UNIVERSIDADE FEDERAL DE SERGIPE
CENTRO DE CIÊNCIAS SOCIAIS APLICADAS
DEPARTAMENTO DE ADMINISTRAÇÃO

GLEICIANE SANTOS OLIVEIRA

LEIS BRASILEIRAS DE ACESSO À INTERNET NA PERCEPÇÃO DOS USUÁRIOS

São Cristóvão – SE
2018

GLEICIANE SANTOS OLIVEIRA

LEIS BRASILEIRAS DE ACESSO À INTERNET NA PERCEPÇÃO DOS USUÁRIOS

Trabalho de Conclusão de Curso apresentado ao Departamento de Administração do Centro de Ciências Sociais Aplicadas da Universidade Federal de Sergipe, em cumprimento às normas de Trabalho de Conclusão de Curso para obtenção da graduação em Administração.

Orientador: Profº. Dr. Jefferson David Araújo Sales

Coorientadora: Profª. Dra. Jenny Dantas Barbosa

São Cristóvão - SE
2018

RESUMO

A presente pesquisa aborda a respeito da percepção dos usuários das redes sociais virtuais sobre as leis de acesso à internet que regem o Brasil. Foram analisadas as leis brasileiras de acesso à internet a fim de conhecer como estão prescritas as penalidades, além da classificação e tipificação dos crimes. Quanto aos aspectos metodológicos, o estudo foi classificado como descritivo. Os dados foram coletados através de questionário tipo *survey* aplicados através da plataforma do *Google Forms*. Os resultados revelaram que apesar de algumas pessoas conheceram os riscos ao navegarem na internet elas ainda são vítimas dos mais diversos crimes cibernéticos. Muitas delas não chegam nem a fazer denúncia formal por não acreditarem na efetividade da legislação brasileira. A pesquisa teve como limitação a dificuldade de coletar dados devido o mundo virtual ser tão vasto e a escassez de trabalho sobre a área. O impacto da internet nas relações sociais, e a utilização da internet na gestão de processos de informação são sugestões para as futuras pesquisas.

PALAVRAS-CHAVES: Internet, Legislação brasileira de acesso a internet, usuários da internet.

SUMÁRIO

1 INTRODUÇÃO

A criação da internet é considerada o marco da inovação dos meios de telecomunicação. Sua criação, entretanto, se deve à necessidade de comunicação entre os militares em meados dos anos 60, época em que o mundo passava por intensas transformações no cenário mundial. Com o final da Segunda Guerra Mundial (1939 – 1945), o mundo se viu dividido em dois grandes blocos econômicos, marcados por disputas estratégicas e conflitos indiretos entre os Estados Unidos e a ex União Soviética, que disputavam entre si a hegemonia política, econômica e militar mundial.

É nesse cenário que o Departamento de Defesa dos Estados Unidos sente a necessidade de criar um meio de comunicação, para fins militares, e que pudesse resistir a possíveis conflitos armados. Um grupo de pesquisadores norte americano se uniu com objetivo desenvolver uma rede de comunicação militar descentralizada, que funcionasse independentemente de um núcleo central, ou seja, as mensagens enviadas não se perderiam caso houvesse conflitos nucleares e que ocasionasse na destruição dos terminais de comunicação, possibilitando que a comunicação fluísse sem interrupção para áreas não afetadas (MONTEIRO, 2001).

Nos anos seguintes, entre as décadas de 70 e 80, observou-se a necessidade de se aprimorar a rede de comunicação já criada, de forma que pudesse aumentar o alcance territorial, permitindo assim que mensagens fossem trocadas a longa distância de maneira rápida e eficaz. Neste cenário é criada na década de 70, a Advanced Research Project Agency (ARPAnet), que em início de 1980, com a criação e utilização do Transmission Control Protocol/Internet Protocol (TCP/IP), é que possibilitou que a conexão entre computadores distantes fosse estabelecida.

Em meados dos anos 80, com a migração da ARPAnet para National Sciencie Foundation (NSFnet), é que a internet, que conhecemos hoje, ganha “corpo” ao permitir que os usuários pudessem se conectar a redes existentes. Vale ressaltar que nesse momento, a internet era usada para troca de comunicação dentro do meio acadêmico, só disseminando para outros usuários em meados dos anos 90, quando deixa de ser uma rede única e homogênea passando a ser uma interligação de muitas redes territoriais que possuem conexão com a grande rede. Assim, a internet se transforma num sistema mundial pública de redes de computadores onde qualquer pessoa previamente habilitada pode se conectar.

Isso foi possível devido a criação da World Wide Web (WWW) por Timothy Berners-Lee, que proporcionava um maior compartilhamento de informações unindo hipertexto e a internet. Assim foi criada HTTP, uma linguagem especial onde foi possível ter informações em diversos formatos (vídeos, imagens, sons, gráficos, etc.).

No Brasil, o primeiro contato com a internet ocorreu em 1988 quando a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapsep) realizou a primeira conexão à rede através de uma parceria com o Fermilab, um dos mais importantes centros de pesquisa científica dos Estados Unidos (VIEIRA, 2003, p. 8). Percebe-se que nesse primeiro contato o uso da internet no Brasil tinha os mesmos fins que nos Estados Unidos: a comunicação entre instituições acadêmicas.

Somente em 1995 que a internet no Brasil começa a se popularizar, permitindo que diversos usuários pudessem usufruir de seus benefícios, como conhecimento de outras culturas, trocas rápidas de informações, sendo elas pessoais ou comerciais, diversão, conhecer ou manter relacionamentos a distância.

Com a popularização da internet foi inevitável a criação de aplicativos que permitissem uma maior interação entre os indivíduos. As chamadas “redes sociais” foram criadas justamente com esse objetivo, aproximar pessoas de diversos lugares em tempo real.

No decorrer dos anos, várias redes sociais surgiram agitando o mundo cibernético com a popularidade alcançada. Entre as mais populares destaca-se o *Facebook*, *youtube*, *Whatasapp*, *Messenger*, *Instagram*. (BELING, 2018).

Todavia, com o frequente uso da internet, as pessoas passaram a ficar suscetíveis a transtornos gerados neste tipo de comunicação, tais como financeiros, disseminação pornográficas (com graves consequências como suicídio), envios de spam, invasão de computadores e compartilhamento de dados de grandes empresas.

Muitos desses crimes eram amparados pelo Código Civil, leis esparsas ou em alguns casos pelo Código de Defesa do Consumidor. Entretanto, faltava um mecanismo de defesa mais efetivo que englobasse todos os crimes cometidos através do uso da internet (JÚNIOR, 2014).

A primeira Lei vigente para punir infratores da internet foi a Lei 12.735/2012, que se originou do projeto de Lei Azeredo nº 84/1999 e mais tarde passando para o nº 89/2003, mas foi somente em 2012 que foi sancionada, a lei regulamenta

condutas realizadas mediante uso de sistema eletrônico digital ou similares; e dá outras providências.

No mesmo ano, após a invasão do computador da atriz Carolina Dieckmann, que teve seus arquivos furtados e pulicados indevidamente na internet, foi criada a Lei 12.737/2012, que visava a defesa a crimes cometidos na internet. Esta lei regulamenta o crime de invasão do dispositivo informático, falsificação de cartões e documentos particulares e interrupção de serviço, onde as penas variam de 3 meses a 2 anos, além de multa, podendo dobrar dependendo da gravidade do crime cometido.

Diante da necessidade de se reforçar a importância da lei supracitada, em 2014 foi aprovada a Lei 12.965/2014, que regulamenta o uso da internet no Brasil, estabelecendo assim princípios, direitos e garantias dos usuários e das empresas.

Infelizmente nem todos têm o devido conhecimento dessas leis. As dificuldades de acesso à informação, bem como a falta de divulgação nas mídias de comunicação tornam estas leis desconhecidas para a maioria dos usuários de internet. Sendo assim, esse trabalho se justifica pela importância dos usuários conhecerem e compreenderem os seus direitos e deveres, perante o acesso da internet.

1.1 Problema

Graças à popularização das internet, uma grande parcela da população tem acesso aos serviços oferecidos pela rede. No entanto, poucos possuem conhecimentos avançados de informática, o que os deixa vulneráveis a ataques de segurança e privacidade. Assim, faz-se necessário, enquanto cidadão, conhecer os direitos previstos em lei sobre o assunto.

Nesta perspectiva, o presente trabalho busca responder à seguinte pergunta: Quais são as percepções dos usuários das redes sociais virtuais sobre as leis brasileiras de acesso à internet?

1.2 Objetivos

"O objetivo final, se alcançado, dá resposta ao problema. Objetivos intermediários são metas de cujo atingimento depende o alcance do objetivo final". (VERGARA, 1998, p. 25).

Aqui está listado o objetivo geral e o os objetivos específicos necessários para o entendimento do problema da pesquisa.

1.2.1 Geral

- Analisar as percepções dos usuários de redes sociais virtuais sobre as leis brasileiras de acesso à internet.

1.2.2 Específicos

- Traçar as características demográficas e econômicas dos usuários das redes sociais virtuais;
- Levantar as formas de acesso às redes sociais virtuais;
- Verificar as medidas preventivas de segurança tomadas pelos usuários no acesso à rede;
- Identificar a aplicabilidade do conhecimento das leis na segurança individual no acesso à internet.

1.3 Justificativa

Com a democratização do acesso à internet, diversas facilidades foram conquistadas pela população em geral no que se refere ao acesso de dados e informações em todos os âmbitos da sociedade. Paralelo a isto foram gerados também muitos problemas, especificamente no que se refere à segurança e à privacidade dos dados que circulam na rede. Com isso, a mídia tem denunciado constantemente diversos crimes cibernéticos cometidos por usuários tanto no campo pessoal quanto no profissional. Sendo assim, justifica-se este estudo pela necessidade de compreender essa problemática, assim como apontar possíveis possibilidades de evitar esses crimes e ajudar as pessoas a se protegerem, assim como conhecerem a legislação que garante os seus direitos e deveres. Espera-se que este estudo possa permitir que os interessados nesta problemática entendam

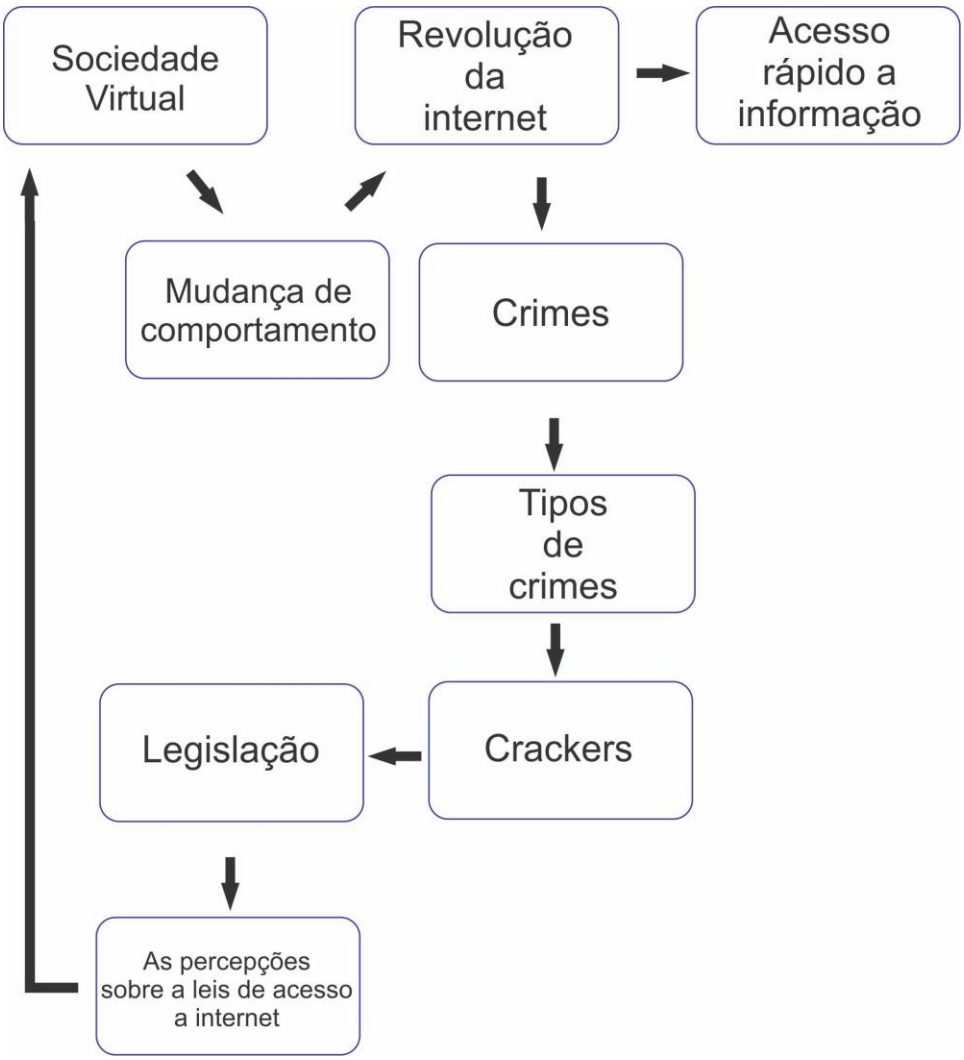
melhor a legislação brasileira de acesso à internet e assim possam utilizá-la nas diferentes situações vivenciadas na rede.

2 FUNDAMENTAÇÃO TEÓRICA

Este capítulo contem cinco tópicos. No primeiro, apresentam-se conceitos sobre sociedade virtual ou em rede, seus principais autores e a definição do universo que está inserido essa sociedade. Na segunda parte, explana-se sobre a evolução da internet e a mudança de comportamento da sociedade perante esses avanços tecnológicos. Na terceira, mostram-se os tipos de crimes ocorridos na internet, como é feita a prevenção e a investigação desses crimes. Na quarta parte, mostra-se a legislação brasileira vigente para os crimes cometidos na internet. Por fim, o estado da arte, onde trabalhos já publicados sobre a temática são apresentados.

A fundamentação teórica aqui descrita segue o seguinte diagrama conceitual (Figura 1):

Figura 1. Diagrama conceitual



2.1 Sociedade Virtual

Imaginar o mundo sem a tecnologia é algo inviável. Por exemplo, no passado as pessoas se comunicavam através de cartas que demoravam meses para chegar a seu destino final, sabiam de notícias apenas pelo rádio ou pela televisão, digitar algum documento importante somente com máquina de datilografia. Hoje, com as facilidades de internet é possível fazer inúmeras coisas, agilizando e desburocratizando muitos processos, sendo possível se conectar com o mundo com apenas um click. Kumar (2006, p. 49) afirma que:

> A nova era de informação opera em um contexto global. O homem não tem mais a necessidade de busca-la, já que ela pode ser trazida ao lar ou ao escritório. Uma rede eletrônica mundial de biblioteca, arquivos, e banco de dados surgiu, teoricamente acessível a qualquer pessoa, em qualquer lugar e a qualquer momento.

A expressão “sociedade da informação” passou a ser muito utilizada nestes últimos anos. Castells (1999) defende que a revolução tecnológica deu origem ao informacionalismo, tornando-se assim a base material desta nova sociedade, em que os valores da liberdade individual e da comunicação aberta tornaram-se supremos. Segundo o autor, no informacionalismo, as tecnologias assumem um papel de destaque em todos os segmentos sociais, permitindo o entendimento da nova estrutura social – sociedade em rede – e consequentemente, de uma nova economia, na qual a tecnologia da informação é considerada uma ferramenta indispensável na manipulação da informação e construção do conhecimento pelos indivíduos, pois “a geração, processamento e transmissão de informação torna-se a principal fonte de produtividade e poder” (CASTELLS, 1999, p. 21).

Já Castells (2002, p. 67), define as características dessa nova sociedade da informação ou sociedade pós-industrial:

- A informação é a sua matéria-prima – Existe uma relação simbiótica entre a tecnologia e a informação, em que uma complementa a outra, fato este que diferencia esta nova era das revoluções anteriores, em que era dada proeminência a um aspecto em detrimento de outro;
- Capacidade de penetração dos efeitos das novas tecnologias – Refere-se ao poder de influência que os meios tecnológicos exercem na vida social, econômica e política da sociedade;

- Lógica de redes – É uma característica predominante deste novo modelo de sociedade, que facilita a interação entre as pessoas, podendo ser implementada em todos os tipos de processos e organizações, graças às recentes tecnologias da informação;
- Flexibilidade – Esta característica refere-se ao poder de reconfigurar, alterar e reorganizar as informações;
- Convergência de tecnologias específicas para um sistema altamente integrado – O contínuo processo de convergência entre os diferentes campos tecnológicos resulta da sua lógica comum de produção da informação, onde todos os utilizadores podem contribuir, exercendo um papel ativo na produção deste conhecimento.

Estas características estão ligadas ao processo de disseminação do conhecimento, uma vez que surgem novos espaços para busca e compartilhamento de informações, democratizando assim o saber.

No entanto, apesar de tantas informações disponíveis, surgem dois problemas: primeiro, que uma grande parcela da população ainda não tem acesso à internet e segundo, que ter acesso às informações não é uma garantia de geração de conhecimento (CASTELLS, 2002, p. 69).

> O que caracteriza a revolução tecnológica atual não é o caráter central do conhecimento e da informação, mas a aplicação deste conhecimento e informação a aparatos de geração de conhecimento e processamento da informação/comunicação, em um círculo de retroalimentação acumulativa entre a inovação e seus usos" (CASTELLS, 2002, p. 69).

Neste contexto, surge um novo tipo de sociedade, a sociedade em rede, que Castells e Cardoso (2005, p. 17) conceitua como:

> A sociedade em rede, em termos simples, é uma estrutura social baseada em redes operadas por tecnologias de comunicação e informação fundamentada na microeletrônica e em redes digitais de computadores que geram, processam e distribuem informação a partir do conhecimento acumulado nos nós dessas redes.

É evidente que os indivíduos estão diante de uma transformação não só cultural mas também econômica, pelos mecanismos de um novo paradigma tecnológico que se organiza com base nas tecnologias de informação (SILVA, 2006). Em suma, a sociedade atual vive em um mundo digitalizado.

O ciberespaço, ou rede, é um novo meio de comunicação que interliga o mundo através do acesso à internet. Esse termo não especifica apenas a infraestrutura material da comunicação digital, mas a grande variedade de informações que ele abriga assim com as pessoas que navegam e alimentam esse universo das mais diferentes formas, como lazer, trabalho, pesquisa científica entre outros. Cibercultura é um conjunto de técnicas, práticas, atitudes de modos de pensamentos e valores que são desenvolvidos juntamente com o crescimento do ciberespaço (LEVY, 1999).

Lemos e Cunha (2003) definem que a cibercultura é a relação entre a sociedade, a cultura e as novas tecnologias que surgiram com a convergência das telecomunicações com a informática na década de 70.

A cibercultura está cada vez mais presente na vida das pessoas, ela representa o modo de viver da sociedade, modificado pelo uso da tecnologia. Essas se mudanças se intensificaram depois da possibilidade de poder estar conectado a qualquer hora ou momento, recriando assim uma nova forma de comunicação entre a sociedade, tendo como característica marcante a cooperação, onde as pessoas trocam e compartilham informações.

Lemos e Cunha (2003) descrevem o que para eles seriam as leis da cibercultura. A primeira lei é a lei da reconfiguração, quer dizer que mesmo com o avanço da tecnologia não deixamos de lado os costumes, mas sim o reconfiguramos para o novo modo de vida. Como exemplo disso, há alguns anos era necessário dirigir-se até o banco para fazer pagamentos, transferências, hoje com a facilidade do mudo virtual é possível resolver pelo computador ou até com um aplicativo para smartphones. A segunda lei é a liberação dos polos de emissão, ela está presente nas novas formas de relacionamento social, onde as pessoas podem elaborar, opinar e compartilhar informações livremente e assim promover uma movimentação social na rede. A terceira e última lei é a lei da conectividade generalizada, com ela pode-se entender que com as mudanças tecnológicas as pessoas sentem a necessidade de estarem conectadas. E essa conexão é possível entre as pessoas ou entre as pessoas e o dispositivo informático para navegação que passam a trocar informação de forma autônoma e independente.

Lévy (1999) define os três princípios que orientam o crescimento do ciberespaço. O primeiro é a interconexão, sendo possível a comunicação dos indivíduos independente da sua localização, quebrando barreias físicas e espaciais.

O segundo, as comunidades virtuais, um meio de socialização, quer suas finalidades sejam lúdicas, econômicas ou intelectuais, com os mais diferentes objetivos, como conhecer pessoas, manter contato, se relacionar, entre outros. O terceiro e último é a inteligência coletiva, que seria o modo de realização da humanidade que a rede digital favorece, sem que saibam a *priori* em direção a quais resultados tendem as organizações que colocam em sinergia seus recursos intelectuais.

Nesse sentido, para Silva (2006), entre os diversos autores que abordam o tema, há um destaque para Castells (2002) e Lévy (1999), pois ambos comprovam, baseados em suas pesquisas, que as transformações culturais e socioeconômicas do mundo atual, são decorrentes do uso e propagação das novas tecnologias de informação.

Muitos autores tentam criar outras definições para a sociedade em rede. Dowbor (2002) se refere à sociedade em rede como uma conectividade instantânea onde qualquer ser humano, independentemente de onde esteja, consegue comunicar-se com qualquer pessoa do planeta apenas com o uso da internet.

A sociedade em rede é denominada por Rheingold de comunidade virtual, que por sua vez caracteriza da seguinte forma:

> As comunidades virtuais são agregados sociais que surgem da Rede [Internet], quando uma quantidade suficiente de gente leva adiante essas discussões públicas durante um tempo suficiente, com suficientes sentimentos humanos, para formar redes de relações pessoais no espaço cibernético [ciberespaço]. (RHEINGOLD,1996 apud RECUERO, 2005, p. 20).

Para Recuero (2005, p. 12), “a comunidade virtual é um grupo de pessoas que estabelecem entre si relações sociais, que permaneçam um tempo suficiente para que elas possam constituir um corpo organizado, através da comunicação mediada por computador”.

A sociedade virtual se caracteriza, portanto, como uma conexão onde as pessoas trocam informações, onde é muito comum ver infinidades de grupos, formados por assuntos afins, na internet e através destes, as pessoas se identificam e formam uma rede onde ocorre a troca de conhecimento entre os participantes. Com isso surgem novos grupos tornando-a assim cada vez maior.

2.2 Revolução da Internet

Não se pode negar que a tecnologia tem impacto significativo na vida das pessoas. Para chegar até aqui a humanidade passou por várias transformações que culminaram no desenvolvimento tecnológico que se observa atualmente. Diferentemente do como a maioria pensa, o mundo não está passando por uma terceira revolução industrial, mas sim por uma revolução tecnológica decorrente da evolução da informação. Para Languer (2004, p 26):

> A informação não deve ser reduzida ao desenvolvimento tecnológico de comunicações, como a Internet ou a televisão, portanto, aos meios. A informação é também conteúdo, pois ela pode ser registrada, arquivada, calculada ('computada') em máquinas e artefatos que se tornam 'informatizados' e não automatizados, como se diz frequentemente.

Entretanto, é possível observar que a revolução tecnológica pode ser considerada como a responsável pelo que chamamos de "desemprego tecnológico", onde a mão de obra humana perde espaço para a mão de obra automatizada, que cresce à medida junto com os novos avanços tecnológicos.

Pode-se comparar a revolução tecnológica com as revoluções industriais, pois ambas causaram grandes transformações na sociedade. A Revolução Industrial do século XVIII teve sua primeira mudança com a implementação das máquinas a vapor gerando assim um impacto no modo de produção. A segunda Revolução Industrial, século XIX, teve como fato central a invenção da energia elétrica, que para Castells (2002) o que a segunda Revolução Industrial tem em comum com a revolução tecnológica é o conhecimento científico. Para ele, o que caracteriza a revolução tecnológica não é a centralidade de conhecimento e informação, mas a aplicação desses conhecimentos e informações para gerar um ciclo de realimentação cumulativo entre a inovação e seu uso.

Para Castells (2002, p. 68):

> A tecnologia da informação é para esta revolução o que as novas fontes de energia foram para as revoluções industriais sucessivas, do motor a vapor à eletricidade, aos combustíveis e até mesmo à energia nuclear, visto que a geração e distribuição de energia foi o elemento principal na base da sociedade industrial" (2002, p. 68).

Uma das principais causadoras dessa revolução tecnológica foi a internet. A internet que surgiu para fins militares em meados dos anos 60, no intuito de trocar

informações, onde o emissor ao enviar mensagens teria a certeza de que o receptor receberia mesmo que o terminal emissor fosse destruído.

Com a popularização da internet surge então a chamada por Castells de revolução da tecnologia da informação. “As redes interativas de computadores estão crescendo exponencialmente, criando novas formas e canais de comunicação, moldando a vida e, ao mesmo tempo, sendo moldadas por ela” (CASTELLS, 2002, p.40).

A tabela a seguir mostra o crescimento dos usuários de internet no mundo nos últimos 17 anos.

Tabela 1: Uso da internet no mundo

Regiões do mundo	População 2018	Usuário de internet em 31/12/2000	Usuário de internet em 31/12/2017	Penetração na população 2017	Crescimento de usuário 2000-2018	Usuário de internet
África	1,287,914,329	4,514,400	453,329,534	35,2 %	9.941%	10.9%
Ásia	4,207,588,157	114,304,000	2,023,630,194	48.1%	1.670%	48.7%
Europa	827,650,849	105,096,093	704,883,752	85.2%	570 %	17.0%
Oriente Médio	254,438,981	3,284,800	164,037,259	64.5%	4,893 %	3.9%
América do Norte	363,844,662	108,096,800	345,660,847	95.0%	219%	8.3%
América Latina e Caribe	652,047,996	18,068,919	437,001,277	67.0%	2,318%	10.5%
Oceania e Austrália	41,273,454	7,620,480	28,439, 277	68.9%	273%	0.7%
Total Mundial	7.634.758.428	360,985,492	4,156,932,140	54.4%	1052.0%	100%

Fonte: Internet World Stats. 2018. http://www.internetworldstats.com/stats.htm

Com a tabela, verifica-se que a internet mundial cresceu 1052% ao longo desses anos. É possível notar também que a economia afeta o crescimento do uso, visto que países desenvolvidos tende a ter mais poder de aquisição para a compra de equipamento eletrônico.

Nesta mesma pesquisa, o Brasil aparece em dezembro de 2017 com mais de 149 milhões de usuários de internet. Segundo dados da PNAD (Pesquisa Nacional por Amostra de Domicílio) realizada pelo IBGE em 2016, constatou-se que a Internet era utilizada em 69,3% dos 69 318 mil domicílios particulares permanentes do País. A utilização da Internet já estava disseminada na maioria dos domicílios em todas as Grandes Regiões, sendo usada em 76,7% das residências da Sudeste, 74,7% da Centro-Oeste e 71,3% da Sul, ficando em 62,4%, na Norte, e 56,6%, no Nordeste.

Pesquisa divulgada pela Secretaria de Comunicação Social da Presidência da República e realizada pela Pesquisa Brasileira de Mídia 2016 mostra que os brasileiros ficam conectados, em média, 4h44m por dia durante a semana e 4h32m nos finais de semana, superior ao tempo médio em que ficam expostos ao televisor, respectivamente 4h31m e 4h14m. A pesquisa mostra ainda que os usuários utilizam a internet, principalmente, para se informar (67%) - sejam notícias ou informações de modo geral -, para se divertir (67%), para passar o tempo livre (38%) e para estudar (24%).

Entre os internautas, 92% estão conectados por meio de redes sociais, sendo as mais utilizadas o *Facebook* (83%), o *Whatsapp* (58%) e o *Youtube* (17%). O *Twitter*, popular entre as elites políticas e formadores de opinião, foi mencionado por apenas 5% dos entrevistados, como mostra a Tabela 2 abaixo:

Tabela 2. Internautas conectados por meio de redes sociais.

Facebook	**83%**
Whatsapp	58%
Youtube	17%
Instagram	12%
Google+	8%
Twitter	5%
Skype	4%
Linkedin	1%
Outros	1%
Não utiliza	6%

Fonte: Pesquisa Brasileira de Mídia, 2015.

Esse novo mundo virtual trouxe consigo diversas comodidades como: acesso à conta bancária para pagamentos de contas, reuniões empresariais com pessoas ao redor do mundo sem sair da empresa, relacionamento entre as pessoas por meio das redes sociais. As ligações de voz vêm sendo substituídas pelos aplicativos de troca instantânea de mensagem, as pessoas querem estar conectadas em tempo integral, seja utilizando o e-mail, navegando na internet ou alimentando a sua página na rede social, isso fez com que houvesse um crescimento tanto no número de vendas de smartphone como no uso da internet pelo celular.

Com a comodidade de compra ou venda de produtos e serviços pela internet, fez com que o e-commerce (comércio virtual) tivesse um aumento significativo para a economia. Segundo dados do E-bit, empresa responsável por fornecer certificação de excelência para lojas virtuais através de depoimentos dos usuários, e que, além disso, é referência na divulgação de informações do e-commerce no Brasil, estima-se que o país terá um faturamento de 53,5 bilhões neste ano de 2018.

Chega-se a era da mobilidade onde, segundo Lemos (2002), a cibercultura desenvolve-se de forma onipresente fazendo com que o usuário não se desloque até a rede e sim a rede que passa a envolver os usuários numa conexão generalizada. A mobilidade está tão presente que fica difícil imaginar como seria a realização de determinadas tarefas sem o uso da internet. Weiser (1991, apud LEMOS 2005) afirma que “as tecnologias mais profundas são aquelas que desaparecem. Elas se entrelaçam no tecido da vida cotidiana até se tornarem indistinguíveis.”

O principal meio de mobilidade são os aparelhos celulares que Lemos (2005) considera como o controle remoto do cotidiano, afinal, com ele é possível realizar as mais diversas tarefas, entre trabalho e lazer.

Vive-se a era da abolição do espaço físico geográfico (LEMOS, 2003), pois o usuário não vai mais ao ponto de rede e sim é a rede que o envolve (LEMOS, 2005). Isso acontece devido a popularização do wifi onde é cada vez mais frequente locais públicos e privados oferecerem aos seus usuários o acesso à rede.

Apesar das inúmeras vantagens que a internet trouxe, algumas pessoas de má fé utilizam-se desse avanço para se beneficiar aplicando os mais variados tipos de golpes, e esses tipos de crimes serão abordados no tópico seguinte.

2.3 Crimes na Internet

É impossível saber como seria o mundo atual se não existisse internet, pois esta se destaca por ser a maior ferramenta de comunicação e um marco para a revolução tecnológica.

Entretanto, é inegável que esse avanço tecnológico que beneficia milhares de pessoas ao redor do mundo, também traz consequências negativas e que causam diversos transtornos à vida dos mesmos. Um exemplo disso é o surgimento de novos crimes cometidos através do acesso à rede.

De acordo com Ferreira (2000, p. 207), os primeiros crimes cometidos por meio da internet originam da década de 60, através de “manipulações, sabotagens, espionagens e o uso abusivo de computadores e sistemas, denunciados em matérias jornalísticas”.

Com o passar dos anos, os delitos cometidos no meio virtual passaram a atuar em maiores proporções. *Crackers*, responsáveis por cometer crimes na rede, passaram a atuar em manipulações de contas bancárias, na pirataria de programas de computadores, entre outros. Neste momento, percebia-se como este novo meio de comunicação era vulnerável a estes ataques e da necessidade de se criar mecanismos de defesa que fossem capazes de proteger o usuário.

É importante diferenciar os termos *hacker* e *cracker*, os dois tem bastante conhecimento sobre informática, mas *hacker* é uma pessoa que testa a segurança do sistema identificando possíveis falhas, já o *cracker* tem o objetivo de utilizar esse tipo de conhecimento para furtar informações e danificar sistemas. Assim, o *cracker* pode ser classificado como criminoso.

Neto e Guimarães (2003, p. 69) destacam que “a informática permite não só o cometimento de novos delitos, como potencializa alguns outros tradicionais”. É o caso de pornografia infantil, que desde a década de 80 já era praticada entre os usuários. Para Pinheiro (2006, p. 21), não se pode esquecer que na maioria das vezes a Internet é apenas “um instrumento de ação dos cybercriminosos”. Alguns autores classificam os crimes virtuais em puros, mistos e comuns.

Neto e Guimarães (2003) definem que o crime virtual puro se caracteriza pela invasão indevida de dispositivo informático, seja ela para obter ou danificar informações atrás do sistema de Software ou Hardware. No crime virtual misto, o invasor não tem a intenção de danificar o sistema, mas a sua utilização é indispensável à prática do delito, como por exemplo, o uso do computador para invadir contas bancárias com o objetivo de fazer transações ilegais entre as contas, e no crime virtual comum, o infrator utiliza o sistema para praticar o crime já previsto em lei, como acontece com a pornografia através de perfis falsos nas redes sociais.

Atualmente são vários os tipos de crimes cometidos na rede. Dentre essas condutas criminosas existentes, podemos citar as mais comuns como: crimes contra honra, crimes contra a liberdade individual, crimes contra o patrimônio, crime contra os costumes. Todos esses crimes estão presentes no Código Penal Brasileiro. Vale

ressaltar que todos esses crimes utilizam a internet como meio de se obter vantagem do usuário do computador alvo.

Com as inúmeras formas da prática de crimes cibernéticos há uma necessidade de identificação de que tipo de crime foi praticado para, assim, começar o processo de investigação. Segundo Wendt e Jorge (2012, p. 52), o processo de investigação se divide em duas fases que ele nomeia como: fase técnica e fase de campo. A fase técnica tem o objetivo de localizar o computador utilizado para o crime. Nessa fase é preciso fazer análise das informações fornecidas pela vítima, orientá-la para que sejam preservadas as provas do delito e como ela pode se proteger de novos crimes e a partir disso começar a coleta de provas no ambiente virtual. Em seguida, registra-se o boletim de ocorrência para que se comece a investigação na internet tentando identificar os possíveis criminosos através de origem de e-mail, registro e hospedagem de domínio. Após essa investigação é feito o relatório de provas coletadas para apuração preliminar. Com essas provas é possível pedir autorização judicial para a quebra de dados, conexão ou acesso ou ainda, e se necessário, solicitar aos provedores dados cadastrais do infrator. A última parte da fase técnica consiste em analisar as informações prestadas pelo provedor de conexão ou provedores de conteúdo.

Na fase de campo, o objetivo é o reconhecimento do local onde está armazenado o dispositivo. Essa fase só pode ser feita com mandato judicial.

Felizmente, no Brasil já existe em alguns estados delegacias especializadas para crimes praticados na internet. De acordo Emerson Wendt (2014), os estados são: São Paulo, Rio Grande do Sul, Paraná, Rio de Janeiro, Espírito Santo, Minas Gerais, Piauí, Pará, Tocantins, Maranhão, Pernambuco, Sergipe, Bahia, Mato Grosso, Goiás e Rondônia.

Nessa nova era tecnológica, um dos grandes desafios é encontrar e punir esses cybercriminosos. Durante anos, a maioria dos crimes cometidos virtualmente era tipificada no Código Penal Brasileiro, entretanto, sentia-se a necessidade de se criar uma legislação jurídica específica que pudesse punir os criminosos e proteger os usuários, assunto a ser tratado na próxima sessão.

2.4 Legislação da Internet

Com o uso cada vez mais frequente da internet e a falta de uma legislação vigente, fez-se necessária a promulgação em 30 de novembro de 2012 de duas leis federais que punissem infratores contra crimes cometidos na internet. São elas: a Lei n.º 12.735 e a Lei n.º 12.737.

Segundo Oliveira (2013), a Lei nº 12.735 originou do projeto de Lei nº 84/1999 conhecido por Projeto Azeredo, passando mais tarde para o projeto de Lei nº 89/2003. Esse projeto, para muitos, era a tentativa de barrar o desenvolvimento tecnológico, seus artigos não punitivos poderiam representar ameaça a liberdade de expressão. O projeto original continha 18 artigos, destes, foram encaminhados à sanção da presidente Dilma Rousseff apenas 5, sendo aprovados 4. Após sancionado, o projeto de Lei passou a ser a Lei nº 12.735/2012.

Esta Lei tipifica condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências. Esta lei alterou o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989.

A Lei 12.737/2012, batizada de Lei Carolina Dieckmann e originada do projeto de Lei 2793/2011, foi sancionada sob pressão da mídia devido às fotos íntimas da atriz Carolina Dieckmann terem sido furtadas e publicadas indevidamente na internet. Vale ressaltar que antes desse fato, a Revista Época publicou em 2011 uma onda de ataques de *hacker*s e *crackers*, no qual diversos sites do país foram invadidos.

A Lei nº 12.737/12 dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências. Ela é considerada por muitos um avanço no que diz respeito ao crime cibernético. Em seu artigo 2º ela acrescenta os Artigos 154-A e o 154-B no Decreto-Lei nº 2.848 – Código Penal.

> Invasão de dispositivo informático
> Art.154-A Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita.
> Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

> § 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no caput.
> § 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

Este novo artigo vem a combater a invasão do dispositivo informático alheio, conectado ou não à rede de internet, independente do objetivo final. Esse tipo de crime é caracterizado por crime puro, pois o delito é praticado pelo chamado cracker.

A pena de detenção de 3 (três) meses a 1 (um) ano e a multa é aumentada de um sexto a um terço se a invasão resultar prejuízo econômico. Conforme Oliveira (2013), com a comodidade de pagamento através de aplicativos do banco, faz com que as pessoas disponibilizem dados da sua conta bancária na rede, esse artigo tem intuito de punir e inibir essa prática.

> § 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:
> Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.
> § 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.
> § 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:
> I - Presidente da República, governadores e prefeitos;
> II - Presidente do Supremo Tribunal Federal;
> III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou
> IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal" (BRASIL, 2012b).

No parágrafo terceiro, se caso a invasão resulte na obtenção de conteúdo sigiloso de informações comerciais ou industriais, prevê reclusão de 6 (seis) meses a 2 (dois) anos, e multa se a conduta não constituir crimes mais grave. Caso haja divulgação, comercialização ou transmissão dos dados obtidos como previsto no parágrafo terceiro, aumenta-se a pena de um a dois terços. Muitos desses crimes são praticados contra grandes empresas onde as mesmas contêm registros sigilosos na rede. Com a inclusão deste artigo no Código Penal passou-se a ter uma proteção legal.

Existe uma falha da lei nesse artigo que segundo Oliveira (2013, p. 43) “não se caracteriza crime, caso o dispositivo informático não contenha antivírus ou venha haver um furto de senhas no momento que o usuário digitar para entrada de um sistema. Pois, no *caput* do artigo acaba por condicionar a invasão do dispositivo a uma violação de mecanismo de segurança”.

> Ação penal
> Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos” (BRASIL, 2012b)

O artigo 154-B, “traz a identificação da ação penal como pública condicionada à representação, desta maneira, para que haja a persecução penal faz-se necessário que a vítima apresente o pedido perante a autoridade pública” (OLIVEIRA, 2013, p. 47). Ele também prevê que no caso de crime cometido contra administração pública ou empresas concessionárias de serviço público, não necessita de provocação para que a ação seja iniciada.

Em seu artigo 3º, a Lei altera a redação dos Arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, que passam a vigorar com seguinte texto:

> Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública
> Art. 266. .....
> § 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.
> § 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)
>
> “Falsificação de documento particular
> Art. 298. .....
> Falsificação de cartão
> Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito. (NR)” (BRASIL, 2012b)

Em relação ao Art. 266, passa a ser crime a interrupção de serviços telefônicos e das demais formas de comunicação atuais. Esta foi uma atualização muito importante dada a atual sociedade tecnológica atual.

Sobre o Art. 298, a alteração do parágrafo único faz a equiparação entre o cartão de crédito ou débito com o documento particular.

> Antes dessa mudança, a falsificação de cartão de crédito só poderia ser punida com a utilização deste, na forma do delito de estelionato Art. 171 do Código Penal, tendo em vista a vantagem ilícita obtida no momento em que as operações de crédito eram realizadas. Desta feita, a clonagem do dispositivo magnético em nada representava para a lei. (OLIVEIRA, 2013, p. 50).

Outra lei muito importante para a legislação da internet é a lei nº 12.965/2014, denominada de Marco Civil, que foi aprovada com intuito de regulamentar o acesso à internet no Brasil, garantindo assim direitos e deveres para os usuários e para as empresas. Segundo Junior (2014), o projeto de Lei nº 2.126 teve início em 2011, passou pelo plenário e por várias comissões, foi proposta sujeita à apreciação do Plenário várias vezes, foi proposto também em apreciação pela Câmara dos Deputados, mas foi cancelado. No início de 2014 o projeto foi novamente trazido em pauta, sendo finalmente aprovado. A Lei foi sancionada pela presidenta simbolicamente na Conferência Internacional (NETMundial) e foi pulicada no Diário Oficial da União dia 24 de abril de 2014.

Todavia, mesmo com a aprovação das leis, Silva (2011) ressalta que é necessário que o usuário use do bom senso e cautela ao utilizar dos serviços disponíveis na rede, pois estes ainda são as melhores precauções contra estes crimes.

O Marco Civil da internet segundo Gomes Júnior (*et al*., 2014),

> traz em seus dispositivos a garantia à defesa dos consumidores que usam a Internet para adquirirem produtos e serviços; regula a comercialização das empresas que utilizam a rede mundial de computadores como meio de comércio, assegurando a regime de livre iniciativa, bem como a livre concorrência; Além de reger os serviços prestados pelos provedores de Internet, estipulando o fornecimento com segurança e a garantia da funcionalidade, sob responsabilidade dos agentes prestadores".

No Art. 2º da Lei prevê a liberdade de expressão e no Art 3º prevê além da liberdade de expressão, a proteção e privacidade dos dados. Essa proteção se estende ao Art 7º, pois nele se garante a inviolabilidade da vida privada e do acesso a suas comunicações na internet, sendo solicitada apenas em caso judicial, assim como a manutenção da qualidade da conexão contrata sendo de dever da prestadora de serviços não divulgar seus dados pessoais, ou registro de conexão para terceiros. Para o Comitê Gestor de Internet no Brasil (CGI.br), a proteção da privacidade é importante porque, principalmente: garante uma relação de confiança entre usuários, empresas e governos no meio digital; protege a criatividade e a

liberdade de expressão e de escolha do usuário, na medida em que protege sua intimidade.

Da neutralidade da rede, no artigo 9º diz que a empresa responsável pelo fornecimento de internet deve tratar de maneira igualitária independente do pacote de dados escolhido, sem distinção por conteúdo, origem e destino, serviço terminal ou aplicação. Portanto, fica proibido que essa empresa bloquei ou monitore qualquer acesso.

Segundo Silva (2011 p. 7),

> não acreditar em propostas impossíveis ou onde haja uma desproporção entre preço e o bem a ser adquirido; se o usuário for pessoa jurídica e manusear informações confidenciais dentro do estabelecimento, isolar, se possível, uma rede interna que não se interligue na Internet daquela que é conectada à Internet, o que evitaria a invasão de *hackers*; ter um programa de segurança (Antivírus) atualizado.

Dessa forma, observa-se que o uso da internet com cautela pode evitar consequências desastrosas, e no caso de casos imprevistos podemos recorrer à nossa Legislação.

Pode-se observar que o mundo cibernético está inserido cada vez mais no cotidiano da sociedade, é inegável os benefícios que esse mundo trouxe, mas, mesmo com tantas facilidades é necessário estar atento para não cair nos mais diversos golpes e crimes praticados na rede ou através dela.

Mesmo sabendo que existem leis que amparem os mais diversos crimes cibernéticos, a população também precisa fazer sua parte tendo atenção e cuidado no uso da internet.

Na sequência, apresenta-se uma revisão da literatura sobre o tema a fim de fundamentar este trabalho.

2.5 Estado da Arte

Os artigos e as pesquisas realizadas na área de segurança virtual ainda são poucos, em virtude de ser um campo de estudo novo e que ainda não atingiu uma grande quantidade de pessoas. Com o intuito de contribuir e enriquecer este campo de pesquisa com um referencial teórico baseado na legislação brasileira, a que o presente trabalho se propõe, foram observados e destacados os artigos produzidos

em nosso país. Para uma melhor visualização, apresenta-se na Tabela 3 os trabalhos encontrados com suas informações principais.

Tabela 3. Principais informações das produções analisadas.

Autoria	Título	Local e ano de publicação	Tipo de publicação	Palavras chave
CERNEV, Adrian Kemmer.	Segurança na Internet: A percepção do usuário como fator de restrição ao crescimento do comércio eletrônico no Brasil.	Fundação Getúlio Vargas, 2002.	Dissertação de Mestrado.	Internet. Comércio eletrônico. Comércio eletrônico – barreiras. Comércio eletrônico – segurança. Confiança do usuário. Percepção do usuário.
OLIVEIRA, Jôline Cristina de.	O Cibercrime e as Leis 12.735 e 12.737/2012	Universidade Federal de Sergipe, 2013.	Trabalho de Conclusão de Curso.	Cibercrime. Leis 12.735 e 12.737/2012. Tipos Informáticos.
SANTOS, Danielly Maia dos.	Os Novos Crimes de Informática Criados com o Advento das Leis 12.735/2012 e 12.737/2012.	Faculdades Integradas "Antônio Eufrásio De Toledo", 2014.	Monografia.	Internet. Crime. Código Penal. Código de Processo Penal. Lei 12.735/2012. Lei 12.737/2012.
SILVA, Vergilio Ricardo Britto da.	Preocupação com a Privacidade na Internet: Uma pesquisa exploratória no cenário brasileiro.	Pontifícia Universidade Católica do Rio Grande do Sul, 2015.	Dissertação de Mestrado.	Segurança da Informação. Privacidade na Internet. Preocupação com a Privacidade. Acesso Indevido. Coleta de Dados. Uso Secundário. Controle sobre as Informações. Risco à Privacidade. Sensibilidade da Informação.

Cernev (2002) realizou pesquisa onde analisa a questão da segurança na compra eletrônica do ponto de vista dos usuários de Internet, uma vez que a percepção de segurança dos internautas determina a sua confiança, e a sua confiança influencia a sua decisão de compra eletrônica e a abrangência das compras realizadas através da Internet. Com o estudo pode-se verificar que a percepção de segurança dos usuários sobre o comércio eletrônico não afeta o crescimento ou a queda das vendas.

No que se trata de legislação na Internet, foram encontrados dois trabalhos que se achou pertinente fazer suas análises. Oliveira (2013) no seu trabalho intitulado “O cibercrime e as leis 12.735 e 12.737” faz uma análise através de pesquisa bibliográfica sobre as leis brasileiras de acesso à internet vigentes e seu histórico, o cibercrime e os tipos de delitos cometidos. No decorrer do trabalho explica a mudança de comportamento da sociedade depois da internet e como a sociedade está vulnerável aos maliciosos que praticam delitos na rede.

Ainda sobre legislação da internet, Santos (2014) com o tema “Os novos crimes de informática criados com o advento das leis 12.735 e 12.737”, aborda a parte histórica do computador e da internet mostrando quando e para que fim surgiu, em seguida fala sobre a relação do direito com a informática. Em relação à legislação faz um levantamento de como os crimes eram julgados antes da legislação vigente específica, e em seguida, analisa as lei 12.735 e 12737, e faz uma explanação não muito aprofundada da Lei 12.795, devido ao fato que a lei foi sancionada no período de finalização da pesquisa. Concluí que a edição de novas leis não será eficaz para o combate aos crimes de informática, já que também é necessário investimento na criação de novos meios de apuração dos crimes, ou seja, na criação de delegacias especializadas e também no treinamento de todos os envolvidos no processo de investigação dos crimes de informática, restabelecendo assim a segurança jurídica, garantindo a paz social e a manutenção do Estado Democrático de Direito.

No estudo sobre privacidade na internet, Silva (2015) procurou identificar o grau de preocupação com a privacidade dos usuários de internet no Brasil. Os resultados indicam um alto grau de preocupação com a privacidade dos usuários de Internet do Brasil, principalmente nas regiões Sul e Sudeste, que apresentaram os maiores índices de preocupação. Entre as informações apontadas como mais sensíveis estão, em ordem de maior preocupação, senhas, número de cartão de crédito, número de conta corrente e agência, saldo bancário, gastos com cartão de crédito e limite de cheque especial. Entre as informações menos sensíveis estão orientação sexual, vícios, escola onde estudou ou estuda, data de nascimento e notas escolares.

2.5.1 Contribuições do estado da arte

Os trabalhos descritos darão grande contribuição para esta pesquisa, principalmente no que concerne ao embasamento teórico, pois a análise das leis de um ponto de vista jurídico nos permite entender melhor como as autoridades podem agir em casos de crimes virtuais e como os usuários devem se prevenir para evitar estes crimes.

Os trabalhos sobre privacidade e comércio eletrônico também nos dão uma ideia de como os usuários se comportam diante da rede, nos guiando pelo procedimento metodológico proposto.

3 METODOLOGIA

Neste capítulo apresentam-se as escolhas metodológicas adotadas para execução desta pesquisa. Apresentam-se as questões que orientam o estudo, em seguida, caracterização de pesquisa, estratégia de pesquisa que será utilizada, o universo e a amostra, a estratégia a ser utilizada para coleta de dados, as variáveis e os indicadores e o processamento de análise dos dados.

3.1 Questões da Pesquisa

A pesquisa teve como objetivo geral verificar as percepções dos usuários de redes sociais virtuais sobre as leis brasileiras de acesso à internet. Nessa etapa foram traçados questões para achar respostas à problemática e assim atingir os objetivos propostos, conforme seguem:

a) Quais as características demográficas e econômicas dos usuários das redes sociais virtuais?
b) Quais as formas de acesso às redes sociais virtuais?
c) Quais as medidas preventivas de segurança tomadas pelos usuários no acesso à rede?
d) Como identificar a aplicabilidade do conhecimento das leis na segurança individual no acesso à internet?

3.2 Caracterização do Estudo

O estudo em questão é caracterizado como descritivo. Essa abordagem foi escolhida pela necessidade de descrever o comportamento dos fenômenos identificando e obtendo informações sobre o problema.

A pesquisa descritiva tem como objetivo conhecer as diversas situações e relações que ocorrem à vida social política, econômica e os demais aspectos do comportamento humano (CERVO *et al*, 2007, p. 62).

Adotando uma classificação ampla, pode-se dizer que há duas grandes abordagens de pesquisas: o quantitativo e o qualitativo. Os métodos se diferenciam não só pela sistemática que pertencem a cada uma delas, mas sim pela forma de abordagem do problema (RICHARDSON, 2012).

A abordagem quantitativa é caracterizada pela coleta de dados estatísticos. Representa em princípio, a intenção de garantir a precisão de resultados evitando distorções de análise e interpretação, possibilitando, assim, uma margem de segurança quanto às inferências (RICHARDSON, 2012). Quanto à abordagem qualitativa, "justifica-se, sobretudo, por ser uma forma adequada para entender a natureza de um fenômeno social" (RICHARDSON, 2012, p. 79).

Sendo assim, nesta pesquisa optou-se por uma abordagem quantitativa, dada as características do objeto de estudo, permitindo enfatizar os pontos de vista dos sujeitos envolvidos na pesquisa.

3.3 Estratégia de Pesquisa

Entre as estratégias para o método quantitativo, optou-se por realizar o levantamento de campo (*survey)*. As pesquisas deste tipo se caracterizam pela interrogação direta das pessoas cujo comportamento se deseja conhecer.

Segundo Gil (2008, p. 55), basicamente, "procede-se à solicitação de informações a um grupo significativo de pessoas acerca do problema estudado para em seguida, mediante análise quantitativa, obter as conclusões correspondentes dos dados coletados".

Gil (2008) aponta ainda como as principais vantagens dos levantamentos: o conhecimento direto da realidade, economia e rapidez e a quantificação dos dados obtidos. Entre as limitações, o autor cita: a ênfase nos aspectos perspectivos, pouca profundidade no estudo da estrutura e dos processos sociais, e limitada apreensão do processo de mudança.

3.4 Universo de Estudo e Amostra

Segundo Eco (2009, p. 10), "quanto mais se restringe o campo, melhor e com mais segurança se trabalha". Com isso, para este estudo o universo da pesquisa será a população da zona urbana da cidade de Umbaúba – Sergipe, com idade acima de 18 anos. Segundo dados do Censo Demográfico 2010, esta população é composta de 9.833 pessoas (IBGE, 2010).

O tamanho mínimo da amostra aleatória e estratificada da população finita foi calculado pelas seguintes equações estatísticas (BARBETTA, 1999, p. 58):

$$No = \left(\frac{1}{Eo}\right)^2; \quad e\ N = \frac{No \times P}{No + P}$$

Onde:

Eo = o erro experimental;

No = a amostra adimensional;

P = a população; e

N = a amostra final.

Para o nosso caso, admitindo um erro experimental de no máximo 10%, têm-se:

$$No = \left(\frac{1}{Eo}\right)^2 \rightarrow \qquad No = \left(\frac{1}{0{,}1}\right)^2 \rightarrow \qquad No = 100$$

$$N = \frac{No \times P}{No + P} \rightarrow \quad No = \frac{100 \times 9.833}{100 + 9.833} \rightarrow \quad No = \frac{983.300}{9.933} \rightarrow \quad No = 98{,}99$$

Que arredondando para o número inteiro acima, é igual a 100 habitantes.

3.5 Estratégia de Coleta de Dados

Nesta pesquisa, o instrumento de coleta de dados utilizado foi um questionário.

Para Hair Jr. *et al*. (2005, p. 157 e 159), “os questionários são usados para coletar dados quantitativos de um número maior de indivíduos de uma maneira relativamente rápida e conveniente”.

O questionário (apêndice 1) que foi utilizado conteve perguntas fechadas, que facilitaram a percepção quanto à realidade do sujeito pesquisado e do universo de estudo em questão. Os questionários foram aplicados no período de 02 a 20 de fevereiro de 2016, sendo obtidos um total de 100 respostas válidas.

3.6 Definições das Variáveis e Indicadores

Para Barbetta (1999, p. 21), as definições das variáveis e indicadores são “características que podem ser observadas (ou medidas) em cada elemento da

população, sob as mesmas condições. Uma variável observada (ou medida) num elemento da população deve gerar um, e apenas um resultado".

Com isso, algumas variáveis foram definidas:

- Características demográficas e econômicas: são traços geográficos das dimensões, estatísticas, estruturadas e distribuídas na vida pessoal dos entrevistados, como gênero, idade e renda familiar.
- Acesso à internet: define a forma e intensidade do acesso à internet pelo usuário.
- Segurança virtual: uma análise de medidas de segurança que os usuários tomam durante o acesso à internet.
- Legislação de acesso à internet: são informações relativas à legislação brasileira para o acesso à internet.

Para tanto, na tabela 4, são apresentadas os objetivos, as questões do instrumento de coleta, as variáveis, os indicadores e os elementos de pesquisa, utilizados no presente estudo.

Tabela 4. Variáveis e Indicadores

Objetivos de pesquisa	Questões do Instrumento de coleta	Variáveis	Indicadores/elementos de pesquisa
Identificar as características demográficas e econômicas.	Questões 1, 2, 3 e 4.	Características demográficas e econômicas	Gênero, idade e formação educacional e renda familiar.
Relatar as formas de acesso às redes sociais virtuais;	Questões 5, 6, 7, 8, 9 e 10.	Acesso à internet.	Uso da internet, local de acesso, frequência de acesso, equipamentos utilizados, uso de redes sociais.
Verificar as medidas preventivas de segurança virtual.	Questões 11, 12, 13 e 14.	Segurança virtual.	Medidas de segurança no acesso à rede, crimes cibernéticos sofridos.
Identificar a aplicabilidade do conhecimento das leis na segurança individual no acesso à internet.	Questões 15, 16, 17 e 18.	Legislação de acesso à internet.	Conhecimento da legislação brasileira, opinião sobre a efetividade das leis.

Fonte: Dados da pesquisa (2016).

3.7 Processamento e Análise dos Dados

Após a coleta de dados, a fase seguinte da pesquisa é a de análise e interpretação. Segundo Gil (2008), a análise tem como o objetivo organizar os dados de uma forma que seja possível fornecer resposta ao problema proposto para a investigação, já a interpretação tem o objetivo de procurar sentido amplo para as respostas no que é feito através de conhecimentos anteriormente obtidos.

A estatística descritiva é o ramo da estatística que coleta, resume e apresenta dados, para uma visualização clara, possibilitando analisar os dados e identificar características importantes. Assim, utiliza-se técnicas descritivas (tabelas e gráficos), tanto para variáveis numéricas, utilizadas neste trabalho, quanto para categóricas. (ARAÚJO NETO *apud* BARBETTA, 2012).

Os dados obtidos através da aplicação do questionário foram submetidos à análise estatística descritiva.

4 ANÁLISE DE DADOS

Neste capítulo apresenta-se a análise dos dados obtidos sobre as leis brasileiras de acesso à internet na percepção do usuário. Os dados foram coletados por meio de aplicação de questionários através da ferramenta gratuita *Google Forms*. Foram enviados os questionários aos usuários através do *Whatsapp*, *Facebook* e e-mails. A amostra foi selecionada utilizando procedimento não probabilístico por acessibilidade, ou seja, longe de qualquer procedimento estatístico onde os usuários forma selecionados pela facilidade de acesso a eles (vergara, 1998).

Para facilitar a compressão, o capítulo está dividido em quatro partes referentes às variáveis eleitas para o estudo, a saber: características demográficas e econômicas; acesso à internet; segurança virtual; e legislação de acesso à internet. Em todas as seções, apresentam-se gráficos para que se tenha melhor visualização e entendimento dos resultados da pesquisa.

Umbaúba é uma pequena cidade do interior de Sergipe, localizada na região Centro Sul do Estado, a 100 km da capital Aracaju. Sua população atual é de 22.434 habitantes (IBGE, 2010).

Tendo um baixo desenvolvimento econômico, Umbaúba tem como atividade predominante o comércio local, a citricultura e o funcionalismo público. Segundo o IBGE (2015), o PIB per capita da cidade de Umbaúba é de aproximadamente R$9.831.68 e apenas 8,5% da população possuem empregos formais.

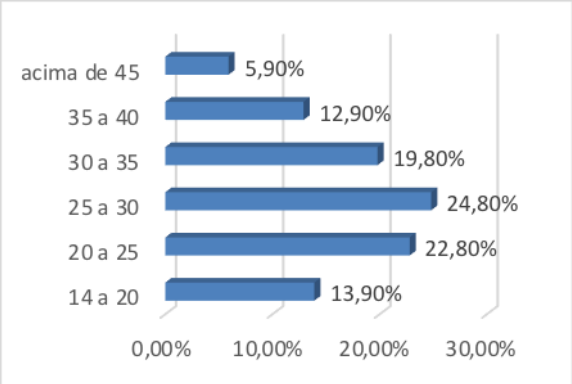
4.1 Características demográficas e econômicas dos usuários das redes sociais virtuais.

Neste item procurou-se conhecer características dos usuários que acessam as redes socais virtuais na cidade de Umbaúba - SE, como: idade, sexo, escolaridade e a renda. O objetivo foi relacionar como essas características influenciaram a percepção dos usuários sobre a legislação brasileira de acesso à internet.

4.1.1 Idade e sexo

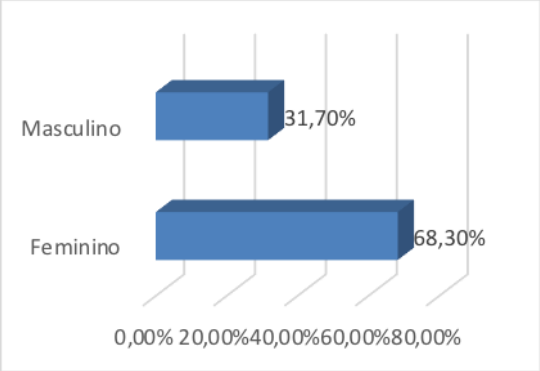
Este tópico contém duas variáveis analisadas que são a idade e o sexo. Elas representam características importantes a respeito dos usuários das redes sociais virtuais da cidade de Umbaúba – SE, que dão uma representatividade sobre sua percepção às leis brasileiras de acesso à internet**.**

Gráfico 1: Idade dos respondentes



Fonte: Dados da pesquisa (2016).

Gráfico 2: Sexo dos respondentes



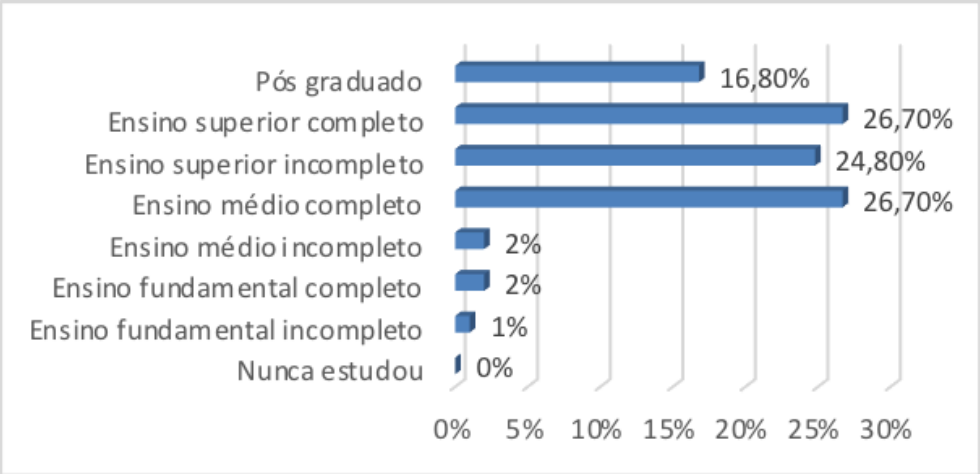
Fonte: Dados da pesquisa (2016).

Foi possível verificar no gráfico 1 que entre os usuários da internet que participaram da pesquisa a maior faixa etária de respondentes se concentra entre 25 a 30, com 24,8% de toda amostra. Esse resultado difere da pesquisa feita no Brasil nos últimos três meses de 2014 pelo Centro Regional de Estudo para o Desenvolvimento da Sociedade da Informação-Cetic.br, onde aponta que maior faixa etária se concentra entre o 16 e 24 anos de idade, com 83%. E em relação à categoria sexo, o gráfico 2 demonstra que houve uma prevalência do sexo feminino dentre os entrevistados dos que utilizam das redes sociais virtuais. Dados do Censo Demográfico 2010 informa que a população feminina de umbaúba é de 51,5%. Essa discrepância entre a população pesquisada pode decorrente da utilização de amostra não probabilística.

4.1.2 Grau de instrução

Neste item verificou-se qual o grau de instrução dos usuários das redes sociais virtuais que compõe esta amostra e se isso influência no seu acesso às redes sociais virtuais.

Gráfico 3: Escolaridade



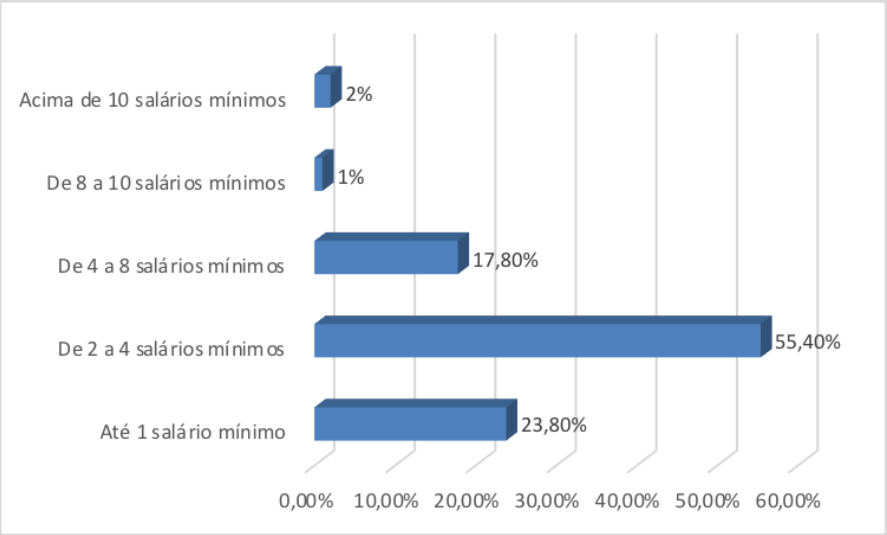
Fonte: Dados da pesquisa (2016).

Quanto ao nível de escolaridade dos usuários da internet pesquisados foi possível verificar que o ensino superior completo e o ensino médio completo têm as mesmas porcentagens, ou seja, 26,7%. Esses dados são semelhantes aos das estatísticas do Centro Regional de Estudo para o Desenvolvimento da Sociedade da Informação-Cetic Br (2014), em que afirmam que a utilização da internet no país cresce de acordo com a escolaridade. Pode-se supor que esse dado deva-se ao fato de que cada vez mais se torna comum o acesso à informática tanto pelos estudantes de educação básica através de atividade em plataformas como entre os universitários que fazem uso da internet para a realização de pesquisa de produção de conhecimento e divulgação. Entre estes, destacam-se os estudantes da modalidade a distância que por meio de ambientes virtuais de aprendizagem (AVA) acessam a internet com frequência.

4.1.3 Renda

Nesta seção foi analisada a influência da renda no acesso à internet, isto é, se a quantidade de salários obtidos pelos usuários interfere no acesso às redes sociais virtuais.

Gráfico 4: Renda



Fonte: Dados da pesquisa (2016).

Quanto ao perfil econômico dos usuários da internet que compuseram a amostra deste estudo, 55,4% apresentam uma renda 2 a 4 salários mínimos destacando-se frente às demais rendas apresentadas no gráfico. Esses dados se aproximam da pesquisa feita em todo Brasil que foi divulgada pela Secretaria de Comunicação Social da Presidência da República e realizada pela Pesquisa Brasileira de Mídia (2016), onde afirma que o acesso à internet quando se tem uma renda superior a cinco salários mínimos é cada vez maior.

A renda da população de Umbaúba é considerada baixa, mas ainda assim é perceptível uma prevalência de usuários das redes sociais virtuais que recebem 2 a 4 salários mínimos.

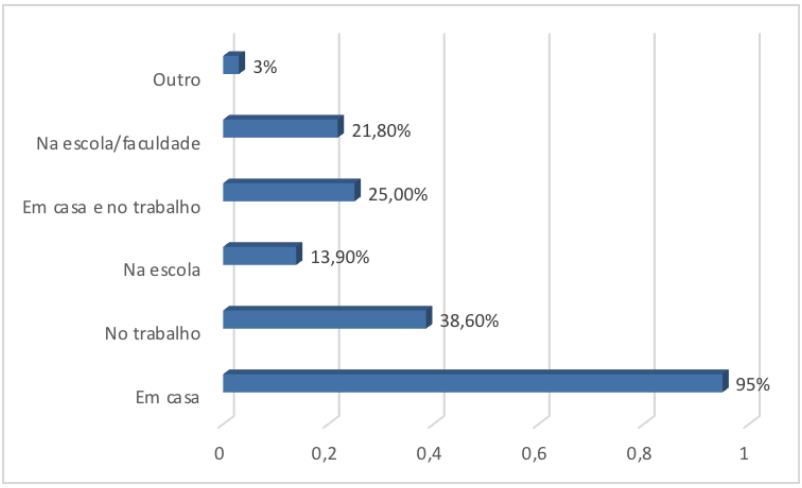
4.2 Identificar as formas de acesso as redes sociais virtuais

Esta seção tem o principal objetivo de identificar as formas de acesso à internet como: Local onde os usuários mais acessam, qual o dispositivo mais utilizado, se faz o uso das redes sociais virtuais, com qual frequência é acessada e qual a rede social virtual mais utilizada.

4.2.1 Locais mais comuns para acessar a internet

Neste item apresentam-se os locais em que os usuários mais acessam a internet, destacando em casa, no trabalho, na escola, em casa e no trabalho, na escola ou faculdade, e em outros.

Gráfico 5: Locais mais comuns para acessar internet



Fonte: Dados do pesquisador (2016).

Através dos dados coletados, nota-se que o acesso à internet em casa teve percentual maior, 95%, sendo que o menor percentual foi de 3%, corresponde a outros, onde as respostas atribuídas pelos usuários foram: duas para academia e uma para barzinho. Com a popularização da internet é muito comum hoje a contratação de serviços de internet doméstica nos lares brasileiros, na pesquisa feita pela Centro Regional de Estudo para o Desenvolvimento da Sociedade da Informação - Cetic br (2014) apresentou que metade (50%) dos domicílios brasileiros possuem acesso à internet e isso representa cerca de 32,3 milhões de habitantes do território brasileiro. No município de Umbaúba o acesso à internet é fornecido por duas empresas que possuem provedores de internet via rádio que atende à população da zona urbana e uma parte da zona rural.

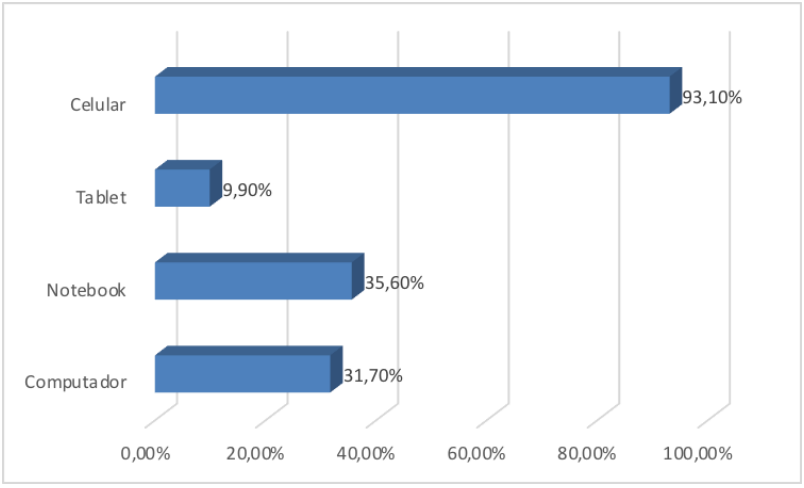
Os usuários da internet podem ter acesso doméstico ou utilizar o *wi-fi* que é disponibilizado em diversos lugares da cidade, como: bares, lojas, escolas e em alguns eventos públicos de grande porte. Encontra-se também na cidade *lan house* onde o usuário paga pelos minutos acessados. As escolas públicas do município situadas na zona urbana, assim como a universidade particular possuem laboratório de informática onde os estudantes podem acessar e navegar na internet livremente.

4.2.2 Dispositivo mais utilizado para se conectar à internet

Nesta seção apresenta-se os dispositivos mais utilizados para o acesso à internet. Os dispositivos destacados foram o celular, o tablet, o notebook e o computador

.

Gráfico 6: Dispositivo mais utilizado para acessar internet



Fonte: Dados da pesquisa (2016).

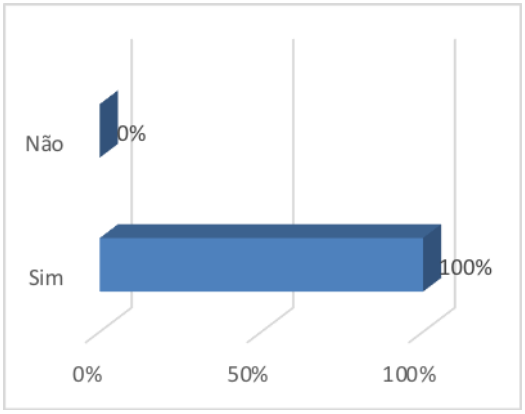
De acordo com o gráfico 6, o celular foi o dispositivo mais utilizado para o acesso à internet com percentual de 93,1%. Isso demonstra que os usuários da amostra dessa pesquisa possuem celular e através dele acessam a internet ou por plano de uma operadora ou pelo *wi-fi* doméstico. Como foi constado que os usuários com renda entre 2 e 4 salários mínimos acessam a internet, pode-se inferir que isso é facilitado pelo poder de compra de um dispositivo como o celular. Em pesquisa feita em 2014 pelo Centro Regional de Estudo para o Desenvolvimento da Sociedade da Informação - Cetic Br (2014), o celular também foi o dispositivo mais usado para o acesso à internet no Brasil, com 76%.

É chegada a era da mobilidade em que, segundo Lemos (2002), a cibercultura está cada vez mais presente fazendo com que os usuários não desloquem até a rede e sim a rede que passa a envolver os usuários numa conexão generalizada. Esse novo padrão de vida faz com que as pessoas sintam a necessidade de estarem conectadas em tempo integral. Lemos (2005) considera que o celular é o controle remoto do cotidiano, pois com ele é possível realizar as mais diversas tarefas entre trabalho e lazer.

4.2.3 Uso das redes sociais e frequência de acesso

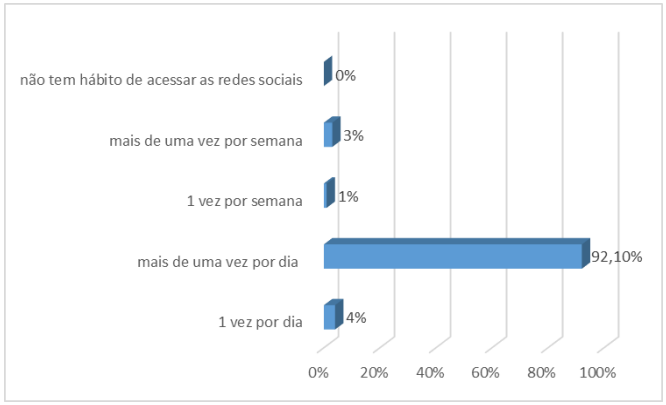
Neste item apresenta-se o uso das redes sociais virtuais pelos usuários da amostra deste estudo, e foi investigado se os usuários utilizam as redes sociais virtuais e com que frequência isso ocorre.

Gráfico 7: Utilização de redes sociais



Fonte: Dados da pesquisa (2016).

Gráfico 8: Frequência de acesso as redes sociais



Fonte: Dados da pesquisa (2016).

A partir da análise do gráfico 7, 100% afirmaram que utilizam alguma rede social. Este fato se deve ao acesso doméstico à internet ter prevalecido pelos usuários, assim como o uso do celular devido à sua mobilidade, conforme mostrado. Esses dados são semelhantes aos da pesquisa divulgada pela Secretaria de Comunicação Social da Presidência da República e realizada pela Pesquisa Brasileira de Mídia (2015), que asseguram que 92% dos internautas no Brasil estão conectados pelas redes sociais.

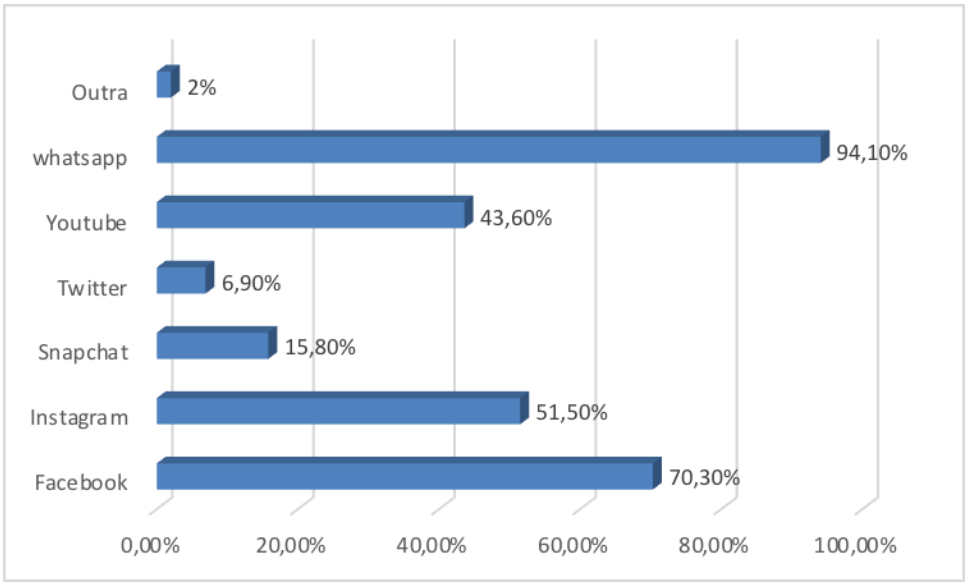
Em relação à frequência de que o usuário acessa a internet, verificou-se no gráfico 8 que prevaleceu o item “mais de uma vez por dia”, obtendo o percentual de 92,1%. Isso demostra que a internet faz parte do novo padrão de vida em que a sociedade sente a necessidade de estar conectada e compartilhando seu cotidiano. Fenômeno este também facilitado por possuir internet doméstica e porque em diversos ambientes frequentados por eles é fornecida internet livre fazendo com que fiquem conectados quase que em tempo integral.

4.2.4 Redes sociais mais utilizadas

Nessa seção apresenta-se as redes sociais virtuais mais utilizadas pelos usuários que compuseram a amostra desse estudo. As redes sociais virtuais

apresentadas foram o *Facebook*, *Instagram, Snapchat, Twitter, Whatsapp*, dentre outras.

Gráfico 9: Redes sociais mais utilizadas



Fonte: Dados da pesquisa (2016).

Como foi possível observar as redes sociais mais utilizadas foram o *Whatsapp* com 94,1%, o *Facebook* com 70,3%, o *Instagram* com 51,5%, e 2% outras redes sociais virtuais cujas respostas foram: *Telegram* e *Google+*.

Os dados diferem com a pesquisa feita em todo Brasil que foi divulgada pela Secretaria de Comunicação Social da Presidência da República e realizada pela Pesquisa Brasileira de Mídia (2015), onde no *ranking* da rede social mais acessada é o *Facebook* com 83%. Os dados diferem devido à crescente popularização do *Whatsapp*, pois é cada vez mais frequente se comunicar através do envio de mensagens instantâneas.

É através dessas redes sociais que surge a sociedade em rede. Recuero (2005) afirma que comunidade virtual é quando um grupo de pessoas estabelecem entre si relações sociais, que permaneçam um tempo suficiente para que se possa constituir um corpo organizado através da comunicação mediada por computador. Com o *Whatsapp* é possível ter uma comunicação individual e também formar grupos de assuntos afins.

A seguir apresenta-se uma tabela contendo apenas uma síntese das categorias sociais dos usuários que fizeram parte da amostra deste estudo, assim

como dos itens abordados a respeito do uso das redes sociais virtuais pelos mesmos.

Tabela 1: Perfil dos respondentes.

	Perfil dos respondentes	Número de respondentes
Faixa etária	25 a 30	25
Sexo	Feminino	69
Grau de instrução	Ensino médio completo Ensino superior completo	27 27
Renda	De 2 a 4 salários mínimos	56
Locais mais comuns para acessar a internet	Em casa No trabalho	96 38
Dispositivo que mais utiliza para se conectar internet	Notebook Celular	36 94
Frequência de acesso	Mais de um vez por dia	93
Redes sociais mais utilizadas	*Facebook* *Instagram* *Whatsapp*	71 52 95

Fonte: Dados da pesquisa (2016).

Com a tabela 1 foi possível traçar o perfil do usuário dessa amostra. Tal perfil é de suma importância para a segunda etapa deste estudo, pois permite conhecer qual o grau de instrução dos usuários das redes sociais virtuais, a sua renda média, as facilidades de acesso à informação e às redes sociais virtuais e se são capazes de compreender seus direitos e deveres, assim como as formas de proteção e punição frente ao uso da internet.

4.3 Medidas preventivas de segurança tomadas pelos usuários no acesso à rede de internet

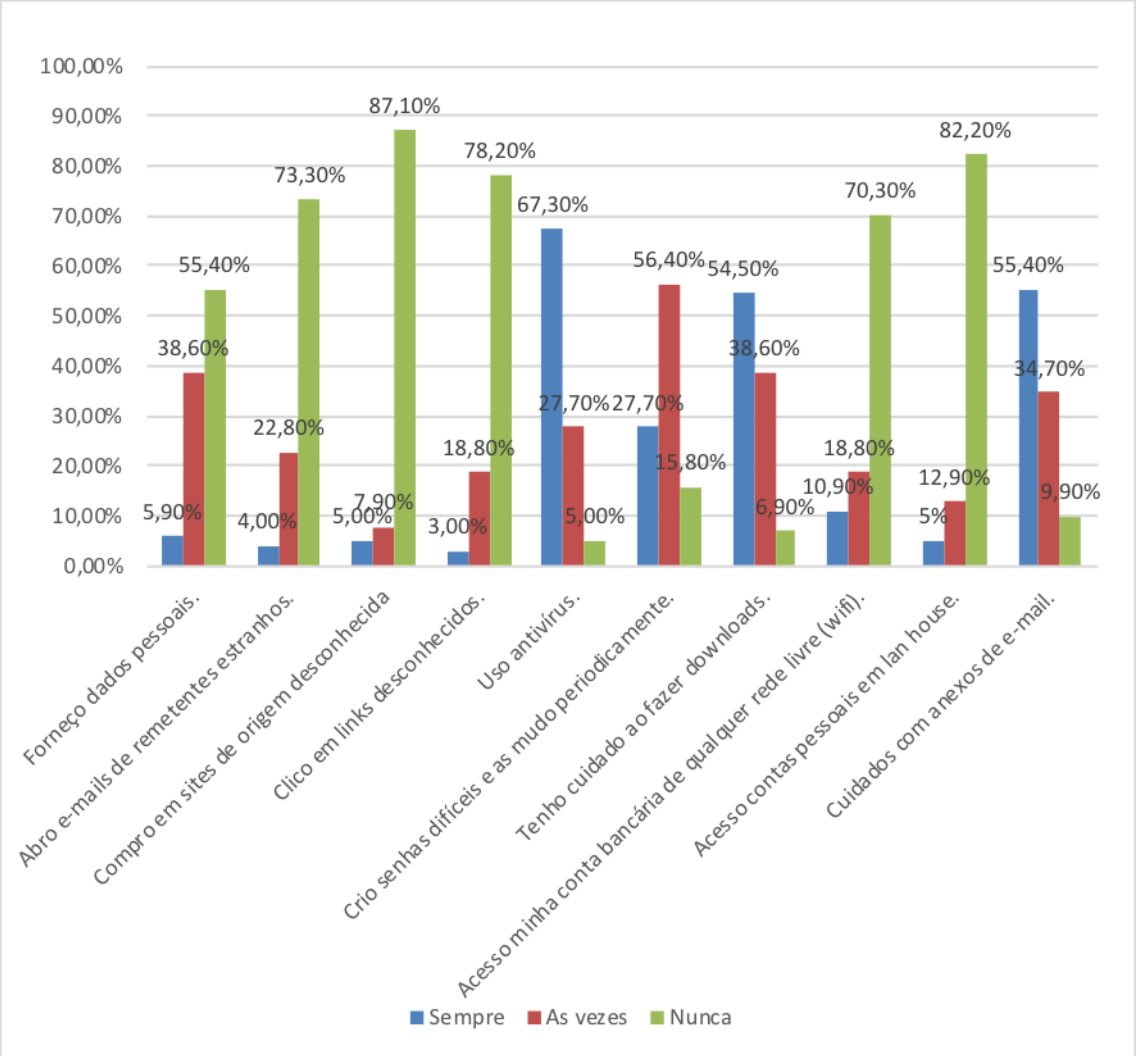
Esta seção teve a finalidade de analisar quais as medidas de segurança que os usuários possuem contra o crime cibernético e se já foram vítima de algum deles. A mesma está dividida em três partes: precauções ao utilizar internet, crimes cibernéticos sofridos e o número de crimes ocorridos.

4.3.1 Precauções ao utilizar a internet

O objetivo desse item é identificar as medidas preventivas que os usuários têm ao acessar a rede, pois estas ajudam a diminuir o risco de crime cibernético.

A seguir, apresenta-se o gráfico com o resultado obtido a partir da amostra pesquisada a respeito das precauções utilizadas pelos usuários da internet.

Gráfico 10: Precauções ao utilizar a internet



Fonte: Dados do pesquisador (2016).

Quando perguntado aos respondentes se fornecem dados pessoais ao utilizarem a internet, 55,4% afirmaram que nunca fornecem. Ao fornecer seus dados pessoais os usuários ficam expostos aos mais diversos tipos de crimes cibernéticos, dentre eles pode-se citar os mais comuns: clonagem de cartão de crédito e compras indevidas no seu nome.

Sobre a questão de abrir e-mails de remetentes estranhos, 73,3% afirmaram que nunca abrem. Ao abrir muitos desses e-mails o usuário pode receber algum tipo de vírus. Estes podem se instalar no seu dispositivo com o intuito de roubar senha de contas bancárias e de arquivos pessoais ou também bloquear dados e arquivos do usuário.

Em relação à compra em site de origem desconhecida na internet, 87,1% afirmaram que não compram. Ao comprar em sites de origem desconhecida o usuário fica sujeito a fraudes, pode não receber o produto comprado ou receber produtos diferentes do que havia escolhido, além de sofrer clonagem de cartão de crédito. No Brasil existe o Código de Defesa do Consumidor, que protege o consumidor contra alguns desses golpes cometidos na rede, porém em caso de compras de site do exterior o comprador não está coberto pelo Código Defesa do Consumidor do Brasil, caso tenha algum problema terá que resolver com o fornecedor ou conhecer as regras do país de origem.

Foi perguntado se eles clicam em links desconhecidos, dentre os entrevistados, 78,2% afirmaram que nunca fazem isso. Acredita-se que muitos desses links possuem conteúdos maliciosos que ao clicar se instalam em seu dispositivo com o intuito de furtar informações ou bloqueá-las.

Assim, ter um antivírus é crucial para se proteger das ameaças virtuais, no entanto, não basta tê-lo instalado no dispositivo, é importante certificar que esteja atualizado para que consiga exercer a sua principal função: a proteção. Ao perguntar aos entrevistados se utilizam o antivírus, 67,3% afirmaram que sempre usam.

Em relação se os usuários criam senhas difíceis e se as mudam periodicamente, 56,4% dos entrevistados afirmaram que agem dessa forma. Esta é uma boa prática de defesa, pois o ato de utilizar as mesmas senhas para diversas finalidades faz com que o usuário fique exposto aos mais diversos ataques cibernéticos.

Foi questionado se os usuários têm cuidado ao fazerem d*ownloads. S*obre essa precaução, 54,5% responderam que sempre tomam cuidado com os

downloads que realizam. *Downloads* são um dos motivos comuns para infestação de vírus em dispositivos, assim, antes de fazer *downloads* alguns *sites* pedem que se faça a instalação de determinados *softwares, porém* muitos desses softwares podem estar infectados.

Foi perguntado se acessam conta bancária em qualquer *wi-fi* livre e 70,3% afirmaram que nunca. Não é recomendado acessar conta bancária em rede pública, pois ela está mais propícia a sofrer invasões devido aos poucos mecanismos de defesa contra aos mais variados tipos de ataque na rede.

Em relação ao acesso a contas pessoais em *lan house,* 82,2% dos respondentes afirmaram que nunca acessam seus dados pessoais nesse local. Ao acessar os dados pessoais em *lan house*, o usuário fica exposto a diversos crimes cibernéticos, pois não se tem certeza de que os computadores estão livres de vírus.

Em relação aos cuidados ao abrir os anexos de e-mails desconhecidos, 55,4% disseram que têm cuidado ao abrir esse tipo de informação. No geral, os usuários recebem e-mails desconhecidos com anexos contendo textos, imagens e informações diversas e que ao serem abertos podem conter vírus que danificam os dispositivos.

Nesse sentido, mesmo diante de todas as precauções tomadas pelos usuários da internet, ainda existem pessoas vítimas de diversos golpes. Portanto, de acordo com a Cartilha de Segurança da Internet (2012), é preciso cuidado ao navegar nas redes, ou seja, ter os mesmos mecanismos de defesa que se tem no dia a dia, como por exemplo, não fornecer dados pessoais a qualquer pessoa, visitar locais somente se ele for seguro, atentar-se quando for ao banco.

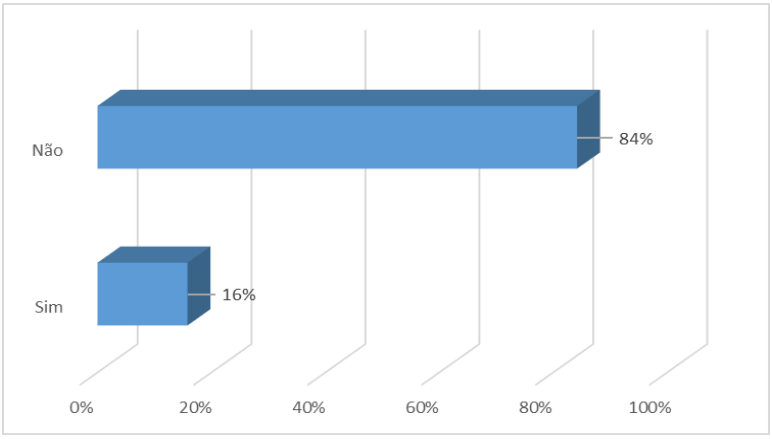
Segundo a referida cartilha, o grande problema em relação à segurança na internet está em achar que não se corre risco, pois supõe que ninguém se interessa em usar seu computador ou que diante de um número muito grande de computadores o seu dificilmente será localizado, assim, é esse tipo de pensamento que é explorado pelos criminosos, afinal o usuário ao sentir-se seguro deixa de se prevenir corretamente. Sendo assim, ter cautela ao acessar a rede é a melhor forma para se proteger dos crimes cibernéticos.

4.3.2 Crime cibernético

Nesta sessão, está quantificado o número de pessoas que já sofreram algum tipo de crime cibernético. Como se pode notar no gráfico 10, muitos usuários tomam

precauções em relação ao uso da internet, porém, ainda assim muitos deles apresentam que já sofreram algum tipo de crime virtual.

Gráfico 11: Número de vítimas de crime cibernético



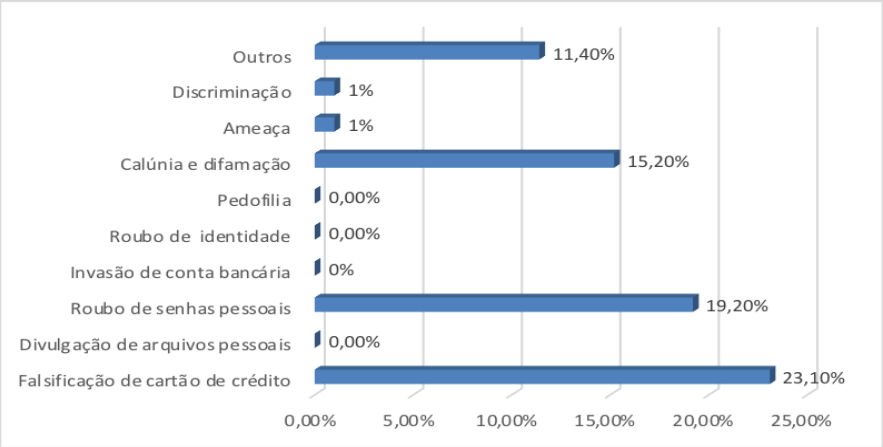
Fonte: Dados da pesquisa (2016).

O gráfico 11 demonstra que 84% dos respondentes afirmaram que nunca foram vítimas de crimes cibernéticos, o que se pode supor que adotando as devidas precauções as chances de sofrer crimes cibernéticos diminuem. Mas, em contrapartida, mesmo possuindo conhecimento das precauções, 16% alegaram já ter sofrido algum tipo de crime na rede.

4.3.3 Crimes sofridos

Neste tópico buscou-se identificar quais os tipos de crimes cibernéticos que os usuários já sofreram. Os crimes perguntados foram falsificação de cartão de credito, divulgação de arquivos pessoais, roubo de senhas pessoais, invasão de conta bancária, roubo de identidade, pedofilia, calúnia e difamação, ameaça, discriminação e outros.

Gráfico 12: Crimes sofridos



Fonte: Dados da pesquisa (2016).

Dos crimes listados, a falsificação de cartão de crédito obteve o maior percentual totalizando 23,1%. Esse delito está tipificado na Lei nº 12.737/12 no Art. 298 do Código Penal que sofreu alterações, pois se compara que clonar cartão de débito ou crédito é o mesmo que falsificar total ou parcialmente documento particular. A Pena - reclusão é de 1 (um) a 5 (cinco) anos e multa. Segundo Pereira (2014), no Brasil, a cada 15 segundos ocorre uma tentativa de fraude contra algum consumidor. O aumento no crime de clonagem de cartão de crédito ou débito cresce junto ao avanço tecnológico devido às mudanças de hábito do consumidor.

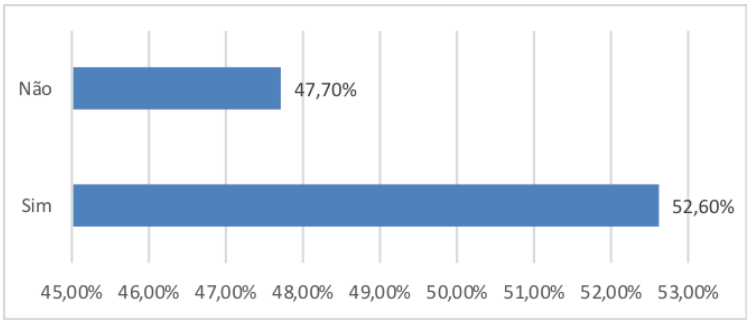
Uma das praticidades do mundo moderno é pagar contas e executar as mais diversas transações bancárias com apenas um click utilizando o seu computador ou celular. Porém, o perigo está em acessar a sua conta em uma rede de *wi-fi* livre, fazer compras em sites desconhecidos ou abrir um e-mail desconhecido e junto desse e-mail conter algum tipo de vírus que roubem ou bloquem seus dados. Assim, é fundamental que os usuários da internet utilizem as precauções disponíveis para que utilize a rede com segurança.

Antes da legislação atual, muitos dos crimes citados no gráfico 12 eram amparados pelo Código Civil, e em alguns casos pelo Código de Defesa do Consumidor. Depois da promulgação das leis da internet os crimes passaram a ser julgados de forma mais justa, visto que é possível tipificar os crimes e aplicar a pena de acordo com o delito cometido.

4.3.4 Medidas tomadas ao sofrer um crime

Este item busca identificar se a vítima, ao sofrer algum tipo de crime cibernético, tomou alguma medida legal e qual a orientação do Poder Público diante do fato ocorrido.

Gráfico 13: Medidas tomadas ao sofrer um crime



Fonte: Dados da pesquisa (2016).

Entre os respondentes que já sofreram crime cibernético, 52,6% disseram que tomaram medidas legais. Essas medidas legais envolvem denúncia em delegacias especializadas em crimes cibernéticos, pois em alguns estados do Brasil já existem este tipo de delegacia. Segundo Wendt (2015), se não houver no estado uma delegacia especializada a vítima pode registrar boletim de ocorrência na delegacia mais próxima. Ao fazer boletim de ocorrência é importante que a vítima consiga relatar em detalhes todas as informações possíveis para que a polícia possa ter um conhecimento real sobre o tipo de crime sofrido (WENDT, 2009). É por meio dessas informações que a polícia dará início ao processo de investigação.

4.4 Identificar a aplicabilidade do conhecimento das leis na segurança individual no acesso à internet

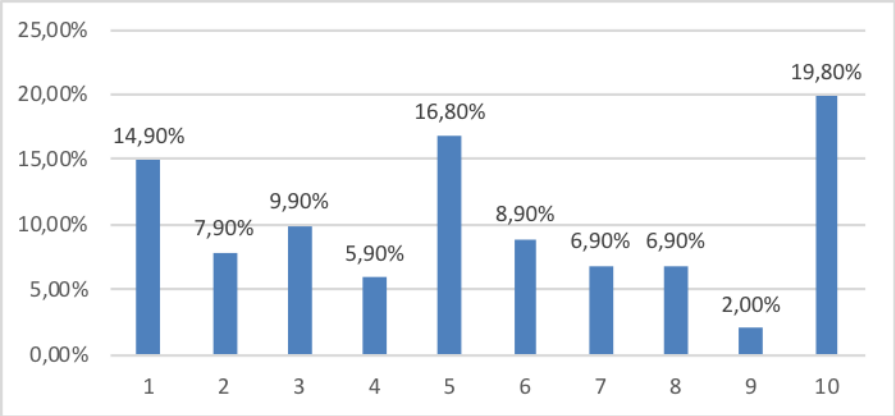
Nesta seção apresenta-se a análise dos dados que se reportam à crença dos usuários a respeito das leis brasileiras de acesso à internet, assim como a sua aplicabilidade. O primeiro sub tópico aborda qual o conhecimento da população sobre as leis de internet vigentes no Brasil, o segundo analisa se ao possuir conhecimento dessas leis os crimes cibernéticos não aconteceriam com os usuários, o terceiro identifica se a população conhece os seus direitos e deveres dispostos na

lei de internet, e o quarto apresenta o quanto os usuários acreditam na efetividade das leis.

4.4.1 Nível de conhecimento das leis brasileiras de acesso à internet

Nesta subseção procurou-se identificar o quanto a população conhece as leis brasileiras de acesso à internet no Brasil.

Gráfico 14: Nível de conhecimento da legislação



Fonte: Dados da pesquisa (2016).

Ao analisar os dados do gráfico 14, percebe-se que apenas 19,8% dos respondentes afirmaram o número 10, que corresponde a “concordo plenamente” baseado na escala de Likert, mostrando assim que a legislação brasileira de acesso à internet ainda é desconhecida pela maioria da população.

As leis brasileiras de acesso à internet são de extrema importância para proteção do usuário da internet, visto que o seu principal objetivo é garantir o uso da rede com segurança evitando abusos e crimes. Mas, para que as leis se cumpram é preciso que a população tenha acesso e busquem os meios de fazê-la ser cumprida e também estar atenta ao que se pode ou não fazer na rede.

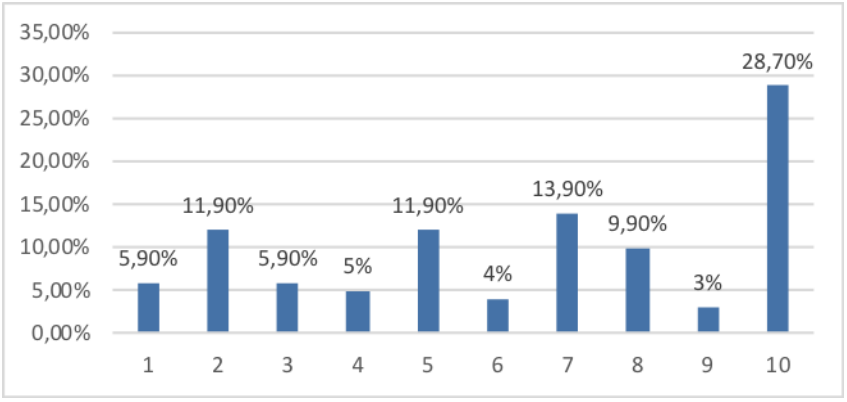
Como já foi citado neste trabalho, a lei Carolina Dieckmann 12.737/2012 foi sancionada depois de sofrer uma pressão midiática quando criminosos furtaram e publicaram fotos íntimas da Atriz Carolina Dieckmann. No período que ocorreu o delito a atriz se dirigiu a uma delegacia para fazer registro de ocorrência detalhando à polícia tudo que aconteceu para que pudesse iniciar o processo de investigação e após isso ser julgada pelo juiz que aplicará a pena correta para o tipo de crime cometido.

A lei do Marco Civil 12.965/2014 é uma “constituição” que vem regulamentar o acesso à internet no Brasil, definindo direitos e deveres de usuário e provedores de internet no país, dentre eles: a proteção à privacidade, liberdade de expressão e acesso de qualidade a todos.

4.4.2 Relação entre ter conhecimento sobre as leis da internet e evitar os crimes cibernéticos

Neste tópico buscou-se conhecer se o usuário possuir conhecimento sobre as leis brasileiras de acesso à internet é o fator que contribui para a não realização dos crimes virtuais onde foram atribuídas as seguintes opções baseadas na escala de Likert: 1, para discordo totalmente e 10, concordo totalmente.

Gráfico 15: Possuir conhecimento das leis não haveria crime.



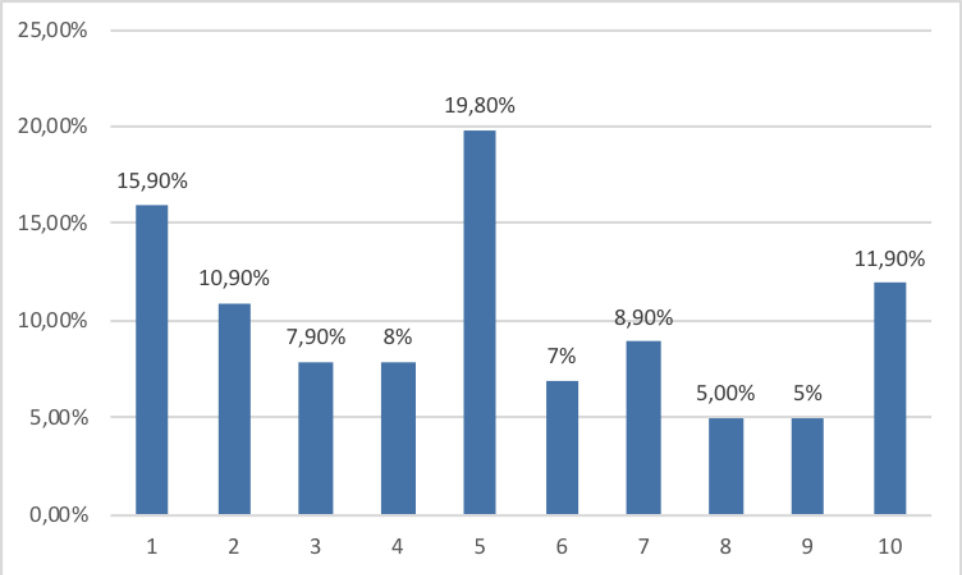
Fonte: Dados da pesquisa (2016).

Os dados apresentados mostram que 28,7% dos respondentes “concordam plenamente” que se a população tivesse mais conhecimento sobre as leis, os crimes sofridos indicados no gráfico 12 não aconteceriam, pois mesmo tendo conhecimento das precauções que se podem ter, muitos desconhecem a lei e com isso não sabem a quem recorrer em caso de crime sofrido, o que faz os infratores ficarem impunes.

4.4.3 Conhecimento dos direitos e deveres dispostos na lei

Nesse item apresenta-se o nível de conhecimento dos respondentes a respeito dos seus direitos e deveres na rede, assim como a legislação brasileira de acesso à internet.

Gráfico 16: Nível de conhecimento dos direitos e deveres na internet



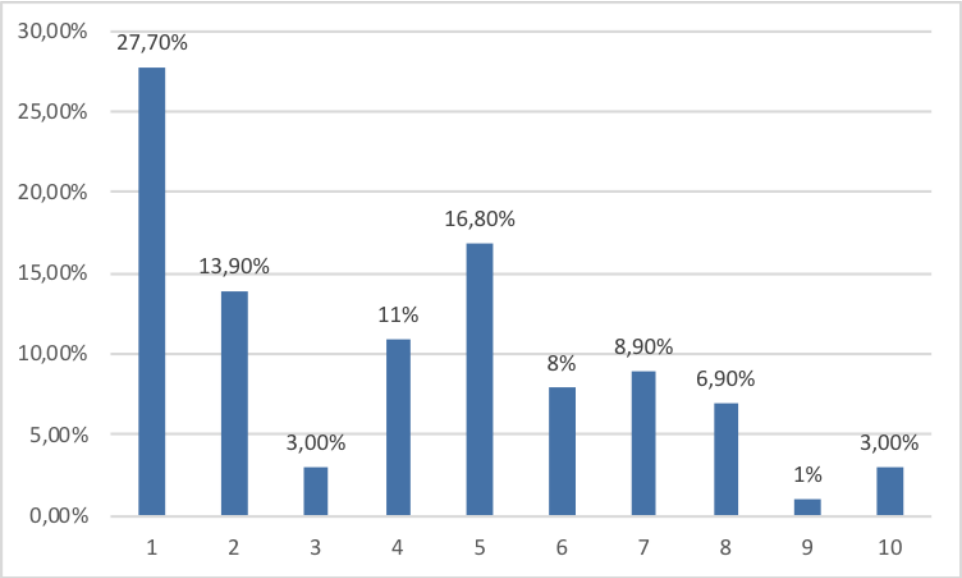
Fonte: Dados da pesquisa (2016).

Com os dados apresentados pode-se perceber que os maiores índices foram as escalas menores que 5, o que indicam que os respondentes apresentam um baixo nível de conhecimento das leis vigentes. É de extrema importância que se conheçam esses direitos e deveres para que consigam saber quais as medidas a serem tomadas em caso de sofrer algum crime virtual. A lei 12.737/2012 protege o usuário contra invasão de dispositivo informático e a disseminação das informações furtadas, sendo que as penas são aplicadas conforme as suas infrações. Já na lei nº 12.965/2014 o Art.7 prevê os diretos e as garantias do usuário, como inviolabilidade e do sigilo de suas comunicações pela internet, conexão de qualidade, dentre outros.

4.4.4 Efetividade da legislação brasileira de acesso à internet

Neste item buscou-se compreender se os respondentes acreditam na efetividade da legislação brasileira de acesso à internet para combater, julgar e punir os infratores de crimes cibernéticos no Brasil.

Gráfico 17: Crença na efetividade da legislação brasileira de acesso à internet



Fonte: Dados da pesquisa (2016).

De acordo com o gráfico 17, houve o maior índice na descrença na efetividade da legislação brasileira de acesso à internet, obteve-se assim 27,7%, que na escala atribuída é referente ao “discordo totalmente”. Observa-se então, que, de maneira geral, os usuários não acreditam que a legislação brasileira é eficaz no combate aos crimes virtuais. Essa constatação pode ser explicada pelo desconhecimento da lei por boa parte dos usuários, conforme foi observado no gráfico 14.

Por desconhecer essas leis as pessoas ao sofrerem algum tipo de crime não sabem o que fazer ou como agir. E apesar de todos os prejuízos causados pelos delitos sofridos acabam não denunciando, fato que aumenta as estatísticas de crimes ocorridos e que não são registrados.

Segundo Zanatta (2010), o maior problema jurídico é a raridade de denúncias e o despreparo da polícia investigativa, pois mesmo sendo possível fazer boletins de ocorrência pela internet são poucas as equipes de policiais preparadas para a investigação dos diversos crimes virtuais praticados pelos infratores. Muitas vezes as vítimas não procuram a justiça devido à crença na dificuldade de se chegar até o criminoso, motivadas pelo despreparo da polícia e também pela falta de informações precisas por parte da vítima diante do crime sofrido dificultando como irá provar que sofreu um delito. Outro fator que diminui as estatísticas das denúncias é a vítima

acreditar que os criminoso não serão punidos pelas suas ações em virtude do desconhecimento da legislação vigente. Assim, quanto maior for a divulgação sobre as leis e as punições sobre os crimes cibernéticos melhor será para a sociedade, pois esta terá condições de buscar a justiça e conseguir punir os criminosos.

Através dos resultados obtidos nesta pesquisa foi possível traçar o perfil dos usuários das redes sociais virtuais presentes na amostra, se acessam as redes sociais, o local que mais acessa e com qual frequência. Foi verificado se tomam medidas preventivas para não sofrer crime cibernético e se conhecem a legislação brasileira de acesso à internet que regem esse país, assim como se acreditam na efetividade das leis. Os resultados mostram que grande parte dos crimes que acontecem são resultantes da desinformação dos usuários quanto aos seus direitos e deveres dispostos nas leis que regulamentam os usos, crimes e punições a respeito da internet.

Nesse sentido, a seguir apresentam-se as conclusões a partir da realização deste estudo.

5 CONCLUSÃO

Com o surgimento da internet foram desencadeados diversos comportamentos referentes ao seu uso, especificamente podemos nos referir aos crimes cibernéticos. A pesquisa foi realizada a fim de verificar se a população conhece seus direitos e deveres ao utilizarem a internet e quais as possíveis precauções para se protegerem dos crimes virtuais.

Esta seção está dividida em três partes. Na primeira, respondem-se às questões formuladas de acordo os objetivos deste estudo. Na segunda, sugerem-se temáticas e questões que poderão servir de base para a realização de novas pesquisas a respeito da internet, e na terceira parte, apresenta-se as considerações finais.

5.1 Respostas aos objetivos de pesquisa

O primeiro objetivo especifico deste estudo foi traçar as características demográficas e econômicas dos usuários das redes sociais virtuais que residem em Umbaúba - SE. Através dos respondentes verifica-se que os referidos usuários predominantes têm entre 25 a 30 anos, são do sexo feminino e possuem grau de instrução superior incompleto ou ensino médio completo. Em relação às características econômicas, constatamos que 55,4% recebem de dois a quatro salários mínimos.

O segundo objetivo especifico foi relatar as formas de acesso às redes sociais virtuais. Obteve-se como respostas que o acesso se dá predominantemente por meio da internet domiciliar. Devido ao avanço tecnológico e à facilidade de contratação de serviço de internet via rádio é cada vez mais comum possuir internet domiciliar, com isso a forma mais utilizada para acesso à internet é através dela. Em relação ao dispositivo de acesso mais utilizado pela amostra da pesquisa, foi o *smartphone*. Este tem conseguido atender o desejo dos usuários da rede estarem conectados quase que integralmente. Verificou-se também que a rede social mais utilizada é o *Whatsapp.*

O terceiro objetivo especifico foi verificar as medidas preventivas de segurança tomadas pelos usuários no acesso à rede. Os respondentes declararam que tomam diversas precauções ao acessarem a rede, dentre elas destacaram: não

compram em site de origem desconhecida e não acessam contas pessoais em *lan house.* Porém, mesmo com esses cuidados, 16% dos respondentes afirmaram que já foram vítimas de algum tipo de crime cibernético. Dentre os delitos mais comuns, foi destacado o de falsificação de cartão de crédito. Em relação à posição diante dos delitos sofridos afirmaram que tomaram medidas legais denunciando às autoridades responsáveis, para que o infrator pudesse ser identificado e punido.

Por fim, o último objetivo especifico foi identificar a aplicabilidade do conhecimento das leis na segurança individual no acesso à internet. Verificou-se que a população desconhece as leis de acesso à internet, assim como também não sabem quais são os seus direitos e deveres sobre ela. Os respondentes acreditam que se tivessem o conhecimento necessário, os crimes não aconteceriam, sendo assim, eles discordam que a legislação brasileira de acesso à internet seja efetiva.

Diante da questão norteadora deste estudo, que foi quais são as percepções dos usuários das redes sociais virtuais sobre as leis brasileiras de acesso à internet, pode-se afirmar que ao mesmo tempo que os respondentes concordam que se possuíssem conhecimento sobre as leis os crimes não aconteceriam, pois se as denúncias fossem realizadas poderiam inibir as ações dos criminosos. Os Usuarios afirmaram ainda que não acreditam que as leis brasileiras de acesso à internet sejam eficazes, pois têm a sensação de que mesmo denunciando os mais diversos crimes cibernéticos, os infratores ficarão impunes.

5.2 Sugestões para futuras pesquisas

Diante do processo da pesquisa e dos resultados obtidos, verifica-se que diversas temáticas a respeito da internet não foram abordadas ou foram pouco aprofundadas, como por exemplo, o impacto da internet nas relações sociais, como a família pode proteger as crianças que utilizam a internet, como a escola pode atuar para ensinar os estudantes a utilizarem positivamente a internet, a utilização da internet na gestão de processos de informação, internet e crimes autorais dentre outros.

5.3 Considerações finais

Com a realização deste estudo constatou-se que a internet é uma área que ainda precisa de muitos estudos para compreendê-la e demonstrar todo o potencial que a mesma possui. Nesse aspecto, procura-se demonstrar que os usuários da rede precisam obter conhecimentos a respeito de como utilizá-la com segurança, bem como das possibilidades de recorrer à legislação quando se sentir lesado por terceiros. Assim, com a pesquisa realizada verifica-se que a amostra utiliza a internet constantemente em diversas situações da vida, porém deixaram claro que desconhecem as leis que os protegem dos crimes cibernéticos e também demonstraram que não acreditam na efetividade da lei, ponto que pareceu contraditório.

REFERÊNCIAS BIBLIOGRÁFICAS

ARAÚJO NETO, João Fernandes de. *Estatística Descritiva e teste Qui-Quadrado Aplicados à Acidentes de Transito Ocorridos em Rodovias Federais na Paraíba em 2012*. Trabalho de Conclusão de Curso. Universidade Federal da Paraíba. Campina Grande/PB. 2014

BRASIL, Presidência da República. 2012a. *Lei N° 12.735*. De 30 de Novembro de 2012. Disponível na internet via WWW. URL: <http://www.planalto.gov.br/ccivil_03/_Ato2011-2014/2012/Lei/L12735.htm>. Acesso em 09/06/2015.

_____. 2012b. *Lei n° 12.737*. De 30 de Novembro de 2012. Disponível na internet via WWW. URL: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2012/lei/l12737.htm>. Acesso em 09/06/2015.

_____. *Lei N° 12.965*. De 23 de Abril de 2014. Disponível na internet via WWW. URL: <http://www.planalto.gov.br/ccivil_03/_ato2011-2014/2014/lei/l12965.htm>. Acesso em 09/06/2015.

BARBETTA, P. A. *Estatística aplicada às Ciências Sociais*. 3. Ed. Florianópolis: UFSC, 1999.

BELING, Fernanda. *As 10 maiores redes sociais*. 2018. Disponível na internet via WWW. URL: < https://www.oficinadanet.com.br/post/16064-quais-sao-as-dez-maiores-redes-sociais/>. Acesso em 22/07/2018.

CARNEV, Adrian Kemmer. *Segurança na Internet*: a percepção dos usuários como fator de restrição ao comércio eletrônico no Brasil. Dissertação (Mestrado). Escola de Administração de Empresas de São Paulo. FGV, São Paulo, 2002.

CASTELLS, Manuel. *A sociedade em rede*. 6ª edição. São Paulo: Paz e Terra, 2002.

_____. *A sociedade em rede*. São Paulo: Paz e Terra, 1999.

CASTELLS, Manuel; CARDOSO, Gustavo. *A Sociedade em Rede*: Do conhecimento à acção política. Debates Presidência da República. Lisboa, Portugal, 2005.

CERVO, A. L.; BERVIAN, P. A; DA SILVA, R. *Metodologia Científica*. 6ª edição. São Paulo: Pearson Prentice Hall, 2007.

Comitê Gestor de Internet no Brasil. *O CGI.br e o Marco Civil da Internet***.** Sd.

DOWBOR, Ladislau. *Tecnologias do Conhecimento*: Os desafios da educação. São Paulo, outubro de 2013.

E-bit. *WebShoppers*. 37ª edição, 2018. Disponível na internet via WWW. URL: <http://www.ebite.com.br>. Acesso em 20/07/2018.

ECO, U. *Como se faz uma tese*. – 22. ed. Tradução Gilson Cesar Cardoso de Souza. São Paulo: Perspectiva, 2009.

FERREIRA, Ivette Senise. A criminalidade informática. IN: LUCCA, Newton de; SIMÃO FILHO, Adalberto (coord.). *Direito e internet*: aspectos jurídicos relevantes. Bauru: Edipro, p. 207-237, 2000.

GIL, Antônio Carlos. *Métodos e Técnicas de Pesquisa Social*. 6ª edição. São Paulo: Atlas, 2008.

GOMES JÚNIOR, Carlos César; GALO, Carlo Henrique da Silva; DATORE, Giselli Vicente; COSTA, Robson Nóbrega da. *Lei nº 12.965/11*: o Marco Civil da Internet – análise crítica. 2014. Disponível na internet via WWW. URL: <http://henriquegalo.jusbrasil.com.br/artigos/118296790/lei-n-12965-11-o-marco-civil-da-internet-analise-critica>. Acesso em 14/05/2015.

HAIR JR., J. F. et al. *Fundamentos de Métodos de Pesquisa em Administração*. Tradução Lene Belon Ribeiro. Porto Alegre: Bookman, 2005.

IBGE. *Censo Demográfico 2010*. Instituto Brasileiro de Geografia e Estatística. 2010. Disponível na internet via WWW. URL: <http://cidades.ibge.gov.br>. Acesso em 05/12/2015.

_____. Instituto Brasileiro de Geografia e Estatística. 2015. Disponível na internet via WWW. URL: < https://cidades.ibge.gov.br/brasil/se/umbauba/panorama>. Acesso em 23/07/2018.

_____. Pesquisa Nacional por Amostra de Domicílio. Instituto Brasileiro de Geografia e Estatística. 2016. Disponível na internet via WWW. URL: < https://www.ibge.gov.br/estatisticas-novoportal/sociais/trabalho/17270-pnad-continua.html?edicao=19937&t=publicacoes>. Acesso em 23/07/2018.

Instituto Nielsen IBOPE. 2014. Disponível na internet via WWW. URL: <http://www.nielsen.com/br/pt/press-room/2014/Numero-de-pessoas-com-acesso-a-internet-no-Brasil-supera-120-milhoes.html>. Acesso em 20/06/2015.

Internet World Stats. 2018. Disponível na internet via WWW. URL: <http://www.internetworldstats.com/stats.htm>. Acesso em 18/07/2018.

KUMAR, Krishan. *Da sociedade pós-industrial à pós moderna*: novas teorias sobre o mundo contemporâneo. 2.ed. ampl.- Rio de Janeiro: Jorge Zahar Ed., 2006.

LANGUER, A. *A revolução tecnológica*. 2004. Disponível na internet via WWW. URL: <http://vinculando.org/brasil/conceito_trabalho/crise.html#_ftnref9>. Acesso em 18/06/2015.

LÉVY, Pierre. *Cibercultura*. São Paulo: Ed 34,1999. 264 p. (Coleção TRANS).

LEMOS, André. *Cibercultura e Mobilidade***:** A era da conexão. XXVIII Congresso Brasileiro de Ciências da Comunicação – Uerj – 5 a 9 de setembro de 2005.

LEMOS, André; CUNHA, Paulo(orgs). *Olhares sobre a Cibercultura*. Sulina, Porto Alegre, 2003; pp.11-23.

LEMOS, A. *Cibercultura*: Tecnologia e Vida Social na Cultura Contemporânea. Sulina, Porto Alegre, 2002.

MONTEIRO, Luís. *A internet como meio de comunicação*: Possibilidades e limitações. XXIV Congresso Brasileiro de Comunicação. Campo Grande/MS. Setembro de 2001.

NETO, Mario Furlaneto; GUIMARÃES, José Augusto Chaves. *Crimes na Internet*: elementos para uma reflexão sobre a ética informacional. R. CEJ. Brasília, n. 20, p. 67-73, 2003.

OLIVEIRA, Jôline Cristina de. *O Cibercrime e as Leis 12.735 e 12.737/2012*. 2013. Trabalho de Conclusão de Curso. Departamento de Direito. São Cristóvão, 2013.

Pesquisa Brasileira de Mídia. 2015. Disponível na internet via WWW. URL: <http://www.brasil.gov.br/governo/2014/12/cerca-de-48-dos-brasileiros-usam-internet-regularmente>. Acesso em 23/06/2015.

_____. 2016. Disponível na internet via WWW. URL: < http://pesquisademidia.gov.br/#/Internet>. Acesso em 21/07/2018.

PINHEIRO, Emeline Piva. *Crimes Virtuais*: Uma análise da criminalidade informática e da resposta estatal. 2006.

RECUERO, Raquel da Cunha. *Comunidades Virtuais em Redes Sociais na Internet*: Uma proposta de estudo. 2005. Disponível na internet via WWW. URL: < http://www.raquelrecuero.com/seminario2005.pdf >. Acesso em 14/05/2015.

Revista Época. 2011. *Maior ataque hacker no Brasil partiu da Itália*. Disponível na internet via WWW. URL: <http://revistaepoca.globo.com/Revista/Epoca/0,,EMI243559-15224,00.html>. Acesso em 14/05/2015.

RICHARDSON, Roberto Jarry. *Pesquisa Social*: Métodos e técnicas. 3ª edição. São Paulo: Atlas, 2012.

ROESCH, S. M. A. *Projetos de estágio do curso de administração*: guia para pesquisas, projetos, estágios e trabalhos de conclusão de curso. São Paulo: Atlas, 1996.

SANTOS, Danielly Maia dos Santos. *Os novos crimes de informática criados com o advento das leis 12.735/2012 e 12.737/2012*. Monografia. Faculdade de Direito de Presidente Prudente. Faculdades Integradas "Antônio Eufrásio de Toledo". Presidente Prudente/SP, 2014.

SILVA, C. M. da. *Tecnologias de informação e comunicação e suas implicações para o exercício da nova cidadania:* as novas tecnologias de informação e comunicação e a emergência da sociedade informacional. 2006. Dissertação. (Especialização em Pensamento Político Brasileiro). Programa de Pós-Graduação. Universidade Federal de Santa Maria. Rio Grande do Sul, 2006.

SILVA, Evandro Andrade da. *Crimes na Internet*. 2011. Disponível na internet via WWW. URL: < http://egov.ufsc.br/portal/conteudo/crimes-na-internet-precau%C3%A7%C3%B5es-necess%C3%A1rias-ao-navegar-pela-interne/>. Acesso em 14/05/2015.

SILVA, Vergílio Ricardo Britto da. *Preocupação com a privacidade na internet:* uma pesquisa exploratória no cenário brasileiro. Dissertação (mestrado). Faculdade de Administração, Contabilidade e Economia. PUCRS. Porto Alegre, 2015.

VERGARA, Sylvia Constante: *Projetos e relatórios de pesquisa em administração.* 2 edição. São Paulo. Editora Atlas S.A, 1998.

VIEIRA, Eduardo. *Os bastidores da internet no Brasil.* Barueri/SP. Ed. Manole, 2003.

WENDT, Emerson. *Lista dos Estados que possuem Delegacia de Polícia de combate aos Crimes Cibernéticos*. 2014. Disponível na internet via WWW. URL:

<http://www.emersonwendt.com.br/2010/07/lista-dos-estados-com-possuem.html>. Acesso em 23/06/2015.

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

ZANATTA, Leonardo. *O Direito Digital e as Implicações Cíveis Decorrentes das Relações Virtuais*. Trabalho de Conclusão de Curso. Pontifícia Universidade Católica do Rio Grande do Sul –PUCRS. 2010.

APÊNDICES

APÊNDICE I – QUESTIONÁRIO

1) Qual a sua idade?
   ( ) 14 a 20
   ( ) 20 a 25
   ( ) 25 a 30
   ( ) 30 a 35
   ( ) 35 a 40
   ( ) acima de 45

2) Qual o seu sexo?
   ( ) Masculino ( ) Feminino

3) Qual seu grau de instrução?
   ( ) nunca estudou
   ( ) Ensino fundamental incompleto
   ( ) Ensino fundamental completo
   ( ) Ensino médio incompleto
   ( ) Ensino médio completo
   ( ) Ensino superior incompleto
   ( ) Ensino superior completo

4) Qual a sua renda familiar?
   ( ) Até 1 salário mínimo
   ( ) De 2 a 3 salários mínimos
   ( ) De 4 a 6 salários mínimos
   ( ) De 7 a 9 salários mínimos
   ( ) Acima de 10 salários mínimos

Caso tenha respondido sim na pergunta anterior responda as perguntas seguintes:

5) Com qual frequência você acessa a internet?
   ( ) 1 vez por mês

( ) 1 vez por semana

( ) Todos os dias

6) Em qual local você costuma acessar a internet?

( ) Em casa

( ) No trabalho

( ) Em casa e no trabalho

( ) Outro. Onde? (_____)

7) Qual o dispositivo que você mais utiliza para se conectar à internet?

( ) Computador

( ) Notebook

( ) Tablet

( ) Celular

8) Você utiliza as redes sociais?

( ) Sim ( ) Não

9) Quais as que mais utiliza?

( ) *Facebook*

( ) *Instagram*

( ) *Snapchat*

( ) *Twitter*

( ) *Youtube*

( ) Outra. Qual? _____

10) Qual as precauções que toma ao utilizar a internet? (Marque quantas opções forem necessárias).

( ) Não forneço dados pessoais

( ) Não abro e-mails de remetentes estranhos

( ) Não compro em sites que não conheça a origem

( ) Não clico em links estranhos

( ) Não tomo nenhum precaução

11) Você já foi vítima de algum crime cibernético?
( ) Sim ( ) Não

12) Caso sim, qual foi o crime sofrido? (Marque quantas opções forem necessárias).
( ) Falsificação de cartão de crédito
( ) Divulgação de arquivos pessoais
( ) Roubo de senhas pessoais
( ) Invasão de conta bancaria
( ) Roubo de identidade
( ) Pedofilia
( ) Calunia e difamação
( ) Ameaça
( ) Discriminação
( ) Outro. Qual?_____

13) Caso tenha respondido sim na questão 10, responda: Você tomou alguma medida legal perante o crime sofrido?
( ) Sim ( ) Não

Para responder as perguntas 14 à 17 utilize a escala de 1 à 10, onde 1 corresponde a “discordo totalmente” e 10, “concordo totalmente”.

14) Você conhece ou já ouviu falar sobre as leis brasileiras de acesso à internet?
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5 ( ) 6 ( ) 7 ( ) 8 ( ) 9 ( ) 10

15) Você acredita que se a população tivesse mais conhecimento sobre as leis, os crimes cometidos não aconteceriam?
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5 ( ) 6 ( ) 7 ( ) 8 ( ) 9 ( ) 10

16) Você conhece o seus direitos e deveres dispostos na lei sobre o acesso à internet?
( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5 ( ) 6 ( ) 7 ( ) 8 ( ) 9 ( ) 10

17) Você acredita na efetividade da legislação brasileira de acesso à internet?

( ) 1 ( ) 2 ( ) 3 ( ) 4 ( ) 5 ( ) 6 ( ) 7 ( ) 8 ( ) 9 ( ) 10

ANEXOS

ANEXO I – LEI Nº 12.735, DE 30 DE NOVEMBRO DE 2012.

Altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, o Decreto-Lei nº 1.001, de 21 de outubro de 1969 - Código Penal Militar, e a Lei nº 7.716, de 5 de janeiro de 1989, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, que sejam praticadas contra sistemas informatizados e similares; e dá outras providências.

Art. 2º (VETADO)

Art. 3º (VETADO)

Art. 4º Os órgãos da polícia judiciária estruturarão, nos termos de regulamento, setores e equipes especializadas no combate à ação delituosa em rede de computadores, dispositivo de comunicação ou sistema informatizado.

Art. 5º O inciso II do § 3º do art. 20 da Lei nº 7.716, de 5 de janeiro de 1989, passa a vigorar com a seguinte redação:

"Art. 20. .....

.....

§ 3º .....

.....

II - a cessação das respectivas transmissões radiofônicas, televisivas, eletrônicas ou da publicação por qualquer meio;

....." (NR)

Art. 6º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Paulo Bernardo Silva
Maria do Rosário Nunes

ANEXO II - LEI Nº 12.737, DE 30 DE NOVEMBRO DE 2012.

Dispõe sobre a tipificação criminal de delitos informáticos; altera o Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal; e dá outras providências.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

Art. 1º Esta Lei dispõe sobre a tipificação criminal de delitos informáticos e dá outras providências.

Art. 2º O Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, fica acrescido dos seguintes arts. 154-A e 154-B:

"Invasão de dispositivo informático

Art. 154-A. Invadir dispositivo informático alheio, conectado ou não à rede de computadores, mediante violação indevida de mecanismo de segurança e com o fim de obter, adulterar ou destruir dados ou informações sem autorização expressa ou tácita do titular do dispositivo ou instalar vulnerabilidades para obter vantagem ilícita:

Pena - detenção, de 3 (três) meses a 1 (um) ano, e multa.

§ 1º Na mesma pena incorre quem produz, oferece, distribui, vende ou difunde dispositivo ou programa de computador com o intuito de permitir a prática da conduta definida no **caput**.

§ 2º Aumenta-se a pena de um sexto a um terço se da invasão resulta prejuízo econômico.

§ 3º Se da invasão resultar a obtenção de conteúdo de comunicações eletrônicas privadas, segredos comerciais ou industriais, informações sigilosas, assim definidas em lei, ou o controle remoto não autorizado do dispositivo invadido:

Pena - reclusão, de 6 (seis) meses a 2 (dois) anos, e multa, se a conduta não constitui crime mais grave.

§ 4º Na hipótese do § 3º, aumenta-se a pena de um a dois terços se houver divulgação, comercialização ou transmissão a terceiro, a qualquer título, dos dados ou informações obtidos.

§ 5º Aumenta-se a pena de um terço à metade se o crime for praticado contra:

I - Presidente da República, governadores e prefeitos;

II - Presidente do Supremo Tribunal Federal;

III - Presidente da Câmara dos Deputados, do Senado Federal, de Assembleia Legislativa de Estado, da Câmara Legislativa do Distrito Federal ou de Câmara Municipal; ou

IV - dirigente máximo da administração direta e indireta federal, estadual, municipal ou do Distrito Federal."

"Ação penal

Art. 154-B. Nos crimes definidos no art. 154-A, somente se procede mediante representação, salvo se o crime é cometido contra a administração pública direta ou indireta de qualquer dos Poderes da União, Estados, Distrito Federal ou Municípios ou contra empresas concessionárias de serviços públicos."

Art. 3º Os arts. 266 e 298 do Decreto-Lei nº 2.848, de 7 de dezembro de 1940 - Código Penal, passam a vigorar com a seguinte redação:

“Interrupção ou perturbação de serviço telegráfico, telefônico, informático, telemático ou de informação de utilidade pública

Art. 266. .....

§ 1º Incorre na mesma pena quem interrompe serviço telemático ou de informação de utilidade pública, ou impede ou dificulta-lhe o restabelecimento.

§ 2º Aplicam-se as penas em dobro se o crime é cometido por ocasião de calamidade pública.” (NR)

“Falsificação de documento particular

Art. 298. .....

Falsificação de cartão

Parágrafo único. Para fins do disposto no caput, equipara-se a documento particular o cartão de crédito ou débito.” (NR)

Art. 4º Esta Lei entra em vigor após decorridos 120 (cento e vinte) dias de sua publicação oficial.

Brasília, 30 de novembro de 2012; 191º da Independência e 124º da República.

DILMA ROUSSEFF

José Eduardo Cardozo

ANEXO III - LEI Nº 12.965, DE 23 DE ABRIL DE 2014.

Estabelece princípios, garantias, direitos e deveres para o uso da Internet no Brasil.

A PRESIDENTA DA REPÚBLICA Faço saber que o Congresso Nacional decreta e eu sanciono a seguinte Lei:

CAPÍTULO I
DISPOSIÇÕES PRELIMINARES

Art. 1º Esta Lei estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e determina as diretrizes para atuação da União, dos Estados, do Distrito Federal e dos Municípios em relação à matéria.

Art. 2º A disciplina do uso da internet no Brasil tem como fundamento o respeito à liberdade de expressão, bem como:

I - o reconhecimento da escala mundial da rede;

II - os direitos humanos, o desenvolvimento da personalidade e o exercício da cidadania em meios digitais;

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

V - a livre iniciativa, a livre concorrência e a defesa do consumidor; e

VI - a finalidade social da rede.

Art. 3º A disciplina do uso da internet no Brasil tem os seguintes princípios:

I - garantia da liberdade de expressão, comunicação e manifestação de pensamento, nos termos da Constituição Federal;

II - proteção da privacidade;

III - proteção dos dados pessoais, na forma da lei;

IV - preservação e garantia da neutralidade de rede;

V - preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;

VI - responsabilização dos agentes de acordo com suas atividades, nos termos da lei;

VII - preservação da natureza participativa da rede;

VIII - liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta Lei.

Parágrafo único. Os princípios expressos nesta Lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:

I - do direito de acesso à internet a todos;

II - do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;

III - da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e

IV - da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta Lei, considera-se:

I - internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;

II - terminal: o computador ou qualquer dispositivo que se conecte à internet;

III - endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;

IV - administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao País;

V - conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI - registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;

VII - aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e

VIII - registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

Art. 6º Na interpretação desta Lei serão levados em conta, além dos fundamentos, princípios e objetivos previstos, a natureza da internet, seus usos e costumes particulares e sua importância para a promoção do desenvolvimento humano, econômico, social e cultural.

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:

I - inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;

II - inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;

III - inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;

IV - não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;

V - manutenção da qualidade contratada da conexão à internet;

VI - informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;

VII - não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;

VIII - informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX - consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;

X - exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta Lei;

XI - publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;

XII - acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e

XIII - aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.

Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no **caput**, tais como aquelas que:

I - impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou

II - em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

Art. 9º O responsável pela transmissão, comutação ou roteamento tem o dever de tratar de forma isonômica quaisquer pacotes de dados, sem distinção por conteúdo, origem e destino, serviço, terminal ou aplicação.

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do Presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta Lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:

I - requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e

II - priorização de serviços de emergência.

§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no **caput** deve:

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

III - informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e

IV - oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.

§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

Seção II

Da Proteção aos Registros, aos Dados Pessoais e às Comunicações Privadas

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta Lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.

§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no **caput**, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste Capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.

§ 3º O disposto no **caput** não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.

§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.

§ 1º O disposto no **caput** aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.

§ 2º O disposto no **caput** aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.

§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao

armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:

I - advertência, com indicação de prazo para adoção de medidas corretivas;

II - multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;

III - suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou

IV - proibição de exercício das atividades que envolvam os atos previstos no art. 11.

Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o **caput** sua filial, sucursal, escritório ou estabelecimento situado no País.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 1 (um) ano, nos termos do regulamento.

§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no **caput**.

§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 60 (sessenta) dias, contados a partir do requerimento, para ingressar com o pedido de autorização judicial de acesso aos registros previstos no **caput**.

§ 4º O provedor responsável pela guarda dos registros deverá manter sigilo em relação ao requerimento previsto no § 2º, que perderá sua eficácia caso o pedido de autorização judicial seja indeferido ou não tenha sido protocolado no prazo previsto no § 3º.

§ 5º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 6º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Subseção II
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Conexão

Art. 14. Na provisão de conexão, onerosa ou gratuita, é vedado guardar os registros de acesso a aplicações de internet.

Subseção III
Da Guarda de Registros de Acesso a Aplicações de Internet na Provisão de Aplicações

Art. 15. O provedor de aplicações de internet constituído na forma de pessoa jurídica e que exerça essa atividade de forma organizada, profissionalmente e com fins econômicos deverá manter os respectivos registros de acesso a aplicações de internet, sob sigilo, em ambiente controlado e de segurança, pelo prazo de 6 (seis) meses, nos termos do regulamento.

§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no **caput** a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.

§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no **caput**, observado o disposto nos §§ 3º e 4º do art. 13.

§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste Capítulo.

§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:

I - dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou

II - de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

Art. 17. Ressalvadas as hipóteses previstas nesta Lei, a opção por não guardar os registros de acesso a aplicações de internet não implica responsabilidade sobre danos decorrentes do uso desses serviços por terceiros.

Seção III
Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

Art. 18. O provedor de conexão à internet não será responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros.

Art. 19. Com o intuito de assegurar a liberdade de expressão e impedir a censura, o provedor de aplicações de internet somente poderá ser responsabilizado civilmente por danos decorrentes de conteúdo gerado por terceiros se, após ordem judicial específica, não tomar as providências para, no âmbito e nos limites técnicos do seu serviço e dentro do prazo assinalado, tornar indisponível o conteúdo apontado como infringente, ressalvadas as disposições legais em contrário.

§ 1º A ordem judicial de que trata o **caput** deverá conter, sob pena de nulidade, identificação clara e específica do conteúdo apontado como infringente, que permita a localização inequívoca do material.

§ 2º A aplicação do disposto neste artigo para infrações a direitos de autor ou a direitos conexos depende de previsão legal específica, que deverá respeitar a liberdade de expressão e demais garantias previstas no art. 5ºda Constituição Federal.

§ 3º As causas que versem sobre ressarcimento por danos decorrentes de conteúdos disponibilizados na internet relacionados à honra, à reputação ou a direitos de personalidade, bem como sobre a indisponibilização desses conteúdos por provedores de aplicações de internet, poderão ser apresentadas perante os juizados especiais.

§ 4º O juiz, inclusive no procedimento previsto no § 3º, poderá antecipar, total ou parcialmente, os efeitos da tutela pretendida no pedido inicial, existindo prova inequívoca do fato e considerado o interesse da coletividade na disponibilização do conteúdo na internet, desde que presentes os requisitos de verossimilhança da alegação do autor e de fundado receio de dano irreparável ou de difícil reparação.

Art. 20. Sempre que tiver informações de contato do usuário diretamente responsável pelo conteúdo a que se refere o art. 19, caberá ao provedor de aplicações de internet comunicar-lhe os motivos e informações relativos à indisponibilização de conteúdo, com informações que permitam o contraditório e a ampla defesa em juízo, salvo expressa previsão legal ou expressa determinação judicial fundamentada em contrário.

Parágrafo único. Quando solicitado pelo usuário que disponibilizou o conteúdo tornado indisponível, o provedor de aplicações de internet que exerce essa atividade de forma organizada, profissionalmente e com fins econômicos substituirá o conteúdo tornado indisponível pela motivação ou pela ordem judicial que deu fundamento à indisponibilização.

Art. 21. O provedor de aplicações de internet que disponibilize conteúdo gerado por terceiros será responsabilizado subsidiariamente pela violação da intimidade decorrente da divulgação, sem autorização de seus participantes, de imagens, de vídeos ou de outros materiais contendo cenas de nudez ou de atos sexuais de caráter privado quando, após o recebimento de notificação pelo participante ou seu representante legal, deixar de promover, de forma diligente, no âmbito e nos limites técnicos do seu serviço, a indisponibilização desse conteúdo.

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

Seção IV
Da Requisição Judicial de Registros

Art. 22. A parte interessada poderá, com o propósito de formar conjunto probatório em processo judicial cível ou penal, em caráter incidental ou autônomo, requerer ao juiz que ordene ao responsável pela guarda o fornecimento de registros de conexão ou de registros de acesso a aplicações de internet.

Parágrafo único. Sem prejuízo dos demais requisitos legais, o requerimento deverá conter, sob pena de inadmissibilidade:

I - fundados indícios da ocorrência do ilícito;

II - justificativa motivada da utilidade dos registros solicitados para fins de investigação ou instrução probatória; e

III - período ao qual se referem os registros.

Art. 23. Cabe ao juiz tomar as providências necessárias à garantia do sigilo das informações recebidas e à preservação da intimidade, da vida privada, da honra e da imagem do usuário, podendo determinar segredo de justiça, inclusive quanto aos pedidos de guarda de registro.

CAPÍTULO IV
DA ATUAÇÃO DO PODER PÚBLICO

Art. 24. Constituem diretrizes para a atuação da União, dos Estados, do Distrito Federal e dos Municípios no desenvolvimento da internet no Brasil:

I - estabelecimento de mecanismos de governança multiparticipativa, transparente, colaborativa e democrática, com a participação do governo, do setor empresarial, da sociedade civil e da comunidade acadêmica;

II - promoção da racionalização da gestão, expansão e uso da internet, com participação do Comitê Gestor da internet no Brasil;

III - promoção da racionalização e da interoperabilidade tecnológica dos serviços de governo eletrônico, entre os diferentes Poderes e âmbitos da Federação, para permitir o intercâmbio de informações e a celeridade de procedimentos;

IV - promoção da interoperabilidade entre sistemas e terminais diversos, inclusive entre os diferentes âmbitos federativos e diversos setores da sociedade;

V - adoção preferencial de tecnologias, padrões e formatos abertos e livres;

VI - publicidade e disseminação de dados e informações públicos, de forma aberta e estruturada;

VII - otimização da infraestrutura das redes e estímulo à implantação de centros de armazenamento, gerenciamento e disseminação de dados no País, promovendo a qualidade técnica, a inovação e a difusão das aplicações de internet, sem prejuízo à abertura, à neutralidade e à natureza participativa;

VIII - desenvolvimento de ações e programas de capacitação para uso da internet;

IX - promoção da cultura e da cidadania; e

X - prestação de serviços públicos de atendimento ao cidadão de forma integrada, eficiente, simplificada e por múltiplos canais de acesso, inclusive remotos.

Art. 25. As aplicações de internet de entes do poder público devem buscar:

I - compatibilidade dos serviços de governo eletrônico com diversos terminais, sistemas operacionais e aplicativos para seu acesso;

II - acessibilidade a todos os interessados, independentemente de suas capacidades físico-motoras, perceptivas, sensoriais, intelectuais, mentais, culturais e sociais, resguardados os aspectos de sigilo e restrições administrativas e legais;

III - compatibilidade tanto com a leitura humana quanto com o tratamento automatizado das informações;

IV - facilidade de uso dos serviços de governo eletrônico; e

V - fortalecimento da participação social nas políticas públicas.

Art. 26. O cumprimento do dever constitucional do Estado na prestação da educação, em todos os níveis de ensino, inclui a capacitação, integrada a outras práticas educacionais, para o uso seguro, consciente e responsável da internet como ferramenta para o exercício da cidadania, a promoção da cultura e o desenvolvimento tecnológico.

Art. 27. As iniciativas públicas de fomento à cultura digital e de promoção da internet como ferramenta social devem:

I - promover a inclusão digital;

II - buscar reduzir as desigualdades, sobretudo entre as diferentes regiões do País, no acesso às tecnologias da informação e comunicação e no seu uso; e

III - fomentar a produção e circulação de conteúdo nacional.

Art. 28. O Estado deve, periodicamente, formular e fomentar estudos, bem como fixar metas, estratégias, planos e cronogramas, referentes ao uso e desenvolvimento da internet no País.

CAPÍTULO V
DISPOSIÇÕES FINAIS

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.

Parágrafo único. Cabe ao poder público, em conjunto com os provedores de conexão e de aplicações de internet e a sociedade civil, promover a educação e fornecer informações sobre o uso dos programas de computador previstos no **caput**, bem como para a definição de boas práticas para a inclusão digital de crianças e adolescentes.

Art. 30. A defesa dos interesses e dos direitos estabelecidos nesta Lei poderá ser exercida em juízo, individual ou coletivamente, na forma da lei.

Art. 31. Até a entrada em vigor da lei específica prevista no § 2º do art. 19, a responsabilidade do provedor de aplicações de internet por danos decorrentes de conteúdo gerado por terceiros, quando se tratar de infração a direitos de autor ou a direitos conexos, continuará a ser disciplinada pela legislação autoral vigente aplicável na data da entrada em vigor desta Lei.

Art. 32. Esta Lei entra em vigor após decorridos 60 (sessenta) dias de sua publicação oficial.

Brasília, 23 de abril de 2014; 193º da Independência e 126º da República.

DILMA ROUSSEFF
José Eduardo Cardozo
Miriam Belchior
Paulo Bernardo Silva
Clélio Campolina Diniz