sua nacionalidade ou residência, o respeito pelos seus direitos e liberdades fundamentais, e especialmente pelo seu direito à vida privada, face ao tratamento automatizado dos dados de carácter pessoal que lhes digam respeito («proteção dos dados»).
>
> Artigo 2º - Definições para os fins da presente Convenção:
> a) «Dados de carácter pessoal» significa qualquer informação relativa a uma pessoa singular identificada ou susceptível de identificação («titular dos dados»);
> b) «Ficheiro automatizado» significa qualquer conjunto de informações objeto de tratamento automatizado;
> c) «Tratamento automatizado» compreende as seguintes operações, efetuadas, no todo ou em parte, com a ajuda de processos automatizados: registo de dados, aplicação a esses dados de operações lógicas e ou aritméticas, bem como a sua modificação, supressão, extração ou difusão;
> d) «Responsável pelo ficheiro» significa a pessoa, singular ou coletiva, autoridade pública, serviço ou qualquer outro organismo competente, segundo a lei nacional, para decidir sobre a finalidade do ficheiro automatizado, as categorias de dados de carácter pessoal que devem ser registadas e as operações que lhes serão aplicadas.

O direito a privacidade ele em sua essência limita e protege o direito à informação do indivíduo, assim como o direito ao anonimato, porém, este é vedado pela Constituição Federal em seu artigo 5º, IV:

> Art. 5º Todos são iguais perante a lei, sem distinção de qualquer natureza, garantindo-se aos brasileiros e aos estrangeiros residentes no País a inviolabilidade do direito à vida, à liberdade, à igualdade, à segurança e à propriedade, nos termos seguintes:
> IV - é livre a manifestação do pensamento, sendo vedado o anonimato;

Esses fatores constituem mecanismos dos quais dificultam a segurança no mundo virtual.

Existem limites para nossa liberdade, no Direito o limite é a partir do momento em que a sua liberdade atinge o interesse coletivo e acaba sobrepondo direitos individuais da sociedade. Portanto, existe uma grande necessidade de se criar diretrizes gerais das quais determinarão como buscar esse equilíbrio entre a linha tênue que é a proteção a privacidade e o direito a liberdade, sendo o Direito Digital o responsável em buscar a resposta desse anseio social.

A Internet foi criada em sua origem baseada em garantir esse “anonimato”, portanto, não existiu uma preocupação em sua origem em identificar os usuários, o foco

nessa época era justamente ter a liberdade de fazer inúmeras coisas de forma anônima. Foi devido a isso o grande sucesso dos serviços de chats, encontros virtuais, sites de sexo, entre outros conteúdos popularizados devido ao fato de se manter anônimo. Porém, em decorrência da evolução e devido a tamanha proporção que tomou, constatou-se que o anonimato era na verdade um empecilho para o desenvolvimento de um mundo digital seguro, devido a inúmeros fatos.

3.3 COMPUTAÇÃO FORENSE E A PERÍCIA DIGITAL

Como sugerem pesquisas atuais da Central Nacional de Crimes Cibernéticos (CNCC), existe uma grande tendência no crescimento dos crimes virtuais, e esses dados apontam que em breve, irão ultrapassar os crimes físicos. Assim sendo, podemos compreender a importância que a computação forense terá para a sociedade, pois é por meio dessa ciência que será possível descortinar os fatos e punir os infratores.

Assim como as outras áreas cientificas estudam os crimes, a computação forense faz parte das ciências criminalísticas. Neste sentido TOCHETTO nos elucida:

> “Trata-se de disciplina autônoma, integrada pelos diferentes ramos do conhecimento técnico-cientifico, auxiliar e informativa das atividades policiais e judiciárias de investigação criminal, tendo por objeto o estudo dos vestígios materiais extrínsecos à pessoa física, no que tiver de útil à elucidação e à prova das infrações penais e, ainda, à identificação dos autores respectivos”

Já a ciência forense pode ser definida como: “A aplicação de princípios das ciências físicas ao Direito na busca da verdade em questões cíveis, criminais e de comportamento social para que não se cometam injustiças contra qualquer membro da sociedade”

A computação forense, então, consiste no uso de métodos científicos na preservação, coleta, validação, identificação, analise, interpretação, documentação e apresentação de evidências digitais.

Em outras palavras, tem por objetivo extrair informações de qualquer vestígio relacionado com o caso investigado, buscando conclusões acerca da infração. No mundo da criminalística, vestígio é qualquer coisa deixada para trás, sendo marca, fato, sinal ou material, que foi encontrado no local onde foi praticado o delito.

Portanto, a evidência digital será toda informação ou dados, que possa ser retirado de um computador ou quaisquer dispositivos eletrônicos. Além disso, a evidência digital sempre deverá estar em formato de entendimento humano. Nenhuma tecnologia, desde o advento do DNA, teve um efeito potencial tão grande em tipos específicos de investigações como a computação forense.

Os indícios que caracterizam a infração, ou relacionam o suspeito ao ato ilícito, são os arquivos de imagens de pornografia infantil, mensagens eletrônicas com ameaças ou chantagens, arquivos com informações incriminatórias ou dados roubados. Exemplos de locais em que podem ser encontrados tais indícios são: os sistemas de arquivos, arquivos de log, espaços não utilizados no dispositivo de armazenagem, arquivos temporários, área de swap, setor de boot, memória, periféricos, comportamento de processos etc.

Outra Ciência que contribui com a computação forense é a network forensic, que trabalha com os logs para aferir determinados fatos, assim como para determinar ponto de acessos, início e fim desse acesso, quais urls foram acessadas, toda a analise do log da rede, etc.

Contudo, mesmo a grande precisão e qualidade das provas obtidas por meio da computação forense, há uma grande preocupação, a coleta dessas evidências, se forem coletadas de forma errônea poderá tornar essa ilícita ou inválida. Também, existe a possibilidade de alguma prova ilícita contaminar as demais e acabar eliminando todas as chances em provar o crime.

Por fim, uma das principais problemáticas na computação forense é o conflito entre a investigação e o direito a privacidade. Até onde se pode ir sem violar a privacidade dos envolvidos, sendo eles diretamente ou indiretamente envolvidos no processo de perícia? Portanto, além de cautela, se faz necessário estar fundamentados nas leis que tratam deste caso, para evitar que seja violada a privacidade alheia, evitando que a perícia passe dos limites legais.

3.4 A IMPORTANCIA DA SEGURANÇA DA INFORMAÇÃO

Vivemos em um mundo cada vez mais conectado com o mundo digital, de bancos de dados pessoais a infraestruturas complexas do governo. Proteger essas redes não é

mais uma opção. Agora, o risco cibernético está no topo das preocupações de todos os Países, já que as violações se tornaram grandes ameaças devido ao seu potencial de gerar problemas, aumentando assim o medo de que ataques de hackers e outras falhas de segurança possam colocar em risco a economia global.

O relatório do The Global Risks de 2015, agencia americana responsável por monitorar e estudar os ataques cibernéticos, publicou no fórum de pesquisas econômicas mundial The World Economy Forum (WEF), em janeiro de 2015 que "90% das empresas em todo o mundo reconhecem que estão insuficientemente preparadas para se protegerem contra ataques cibernéticos".

O crime cibernético custa à economia global mais de 400 bilhões de dólares por ano, segundo estimativas do The Center For Strategic and International Studies. Em 2013, cerca de 3.000 empresas nos Estados Unidos tiveram seus sistemas comprometidos por cibercriminosos.

Muitas empresas em todo o mundo perderam dados de clientes e informações de cartão de crédito. Em outras empresas, os cibercriminosos roubaram dinheiro de contas, realizaram espionagem industrial e, em alguns casos, até assumiram os sistemas da empresa e exigiram dinheiro de resgate para desbloqueá-los.

Não surpreende que governos e empresas de todo o mundo estejam buscando melhores estratégias de defesa cibernética. A Agência Europeia de Segurança de Redes e Informações realizou um exercício de segurança cibernética em outubro de 2014, envolvendo 29 países e mais de 200 organizações, incluindo órgãos governamentais, empresas de telecomunicações, fornecedores de energia, instituições financeiras e provedores de serviços de Internet.

Os testes incluíram a simulação de mais de 2.000 incidentes separados: ataques de negação de serviço, alterações no site, acesso a informações confidenciais e ataques a infraestrutura crítica. Falhas de software e hardware foram consideradas as maiores ameaças à segurança.

Em fevereiro de 2015, o então presidente dos Estados Unidos da America, Barack Obama discursou a respeito da Segurança Cibernética e Proteção ao Consumidor mundial, na Universidade de Stanford. Nele participaram líderes políticos, CEOs e representantes de empresas de segurança de computadores, grandes varejistas, policiais e especialistas técnicos de todo o mundo, para "colaborar e explorar parcerias

que ajudarão a desenvolver as melhores maneiras de reforçar nossa segurança cibernética".

Claramente, ainda há muito trabalho a ser feito, e as pessoas por trás dos ataques veem se adaptando e evoluindo junto com o desenvolvimento da segurança tendo um avanço significativo na especialização desses criminosos. Podemos dizer que a segurança cibernética se tornou uma questão de urgência.

3.5 AS CONSEQUÊNCIAS DOS CRIMES CIBERNÉTICOS

Os ataques cibernéticos se enquadram em duas grandes categorias: violações na segurança e sabotagem de dados. Dados pessoais, propriedade intelectual, segredos comerciais e informações relacionadas a ofertas, são alvos tentadores para uma violação de segurança de dados. A sabotagem pode assumir a forma de ataques de negação de serviço, que inundam os serviços da Web com mensagens falsas, para desativar sistemas e infraestrutura.

Além de perdas comerciais e problemas de relações públicas, interrupção das operações e possibilidade de extorsão, os ataques cibernéticos também podem expor uma organização a ações regulatórias, reclamações por negligência, incapacidade de cumprir obrigações contratuais e uma perda prejudicial de confiança entre clientes e fornecedores.

A maioria dos incidentes de crimes cibernéticos não é relatada e poucas empresas apresentam informações sobre suas perdas. Isso não é surpreendente, dado o risco à reputação de uma organização e a perspetiva de ação legal contra aqueles que praticam crimes cibernéticos. Poucos são os cibercriminosos que são presos, sequer são identificados.

Uma proporção significativa de crimes cibernéticos também não é detectada, principalmente espionagem industrial, onde é difícil detectar o acesso a documentos e dados confidenciais. Existe o risco de que uma empresa possa negociar em desvantagem por meses ou até anos, em decorrência de uma violação de segurança contínua, não detectada.

3.6 A VULNERABILIDADE ESTÁ EM ASCENSÃO

É provável que o crime cibernético aumente, apesar dos melhores esforços de agências governamentais e especialistas em segurança cibernética. Seu crescimento está sendo impulsionado pelo crescente número de serviços disponíveis on-line e pela crescente sofisticação de criminosos cibernéticos.

A inovação técnica lança novos perigos online. Por exemplo, a migração de dados para provedores de nuvem de terceiros criou uma centralização de dados e, portanto, mais oportunidades para os criminosos desviarem informações críticas de um único ataque de destino. Da mesma forma, a ênfase nos serviços móveis abriu os sistemas corporativos para mais usuários, multiplicando as oportunidades de penetrar nas medidas de segurança.

Os aplicativos que envolvem a coleta e análise de dados em grandes quantidades, os chamados Big Datas, vem exigindo mais dos responsáveis pela segurança. Montanhas de dados confidenciais sobre decisões do comprador, seus hábitos e outras informações pessoais devem ser mantidas em segurança, mas até recentemente a segurança não era uma prioridade nos sistemas que lidam com o Big Data.

O desenvolvimento da Internet das Coisas, que permite a comunicação entre máquinas, aumenta a possibilidade de os aparelhos serem manipulados por hackers. O uso generalizado da comunicação máquina entre máquina (M2M) provavelmente aumentará a possibilidade de uso indevido de informações.

Grande parte da infraestrutura crítica do mundo, controlando serviços como geração de energia, transporte e serviços públicos, já depende do M2M. Proteger as redes que transportam as comunicações que controlam esses serviços é vital, especialmente porque a tomada de decisões é frequentemente feita sem o envolvimento humano.

3.7 COMBATE AOS RISCOS NO MUNDO DIGITAL

Segundo Detlev Gabel, especialista em segurança de dados: "A cibersegurança é considerada uma responsabilidade do conselho". Isso nos diz que os diretores

responsáveis pela segurança podem ser responsabilizados por não cumprirem seu dever de evitar danos à corporação. No desempenho de sua função de supervisão, os diretores devem se manter informados sobre as defesas de segurança cibernética da corporação. Eles devem perguntar quais são os riscos e determinar o que precisa ser feito para mitiga-los. No mundo digital de hoje, infelizmente, está se tornando uma questão de “quando”, em vez de “se” algum tipo de violação de dados ocorrerá.

Nos Estados Unidos e União europeia já se discute da obrigatoriedade das empresas públicas divulgarem dados dos riscos materiais das quais passaram em ataques cibernéticos e até mesmo incluir detalhes específicos e técnicos para permitir que os profissionais da área consigam avaliar e melhorar a segurança em geral para todos.

As empresas norte-americanas também devem considerar a divulgação sobre os possíveis custos associados à prevenção de ataques cibernéticos e quaisquer métodos de contingentes ou estratégias relacionadas a violações anteriores. Em suma, uma falha em fazer divulgações adequadas pode levar a uma responsabilidade adicional no caso de um ataque cibernético.

Não faltam recomendações disponíveis para as organizações seguirem e avaliarem seus riscos e desenvolver planos adequados para combatê-los. Governos de todo o mundo estão desenvolvendo diretrizes de segurança cibernética.

No ano de 2014, a pedido do então presidente dos Estados Unidos Barack Obama, o Instituto Nacional de Padrões e Tecnologia (NIST), nos Estados Unidos, emitiu uma estrutura para melhorar a segurança da infraestrutura crítica. A infraestrutura crítica não inclui apenas redes de suprimento de energia e telecomunicações, mas também serviços financeiros e afins.

A junção de todo o exposto é denominada Framework, que em suma é: um conjunto de padrões e práticas recomendadas, elaborados com a participação de milhares de especialistas em segurança e projetados para ajudar as organizações a gerenciar os riscos de uma violação de segurança cibernética. Com a ajuda do Framework, eles traçam seu perfil de segurança atual, definem qual perfil devem procurar e criam um plano para alcançá-lo.

3.8 ASPECTOS LEGAIS DO RISCO CIBERNÉTICO

Os governos de todo o mundo estão reforçando as leis para garantir que as organizações assumam maior responsabilidade pela segurança cibernética e relatem violações cibernéticas. O relato de violações é importante, pois permite que as agências governamentais tomem medidas para fortalecer a segurança, permita que os indivíduos atenuem os danos e incentive as organizações a adotar medidas eficazes de segurança.

Por exemplo, nos Estados Unidos, 47 estados promulgaram leis que exigem que sejam relatadas violações de segurança envolvendo dados pessoais. O Congresso Nacional dos Estado Unidos da América também está considerando várias propostas, incluindo uma do apresentado pelo governo Obama no início de 2015, relativa a uma lei nacional de notificação de violações. A Lei de Segurança de Dados e Notificação de Violação de 2015 é uma companheira da Lei de Direitos de Privacidade do Consumidor de 2015, divulgada pelo Presidente Obama em fevereiro de 2015, que rege a coleta e disseminação de dados do consumidor. De acordo com um porta-voz da Casa Branca, eles "fornecerão aos clientes mais controle sobre seus dados, empresas com maneiras mais claras de sinalizar sua administração responsável sobre os dados e todos com flexibilidade para continuar inovando na era digital".

Embora tais movimentos legislativos sejam bem-vindos, eles têm seus críticos: as multas não são particularmente proibitivas e não está claro como elas serão aplicadas, e as empresas poderão elaborar seus próprios códigos de conduta, deixando espaço para brechas.

A União Europeia e vários de seus estados membros introduziram regulamentos semelhantes, alguns dos quais são específicos para setores específicos, com o resultado de que organizações que operam em diferentes jurisdições legais têm o ônus adicional de garantir que cumpram as diferentes leis, elevando os custos e a complexidade para as empresas.

Enquanto isso, a União Europeia está desenvolvendo uma proposta de regulamento geral de proteção de dados para substituir e harmonizar a legislação atual de proteção de dados. O novo regime exigiria que as organizações relatassem violações de dados imediatamente às autoridades competentes e às pessoas afetadas. Se dependesse do Parlamento Europeu, como um dos órgãos legislativos que decidia a proposta, o não cumprimento deste requisito poderia levar a sanções equivalentes a 5% do faturamento global da empresa infratora.

A prevenção contra uma possível violação da segurança, é particularmente importante quando os incidentes podem resultar em multas, ações legais ou medidas por agências governamentais. Um plano eficaz reduz os riscos de perdas financeiras e danos à reputação de uma organização, garantindo a conformidade com os requisitos legais relevantes.

No caso de um incidente, recomenda-se fortemente que seja incluído um advogado na equipe encarregada de qualquer missão de investigação de fatos, para que a empresa possa reivindicar privilégios e proteção do produto do trabalho. Essas proteções, podem impedir a divulgação de informações que possam ser prejudiciais para o cliente, se surgir um litígio futuro após um incidente.

CONSIDERAÇÕES FINAIS

Conclui-se, por fim, que cabe ao Direito adaptar-se e suprir as necessidades provenientes dos conflitos do mundo digital. No Brasil, vem sendo propostas para sanar essas necessidades por intermédio do Direito Digital, com respaldo principalmente pela Lei do Marco Civil da Internet no Brasil e demais legislações a respeito de segurança no mundo digital e proteção de dados. É sabido, que as redes de computadores e toda a infraestrutura ao redor disso, desde o inicio são alvos de criminosos, e é muito provável que no futuro isso aumente cada vez mais, devido a crescente expansão e migração dos serviços essenciais e de grande relevância social para os meios digitais.

Essas transformações atingem diretamente a sociedade como um todo, exigindo assim que o Direito e seus ramos se especializem e se atualizem, para conseguir atender essas demandas, tanto, sociais, como jurídicas.

Portanto, ao que tudo indica, em um mundo cada vez mais conectado, em que o mundo digital passou a fazer parte do mundo real, devido as relações de consumo, transações bancárias, troca de informações e convívio social, o desenvolvimento do Direito Digital e a segurança da informação provam a cada dia sua necessidade e tamanha importância.

REFERENCIAS BIBLIOGRÁFICAS

BRASIL. **CONSTITUIÇÃO DA REPÚBLICA FEDERATIVA DO BRASIL DE 1988**. Brasil, 05 de outubro de 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 28 de maio de 2020.

BRASIL. **Justiça usa Código Penal para combater crime virtual**. Disponível em: http://stj.jus.br/portal_stj/publicacao/engine.wsp?tmp.area=398&tmp.texto=90108. Acesso em: 28 junho de 2020.

BRASIL. **CÓDIGO DE PROCESSO CIVIL, Lei n.º 13.105 de 2015,** 16 de março de 2015. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2015/lei/l13105.htm. Acesso em 29 de junho de 2020.

FARAH, Rafael Mott. **A responsabilidade dos estabelecimentos comerciais no fornecimento de rede wi-fi a seus clientes**. In: PINHEIRO, Patrícia Peck (coord.). Direito digital aplicado 2.0. 2.ed. São Paulo: Thomson Reuters, 2016.

GALO, Carlos Henrique. Lei nº 12.965/11: **o Marco Civil da Internet – Análise Crítica**, 23 de abril de 2014. Disponível em: http://henriquegalo.jusbrasil.com.br/artigos/118296790/lein-12965-11-o-marco-civil-da-internet-analise-critica. Acesso em 05 de julho de 2020.

GRILO, Brenno. **Informatização reduz 70% do tempo gasto com burocracias, diz Nalini**. Disponível em: https://www.conjur.com.br/2015-nov-30/informatizacao-reduz-70tempo-gasto-burocracias-nalini. Acesso em: 24 junho de 2020.

HAIKAL, Victor Auilio. **Enfim, o marco civil da internet. In**: PINHEIRO, Patrícia Peck (coord.). Direito digital aplicado 2.0. 2.ed. São Paulo: Thomson Reuters, 2016.

KAC, Fernanda, e, GUZZO, Douglas Pinto. **Responsabilidade civil dos pais pelos atos dos filhos menores na internet.** Disponível em: https://www.migalhas.com.br/depeso/282629/a-responsabilidade-civil-dos-pais-pelos-atosdos-filhos-menores-na-internet. Acesso em: 28 junho de 2020.

LIMA, Glaydson de Farias. **Da responsabilidade jurídica dos pais e responsáveis. Manual de direito digital**: fundamentos, legislação e jurisprudência. Curitiba: Appris, 2016.

PECK, Patricia Pinheiro. **Direito Digital**, 6ª ed. São Paulo, Saraiva, 2016. Disponível em: https://integrada.minhabiblioteca.com.br/#/books/9788502635647/. Acesso em: 23 junho de 2020.

PACI, Maria Fernanda. **Considerações gerais sobre direito eletrônico**. Disponível em:

https://ambitojuridico.com.br/edicoes/revista-162/consideracoes-gerais-sobre-direitoeletronico/. Acesso em: 24 junho de 2020.

PEREIRA, Sebastião Tavares**. Elementos tecnológicos para o avanço da teoria geral do (e)processo**. In: ROVER, A. J. (Org.). Engenharia e Gestão do Judiciário Brasileiro: Estudos sobre E-Justiça. Florianópolis: Deviant, 2016, localização 8263.

ROVER, Aires José apud ROTTA, Maurício et. al. **Alterações Resultantes do Processo Judicial Eletrônico**. In: ROVER, A. J. (Org.). Engenharia e Gestão do Judiciário Brasileiro: Estudos sobre EJustiça. Florianópolis: Deviant, 2016, localização 7344.

STABILE, Ilison. **Chegou a hora da segunda transformação digital da justiça**. Disponível em: https://www.migalhas.com.br/depeso/303063/chegou-a-hora-da-segundatransformacao-digital-da-justica. Acesso em: 24 junho de 2020.

GLOSSARIO

Arquivos de log: representam um papel importante na análise do sistema, pois permitem a reconstituição de fatos que ocorreram no sistema computacional. Variam de acordo com o sistema operacional, os aplicativos e serviços executados no sistema e as configurações determinadas pelo administrador. Registram, por exemplo: as atividades do usuário, dos processos e do sistema, as conexões de rede, as atividades da rede e informações específicas dos aplicativos e dos serviços.

Espaços não utilizados no dispositivo de armazenagem: tais espaços podem conter indícios que o usuário tentou apagar. Entretanto, a “deleção” de arquivos e diretórios não apaga os dados do dispositivo de armazenagem, apenas disponibiliza o espaço ocupado para ser sobrescrito por novos arquivos. São caracterizados por espaços não alocados dentro do sistema de arquivos, espaços alocados, mas não totalmente utilizados e áreas do dispositivo de armazenagem que não constituem uma partição do disco ou que não contém um sistema de arquivos.

Arquivos temporários: alguns programas criam arquivos temporários durante sua execução, que são normalmente apagados automaticamente ao final da sessão de trabalho.

Área de SWAP: é a área utilizada pelo gerenciador de memória do sistema operacional como uma grande área de armazenamento temporário, permitindo que processos sejam momentaneamente descarregados da memória principal, liberando espaço para execução de outros.

Setor de BOOT: contém informações relativas aos programas que são carregados quando o computador é inicializado. Se tais informações forem modificadas, é possível carregar qualquer programa durante a inicialização do computador.

Memoria: armazena todo tipo de informação volátil, como, por exemplo, informações dos processos que estão em execução, dados que estão sendo manipulados e, muitas vezes, ainda não foram salvos no disco e informações do sistema operacional.

Periféricos: dispositivos como modems, pagers, aparelhos de fax e impressoras. Contém memórias que podem ser acessadas e salvas. Além disso, dispositivos não autorizados podem ser implantados no sistema operacional, possibilitando a execução da infração.

Comportamento de processos: cada processo se executa em um ambiente com privilégios específicos que determinam quais recursos do sistema, programas e arquivos de dados podem ser acessados, e de que modo. Qualquer alteração nesse comportamento pode ser um indicador de interferência intencional. Um invasor pode desvirtuar a execução de um programa, causando sua falência, ou fazendo com que ele opere de maneira inesperada ao administrador ou usuário (acessando informações não autorizadas ou consumindo recursos excessivos, por exemplo).

Buffer overflow: além de saber as fontes de busca o ideal é que o perito reconheça alguns elementos dos principais ataques realizados em ambientes computacionais, tais como o erro causado quando o programa tenta armazenar muitos dados na área de memória temporária e que pode ser explorado por hackers para executar códigos maliciosos.

Denial of Service: método de ataque de negação de serviço a um computador ou rede que atenta contra o limite ou previne acesso para a Internet pela “inundação” de pedidos (para uma webpage ou recurso online) ou e-mail (causando sobrecarga no sistema). Uma variante desse ataque é conhecida como Negação de Serviço Distribuído, que se utiliza de múltiplos computadores, aumentando o tráfego e reduzindo as defesas da máquina vítima ou rede.

Big Data: é a área do conhecimento que estuda como tratar, analisar e obter informações a partir de conjuntos de dados grandes demais para serem analisados por sistemas tradicionais.

Ataque Sniffer: Um sniffer não necessariamente é malicioso. Na verdade, este tipo de software é usado com frequência para monitorar e analisar o tráfego de rede para detectar problemas e manter um fluxo eficiente. No entanto, um sniffer também pode ser usado com má fé. Eles capturam tudo o que passa por eles, inclusive senhas e nomes de usuários não criptografados. Dessa forma, os hackers com acesso a um sniffer terão acesso também a qualquer conta que passar por ele. Além disso, um sniffer pode ser instalado em qualquer computador conectado a uma rede local. Ele não precisa ser instalado no próprio aparelho que se deseja monitorar.

Ransomware: um tipo de malware que sequestra o computador da vítima e cobra um valor em dinheiro pelo resgate, geralmente usando a moeda virtual bitcoin, que torna quase impossível rastrear o criminoso que pode vir a receber o valor.

Software: é um termo técnico que foi traduzido para a língua portuguesa como logiciário ou suporte lógico, é uma sequência de instruções a serem seguidas e/ou executadas, na manipulação, redirecionamento ou modificação de um dado ou acontecimento.

Hardware: parte física de um computador, é formado pelos componentes eletrônicos, como por exemplo, circuitos de fios e luz, placas, utensílios, correntes, e qualquer outro material em estado físico, que seja necessário para fazer com o que computador funcione.

Deep Web: Uma Internet obscura ou endereço sombrio refere-se a qualquer ou todos os servidores de rede inalcançáveis na Internet, por requererem softwares, configurações ou autorizações específicas para o acesso.

Serch Engine: Um mecanismo de pesquisa na Web ou mecanismo de pesquisa na Internet é um sistema de software projetado para realizar pesquisas na Web

Firewall: uma solução de segurança baseada em hardware ou software (mais comum) que, a partir de um conjunto de regras ou instruções, analisa o tráfego de rede para determinar quais operações de transmissão ou recepção de dados podem ser executadas.

Criptografia: Criptografia ou criptologia é o estudo e prática de princípios e técnicas para comunicação segura na presença de terceiros, chamados "adversários". Mas geralmente, a criptografia refere-se à construção e análise de protocolos que impedem terceiros, ou o público, de lerem mensagens privadas.

Hacker: são pessoas com um conhecimento profundo de informática e computação que trabalham desenvolvendo e modificando softwares e hardwares de computadores, não necessariamente para cometer algum crime. Eles também desenvolvem novas funcionalidades no que diz respeito a sistemas de informática.

Cracker: hackers que utilizam o conhecimento em informática, computação e demais tecnologias para invadir ilegalmente sistemas, sites, servidores, bancos de dados etc. Em alguns casos, o objetivo é apenas testar a vulnerabilidade dos serviços, mas, em outros, é obter algum ganho financeiro ou pessoal.

Network forensics: O forense de rede é um sub-ramo do forense digital relacionado ao monitoramento e análise do tráfego de rede de computadores para fins de coleta de informações, evidências legais ou detecção de intrusão.

Url: Uniform Resource Locator, é um termo técnico que foi traduzido para a língua portuguesa como "localizador uniforme de recursos". Um URL se refere ao endereço de

rede no qual se encontra algum recurso informático, como por exemplo um arquivo de computador ou um dispositivo periférico.