

**UNIVERSIDADE FEDERAL DE CAMPINA GRANDE - UFCG  
CENTRO DE CIÊNCIAS JURÍDICAS E SOCIAIS - CCJS  
UNIDADE ACADÊMICA DE DIREITO**

**DIÊGO MARTINS DINIZ**

**A RESPONSABILIDADE DO MANTENEDOR DO SITE EM CASO DE DANO MO-  
RAL PRATICADO EM REDES SOCIAIS**

**SOUSA  
2013**

DIÊGO MARTINS DINIZ

**A RESPONSABILIDADE DO MANTENEDOR DO SITE EM CASO DE DANO MORAL PRATICADO EM REDES SOCIAIS**

Trabalho monográfico apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Esp. Admilson Leite de Almeida Júnior.

SOUSA  
2013

DIÊGO MARTINS DINIZ

A RESPONSABILIDADE DO MANTENEDOR DO SITE EM CASO DE DANO MORAL  
PRATICADO EM REDES SOCIAIS

Trabalho monográfico apresentado ao Curso de Direito do Centro de Ciências Jurídicas e Sociais da Universidade Federal de Campina Grande, como exigência parcial da obtenção do título de Bacharel em Ciências Jurídicas e Sociais.

Orientador: Prof. Esp. Admilson Leite de Almeida Júnior.

BANCA EXAMINADORA:

Data da Aprovação: 19 de setembro de 2013.

---

Professor Esp. Admilson Leite de Almeida Júnior  
Orientador

---

Professor Me. Eduardo Jorge P. de Oliveira  
Examinador

---

Professora Esp. Cecília Paranhos  
Examinadora

SOUSA  
2013

Ao Deus todo poderoso e ocupado, por atender as minhas súplicas de força para não desistir.  
À minha avó Raimunda, por ter guiado meus primeiros passos nos estudos com a garra de uma mãe.  
Aos meus pais, por me dedicarem o sentimento da proteção nos momentos de maior dificuldade.

## **AGRADECIMENTOS**

Um grande muro não se constrói sozinho. Grandes sonhos não se realizam de forma unilateral. O sucesso é formado por um conjunto de fatores que convergem para a vitória.

Ao bom Deus todo poderoso e ocupado, agradeço por guiar e iluminar meus passos nessa longa caminhada.

Agradeço aos meus pais Iolando e Josiana, que são as bases mais fortes de minha vida.

Agradeço à minha avó Raimunda, pela garra em guiar meus primeiros passos escolares e por me ensinar o verdadeiro valor da palavra esforço.

Sou grato à minha Tia Joana Darc por ter protagonizado o papel de mãe em diversas fazes da minha vida.

Com muito carinho, agradeço também ao meu irmão Eloi, por ser parceiro e amigo em todos os momentos, sejam estes fáceis ou difíceis.

Agradeço também a minha namorada Amanda, pelo carinho e cumplicidade, por compreender as ausências e me apoiar nos momentos de dificuldade.

Rendo meus agradecimentos ao meu orientador Professor Admilson Leite, que disponibilizou e dedicou seu tempo para feitura deste trabalho com a capacidade que lhe é peculiar.

Por fim, agradeço a todos os meus amigos que de alguma forma contribuíram no caminhar deste árduo percurso.

*“Sonho que se sonha só é só um sonho que se sonha só, mas sonho que se sonha junto é realidade.”*

Raul Seixas

## RESUMO

Em razão da ausência de legislação específica, a responsabilização do mantenedor de sites em caso de dano moral praticado em redes sociais tornou-se matéria de entendimento controverso na doutrina e na jurisprudência. Há uma ampla divergência quanto a teoria da responsabilidade a ser aplicada. Se objetiva, o mantenedor será responsabilizado independentemente da comprovação de culpa, sob o fundamento de que a publicação de conteúdo ofensivo nas mídias sociais constitui risco inerente à própria atividade do negócio. Se subjetiva, ao provedor de conteúdo só será atribuída a responsabilidade nos casos em que for omissor na exclusão imediata do conteúdo moralmente danoso, quando a retirada for pleiteada pela vítima ou por quem de direito, situação em que responderá de forma solidária com o autor do dano, como consequência da sua inércia. O objetivo geral buscado no trabalho é a compreensão dos novos paradigmas jurídicos da tutela civil da intimidade, na responsabilização dos causadores de danos dessa natureza em redes sociais. De forma específica objetiva analisar o instituto da responsabilidade civil na sociedade da informação, assim como a responsabilidade do site em caso de dano moral. O método empregado na pesquisa é o dedutivo, partindo de uma premissa maior para uma específica. Para isso, é adotada uma pesquisa indireta, com análise de leis, acórdãos, entendimentos jurisprudenciais, bem como doutrinária através de livros, revistas, artigos científicos, estatísticas e sites da Internet. Como resultado da pesquisa, se compreende pela responsabilização subjetiva do mantenedor dos sites em caso de dano moral praticado nas redes sociais, com a observância de que em sendo provada a sua negligência responderá de forma solidária com o causador do dano pela inércia.

Palavras-chave: Responsabilidade. Mantenedor. Internet. Redes Sociais.

## ABSTRACT

Due to the absence of specific legislation, the responsabilization of websites' maintainer in events of damage practiced in social networks has become a controversial matter of understanding for the doctrine and jurisprudence. There is a wide disagreement about what theory of responsibility has to be applied. If objective, the maintainer shall be liable independently of proof of guilt, on the grounds that the publication of offensive content in social media is risk inherent in this business activity. If subjective, the content provider will only be blamed in cases where he stay absent in the immediate exclusion of the content morally harmful, when the withdrawal is being claimed by the victim or those eligible, in which respond in solidarity with the author's damage as a result of its inertia. However, to discover the placement majority applied in national courts as matter, it is first necessary a historical analysis of the development of communication's technologies, especially the Internet and computer science, as well as its importance in expanding access to information. The general objective sought in the work is to understand the new paradigms civil legal guardianship of intimacy, accountability of causing such damage on social networks. Specifically aims to analyze the institution of civil liability in the information society, as well as the responsibility of the site in case of damage. The research method employed is an deductive, based on a major premise for a specific. For this, we adopted a documentary research with analysis of laws, judgments, jurisprudential understandings and doctrinal through books, magazines, papers, statistics and websites. As the research result, we conclude for the maintainer's subjective liability in the event of damage practiced in social networks, with the observance of, if its proven negligence, respond in solidarity with the causer by inertia.

Key words: Responsibility. Sites's Maintainer. Internet. Social Networks

## **LISTA DE SIGLAS E ABREVIATURAS**

ARPA - Advanced Research Projects Agency  
CC – Código Civil  
CGI.br – Comitê Gestor de Internet no Brasil  
CGU – Controladoria Geral da União  
CPC – Código de Processo Civil  
DRDoS – Distribution Reflection Denial of Service  
DUDH – Declaração Universal dos Direitos do Homem  
ENIAC - Electronic Numerical Integrator And Calculator  
e-SIC – Sistema Eletrônico do Serviço de Informação aos Cidadãos  
EUA – Estados Unidos da América  
FAPESP – Fundação de Amparo à Pesquisa do Estado de São Paulo  
IP- Internet Protocol  
LAI – Lei de Acesso a Informação  
NSA - National Security Agency  
NSFnet - National Science Foundation Network  
ONGs – Organizações Não Governamentais  
ONU – Organizações das Nações Unidas  
PAND – Pesquisa Nacional por Amostra de Domicílios  
RPN – Rede Nacional de Pesquisa  
STJ – Superior Tribunal de Justiça  
TCP - Transmission Control Protocol  
URLs – Uniform Resource Locators  
WWW – World Wide Web

## SUMÁRIO

<b>1 INTRODUÇÃO</b> .....	10
<b>2 O DIREITO À INFORMAÇÃO E SEUS EFEITOS JURÍDICOS</b> .....	12
2.1 O DIREITO À INFORMAÇÃO ENQUANTO DIREITO FUNDAMENTAL.....	12
2.2 A INFORMÁTICA E SUA APLICAÇÃO NA AMPLIAÇÃO DO ACESSO À INFORMAÇÃO .....	15
2.3 OS EFEITOS JURÍDICOS DA VIOLAÇÃO AO DIREITO À INFORMAÇÃO .....	19
<b>3 A INTERNET E O DIREITO À INTIMIDADE</b> .....	22
3.1 O SURGIMENTO DA INTERNET.....	22
3.2 A INTERNET NO BRASIL E SUA REGULAMENTAÇÃO .....	24
3.3 O DIREITO À INTIMIDADE E A DIGNIDADE DA PESSOA HUMANA .....	27
3.4 A VIOLAÇÃO DA INTIMIDADE ATRAVÉS DA INTERNET .....	29
<b>4 AS REDES SOCIAIS E A INVASÃO DA PRIVACIDADE</b> .....	33
4.1 AS REDES SOCIAIS E SUA IMPORTÂNCIA.....	33
4.2 A INVASÃO DA PRIVACIDADE PELAS REDES SOCIAIS .....	36
4.3 O CASO CAROLINA DIECHMANN E O ADVENTO DA LEI Nº 12.737/2012.....	40
4.3 OS EFEITOS CIVIS NA INVASÃO DA PRIVACIDADE PELAS REDES SOCIAIS E A IDENTIFICAÇÃO DO RESPONSÁVEL .....	43
<b>CONSIDERAÇÕES FINAIS</b> .....	47
<b>REFERÊNCIAS</b> .....	49
<b>ANEXOS</b> .....	53

## 1 INTRODUÇÃO

Concomitantemente ao surgimento da sociedade nasceu a necessidade de o homem comunicar-se com seus pares. Desde os primórdios, a informação passou a figurar como a mais importante ferramenta no desenvolvimento da sociedade. Em razão dessa relevância, ao longo da história, a informação passou por diversas mudanças conceituais, sendo tratada como direito fundamental apenas com a normatização dos direitos humanos, instituída pela Revolução Francesa em 1789.

Após a Segunda Guerra Mundial, os avanços tecnológicos no trato da informação enveredaram para o surgimento de mecanismos cada vez mais céleres e gigantescos, o que culminou na descoberta da maior criação humana de todos os tempos, a Internet.

Também denominada de rede mundial de computadores, a Internet, passou a interligar de forma instantânea terras de distâncias imensuráveis. Como resultado desse encurtamento de espaços, um novo gênero de interação social eclodiu no mundo, as chamadas redes sociais, conceituada aqui como um ambiente virtual de relações instantâneas livres de restrições. Acontece que, essa liberdade excessiva trouxe como consequência primeira, a afeição pela exposição da intimidade em detrimento do direito à privacidade.

A problemática surge quando essa invasão da privacidade alheia acarreta uma consequência danosas ao indivíduo, havendo, por conseguinte, a necessidade de uma intervenção jurídica para reparação do dano, o que no âmbito virtual se apresenta de forma peculiar, em face da dificuldade de identificação do agente causador do dano. Exemplo disso é o caso Carolina Dieckmann, que deu origem a Lei nº 12.737/2012, responsável por tipificar os crimes cibernéticos no Brasil.

O ponto central da presente pesquisa objetiva analisar a responsabilidade do mantenedor do site em caso de dano moral ocorrido nas redes sociais, que em vista da ausência legislativa no trato da matéria, ainda é assunto divergente na jurisprudência pátria.

Para realização deste estudo utilizar-se-á como metodologia de abordagem o método dedutivo, uma vez que partirá de uma premissa maior para uma premissa menor e específica. No que se refere ao método de procedimento aplicar-se-á o monográfico com um estudo detalhado do tema proposto. Quanto à técnica de pesquisa far-se-á uso de documentação indireta, pois terá como suporte: livros, artigos científicos, a Constituição Federal, Leis infraconstitucionais, pesquisas de dados estatísticos e sites de Internet.

Para tanto, estruturar-se-á o corrente trabalho em três capítulos. Inicialmente, será feita uma análise do direito à informação, explicando-se a sua origem e classificação, bem como a aplicação da ciência informática na melhoria do acesso à informação e os efeitos jurídicos da sua violação.

No segundo capítulo será feito um estudo a cerca da Internet e da sua relação com o direito à intimidade. Com esse intuito, apresentar-se-á um histórico sobre a gênese militar da Internet, a sua chegada e regulamentação no Brasil para, só depois, analisar os efeitos jurídicos da violação do direito à intimidade e a dignidade da pessoa humana.

Por fim, no terceiro capítulo o enfoque será destinado ao novo modelo de interação da humanidade, as redes sociais, mostrando a sua importância, o número de usuários atualmente no mundo e no Brasil, bem como os efeitos jurídicos e sociais ocasionados pela sua mitigação no conceito de privacidade e intimidade. O ponto primordial deste capítulo será a análise da nova lei que tipificou os delitos informáticos, a Lei Carolina Diechmann, no âmbito penal, bem como o estudo a cerca da responsabilidade do mantenedor de site em caso de dano moral ocasionado em redes sociais, com a análise da jurisprudência pátria e da doutrina especializada no assunto, tendo em vista a ausência de regulamentação específica na seara civil.

## 2 O DIREITO À INFORMAÇÃO E SEUS EFEITOS JURÍDICOS

O progresso da sociedade está totalmente interligado com a expansão da comunicação. A informação e sua transmissão por entre os povos são fatores imprescindíveis ao homem.

Carvalho (1999, p. 01) relata que “não há sociedade sem comunicação. O pensar e o transmitir o pensamento são tão vitais para o homem como a liberdade física”. Deduz-se, portanto, que o dever de informar e o direito de ser informado andam juntos ao crescimento de uma sociedade democrática.

A globalização encurtando os espaços e o acelerado avanço da tecnologia criou um mundo virtual, onde a rapidez na difusão das informações fez com que a sociedade passasse a existir em um novo modelo de interação. Novas técnicas comerciais e econômicas, de marketing, de relacionamento entre as pessoas, de conflitos e de danos, bem como de novos delitos, até então desconhecidos, vêm surgir nesse novo mundo. É o contemporâneo mundo da Internet.

Surge uma nova era para a humanidade, a “Era da Informação” ou também chamada de “Era Digital”, com novos conceitos e novos padrões, bem como novos conflitos geradores de danos, acarretando em uma urgente obrigação de se analisar a interação entre as novas tecnologias da informação e a sociedade, e seus efeitos jurídicos.

### 2.1 O DIREITO À INFORMAÇÃO ENQUANTO DIREITO FUNDAMENTAL

O direito à informação faz parte de uma tríade de direitos englobados pela Liberdade de Informação, princípio amplamente assegurado na Declaração Universal dos Direitos do Homem.

A tríade consiste no direito de informar, referente a faculdade de comunicar informações a outrem; o direito de se informar, que consiste na possibilidade de obter informações sem impedimentos, e o direito de ser informado ou direito à informação, relacionado a liberdade de receber informações condizentes com a realidade, íntegras e sem restrições.

Considerado de importância incomparável, por ser o que mais se aproxima do “núcleo axiológico da dignidade da pessoa humana” (ALEXANDRINO, 1998, p. 123). Conforme Lopes apud Rodrigues Júnior (2009, p. 62), o direito à informação é:

O direito de toda a sociedade em ser bem informada, de forma ampla e diversa, de modo a propiciar a formação e consciência política, social, cultural dos indivíduos livre e isonomicamente, garantindo a todos o acesso aos meios de comunicação de massa para que possam receber e transmitir pensamentos e opiniões, com vistas a assegurar também o pluralismo político e social definidores de uma sociedade democrática.

Porém, longo foi o caminho na história até que o direito à informação viesse a fazer parte do rol de direitos fundamentais nos Estados democráticos, tendo seus primórdios já no século XVIII.

Considerada a prova definitiva da maturidade revolucionária, a Revolução Francesa veio eclodir por volta de 1789 com a queda do absolutismo, a tomada do poder pela burguesia e a evolução do capitalismo. Enfatiza Vicentino (2000, p. 263) que a “burguesia da Revolução Francesa sentia-se como a locomotiva impulsionando toda a nação, e via a Revolução como algo para todo o povo e não apenas para o burguês”.

Foi a Revolução Francesa que proclamou, através da Declaração dos Direitos do Homem e do Cidadão de 1789, o início de uma normatização dos direitos humanos. Esta Declaração “também reconheceu como fundamental a necessidade de instituir garantias penais e processuais, a liberdade de opinião, inclusive a religiosa, a liberdade de imprensa e o direito de propriedade” consoante salienta Rodrigues Júnior (2009, p. 31), além de outros direitos individuais.

Ainda que de forma discreta, a Declaração proveniente da revolução, em seu artigo quinze, já trazia os indícios de um princípio da transparência e do direito à informação quando elencava que “*La société a le droit de demander compte à tout agent public de son administration*”, ou seja, que a sociedade tem o direito de requerer ao agente público a prestação de contas de sua administração.

Entretanto, mesmo sendo indiscutível a relevância da referida Declaração, só após a crueldade vivida na Segunda Guerra Mundial, é que um despertar em todas as nações surgiu como condição à existência da própria humanidade, eclodindo a partir de então, um consenso entre os Estados quanto à necessidade de salvaguardar os direitos humanos.

Na realidade, o que motivou esse consenso das nações foi a:

Vontade de impedir a repetição das atrocidades cometidas durante a Segunda Grande Guerra, ideia que acabou culminando com a proclamação da *Declaração Universal dos Direitos do Homem (DUDH)* pela Organização das Nações Unidas, em 10.12.1948 (RODRIGUES JÚNIOR, 2009, p. 36).

Citado em Silva (2008, p. 163), constitui o Preâmbulo da referida Declaração, proclamada pela Assembleia da ONU, o:

Ideal comum a ser atingido por todos os povos e todas as nações, a fim de que todos os indivíduos e todos os órgãos da Sociedade, tendo esta Declaração constantemente no espírito, se esforcem, pelo ensinamento e pela educação, a desenvolver o respeito desses direitos e liberdades [...].

Vale salientar que essa Declaração exerceu enorme influência sobre as constituições elaboradas após a sua proclamação. No Brasil, já na Constituição Imperial de 1824, uma declaração dos direitos do homem brasileiro e do estrangeiro residente no país já aparecia, ainda que de forma tímida. Entretanto, só na Carta de 1988 aparece de forma mais técnica e aprofundada, com a observância do princípio da prevalência dos direitos humanos já em seu art.4º e com o Título II que tratava – Dos Direitos e Deveres Individuais e Coletivos (Cap. I); Os Direitos Sociais (Cap. II); os Direitos da Nacionalidade (Cap. III), e os Direitos Políticos (Cap. IV).

Já em seu artigo primeiro, a Constituição Brasileira de 1988 declara como fundamento do Estado Democrático de Direito a dignidade da pessoa humana, expressão que segundo Silva (2008, p. 178):

[...] além de referir-se a princípios que resumem a concepção do mundo e informam a ideologia política de cada ordenamento jurídico, é reservada para designar, no nível do direito positivo, aquelas prerrogativas e instituições que ele concretiza em garantias de uma convivência digna, livre e igual de todas as pessoas.

Entre os referidos direitos elencados na Carta Magna de 1988, estão os direitos à liberdade de expressão, de opinião e de informação, situados no artigo 5º em seus incisos IX, XIV, XXXIII, XXXIV “b”, e no art. 220.

Aqui se torna válido fazer uma distinção entre liberdade de informação e o direito à informação. Aquela compreenderia o direito de informação, individual por excelência, a própria liberdade jornalística, com o acesso e a difusão sem censura, através de livros, jornais, revistas, rádio e televisão. O próprio direito de poder se expressar assegurado pelo artigo 5º, inciso IV, que garante a livre manifestação do pensamento. Já este, consagrado como direito à informação e inserido no rol de direitos fundamentais da coletividade, atende a toda uma pluralidade de pessoas, na convicção que “não é um direito pessoal, nem simplesmente um direito profissional, mas um direito coletivo” (NOBRE apud SILVA, 2008, p. 259-260).

O Direito à informação, discutido neste capítulo, prioriza em regra o interesse da coletividade em detrimento do segredo da Administração, e que de forma mais específica, é demonstrado no artigo 5º, inciso XXXIII, da Constituição Federal de 1988 ao estatuir que:

Todos têm direito a receber dos órgãos públicos informações de seu interesse particular, ou de interesse coletivo em geral, que serão prestadas no prazo da lei, sob pena de responsabilidade, ressalvadas aquelas cujo sigilo seja imprescindível à segurança da sociedade e do Estado.

A doutrina costuma classificar os direitos fundamentais em gerações de direito. No momento atual, a expressão “dimensões” vem sendo mais utilizada, já que o “surgimento de novas gerações não ocasiona a extinção das anteriores” (NOVELINO, 2009, p. 362) havendo, pois, uma coexistência de direitos.

Divergências doutrinárias a parte, o direito à informação constitui um dos novos direitos do cidadão, classificado como de quarta dimensão, sendo estes os pressupostos basilares da democracia. Novelino (2009, p. 362) entende que os “direitos de quarta geração compreendem os direitos à democracia, informação e pluralismo” que foram “introduzidos no âmbito jurídico pela globalização política”.

A definição de direito à informação se distribui em dois objetivos primordiais. O primeiro seria a fiscalização de todas às atividades da Administração como meio de coibir possíveis irregularidades dos gestores. O segundo e não menos importante, seria a própria participação do administrado no trato com a coisa pública. Portanto, com a informação clara e verdadeira, a sociedade poderá participar e fiscalizar a organização do Estado e sua Administração, para só assim fazer jus ao princípio da publicidade e transparência, o que consequentemente gerará uma maior credibilidade dos atos administrativos em prol da coletividade.

## 2.2 A INFORMÁTICA E SUA APLICAÇÃO NA AMPLIAÇÃO DO ACESSO À INFORMAÇÃO

A informática é uma ciência de conceitos próprios e distintos que objetiva estudar, viabilizar, garantir e suportar o tratamento da informação, utilizando como ferramenta os recursos de sistema de computação.

Para Alcade *apud* Marçula (2005, p.46), a informática pode ser considerada como o “estudo de tudo o que se relaciona com a tecnologia da informação. É uma reunião de trechos de duas outras palavras e foi criada pelos franceses”.

Em outra perspectiva pode-se dizer que a Informática é a “ciência que visa o tratamento da informação através do uso de equipamentos da área de processamento de dados”. (FERREIRA, 2000, p.388)

O termo informática é de utilização muito genérica e engloba vários componentes para o tratamento da informação.

Ao elencar vários conceitos Ferreira *apud* Albertin (2009, p. 5-6) afirma que a informática é “a ciência do tratamento racional e automático da informação, considerada esta como suporte dos conhecimentos e comunicações”. A informação seria o “conhecimento amplo e bem fundamentado, resultante da análise e combinação de vários informes”. O conhecimento como sendo a “informação, notícia e ciência”. E a comunicação seria o próprio “ato ou efeito de emitir, transmitir e receber mensagens por meio de métodos e/ou processos convencionados”.

Porém, para entender como se chegou aos citados conceitos, faz-se necessário apresentar um breve histórico sobre a evolução dessa tecnologia que uniu as palavras informação e automática, até chegar a um conceito comum.

Os primórdios os quais se baseiam os atuais computadores remontam a tempos muito remotos. A necessidade de um instrumento para auxiliar nos cálculos, inicialmente ligados a agricultura, fez surgir há cerca de dois mil anos antes de Cristo um instrumento utilizado até hoje, conhecido por Ábaco e considerado como a gênese do computador atual.

Dando um salto na história, já em tempos modernos, no século XX, iniciada a Segunda Grande Guerra Mundial, a corrida pelo desenvolvimento de novas tecnologias avançou de forma considerável. Com o objetivo de se codificar mensagens e prevenir ataques, muitos computadores foram desenvolvidos, o que na época ainda eram chamados de calculadoras.

Os Estados Unidos da América desenvolveram o projeto ENIAC (*Electronic Numerical Integrator And Calculator*), considerado como uma verdadeira evolução para o mundo. A nova tecnologia tinha cerca de trinta toneladas e ocupava uma extensa área, porém com poucas utilidades práticas ainda. Seria este o precursor do computador eletrônico.

E passando pela corrida espacial até os dias contemporâneos, as novas tecnologias foram se desenvolvendo, criando os mais modernos sistemas operacionais, com computadores rápidos, eficientes e imprescindíveis à atualidade. Coincide ainda com o avanço dos computadores o surgimento da Internet, ferramenta de comunicação que veio proporcionar a maior interligação de conhecimentos e informações entre toda a população mundial.

A história demonstra que o avanço tecnológico tem sido muito grande e que sua velocidade aumenta na mesma intensidade. Como argumentado por Albertin (2009, p. 8) “as inovações nas tecnologias de informação das últimas duas décadas têm reduzido radicalmente o tempo e o custo do processamento e comunicação de informações”.

Hoje, em um mundo globalizado pelas tecnologias, pode-se afirmar que a informática está presente em todos os seguimentos da sociedade. Seja no trabalho, nos estudos, nos relacionamentos afetivos, na indústria, no comércio ou na Administração Pública, a informática tem ampliado as possibilidades e o acesso à informação.

No que diz respeito a ampliação do acesso à informação na Administração Pública, no Brasil, em 2011, foi sancionada a Lei Geral de Acesso à Informação com o número 12.257. Sua entrada em vigor se deu em dezesseis de maio de 2012, vindo regulamentar um direito fundamental garantido na Constituição Federal de 1988, e trazendo já em seu art. 3º, incisos I e II, a “observância da publicidade como preceito geral e do sigilo como exceção”, assim como a “utilização de meios de comunicação viabilizados pela tecnologia da informação”.

A Lei de Acesso à Informação (LAI) é considerada como um avanço nos conceitos de transparência e de prevenção da corrupção, além de um potente instrumento na prestação de informações ao cidadão.

Ao regulamentar o inciso XXXIII do art. 5º, inciso II, §3º do art. 37 e §2º do art. 216 da Constituição Federal, a LAI possibilitou a realização da transparência por duas vertentes distintas. A primeira é a transparência espontânea, na qual o estado deve disponibilizar informações de interesse público, independentemente de requerimentos. E a segunda é a transparência passiva entendida como a que resulta das solicitações feitas pelos cidadãos.

Em parecer emitido pela Controladoria-Geral da União no 1º Balanço (2011/2012) da Lei de Acesso à Informação, o Ministro Chefe da Controladoria Geral da União (CGU), Jorge Hage Sobrinho, relatou a importância para a democracia, da ligação entre a tecnologia e o acesso à informação, destacando que:

A busca da transparência na vida pública e do amplo acesso dos cidadãos à informação produzida ou gerida pelo Poder Público é uma das principais marcas das verdadeiras democracias modernas e, graças ao que se tornou possível com o desenvolvimento tecnológico atual, veio a proporcionar a realização, no século 21, de uma forma de democracia contemporânea que nos aproxima, de certo modo e até certo ponto, daquele ideal clássico da democracia direta.

Os avanços são nítidos e de fácil observação. Segundo o Relatório de Pedidos de Acesso à Informação emitido pelo Sistema Eletrônico do Serviço de Informação aos Cidadãos

(e-SIC), a quantidade de pedidos de acesso à informação apresentou uma considerável evolução (vide gráfico I em anexo), com uma média mensal de 6.856,25 pedidos por mês, como se pode ver na tabela abaixo:

Tabela 1. Evolução mensal do número de pedidos de acesso à informação

<b>Mês</b>	<b>Número de Pedidos</b>	<b>Evolução Mensal</b>
<b>Maio/2012</b>	6658	-
<b>Junho/2012</b>	7264	8.34%
<b>Julho/2012</b>	7723	5.94%
<b>Agosto/2012</b>	7886	2.07%
<b>Setembro/2012</b>	6920	-12.25%
<b>Outubro/2012</b>	7405	6.55%
<b>Novembro/2012</b>	6587	-11.05%
<b>Dezembro/2012</b>	4771	-27.57%
<b>Janeiro/2013</b>	8003	40.38%
<b>Fevereiro/2013</b>	6746	-15.71%
<b>Marco/2013</b>	7293	7.5%
<b>Abril/2013</b>	8059	9.5%
<b>Maio/2013</b>	7609	-5.58%
<b>Junho/2013</b>	6613	-13.09%
<b>Julho/2013</b>	7902	16.31%
<b>Agosto/2013</b>	2261	-71.39%
<b>TOTAL:</b>	109700	
<b>MÉDIA:</b>	6856,25	

Fonte: <http://www.acessoainformacao.gov.br> (e-SIC), ano de 2013 – Gráfico I do anexo A.

A referida lei veio então consolidar o princípio da transparência, inerente a toda Administração Pública, bem como estabelecer regras e procedimentos específicos para possibilitar o exercício do direito constitucional de obtenção a informações públicas pela sociedade.

Na tabela abaixo, em uma linha de tempo, percebem-se os avanços nas medidas voltadas à transparência pública no Brasil, a partir dos anos 2000.

Tabela 02. Avanços nas medidas voltadas à transparência pública no Brasil

<b>Ano</b>	<b>Avanço na Transparência</b>
2000	Lei de Responsabilidade Fiscal (LRF)
2003	Criação da Controladoria Geral da União (CGU)
2004	Criação do Portal da Transparência
2005	Regulamentação do Pregão Eletrônico
2007	Criação do Sistema de Convênios e Contratos de Repasse (Siconv)
2008	Criação do Cadastro de Empresas Inidôneas e Suspensas (CEIS)
2009	Lei Complementar N° 131
2010	Sites relacionados a Copa e Jogos Olímpicos
2011	1° Plano de Ação Nacional sobre Governo Aberto (OGP)
2012	Lei Geral de Acesso à Informação

Fonte: <http://www.acessoainformacao.gov.br> (CGU), ano 2011/2012 – Gráfico II do anexo A.

Portanto, mesmo que de forma tímida, o Brasil vem avançando com compromissos concretos nas áreas de promoção da transparência, participação social e de incentivo ao desenvolvimento de novas tecnologias, utilizando-se de meios proporcionados pela informática na ampliação do acesso à informação, assim como em outras nações pelo mundo, que buscam incessantemente instrumentos aplicáveis em matérias de direitos humanos e de governo aberto.

### 2.3 OS EFEITOS JURÍDICOS DA VIOLAÇÃO AO DIREITO À INFORMAÇÃO

A acelerada difusão da Internet é considerada como um dos primordiais fatores motivadores dos incidentes de segurança da informação. Devido à rapidez com que se propagam as informações e a livre manifestação dos usuários, informações abusivas podem vir a lesionar direitos essenciais à própria dignidade da pessoa humana.

Além da globalização da informação, a internet propiciou o crescimento do mundo dos negócios *online* que, envolve, atualmente, transações financeiras inestimáveis. E, “onde há riqueza há crime.” Considera-se a Internet como sendo um “paraíso de informações, e pelo fato de estas serem riqueza, inevitavelmente atraem o crime” (CORRÊA, 2008, p. 44) Portanto, simultaneamente ao desenvolvimento tecnológico e econômico, a vulnerabilidade dos sistemas informáticos tem propiciado a prática de diversas condutas ilícitas.

A criminalidade, a informática e o fenômeno da informatização global são possuidores de características semelhantes que, nas palavras de Couri (2009, p. 5) são:

A transnacionalidade, a universalidade e a ubiquidade. Isso porque, todos os países fazem uso da informática independentemente do seu estágio econômico, social ou cultural, bem como todas as pessoas de qualquer plano econômico, social ou cultural têm acesso aos produtos informatizados; sendo certo que a informatização está presente em todos os setores públicos e privados no planeta.

E é assim, que a informática tem despontado como sendo uma nova fonte de criminalidade, seja com a prática de delitos já tipificados nas legislações como o furto, a pedofilia ou estelionato, seja com o surgimento de novos crimes como o de invasão de sistemas da informação, todos cometidos com subsídio do computador.

Entretanto, não é de hoje que os discutidos crimes cibernéticos são analisados sob um aspecto criminológico. Para Ferreira apud Lucca; Simão Filho (2005, p. 239):

Ulrich Sieber, professor da Universidade Wurzburg e grande especialista no assunto, afirma que o surgimento dessa espécie de criminalidade remonta à década de 1960, época em que aparecem na imprensa e na literatura científica os primeiros casos do uso do computador para a prática de delitos, constituídos, sobretudo por manipulações, sabotagens, espionagem e uso abusivo de computadores e sistemas, denunciados, sobretudo em matérias jornalísticas. Somente na década seguinte é que iriam iniciar-se os estudos sistemáticos e científicos sobre essa matéria, com emprego de métodos criminológicos, analisando-se um limitado número de delitos informáticos que haviam sido denunciados, entre os quais alguns casos de grande repercussão na Europa por envolverem empresas de renome mundial, sabendo-se porém da existência de uma grande *cifra negra* não considerada nas estatísticas.

A violação dos direitos à informação na atualidade tem como consequência o advento de uma nova figura de delito, os chamados crimes digitais, que são a “utilização de computadores para ajuda em atividades ilegais, subvertendo a segurança de sistemas, ou usando a internet ou redes bancárias de maneira ilícita” (BARRET apud CORRÊA, 2008, p. 44).

A terminologia varia muito de acordo com o autor. Para Ferreira (1992, p. 141) o crime digital ou crime de informática seria “toda ação típica, antijurídica e culpável contra ou pela utilização de processamento automático e/ou eletrônico de dados ou sua transmissão”.

Sem adentrar as divergências doutrinárias quanto a nomenclatura do termo, em uma visão mais ampla, Rosa (2006, p. 55), define o crime de informática como sendo uma conduta que atenta:

Contra o estado natural dos dados e recursos oferecidos por um sistema de processamento de dados, na sua forma, compreendida pelos elementos que compõem um sistema de tratamento, transmissão ou armazenagem de dados, ou seja, ainda, na forma mais rudimentar.

Nos tribunais brasileiros e na doutrina penal a concepção de crimes informáticos tem definição “similar a que foi cunhada pela Organização para Cooperação Econômica e Desenvolvimento da ONU que é qualquer conduta ilegal não ética, ou não autorizada, que envolva processamento automático de dados e/ou transmissão de dados” (DAOUN; LIMA, 2009, p. 25).

São muitos os personagens envolvidos nos crimes digitais. Em tese, qualquer pessoa que tenha acesso a um computador poderá ser sujeito ativo ou passivo de um crime virtual. A praxe midiática costuma englobar todos os delinquentes da informática no termo *hacker*. Entretanto, a doutrina faz distinções, demonstrando inclusive que há uma hierarquia entre os sujeitos. Nogueira (2008, p. 61) diz que *hacker* é sujeito que:

Em geral domina a informática e é muito inteligente, adora invadir sites, mas na maioria das vezes não com a finalidade de cometer crimes, costumam se desafiar entre si, para ver quem consegue invadir tal sistema ou página na Internet, isto apenas para mostrar como estamos vulneráveis no mundo virtual.

Tem-se como primeiro caso relatado sobre a atuação de um *hacker* na Universidade de Oxford em 1978, onde um estudante fez cópia de uma atividade/prova por intermédio de uma invasão do sistema.

A distinção do termo ocorre quando o indivíduo comete ações ilegais, passando a se chamar de *cracker*. Esse termo foi “criado em 1985 por *hackers* em defesa do uso jornalístico depreciativo do termo *hacker*” (CORRÊA, 2008, p. 60). O *craker* usa seus vastos conhecimentos de informática para “roubar senhas, documentos, causar danos ou mesmo realizar espionagem industrial” (ASSUNÇÃO, 2008, p. 13).

Alguns outros termos são considerados como subdivisões dos *crackers*, e que se distinguem conforme a área quem atuam, tais como os *lamer*, *defacer*, *phreaker* e os *spammers*.

O *Lamer* está na última posição hierárquica dos *crackers*, sendo considerado como o indivíduo que não tem conhecimentos específicos na informática. O *defacer* ou também chamado de “pichador virtual”, é aquele coloca figuras e/ou marcações indevidas nos sites. *Phreaker* é a definição dada aos indivíduos que cometem crimes através das linhas telefônicas como a escuta via frequência, a clonagem de celulares, etc. Já os *spammers* são aqueles indivíduos que enviam os chamados *spams*, propagandas eletrônicas indesejadas geralmente enviadas através de e-mails.

Ademais, independentemente da nomenclatura utilizada para o sujeito, ou para a categoria de crime, a facilidade na violação de informações pelas novas tecnologias tem causado imensos transtornos a população do mundo inteiro, com reflexos jurídicos em todas as esferas da sociedade, o que faz surgir a urgente necessidade de se impor limites, através de uma normatização mais eficaz e uma constituição de sistemas de prevenção aos delitos da “Era da Informação”.

### 3 A INTERNET E O DIREITO À INTIMIDADE

Os avanços tecnológicos têm trazido consigo uma invasão na vida privada das pessoas, acarretando em uma atual preocupação com o direito à intimidade do indivíduo.

O surgimento da Internet veio proporcionar uma maior velocidade nas relações sociais, com uma interação global entre as pessoas sem precedentes históricos. Essa rapidez, porém, veio acarretar também em uma colisão de direitos fundamentais, já que as relações humanas, com suas benesses e problemáticas foram transportadas para o mundo virtual.

Faz-se necessário apresentar um pequeno aparato histórico da criação e evolução da Internet, bem como da sua chegada ao Brasil, para só depois analisar as consequências jurídicas e sociais ocasionadas por esta veloz ferramenta tecnológica no mundo atual.

#### 3.1 O SURGIMENTO DA INTERNET

Após a Segunda Guerra Mundial, a oposição entre capitalismo e socialismo, protagonizada pelos Estados Unidos da América e pela então União Soviética, foi elevada a patamares extremos com uma disputa tecnológica, política, ideológica e armamentista, que perdurou até o ano de 1991. Foi a chamada Guerra Fria.

No final da década 1960, na tentativa de se alcançar o auge do crescimento econômico e tecnológico, os soviéticos tornaram-se precursores na corrida espacial ao “lançar [...] o primeiro satélite artificial do mundo, o Sputnik, e ao concretizar o primeiro voo espacial tripulado, com o astronauta Iúri Gagarin, em 1961” (VICENTINO, 2000, p. 408)

E é nesse contexto, na tentativa de se equiparar os avanços tecnológicos, que os USA lançaram um projeto de pesquisa militar denominado de ARPA (*Advanced Research Projects Agency*), mais tarde chamado de ARPAnet, com a finalidade inicial de interligar centros de pesquisas, laboratórios, bases militares e o Pentágono para permuta de informações rápidas, bem como preservar dados importantes, caso viesse a eclodir uma guerra nuclear.

Com a extensão desse projeto às Universidades, surge então os primórdios do que se conhece hoje de Internet. Nas palavras de Corrêa (2008, p. 7) a Internet:

Teve sua origem nos Estados Unidos, onde uma rede de computadores de uso exclusivamente militar foi desenvolvida nos anos 60 como importante arma na guerra fria. Seus princípios de funcionamento eram, e ainda são, a procura de vários caminhos para alcançar determinado ponto, ou seja, na hipótese de um dos troncos (caminho pelo qual trafega o sinal eletrônico) estar obstruído, procuraria ela, automaticamente, um outro caminho que o substituísse.

O problema agora era fazer com que essa ferramenta pudesse alcançar outras distâncias. E isso só seria possível através de uma conexão com outras redes de computadores. Porém, para que todos os computadores, em uma única “linguagem”, pudessem se comunicar haveria a necessidade de criar protocolos padronizados de comunicação.

Foi na década de 1970 que surgiu uma linguagem de protocolo específico, chamada de TCP (*Transmission Control Protocol*). Pouco tempo depois foi acrescentada de outro protocolo chamado de IP (*Internet Protocol*), e que segundo Bruno (2006, p. 12) gerou o protocolo TCP/IP, padrão segundo o qual a Internet continua a operar nos dias atuais.

Iniciando a década de 1990, a ARPAnet que antes basicamente se concentrava no ambiente militar se torna ultrapassada, sendo substituída pela *National Science Foundation Network* (NSFnet), que logo tratou de criar sistemas regionais interligados, abrindo espaço à privatização da Internet e ao domínio público.

Porém, a popularização da Internet só veio acontecer com a formação de um sistema de interface gráfica que possibilitou o uso de imagens e sons, evoluindo consideravelmente a ideia de transmissão pura de textos. Esse sistema ficou conhecido como o WWW (*World Wide Web*), uma espécie de protocolo universal que veio possibilitar o acesso fácil de qualquer pessoa, utilizando apenas um simples computador.

De forma sucinta, Corrêa (2008, p. 11) conceituou a WWW como sendo um composto de padrões e tecnologias que:

Possibilitam a utilização da Internet por meio dos programas navegadores, que por sua vez tiram todas as vantagens desse conjunto de padrões e tecnologias do hipertexto e suas relações com a multimídia, como som e imagem, proporcionando ao usuário maior facilidade na sua utilização, e também a obtenção de melhores resultados.

Para utilizar esse sistema, um programa de computador criado por Marc Andressen da Universidade de Illinois nos EUA foi o responsável pela grande expansão em massa da Internet, que em pouco tempo já tinha milhares de usuários realizando as mais variadas tarefas, como a troca de imagens e de arquivos multimídia. O navegador ficou conhecido como *Mosaic*, precursor do que chamamos hoje de Internet Explorer.

A Internet passa a protagonizar a história da maior criação de todos os tempos. Um sistema público que veio proporcionar uma troca de informações de abrangência incalculável, através de uma rede de computadores interligada mundialmente, onde uma pessoa em qualquer lugar do planeta, conectada a um simples computador, pode ter acesso a informações há pouco inimagináveis nos mais profundos sonhos.

Assim, a Internet é um “sistema global de rede de computadores que possibilita a comunicação e a transferência de arquivos de uma máquina a qualquer outra máquina conectada na rede, possibilitando, assim, um intercâmbio de informações sem precedentes na história, de maneira rápida, eficiente e sem a limitação de fronteiras, culminando na criação de novos mecanismos de relacionamento. (CORRÊA, 2008, p. 8)

Para Schachter; Kurtzberg *apud* Nascimento (2009, p. 25) ao falar da estrutura, definiu a Internet como sendo “uma rede mundial de computadores composta por redes menores, ou seja, como uma rede de redes”.

Ao tratar da estrutura da Internet, Nascimento (2009, p. 27) distinguiu a Internet da mídia televisiva, jornalística ou radiofônica, por não haver um exclusivo órgão controlador que a administre de forma centralizada, pois “não há um único centro de armazenamento de arquivos e o sistema de transmissão se mantém ativo sem necessidade de controle ou envolvimento humano direto”.

Outra característica fundamental da Internet é a sua capacidade de troca de informações. Isso a distingue também das mídias televisivas e jornalísticas, já que estas possuem apenas meros receptores de informações que ficam de forma passiva absorvendo as notícias transmitidas.

A Internet na atual era da informação é parte integrante e indispensável ao desenvolvimento tecnológico do mundo. É um ambiente virtual que, pelo incalculável número de usuários, além da troca de informações e a interação entre o homem e a máquina, se tornou uma ferramenta de enorme exploração econômica por pequenas e grandes empresas, que utilizam os meios de publicidade eletrônica para fortalecer o seu mercado. Em síntese, a Internet é a maior ferramenta de divulgação do pensamento e, por conseguinte, a maior fonte de informações de todos os tempos.

### 3.2 A INTERNET NO BRASIL E SUA REGULAMENTAÇÃO

Com a expansão do novo modelo prático de protocolo, o WWW (*World Wide Web*), mais conhecido como *Web*, a internet deu um enorme salto de popularidade em todo o mundo. Esta expansão, aliada aos interesses comerciais que surgiam, fez com que a ferramenta em desenvolvimento despertasse os olhares visionários do capitalismo.

O ano de 1988 pode ser considerado como o marco inicial da Internet no Brasil como bem explica Bruno (2006, p. 14), quando bolsistas que retornavam de cursos de doutorado

nos Estados Unidos criticaram a ausência de um intercâmbio de conhecimentos com outras instituições científicas. Coube então a Fundação de Amparo à Pesquisa do Estado de São Paulo (Fapesp), ligada à Secretaria Estadual de Ciência e Tecnologia, a iniciativa a fim de se conseguir uma conexão do Brasil com a rede mundial em expansão.

Em 1991, a internet já era acessível aos brasileiros, porém sem muita expansão. Foi com a Conferência das Nações Unidas sobre o Meio Ambiente e o Desenvolvimento, conhecida como ECO-92, que os ativistas do terceiro setor, as ONGs, com intuito de possibilitar um maior acesso das informações da Conferência pela sociedade, requereram o uso da nova ferramenta de comunicação aos cientistas brasileiros. Esse é o despertar de interesse de alguns empresários que viam com olhares futuristas o uso da Internet em auxílio a economia.

Porém, só em 1994 é que a Internet no Brasil iniciou a sua abertura comercial. A então RPN (Rede Nacional de Pesquisa), que fora criada em 1989 pelo Ministério de Ciência e Tecnologia com o objetivo de dar início a construção de uma rede de internet nacional para as universidades, passou a estender seu foco para toda a sociedade. A Embratel recebeu do Governo Federal o encargo de criar toda a estrutura responsável pela exploração comercial, utilizando-se para isso do apoio da Rede Nacional de Pesquisa (RPN), experiente no desenvolvimento da internet acadêmica.

De acordo com o coordenador do Grupo de Engenharia de Operações dos Serviços de Internet da Embratel Maceira apud Carvalho (2006, p. 137):

Em 1994, a Embratel começou a analisar a questão do uso comercial da Internet nos Estados Unidos e decidiu ver como poderia participar disso também, aqui no Brasil. Fui designado para integrar um grupo de três pessoas, formado por mim, pelo Hélio Daldegan e pelo Aloysio Xavier, criado com a missão de analisar a oportunidade de negócio nisso tudo. [...] No final de 1994, a diretoria da Embratel recebeu a proposta de iniciar a prestação de serviços Internet e começamos a testar isso através de usuários convidados por nós. [...] Terminado esse trabalho, começamos a montar a rede e a desenvolver o serviço. Foi justamente quando o grupo se solidificou, cresceu, tornando-se uma estrutura de gerência em serviços Internet.

Entretanto, o poder conferido a Embratel gerou enorme descontentamento na sociedade em geral. Era o temor do monopólio de um setor novo ainda a se desenvolver. A reação governamental foi imediata, afirmando que para se efetivar a presença da sociedade nas decisões, tanto na implantação como no uso da Internet, haveria a necessidade de criar um Comitê Gestor de Internet.

O Governo, reconhecendo a importância desse serviço, através da Portaria Interministerial Número 147, de 31 de maio de 1995 (em Anexo), criou o Comitê Gestor de Internet no

Brasil (CGI.br), com “a participação de entidades operadoras e gestoras de espinhas dorsais, de representantes de provedores de acesso ou de informações, de representantes dos usuários e da comunidade acadêmica” (CORRÊA, 2008, p. 17)

O Brasil adotou o modelo pluralista e multiparticipativo de governança da Internet, onde as propostas e decisões são sempre baseadas no consenso de seus representantes.

De acordo com informações colhidas no site do CGI (<http://www.cgi.br>), entre 1995 e 2003, o Governo indicava seus representantes e aprovava as indicações dos demais setores. A partir de 2003, o CGI.br foi então redimensionado e os membros da Sociedade Civil passaram a ser eleitos pelos respectivos colégios eleitorais. Atualmente, os onze membros da Sociedade Civil são eleitos a cada três anos. O governo brasileiro continua indicando nove representantes e, mais um é indicado pelo Ministério da Ciência, Tecnologia e Informação, como especialista em assuntos da Internet.

Segundo Corrêa (2008, p. 17-18) o Comitê Gestor de Internet no Brasil (CGI.br) é:

O maior exemplo da tendência mundial a tornar a Grande Rede algo desvinculado do Poder Público, incentivando a participação da sociedade civil na formulação de diretrizes básicas para o desenvolvimento organizado.

A Internet, hoje, faz parte da vida de quase todos os brasileiros. Veio possibilitar, dentre outras coisas, uma descentralização da informação, cultura e educação, bem como a exploração de novas oportunidades, ofertas de emprego e prestação de serviços. Seja na educação, na política ou no comércio, a Internet já se tornou a ferramenta mais importante de compartilhamento de informações, presente em todas as faixas etárias da sociedade de todos os tempos.

Prova-se isso com um estudo desenvolvido com base em dados da Pesquisa Nacional por Amostra de Domicílios, o PAND realizado nos anos de 2005, 2008, 2009 e 2011, disponível em [www.ibge.gov.br](http://www.ibge.gov.br). De acordo com a pesquisa, no ano de 2011, 77,7 milhões de pessoas de 10 anos ou mais de idade acessaram a Internet no período de referência nos últimos três meses. Em termos percentuais, este índice equivalia a 46,5 % do total da população de 10 anos ou mais de idade.

Ainda de acordo com a pesquisa de 2005 para 2011, a população em idade ativa de 10 anos ou mais cresceu 9,7%, enquanto que o contingente de pessoas que utilizaram a Internet aumentou 143,8%, ou seja, o número de internautas no Brasil em seis anos cresceu 45,8 milhões. Podemos ver esses dados no Gráfico III em anexo.

Outro dado importante da pesquisa é quanto ao número de indivíduos que possuíam computador em casa com acesso a internet. No ano de 2005, 22,3 milhões de pessoas com 10 anos ou mais de idade residiam em domicílios que possuíam microcomputador com acesso à Internet (14,6% domicílios) e 130,0 milhões (85,4% do total) residiam em domicílios sem microcomputador com acesso à Internet. Em 2011, o total de domicílios que tinham acesso à Internet passou para 65,7 milhões, ou seja, 39,4% do total, como demonstrado no Gráfico IV em anexo.

Compreende-se pela pesquisa que da população de 10 anos ou mais de idade, que 21,0% das pessoas acessaram a Internet em algum local, seja domicílio, local de trabalho, estabelecimento de ensino, centro público de acesso gratuito ou pago, domicílio de outra pessoa ou qualquer outro local, por meio de um computador, pelo menos uma vez no período de referência pesquisado.

Isso mostra a crescente dependência dos cidadãos brasileiros quanto a essas novas tecnologias, que ao lado dos benefícios, acarretam também alguns problemas, que serão tema dos tópicos subsequentes deste trabalho.

### **3.3 O DIREITO À INTIMIDADE E A DIGNIDADE DA PESSOA HUMANA**

A dignidade da pessoa humana é prerrogativa inerente do indivíduo, trata-se de prevalência dos valores éticos, sociais e da família, de caráter irrenunciável.

“O princípio da dignidade da pessoa humana, assim como o princípio da inviolabilidade da vida humana, é indeclinável, indisponível e irrenunciável [...]” (OTERO apud RODRIGUES JÚNIOR, 2009, p. 93).

A Constituição de 1988 inseriu a dignidade da pessoa humana como um dos fundamentos do Estado Democrático de Direito, já em seu artigo 1º, que segundo Bastos (2002, p.425) tal inserção teve o objetivo de indicar o princípio como sendo “um dos fins do Estado propiciar as condições para que as pessoas se tornem dignas”.

A Carta Magna reconheceu a pessoa, o indivíduo em si mesmo, como sendo o foco central e o fim do direito, um valor constitucionalmente absoluto e protegido, tornando o princípio da dignidade da pessoa humana na base de todos os direitos fundamentais. É o reconhecimento categórico de que é o “Estado que existe em função da pessoa humana, e não o contrário, já que o ser humano constitui a finalidade precípua e não meio da atividade estatal” (SARLET, 2001, p. 103).

Ademais, o respeito ao fundamento da dignidade da pessoa humana acarreta como consequências a:

- a) igualdade de direitos entre todos os homens, uma vez integrarem a sociedade como pessoas e não como cidadãos;
- b) garantia da independência e autonomia do ser humano, de forma a obstar toda coação externa ao desenvolvimento de sua personalidade, bem como toda atuação que implique na sua degradação e desrespeito à sua condição de pessoa, tal como se verifica nas hipóteses de risco de vida;
- c) não admissibilidade da negativa dos meios fundamentais para o desenvolvimento de alguém como pessoa ou imposição de condições subumanas de vida. (NOBRE JÚNIOR, 2000, p. 4)

Vale aqui frisar o inseparável vínculo existente entre os direitos fundamentais e o referido princípio da dignidade da pessoa humana, como sendo um dos principais fundamentos do Direito Constitucional Contemporâneo. Em uma ordem hierárquica e axiológica, a dignidade da pessoa humana, tem o condão não só de guiar todos os direitos fundamentais, como também, estruturar toda a ordem constitucional.

Essa ligação é facilmente percebida ao se analisar o direito à intimidade. A Constituição o destaca como um direito fundamental em seu artigo 5º, inciso X, ao declarar serem invioláveis o direito a intimidade, a vida privada, a honra e a imagem das pessoas. José Afonso da Silva (2008, p. 206) faz uma distinção entre o direito a intimidade e à vida privada, honra e imagem, preferindo o uso da expressão Direito à Privacidade, em um sentido amplo, de modo a abranger todas as manifestações da esfera íntima, privada e da personalidade, consagradas pelo texto constitucional.

São muitos os autores que fazem essa distinção, descrevendo o direito à intimidade como parte do direito à privacidade. Nessa linha, Mendes; Branco (2012, p. 318) fazem uma diferenciação quanto ao objeto discorrendo que:

O direito à privacidade teria por objeto os comportamentos e acontecimentos atinentes aos relacionamentos pessoais em geral, às relações comerciais e profissionais que o indivíduo não deseja que se espalhem ao conhecimento público. O objeto do direito à intimidade seriam as conversações e os episódios ainda mais íntimos, envolvendo relações familiares e amizades mais próximas.

A doutrina norte-americana sempre lembra que o Juiz Cooly, em 1873, identificou a privacidade como o direito de estar só, chamado de *Right to be alone*. Outra expressão também utilizada pelos juristas americanos é o *Right of privacy*, que seria o direito de qualquer indivíduo guiar suas próprias decisões sem interferência.

Entretanto, trataremos aqui de forma mais específica do Direito à Intimidade, como sendo a “esfera secreta da vida do indivíduo na qual este tem o poder legal de evitar os demais” (DOTTI *apud* SILVA, 2008, p. 207).

De acordo com Álvaro Rodrigues Júnior (2009, p. 100) o conceito de intimidade tem origem na Grécia e Roma antigas, onde o lar era encarado como um lugar santo e inviolável. Trás ainda o referido autor, a ideia do amadurecimento do direito à intimidade com a afirmação da burguesia como classe social e a Revolução Francesa, que fizeram surgir os precursores dos direitos do homem.

De forma mais contemporânea, referindo-se sucintamente às legislações de Direito Comparado, a doutrina germânica teria um maior domínio no tratamento do direito à reserva de intimidade da vida privada e familiar, com a chamada:

Teoria das esferas de proteção, que distingue, na sua formulação mais usual, e paralelamente a uma esfera de publicidade, entre uma esfera pessoal, compreendendo as relações que o indivíduo estabelece com o meio social, uma esfera privada, relativamente à trajetória do sujeito ou à sua inserção em contextos de maior proximidade afetiva e relacional e uma esfera íntima, a que se subsumem os aspectos relativos ao mundo dos sentimentos, da existência biopsíquica, da sexualidade (CANOTILHO; MACHADO, 2003, p.53).

Ainda seguindo a linha de pensamento de Álvaro Rodrigues Júnior (2009, p. 102), na Declaração Universal dos Direitos do Homem, a proteção à intimidade está totalmente vinculada aos conceitos da vida privada do indivíduo e de toda a sua família, assim como o caráter privado do domicílio e da correspondência. Por essa razão, sem querer discutir de forma pormenorizada a cerca do conflito de normas fundamentais, que não é foco deste trabalho, seria o direito à intimidade da vida privada e familiar, a primeira limitação às liberdades de expressão e informação.

Assim sendo, o vínculo indissociável existente entre o princípio fundamental da dignidade da pessoa humana e o direito à intimidade, neste tópico referido, conclui não só que este é consequência daquele, como também que são juntos, os postulados estruturantes de toda uma sociedade democrática de direito. Entretanto, esses postulados vêm sofrendo abalos na atualidade, devido à mitigação dos valores sociais na “Era da informação”.

### 3.4 A VIOLAÇÃO DA INTIMIDADE ATRAVÉS DA INTERNET

O acelerado avanço das tecnologias de informação construiu um mundo onde a violação de direitos até então intransponíveis se tornou algo banal. Novas técnicas comerciais e

econômicas, de marketing, de relacionamento entre as pessoas, de conflitos e de danos, bem como de novos delitos, até então desconhecidos, vêm surgir nesse novo mundo. É o contemporâneo mundo da Internet, que em outra perspectiva, reflete também em uma poderosa ameaça à intimidade do ser humano.

A Internet tem mitigado as liberdades individuais. O conceito de privacidade tem sofrido mutações axiológicas com a velocidade das novas tecnologias, fato que tem gerado uma fragilidade nos direitos fundamentais e uma preocupação por parte de toda a comunidade jurídica. Rodota apud Oliveira, (2012, p. 67-68) preocupado com esta desenfreada evolução diz que:

A Internet é um imenso espaço público e não deve ser nem privatizado nem colonizado. Mas quais as forças que podem redefinir este espaço, quais os recursos políticos que estão presentes neste espaço e quem pode utilizá-los? A Internet não é mais o espaço da liberdade infinita, de um poder anárquico que ninguém pode domar. Hoje, é um espaço de conflitos, onde a liberdade é apresentada como inimiga da segurança; onde os argumentos da propriedade contrastam com aqueles do acesso; o livre pensar desafia a censura.

Vale aqui destacar o argumento de Mendes; Branco (2012, p. 318, 319) ao afirmar que a importância da vida privada e da não violação à intimidade do indivíduo, como sendo necessidades de todo homem, para a sua própria saúde mental. A livre personalidade não se desenvolve sem privacidade. Aduz não ser saudável à própria capacidade de superação do ser humano, a exposição desenfreada dos próprios erros, fracassos, críticas e desgostos.

A Constituição Federal de 1988 elencou em seu artigo 5º, inciso X, a inviolabilidade do direito à intimidade, “assegurando o direito à indenização pelo dano material ou moral decorrente de sua violação”. Entretanto, há a necessidade de se regulamentar de forma enfática uma legislação verdadeiramente eficaz, no combate aos delitos informáticos praticados através da Internet, pois na mesma velocidade em que se aprimoram as novas tecnologias, novos danos também surgem, aumentando ainda mais as estatísticas da impunidade.

Um caso recente, que repercutiu continentalmente nas redes midiáticas e teve reflexo, também, na esfera legislativa brasileira foi o da atriz e modelo Carolina Dieckman, que teve fotos da sua intimidade copiadas de seu computador e, logo depois foi vítima de extorsão praticada pelos delinquentes, para que as imagens não fossem divulgadas na Internet. Sem adentrar a recorrente questão do “Populismo Penal” e a influência do sensacionalismo midiático na desenfreada normatização criminal, o caso da atriz tomou tamanha repercussão que deu origem a Lei 12. 737 de 02 de abril de 2012, que criou o tipo penal de “Invasão de Dispositivo

Informático”. A referida lei e todas as suas nuances serão objeto de estudo em tópico oportuno no capítulo seguinte desta obra.

Também decretada como reflexo do caso Carolina Dieckman foi a lei de número 12.735 de 2012, para tipificar condutas realizadas mediante uso de sistema eletrônico, digital ou similares, contra sistemas informatizados.

Outro caso de repercussão mundial, e que mostra a fragilidade dos sistemas de proteção a possíveis invasões através da Internet, porém de pouca divulgação midiática ocorreu em março de 2013, que ficou conhecido por especialistas em segurança como o “Maior ataque cibernético da história”. Segundo o Jornal online G1.globo.com os ataques tiveram início em 18 de março depois que a Spamhaus, uma organização *antispam*, bloqueou o provedor holandês “Cyberbunker”. Segundo o periódico, os criminosos da Internet, os *crackers*, usaram uma técnica conhecida como *Distribution Reflection Denial of Service (DRDoS)* ou “ataque de negação de serviço refletido”, causando uma sobrecarga nas conexões do mundo inteiro e gerando uma espécie de apagão na grande rede.

O caso mais recente de violação da privacidade através da Internet no Brasil foi noticiado como um ataque a própria soberania de um Estado. O programa de televisão da Rede Globo, o Fantástico, exibiu uma matéria em que descreve todos os passos de um possível monitoramento não consentido das comunicações da atual Presidente do Brasil Dilma Rousseff, bem como de seus assessores, realizado pelos Estados Unidos.

Segundo a reportagem exibida em 01 de Setembro de 2013, as provas foram cedidas pelo ex-analista da *National Security Agency (NSA)*, o Edward Snowden, que deixou os Estados Unidos portando secretos documentos da agência, com a intenção de divulgar o sistema de espionagem americano no mundo. A matéria mostrou que os documentos faziam parte de um relatório que fora apresentado de forma comemorativa para os agentes, com o título “Filtragem inteligente de dados: estudo de caso México e Brasil”. Através das redes de telefone e, principalmente, pela rede mundial de computadores, a Internet, as comunicações, as redes sociais e os servidores de e-mail foram interceptados.

O sistema de espionagem funciona da seguinte forma:

Selecionado o alvo, são monitorados os números de telefone, os e-mails e o IP, a identificação do computador. O mesmo para os interlocutores escolhidos, no caso, assessores. O que eles chamam de ‘um pulo’, é toda a comunicação entre o alvo e os assessores. Um pulo e meio, quando os assessores conversam entre eles. Dois pulos, quando eles conversam com outras pessoas (BRIDI; GREENWALD, 2013).

Foi uma clara violação do princípio da Soberania de um Estado. Segundo o ex-agente Edward Snowden, o verdadeiro objetivo dos Estados Unidos na espionagem é de cunho totalmente econômico, que nas suas palavras:

A tática do governo americano desde o 11 de setembro é dizer que tudo é justificado pelo terrorismo, assustando o povo para que aceite essas medidas como necessárias. Mas a maior parte da espionagem que eles fazem não tem nada a ver com segurança nacional, é para obter vantagens injustas sobre outras nações em suas indústrias e comércio em acordos econômicos (BRIDI; GREENWALD, 2013).

Portanto, tudo isso prova mais uma vez as desvantagens trazidas pelas novas tecnologias da informação, o que gera a necessidade de uma urgente medida de proteção aos direitos mais basilares da pessoa humana, sob pena de um retrocesso social no mundo inteiro. É inegável a relevância da Internet no desenvolvimento da humanidade, mas é questionável a sua evolução desenfreada sem medidas, em detrimento dos direitos e princípios fundamentais de uma sociedade democrática de direito, como o direito à intimidade.

## 4 AS REDES SOCIAIS E A INVASÃO DA PRIVACIDADE

O que era inimaginável há pelo menos três décadas já se tornou possível atualmente. Trocar informações, vídeos, imagens ou áudios em tempo real, com qualquer pessoa do mundo, não mais faz parte dos pensamentos surreais e futuristas do ser humano. Definitivamente, as mídias sociais têm mudado a vida e as interações de toda a sociedade.

Se já era impossível visualizar um mundo sem a Internet, hoje, já não se pode imaginar a Internet sem as redes sociais. Seja no comércio, na economia, na educação, na cultura, na política, nos movimentos sociais, nas entrevistas de emprego, nas opções de diversão ou até nos relacionamentos amorosos, as redes sociais tornaram-se as protagonistas na era da informação.

Entretanto, devido à velocidade dos avanços, aspectos negativos também vêm surgir com essa socialização digital das comunicações. A liberdade da troca de informações despon-ta como prioridade em detrimento do direito fundamental à privacidade, inerente e imprescindível a todos os seres humanos. Há uma verdadeira confusão de significados no que seria público e no que seria privado.

Nesse contexto, onde as pessoas estão conectadas o tempo todo, tudo que é postado nas mídias *online* pode se tornar a favor ou contra o indivíduo. E através desse dinamismo de informações, em face do enorme poder formador de opinião, uma marca de empresa ou a reputação de uma pessoa pode ser construída, assim como destruída em uma pequena fração de segundos com apenas um “clique”.

Surge, portanto, a necessidade da interferência estatal para regulamentar as novas interações da “Era Digital”, na tentativa de sopesar os efeitos negativos desse excesso de exposição da intimidade das pessoas.

### 4.1 AS REDES SOCIAIS E SUA IMPORTÂNCIA

A rede social é, antes de qualquer explanação, um conglomerado de pessoas que troca informações em uma relação de *feedback*. Faz parte da primitiva necessidade do ser humano de se socializar para se desenvolver. Viver em sociedade é viver em uma rede social. No entanto, esse conceito vem evoluindo de significado concomitantemente aos avanços tecnológicos. As relações que antes eram puramente físicas passaram a integrar um ambiente desmate-

realizado. As interações entre as pessoas deslocaram-se para o espaço virtual, onde a Internet é a ferramenta das possibilidades.

Em uma conceituação mais moderna do que é uma rede social, pode-se definir como sendo um ambiente de relações instantâneas, independentemente de lugar e tempo, onde pessoas interagem entre si criando uma rede de amigos que se reúnem em torno de interesses comuns na *web*.

Segundo Duarte; Frei (2008, p. 156) a rede social seria uma “estrutura social composta por pessoas ou organizações, conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns”.

Em outra perspectiva, as redes sociais são consideradas como sites de relacionamento que têm o objetivo preponderante de troca de experiências. Na visão de Recuero apud Madeira; Gallucci (2009, p. 2), a rede social:

É gente, é interação, é troca social. É um grupo de pessoas, compreendido através de uma metáfora de estrutura, a estrutura da rede. Os nós da rede representam cada indivíduo e suas conexões, os laços sociais que compõem os grupos. Esses laços são ampliados, complexificados e modificados a cada nova pessoa que conhecemos e interagimos.

Assim sendo, pode-se entender que a rede social na atualidade representa uma atmosfera de troca recíproca de informações, das relações desmaterializadas, de provas documentadas por escrito e irretiráveis e, acima de tudo, de alcance global via Internet.

A importância das redes sociais na *web* é perceptível em todos os seguimentos da sociedade. Por mais impactante que seja, falar em um mundo sem as redes sociais já não é mais possível.

No seguimento econômico, as empresas encontraram nas redes sociais a ferramenta indispensável para seu desenvolvimento. E esse desenvolvimento pode ser analisado através de níveis que medem a presença das empresas nas redes sociais.

Em um nível inicial as redes *online* são usadas apenas como meio informativo, uma ferramenta de anúncio em estratégias de *marketing* modernas.

Em um segundo nível mais avançado, através de uma interação com seus clientes, as empresas passam a discutir as melhorias de seus produtos e serviços através das redes, o que possibilita traçar um perfil de seus futuros compradores. Alertando para o risco de essa interatividade refletir de forma negativa, Madeira; Gallucci (2009, p. 3) dizem que antes de tudo é preciso ouvir e entender as opiniões dos consumidores para que, dessa forma, passe a conhecer seu público, minimize as possíveis crises e crie novas estratégias de mercado.

Evoluindo ainda mais essa interatividade, em um terceiro nível, as empresas criam o que chamam de “Social SAC”, ou seja, um canal de atendimento ao cliente em rede social, que objetiva melhorar o relacionamento da empresa com seus clientes e colaboradores, para se atingir um objetivo final, que é o aumento do lucro.

Na educação, também é fácil perceber a importância das redes sociais. As instituições de ensino na tentativa de potencializar o aprendizado de forma rápida e eficiente têm criado ferramentas que possibilitam uma melhor interação aluno-professor. Criam canais de discussões em tempo real, que são chamados de *chat* para tirar dúvidas, postam vídeo aulas complementares às presenciais, publicam eventos e coletam opiniões a cerca de melhorias do ensino através de enquetes virtuais.

Já na política, as redes da *web* despontaram como uma importante ferramenta no auxílio aos movimentos sociais em todo o mundo. O Brasil foi palco de inúmeras manifestações que se iniciaram em meados de 2013. Milhares de jovens, estudantes e população em geral, insatisfeitos com o panorama político e social, saíram em passeatas pelas ruas de todo o país, onde os locais e horários dos movimentos eram agendados através das redes sociais.

Ademais, outro seguimento de fácil visualização é o de relacionamentos amorosos. As redes sociais têm ocasionado um verdadeiro impacto na vida sentimental das pessoas. Um simples “adicionar”, “seguir”, “curtir”, “compartilhar” ou “cutucar” pode desencadear um elo mais contundente entre os usuários. A força dessas mídias sociais é tão grande que a maioria dos casais nos dias de hoje, só passa a encarar a relação como autêntica depois de alterar o seu “status” na rede social para “namorando” ou para “em um relacionamento sério”. Entretanto, na contramão dessa velocidade também está o término dos relacionamentos, que acontece na mesma rapidez que o seu início.

São muitas as redes sociais espalhadas por todo o mundo. As mais conhecidas são o *Facebook*, o *Youtube*, *ask.fm*, o *Twitter*, *Orkut*, *Google+*, *Instagram*, *Myspace*, dentre outras. O *Facebook*, criado em 2004, lidera como a rede social de maior número de usuários ativos no mundo.

Segundo pesquisa realizada pela Midiatix, agência especializada em redes sociais, este *site* de relacionamentos já tem mais de 1 bilhão de usuários pelo mundo, com presença em 213 países. Fazendo um comparativo, se esse número representasse a população de um país, o *Facebook* figuraria como o terceiro maior do mundo, só perdendo para China e Índia. Ainda segundo a pesquisa, o *Twitter* é a segunda maior rede social do mundo, com cerca de 200 mi-

lhões de usuários ativos. Em média 70 % dos usuários de Internet estão cadastrados em pelo menos uma rede social no planeta<sup>1</sup>.

Vale aqui apresentar alguns importantes dados estatísticos referentes ao uso das redes sociais no Brasil, através de uma pesquisa realizada pela *ComScore* que publicou um relatório em março de 2013 com as principais tendências no uso da Internet em 2012 e o que isso significa para o mercado nacional nos próximos anos<sup>2</sup>.

Segundo o relatório, o Brasil comporta o mercado mais participativo da América Latina com consumidores que ultrapassam as 27 horas por mês *online* em seus computadores (vide Gráfico I do Anexo C)

Quanto ao uso das redes sociais, o Brasil atingiu uma média de cerca de 10 horas de acesso no mês de dezembro de 2012 (vide Gráfico II do Anexo C), o que mostra como os brasileiros estão envolvidos e cada vez mais dependentes das mídias sociais.

No que diz respeito a lista das redes mais acessadas pelos brasileiros o *Facebook* desponta na liderança como a mais utilizada. Logo depois, vem o *Orkut*, o *Twitter*, o *Ask.FM* que está com o crescimento em ascensão, o *Linkedin* que é mais direcionado para relacionamentos profissionais, o *Tumblr.com*, o *Badoo.com*, o *Deviantart.com* e, por último o *Myspace*, nessa ordem (vide Gráfico III do Anexo C).

Assim sendo, pode-se depreender que o continuado crescimento do número de usuários nas redes sociais tem adquirido importância imprescindível na vida das pessoas de todo o mundo. Todavia, aspectos negativos desse acelerado crescimento também têm atingido a sociedade pós-moderna, como por exemplo, a invasão da privacidade dos indivíduos em face da excessiva exposição da intimidade nas redes sociais.

#### 4.2 A INVASÃO DA PRIVACIDADE PELAS REDES SOCIAIS

No capítulo anterior, ao tratar da violação da intimidade através da Internet, acentuou-se a perceptível mitigação do direito à privacidade em razão das novas tecnologias de informação. E nesse panorama, as redes sociais figuram como a principal ferramenta de mudança nos conceitos de público e privado.

<sup>1</sup> MIDIATIX. **Números e fatos das mídias sociais em 2013**. Disponível em: <<http://www.youtube.com/watch?v=dGeuNF4oUHE>>. Acesso em 02 de Setembro de 2013.

<sup>2</sup> BRAZIL Digital Future in Focus. **Principais insights de 2012 e o que eles significam para o novo ano**. Relatório anual realizado pela ComScore.Inc. 2013. Disponível em: <<http://www.slideshare.net/iFulvio/2013-brazil-futureinfocusfinalportuguese>>. Acesso em: 02 set. 2013.

Nas palavras de Tércio Sampaio Ferraz (1992, p. 77) a privacidade é um direito subjetivo fundamental, cujo titular é:

Toda pessoa, física ou jurídica, brasileira ou estrangeira, residente ou em trânsito no país; cujo conteúdo é a faculdade de constranger os outros ao respeito e de resistir à violação do que lhe é próprio, isto é, das situações vitais que, por só a ele lhe dizem respeito, deseja manter para si, ao abrigo de sua única e discricionária decisão; e cujo objeto é integridade moral do titular.

Em acertada definição do direito à privacidade, Costa Júnior apud Mendes; Branco (2012, p. 318) elenca que é resultado da necessidade do indivíduo de “encontrar na solidão aquela paz e aquele equilíbrio, continuamente comprometido pelo ritmo da vida moderna”.

A privacidade, tal como protegida pela constituição é o direito de estar só e de:

Ser deixado em paz para, sozinho, tomar as decisões na esfera da intimidade, e assim evitar que certos aspectos da vida privada cheguem ao conhecimento de terceiros, tais como confidências, hábitos pessoais, relações familiares, vida amorosa, saúde física ou mental, etc. É um direito de conteúdo negativo, dizem os autores, porque veda a exposição de elementos particulares da esfera reservada do seu titular a conhecimento de terceiros (Cavaliere Filho, 2010, p. 113).

O direito à privacidade está presente em praticamente todas as constituições democráticas. No Brasil, na Constituição de 1988 é tratado como um direito fundamental, que diz já em seu artigo 5º:

X – são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito à indenização pelo dano material ou moral decorrente de sua violação.

(...)

XII – é inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, salvo, no último caso, por ordem judicial, nas hipóteses e na forma em que a lei estabelecer para fins de investigação criminal ou instrução processual penal.

Ocorre que, a moderna sociedade digital essencialmente formada por componentes intangíveis e incorpóreos tem como consequência o apreço pela liberdade e pela exposição da vida cotidiana, sem observância do mínimo de restrição. Essa ausência de seleção do que publicar na *web*, onde a palavra de ordem é “divulgar tudo”, põe em risco o próprio direito de pleitear a reparação em casos de dano, já que os próprios usuários das redes, muitas vezes de forma impensada, expõem a própria intimidade.

Destaca-se aqui uma das características marcantes das redes sociais que é a documentação irretratável do que se publica. Uma vez divulgada, a informação passa a fazer parte de

um ambiente multiplicador de dados em cadeia. É uma verdadeira difusão de informações de maneira epidêmica. O problema é que as consequências no futuro são imprevisíveis e, uma informação que no contexto da publicação não teria um cunho negativo, tempos depois, pode ser usada contra o internauta.

Um exemplo dessa situação, mais comum do que se imagina, é o de estudantes que divulgam nas mídias sociais fotos e/ou vídeos de sua intimidade, que no contexto da situação parecem ser naturais. Todavia, tempos depois, ao passarem por uma seleção de emprego, onde atualmente é comum se fazer uma análise do perfil dos candidatos nas redes sociais, perdem a vaga por conta do registro de situações comprometedoras para o profissional pretendido pela empresa.

Outro ponto a se destacar é a questão financeira envolvida por trás das redes sociais e que está totalmente interligada à invasão da privacidade do usuário. Muito se questiona como os fundadores e proprietários desses *sites* de mídias sociais conseguem captar lucros, já que o cadastro é gratuito com o simples preenchimento de alguns dados.

A resposta é muito simples. Quando as pessoas navegam na Internet, fazem coisas do cotidiano como se estivessem em ambientes físicos, como o simples ato de visitar uma loja e avaliar produtos. Ao participar de uma rede social, se compartilha os interesses em determinadas mercadorias, os ambientes mais frequentados, as marcas favoritas, as necessidades rotineiras, dentre outras preferências do dia-a-dia. E com uma simples avaliação das atividades mais frequentes do internauta, facilmente consegue-se traçar o seu perfil que agora passa a ser um consumidor em potencial.

O produto de valor econômico a ser comercializado é exatamente o perfil do internauta. Redes de relacionamento como o *Facebook*, *Twitter* e *Orkut* funcionam como bancos de dados que armazenam as características dos usuários. Com essas informações, contas de e-mail, endereços, contatos e preferências disponíveis, elabora-se um verdadeiro “dossiê comercial” que é vendido para as grandes empresas que, após traçarem o perfil do provável comprador/consumidor, direcionam as mais variadas estratégias de *marketing* para venda de produtos e serviços.

Assim sendo, pode-se concluir que as ações efetuadas em uma rede social estão envolvidas por um sistema de riscos, onde a reputação e o comportamento do indivíduo na *web* podem comprometer aspectos da vida pessoal e profissional, o que demonstra mais uma vez o poder de invasão da Internet na privacidade dos usuários.

Toda essa problemática em torno da Internet, a invasão da intimidade das pessoas e ausência de regulamentação sobre o tema, eclodiu de forma impactante na comunidade jurídica do Brasil, refletindo em diversas movimentações no sentido de estabelecer regras e princípios no uso dessa veloz ferramenta de comunicação da Era Digital.

A inquietação inicial foi direcionada para a necessidade de uma normatização penal que viesse a tutelar as relações jurídicas *online*. Entretanto, essa ideia foi logo rechaçada pelos estudiosos, como bem descreve Tainá Cristina de Oliveira (2012, p. 55), ao defender que a normatização da Internet deveria iniciar na esfera civil para, só depois, partir para esfera criminal.

Nesse sentido, assenta-se o princípio da intervenção mínima do Direito Penal que tem como consequência a sua característica de subsidiariedade, como bem explica Capez (2005, p. 22) ao pronunciar que:

O ramo penal só deve atuar quando os demais campos do Direito, os controles formais e sociais tenham perdido a eficácia e não sejam capazes de exercer essa tutela. Sua intervenção só deve operar quando fracassam as demais barreiras protetoras do bem jurídico predispostas por outros ramos do Direito.

(...)

A intervenção mínima e o caráter subsidiário do Direito Penal decorrem da dignidade da pessoa humana, pressuposto do Estado Democrático de Direito, e são uma exigência para a distribuição mais equilibrada da justiça.

As discussões sobre o tema resultaram no Projeto de Lei de nº 2.126/2011 chamado de “Marco Civil da Internet”, de iniciativa do Ministério da Justiça e com a participação da sociedade, que objetivou estabelecer regras, princípios, garantias e deveres no uso e desenvolvimento da Internet no Brasil, bem como regular as relações e responsabilidades dos provedores.

Na Exposição de Motivos (2011), o Projeto de Lei do Marco Civil, explica todos os fundamentos do projeto, considerando-o como o primeiro passo no caminho legislativo para se regulamentar questões importantes ligadas ao uso na Internet (BRASIL, 2013).

A Exposição de Motivos que teve a assinatura do então Ministro da Justiça José Eduardo Martins Cardozo, Ministro das Ciências e Tecnologia Aloizio Mercadante Oliva, Ministro das Comunicações Paulo Bernardo Silva, e da Ministra do Planejamento, Orçamento e Gestão Miriam Aparecida Belchior, tramita atualmente na Câmara dos Deputados está sujeita à apreciação do Plenário em regime de urgência. O Projeto submetido à apreciação da Presidente da República estabelece:

Princípios, garantias, direitos e deveres para o uso da rede mundial de computadores no país, e dá outras providências. Tal projeto foi construído em conjunto com a sociedade, em processo que ficou conhecido sob a denominação de Marco Civil da Internet (BRASIL, 2013).

Em que pese às críticas na demora da regulamentação do projeto que ainda tramita na Câmara dos Deputados, o Comitê Gestor de Internet do Brasil (CGI.br), que representa um respeitado modelo de governança multissetorial da Internet com legítima participação popular, destacou a importância de se aprovar com urgência o projeto do “Marco Civil” para afastar:

Movimentos nacionais e internacionais que violem os princípios e garantias de uso e desenvolvimento da Internet e de direitos civis constitucionais da sociedade brasileira e de consolidar, no arcabouço legal brasileiro, os princípios fundamentais de neutralidade de rede, de defesa da privacidade de todos que utilizam a Internet e de inimizabilidade da rede (CGI.br, 2012, p. 5).

No que tange a esfera penal, com os chamados crimes digitais ou cibernéticos, um caso de grande repercussão midiática veio eclodir na rápida sanção da Lei nº 12.737/2012, conhecida como “Lei Carolina Dieckmann”, que será objeto de estudo no tópico subsequente.

#### 4.3 O CASO CAROLINA DIECHMANN E O ADVENTO DA LEI Nº 12.737/2012

Assim como em um ambiente físico, no “mundo virtual” crimes também são praticados. A terminologia usada agora é de crimes virtuais, crimes cibernéticos, cibercrimes, crimes digitais, dentre outras nomenclaturas. Em uma definição genérica, são os delitos praticados por meios eletrônicos com o uso de sistemas da informação, onde a Internet é a principal ferramenta, mas não a única, facilitadora no cometimento dos crimes.

Em definição mais complexa Gustavo Testa Corrêa (2008, p. 44, 45) entende por crimes digitais:

Todos aqueles relacionados às informações arquivadas ou em trânsito por computadores, sendo esses dados, acessados ilicitamente, usados para ameaçar ou fraudar; para tal prática é indispensável à utilização de um meio eletrônico. Toda sociedade dependente da informação acaba sendo vítima de simples ameaças e até do terrorismo e do vandalismo eletrônico.

A legislação penal brasileira até dezembro de 2012 não tinha ainda uma lei específica que tratasse dos crimes cibernéticos. No entanto, um caso de repercussão continental na mídia, que envolveu a famosa atriz Carolina Dieckmann deu ensejo à primeira lei penal brasilei-

ra a tipificar os delitos informáticos. A atriz teve seu computador invadido por *crackers*, que fizeram cópias de fotos íntimas da atriz e depois as usaram na tentativa de extorsão. Devido à resistência da vítima em pagar os valores exigidos, os delinquentes publicaram as imagens nas mídias sociais que logo se espalharam por toda a rede em proporções inimagináveis.

Segundo matéria publicada pela Revista Veja, em meados de 2012, criminosos da informática, conhecidos como *crakers*, de cidades interioranas de Minas Gerais e São Paulo, invadiram o computador da atriz Carolina Diechmann, de onde coletaram fotos de sua intimidade. Acontece que, após resistir às chantagens desferidas pelos delinquentes, que exigiam cerca de dez mil reais para não divulgarem as imagens, o conteúdo acabou sendo publicado na Internet. Daí em diante, a velocidade de propagação das informações das redes sociais protagonizou durante alguns meses as notícias dos mais variados meios de comunicação <sup>3</sup>.

O Projeto de Lei nº 2.793 de 2011 de autoria dos Deputados Paulo Teixeira, Luiz E-rundina, Manuela D'Ávila, João Arruda, Brizola Neto e Emiliano José, que tratava sobre a tipificação criminal dos delitos informáticos teve sua tramitação acelerada em face da grande repercussão midiática do caso da atriz. Segundo a exposição de motivos do Projeto os avanços da tecnologia trazem a necessidade de regulamentação “de aspectos relativos à sociedade da informação, com o intuito de assegurar os direitos dos cidadãos e garantir que a utilização destas tecnologias possa ser potencializada <sup>4</sup>”.

Foi tão grande o impacto na mídia nacional e internacional que a tramitação rápida do Projeto deu origem a Lei nº 12.737/2012 (anexo C), apelidada popularmente de “Lei Carolina Diechmann”, introduzindo o artigo 154-A no Código Penal Brasileiro, tipificando a conduta de “Invasão de dispositivo informático” e, ao mesmo tempo criando, uma nova classe de crimes, os cibernéticos.

A Lei que entrou em vigor no dia 02 de abril de 2013 descreve no *caput* do artigo introduzido na Legislação Penal, como sendo crime a conduta de:

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.

---

<sup>3</sup> VALLE, James Della. Vida Digital. **Lei Carolina Dieckmann entra em vigor nesta terça-feira**. Reportagem publicada na revista Veja em 02/04/2013. Disponível em: < <http://veja.abril.com.br/noticia/vida-digital/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira>>. Acesso em 03 set. 2013.

<sup>4</sup> BRASIL. Câmara dos Deputados. **Projeto nº 2793/2011**. Disponível em: < <http://www.camara.gov.br/sileg/integras/944218.pdf>>. Acesso em 07 de setembro de 2013.

Aqui vale destacar alguns aspectos no âmbito do Direito Penal referentes à Lei Carolina Diechmann. No âmbito da informática os crimes podem ser cometidos com o computador ou contra o computador. No primeiro caso o criminoso utiliza-se de um aparelho informático para a prática de crimes. É o caso dos crimes contra a honra, como a calúnia, a injúria e a difamação, que já estão tipificados no Código Penal, mas que agora são cometidos em redes sociais. No segundo caso, o sujeito comete o crime contra o computador. É neste último que o novo tipo penal previsto no artigo 154-A de enquadra, onde se combate a conduta de “invadir” dispositivo informático alheio.

Outro ponto a se destacar é o fato de que o crime de invasão de dispositivo informático está alocado no Código Penal, Capítulo VI que trata dos crimes contra a liberdade individual, em seção específica dos crimes contra a inviolabilidade dos segredos.

Quanto aos aspectos doutrinários é possível fazer uma breve classificação do crime tipificado na Lei Carolina Diechmann. É um crime comissivo, pois pressupõe uma conduta de fazer do agente delitivo. No que se refere ao momento consumativo é classificado como instantâneo, pois não se prolonga no tempo, bastando ocorrer o simples “invadir” ou “instalar”. Quanto ao resultado é considerado como crime formal, já que o desfecho naturalístico é um mero ato de exaurimento, ou seja, independe da obtenção da vantagem ilícita por parte do criminoso. Quanto aos sujeitos é classificado como unissubjetivo, bastando a conduta de uma única pessoa para a prática do crime. Por fim, o crime em análise é punido apenas na forma dolosa, além de demandar uma finalidade específica de agir que é “obter, adulterar ou destruir dados” na primeira parte do tipo e, para “obter vantagem ilícita”, na parte final.

Ainda que pese as críticas feitas à técnica legislativa empregada no tipo penal do art. 154-A, vale ressaltar que no §1º do artigo, a lei apresenta uma figura de equiparação ao elencar que 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”. Exemplifica-se com a situação hipotética de um sujeito vender ou oferece um vírus de computador que invade dispositivos informáticos.

No §2º do artigo em análise, é apresentada uma majorante nos casos em que “da invasão resulta prejuízo econômico”.

No que se refere ao §3º do artigo 154-A do Decreto-lei nº 2.848/1940, uma qualificadora que pode ensejar a pena de reclusão, caso a invasão do dispositivo informático:

Resultar na 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.

O último ponto a se destacar é o fato de que para configuração do crime de Invasão de dispositivo informático, há a necessidade de se romper um mecanismo de segurança, ou seja, caso a suposta vítima não tenha em seu computador um sistema de proteção, o autor da ação pode não ser considerado culpado.

A título de informação, a lei 12.735 de novembro de 2012 também foi sancionada de forma simultânea a Lei Carolina Diechmann. Em seu artigo 4º prevê que os órgãos da polícia judiciária criarão setores especializados no combate aos crimes cibernéticos. A crítica feita a esse dispositivo é a ausência de condições dadas as polícias para a referida especialização, seja do ponto de vista técnico, material ou estrutural, o que acaba dificultando na solução dos crimes cibernéticos e, aumenta cada vez mais a sensação de impunidade da população.

#### 4.3 OS EFEITOS CIVIS NA INVASÃO DA PRIVACIDADE PELAS REDES SOCIAIS E A IDENTIFICAÇÃO DO RESPONSÁVEL

A Internet tem proporcionado uma rápida evolução nas comunicações do mundo contemporâneo. Conhecer os mais longínquos lugares do planeta sem sequer sair de casa, algo que há muito pouco tempo era impossível, já faz parte da nova realidade tecnológica. Com o advento das redes sociais as pessoas passaram a interagir de forma mais intensa, divulgando no ambiente virtual suas preferências, pensamentos, gostos e desgostos. O problema é que a excessiva exposição da intimidade tem originado novos conflitos de reflexos na seara jurídica e social, só que com particularidades ainda pouco conhecidas pelos aplicadores do direito.

A consequência direta da vertente negativa das redes sociais é exatamente o efeito jurídico, civil ou penal, que a invasão danosa da privacidade pode originar.

No que se refere aos efeitos penais, o tema já fora tratado em tópico anterior com a entrada em vigor das Leis 12.737/2012 e 12.735/2012, que dispõem sobre os delitos informáticos. Neste tópico tratar-se-á de forma mais específica dos efeitos civis, da identificação do responsável e como os Tribunais brasileiros têm entendido a matéria na ausência de regulamentação específica.

Em que pese à ausência de regulamentação específica no âmbito civil quanto aos danos praticados em redes sociais, pelo simples fato de causarem prejuízo devem ser estes reparados.

De acordo com o Código Civil Brasileiro de 2002, em seu art. 186, “aquele que, por ação ou omissão voluntária, negligência ou imprudência, violar direito e causar dano a outrem, ainda que exclusivamente moral, comete ato ilícito”.

O dano, nas palavras de Sérgio Cavalieri Filho (2010, p. 73) conceitua-se como sendo:

A subtração ou diminuição de um bem jurídico, qualquer que seja a sua natureza, quer se trate de um bem patrimonial, quer se trate de um bem integrante da própria personalidade da vítima, como a sua honra, a imagem, a liberdade, etc. Em suma, dano é lesão de um bem jurídico, tanto patrimonial como moral, vindo daí a conhecida divisão do dano em patrimonial e moral.

Os danos praticados em redes sociais, na sua maioria, são de cunho eminentemente moral, já que pela natureza do ambiente virtual em que acontecem, atingem os direitos da personalidade dos usuários, como a intimidade, imagem e honra, elencados no artigo 5º da Constituição Brasileira de 1988.

O maior problema no que se refere aos danos cometidos nas mídias sociais é na responsabilização dos agentes, em face da particular interação entre os indivíduos no ambiente virtual. Além dos próprios sujeitos causadores do dano, destaca-se a presença de outros agentes nesse tipo de dano, que são os provedores e os propagadores das informações ilícitas.

Quanto aos provedores, podem ser classificados como de acesso e de serviços. Aqueles são as “empresas com dispositivos ligados à Rede para obter conectividade IP e repassá-la a outros dispositivos”. Já estes “organizam e mantêm informação *online*”, também chamados de provedores de hospedagem ou mantenedores de *sites*. Para efeito deste trabalho os provedores serão tratados num conceito genérico como sendo aqueles que, de alguma forma, tem gerenciamento sobre as informações divulgadas na Internet. No que se refere aos propagadores de informações são os sujeitos que multiplicam pelas redes as informações, fazendo uma transmissão em cadeia (GABRIEL, 2009).

Devido a grande dificuldade de se identificar o agente criminoso que causou o dano nas redes sociais, doutrina e jurisprudência passaram a discutir a cerca da responsabilidade solidária dos provedores por informações ilícitas divulgadas nos sistemas por terceiros.

O primeiro entendimento se baseava na teoria da responsabilidade objetiva, pelo simples fato do risco inerente à natureza da atividade das mídias sociais, com fundamento legal no artigo 927, parágrafo único, do Código Civil Brasileiro, que trata da responsabilização do dano independentemente da comprovação de culpa.

Na outra ponta, a responsabilidade dos mantenedores dos *sites* era baseada na teoria subjetiva, onde os provedores só seriam responsabilizados pela negligência de não retirar o

conteúdo ilícito quando previamente solicitados. O fundamento desse entendimento era a impossibilidade de se fazer um filtro prévio do que era ou não postado nas redes sociais.

Este segundo entendimento se baseava na jurisprudência norte-americana do caso *Cubby versus* o provedor CompuServe, senão vejamos:

Um dos primeiros julgados sobre difamação na Internet (em 1991), onde a Corte Distrital de Nova Iorque concluiu que o provedor não teve oportunidade de rever o conteúdo da publicação antes dela ser enviada para o seu sistema, daí que não podia ser responsabilizado pela mensagem eletrônica (REINALDO FILHO, 2011).

Segundo Reinaldo Filho (2011) a divergência quanto a responsabilidade dos provedores na divulgação de conteúdo lesivo nas redes sociais foi pacificada quando o caso chegou ao Superior Tribunal de Justiça, em julgamento que teve a empresa Google Brasil Internet Ltda. em um dos polos e, no outro, uma mulher que fora vítima de danos morais ocasionados por publicações ofensivas a sua pessoa.

No caso em epígrafe, o Superior Tribunal de Justiça (2010), na análise do Recurso Especial nº 1193764/SP, cuja relatoria do caso coube a ministra Nancy Andrighi, entendeu pela não aplicabilidade da responsabilidade objetiva prevista no art. 927 do Código Civil, compreendendo que o dano moral por publicações danosas não constituíam risco próprio da atividade de risco. Entretanto, nas palavras da Ministra, o provedor:

Ao ser comunicado de que determinado texto ou imagem possui conteúdo ilícito, deve [...] agir de forma enérgica, retirando o material do ar imediatamente, sob pena de responder solidariamente com o autor direto do dano, em virtude da omissão praticada.

Portanto, apesar de a relatora não ter se filiado ao entendimento da responsabilidade independentemente de culpa, acrescentou que poderá o provedor/mantenedor responder pelos danos causados a outrem de forma solidária ao agente que cometeu a ofensa, caso venha a agir de forma negligente na exclusão das informações danosas, após requerida a retirada pela vítima ou órgão judicial.

A jurisprudência dos tribunais brasileiros passou a acompanhar de forma majoritária o entendimento da ministra, no sentido da responsabilidade subjetiva com as ressalvas, no caso de omissão por parte dos provedores:

AGRAVO REGIMENTAL NO AGRAVO (ART. 544 DO CPC) - AÇÃO INDENIZATÓRIA POR DANO MORAL - CRIAÇÃO DE PERFIL FALSO EM SÍTIO DE RELACIONAMENTO (ORKUT) - AUSÊNCIA DE RETIRADA IMEDIATA DO

MATERIAL OFENSIVO - DESÍDIA DO RESPONSÁVEL PELA PÁGINA NA INTERNET - SÚMULA N. 7 DO STJ - DECISÃO MONOCRÁTICA NEGANDO PROVIMENTO AO RECURSO - INSURGÊNCIA DA RÉ. A jurisprudência desta Corte firmou-se no sentido de que "o dano moral decorrente de mensagens com conteúdo ofensivo inseridas no site pelo usuário não constitui risco inerente à atividade dos provedores de conteúdo, de modo que não se lhes aplica a responsabilidade objetiva prevista no art. 927, parágrafo único, do CC/02" (REsp 1308830/RS, Rel. Ministra NANCY ANDRIGHI, TERCEIRA TURMA, julgado em 08/05/2012, DJe 19/06/2012). Contudo, o provedor de internet responderá solidariamente com o usuário autor do dano se não retirar imediatamente o material moralmente ofensivo inserido em sítio eletrônico. Agravo regimental desprovido. (STJ, 2013. Agravo Regimental no Agravo em Recurso Especial nº 308163/ RS. Relator: Ministro Marco Buzzi, julgado em 14/05/2013).

No mesmo sentido, outro julgado do Superior Tribunal de Justiça já do ano de 2013, destaca:

AGRAVO REGIMENTAL EM AGRAVO EM RECURSO ESPECIAL. RESPONSABILIDADE DE PROVEDOR DE INTERNET PELA RETIRADA DE CONTEÚDO DENUNCIADO POR QUEM SE SINTA PREJUDICADO. DESNECESSIDADE DE INDICAÇÃO DAS URLs. VIOLAÇÃO AO ART. 535 DO CPC. NÃO OCORRÊNCIA. INEXISTÊNCIA DE CERCEAMENTO DE DEFESA. 1. Não há que se falar em violação ao art. 535 do CPC, quando o Tribunal de origem emite pronunciamento sobre a matéria impugnada de forma fundamentada, ainda que em sentido contrário à pretensão da recorrente. 2. Não configura o cerceamento de defesa o julgamento da causa sem a produção de prova considerada essencial por uma das partes, quando o tribunal de origem entender que o feito foi corretamente instruído, declarando a existência de provas suficientes para o seu convencimento. 3. Notificada a empresa para retirar material moralmente ofensivo inserido em sítio eletrônico e tendo permanecido inerte, correta a sua condenação em danos morais, uma vez que não lhe serve de defesa a falta de indicação, pelo ofendido, das Uniform Resource Locators (URLs) das páginas a serem retiradas. Precedentes. 4. Agravo regimental não provido. (STJ, 2013. Agravo Regimental no Agravo em Recurso Especial nº 230095 / RS. Relator: Luis Felipe Salomão, julgado em 06/08/2013) ?

Malgrado ainda haver entendimentos divergentes quanto à matéria, bem como não existir até então uma legislação civil específica quanto à responsabilização do mantenedor dos *sites* de relacionamento, jurisprudência e doutrina predominantes acordam no sentido de aplicar a responsabilidade subjetiva em casos de danos morais praticados em redes sociais, com a ressalva de ser esta executada de forma solidária nos casos específicos de inércia, na exclusão da informação ofensiva após a solicitação do ofendido ou de quem por direito.

## CONSIDERAÇÕES FINAIS

A pesquisa objetivou analisar a responsabilidade do mantenedor de sites quanto aos danos ocasionados por ofensas nas redes sociais de cunho eminentemente moral, haja vista não ser matéria regulamentada no ordenamento jurídico pátrio, tampouco ser assunto de entendimento pacífico na doutrina e na jurisprudência.

Pela análise histórica inicial compreendeu-se que apesar da relevância da Declaração dos Direitos do Homem proclamada na Revolução Francesa, só após a crueldade vivida na Segunda Guerra Mundial, é que se deu um consenso ideológico entre as nações concernente à necessidade de se proteger direitos essenciais da humanidade.

No que concerne a firmação da Informática como ciência, pode-se perceber que isso só foi possível devido a necessidade de se desenvolver sistemas de prevenção contra ataques aéreos na guerra, o que acabou culminando na criação dos primeiros computadores, como o ENIAC desenvolvido pelos Estados Unidos.

Como se analisou, as grandes descobertas tecnológicas da humanidade partiram de um enfrentamento de guerra. Prova disso, foi o surgimento da Internet, a maior ferramenta de comunicação de todos os tempos, nascida de um projeto de pesquisa militar chamado de ARPANet, que tinha a finalidade de interligar dados em pontos estratégicos caso viesse a eclodir uma terceira guerra mundial.

Entretanto, a expansão global da Internet só se deu com a criação do WWW (*World Wide Web*), um sistema de interface gráfica até hoje utilizado, que possibilitou a transmissão de imagens, áudios e vídeos através de uma rede de computadores.

Estudando a chegada da Internet no Brasil, viu-se que aconteceu de forma tardia na década de 1980. O destaque é que só foi possível a sua popularização com a abertura comercial na década seguinte, o que culminou na criação de um Comitê Gestor de Internet (CGI.br) de efetiva participação popular. O rápido desenvolvimento logo conseguiu potencializar a primitiva necessidade humana de trocar informações que, antes restrita aos ambientes físicos, passou a acontecer nos novos ambientes virtuais. A partir de então nasceram as conhecidas redes sociais, onde pessoas passaram a trocar mensagens, fotos, vídeos e experiências através da web, independentemente de lugar e tempo.

Apesar da grande importância para o desenvolvimento social, observou-se que o crescimento acelerado das redes sociais trouxe consequências negativas, como por exemplo, o excesso de invasão na privacidade alheia, tornando tarefa difícil a diferenciação do que seria

público e privado. Neste ponto destacou-se a característica da publicação irretratável nas redes sociais, já que uma vez publicada a informação, a sua rápida multiplicação impede que ela não se propague na rede.

Como exemplo, analisou-se a Lei nº 12.737 de 2012, que veio tipificar os crimes informáticos. A referida lei ficou conhecida como Lei Carolina Diechmann, devido a grande repercussão midiática de um caso envolvendo uma atriz que teve fotos de seu computador roubadas e divulgadas nas mídias sociais.

Em seguida, ao se investigar os efeitos civis decorrentes da invasão da privacidade através das redes sociais, restou demonstrado o caráter eminentemente moral dos danos, haja vista serem classificados como direitos da personalidade, como a honra, a imagem e a intimidade.

Por último, ficou demonstrado que devido à característica do próprio ambiente virtual das redes, bem como pela ausência de regulamentação da matéria, a dificuldade na identificação do agente causador do dano em redes sociais colocava em risco a própria possibilidade de reparação dos prejuízos. A doutrina e a jurisprudência trataram a matéria de forma não pacífica, onde a divergência se concentrou na teoria da responsabilidade a ser adotada. O primeiro entendimento defendia a responsabilização objetiva dos provedores de serviço, também chamados de mantenedores dos sites, independentemente da comprovação de culpa, com fundamento da teoria do risco inerente ao serviço prestado. A segunda vertente passou a adotar a teoria da responsabilidade subjetiva, onde o mantenedor do site só seria responsabilizado pelos danos causados, se fosse comprovada a sua omissão em retirar o conteúdo ofensivo depois de feita à solicitação por parte da vítima.

Como resultado do estudo, restou comprovado o entendimento majoritário dos tribunais brasileiros, no sentido de adotar a responsabilidade subjetiva dos provedores e/ou mantenedores de sites, com a ressalva de que sendo comprovada a inércia por parte destes, em retirar imediatamente os conteúdos moralmente ofensivos da rede, irão responder de forma solidária com os agentes causadores do dano. Este entendimento se pauta na afirmação de que o conteúdo compartilhado nas redes sociais, mesmo de caráter ofensivo, não constitui um risco inerente à atividade dos provedores de serviço, pois estes não têm ferramentas específicas que possibilite a realização de um filtro de todas as publicações.

## REFERÊNCIAS

ALBERTIN, Alberto Luiz. **Administração de Informática: funções e fatores críticos de sucesso.** 6ª Ed. São Paulo: Atlas, 2009.

ALEXANDRINO, José Alberto de Melo. **Estatuto constitucional da atividade de televisão.** Coimbra: Coimbra, 1998.

ASSUNÇÃO, Marco Flávio Araújo. **Segredos do Hacker Ético.** 2ª Ed. Visual Books: Florianópolis, 2008.

BASTOS, Celso Ribeiro. **Comentários à Constituição do Brasil:** promulgada em 5 de outubro de 1988. 2ª Ed. São Paulo: Saraiva, 2002.

BRASIL. Câmara dos Deputados. **PL 2126/2011.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm](http://www.planalto.gov.br/ccivil_03/Projetos/ExpMotiv/EMI/2011/86-MJ%20MP%20MCT%20MC.htm)>. Acesso em: 07 set. 2013.

BRASIL. **Código Civil Brasileiro.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/leis/2002/110406.htm](http://www.planalto.gov.br/ccivil_03/leis/2002/110406.htm)> Acesso em: 05 set. 2013.

Brasil. **Código Penal Brasileiro.** Disponível em: <[http://www.planalto.gov.br/ccivil\\_03/decreto-lei/del2848.htm](http://www.planalto.gov.br/ccivil_03/decreto-lei/del2848.htm)>. Acesso em: 05 set. 2013.

BRASIL. **Constituição da República Federativa do Brasil.** Brasília: Senado Federal, 1988.

BRASIL. Lei Nº 12.527: **Lei de acesso à informação.** Poder Executivo Federal. Brasília, 2013. Disponível em: <[http://www.acaoainformacao.gov.br/acaoainformacaogov/publicacoes/SumarioExecutivo\\_1anoLAI.pdf](http://www.acaoainformacao.gov.br/acaoainformacaogov/publicacoes/SumarioExecutivo_1anoLAI.pdf)>. Acesso em: 02 set. 2013.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial nº 308163/ RS.** Relator: Ministro Marco Buzzi. Brasília, julgado em 14 de maio de 2013. Disponível em: <[https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=201300614724&dt\\_publicacao=21/05/2013](https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=201300614724&dt_publicacao=21/05/2013)>. Acesso em: 06 set. 2013.

BRASIL. Superior Tribunal de Justiça. **Agravo Regimental no Agravo em Recurso Especial nº 230095 / RS.** Relator: Luis Felipe Salomão. Brasília, julgado em 06 de agosto de 2013. Disponível em: <[https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=201201929407&dt\\_publicacao=14/08/2013](https://ww2.stj.jus.br/revistaeletronica/ita.asp?registro=201201929407&dt_publicacao=14/08/2013)>. Acesso em: 06 set. 2013.

BRASIL. Superior Tribunal de Justiça. **Recurso Especial nº 1193764/SP.** Relatora: Ministra Nancy Andrighi. Brasília, julgado em 14 de dezembro de 2010. Disponível em: <<http://www.stj.jus.br/SCON/pesquisar.jsp>>. Acesso em: 06 set. 2013.

BRAZIL Digital Future in Focus. **Principais insights de 2012 e o que eles significam para o novo ano.** Relatório anual realizado pela ComScore.Inc. 2013. Disponível em: <<http://www.slideshare.net/iFulvio/2013-brazil-futureinfocusfinalportuguese>>. Acesso em: 02 set. 2013.

BRIDI, Sônia; GREENWALD, Glenn. Documentos revelam esquema de agência dos EUA para espionar Dilma. **Jornal Online G1.globo.com/fantástico**. 01 de setembro de 2013. Disponível em <<http://g1.globo.com/fantastico/noticia/2013/09/documentos-revelam-esquema-de-agencia-dos-eua-para-espionar-dilma-rousseff.html>>. Acesso em: 02 de setembro de 2013.

BRUNO, Marcio Roberto. **A Influência da Internet no Setor Bancário do Brasil**. Monografia. Programa de Pós-Graduação Lato Sensu. Pontifícia Universidade Católica de São Paulo. São Paulo, 2006.

BRUNO, Marcio Roberto. **A influência da Internet no setor bancário do Brasil**. MBIS-Master Business Information Systems. Programa de Pós-Graduação Lato Sensu. Pontifícia Universidade Católica de São Paulo. São Paulo, 2006.

CAHALI, Yussef Said. **Dano Moral**. 4ª Ed. São Paulo: Revista dos Tribunais, 2011.

CANOTILHO, J.J. Gomes; MACHADO, Jónatas E. M. **“Reality shows” e liberdade de programação**. Coimbra: Coimbra, 2003.

CAPEZ, Fernando. **Curso de direito penal: parte geral**. 8ª Ed. São Paulo: Saraiva, 2005.

CARVALHO, Marcelo Sávio Revoredo Menezes de. **A trajetória da Internet no Brasil: do surgimento das redes de computadores à instituição dos mecanismos de governança**. Dissertação de Pós-Graduação. Universidade Federal do Rio de Janeiro. Rio de Janeiro, 2006.

CGI.br. **O CGI.br e o Marco Civil da Internet**. 2012. Disponível em: <<http://www.cgi.br/publicacoes/documentacao/CGI-e-o-Marco-Civil.pdf>>. Acesso em 22 ago. 2013.

CORRÊA, Gustavo Testa. **Aspectos Jurídicos da Internet**. 4ª ed. São Paulo: Saraiva, 2008.

COURI, Gustavo Fuscaldo. **Crimes pela Internet**. Monografia. Escola da Magistratura do Estado do Rio de Janeiro. Rio de Janeiro, 2009.

DALMARTELLO. **Danno morali contrattuali**, Revista di Diritto Civile. 1933/55.

DAOUN, Alexandre Jean; LIMA, Gisele Truzzi de. **Crimes Informáticos: o Direito Penal na Era da Informação**. Disponível em: <[www.truzzi.com.br](http://www.truzzi.com.br)>. Acesso em: 21 ago. 2013.

DUARTE, Fábio e FREI, Klaus. Redes Urbanas. In: Duarte, Fábio; Quandt, Carlos; Souza, Queila. **O Tempo Das Redes**. São Paulo: Perspectiva, 2008.

FECOMERCIO. 5ª Pesquisa sobre o comportamento dos usuários na Internet. **V Congresso de Crimes Eletrônicos: formas de proteção**. 2013. São Paulo. Disponível em: <[http://www.fecomercio.com.br/arquivos/arquivo/pesquisa\\_crimes\\_eletronicos\\_rakaaaaa4.pdf](http://www.fecomercio.com.br/arquivos/arquivo/pesquisa_crimes_eletronicos_rakaaaaa4.pdf)>. Acesso em: 06 set. 2013.

FERRAZ JÚNIOR, Tercio Sampaio. **Sigilo de dados: o direito à privacidade e os limites à função fiscalizadora do Estado**. *Cadernos de Direito Constitucional e Ciência Política*. São Paulo: Revista do Tribunais, n.1, 1992.

FERREIRA, Aurélio Buarque de Holanda. **Minidicionário da língua portuguesa**. 4ª Ed. Rio de Janeiro: Nova Esperança, 2001.

- FERREIRA, Ivette Senise. **Os crimes da Informática. Estudos em Homenagem a Manoel Pedro Pimentel**, São Paulo: RT, 1992.
- FILHO, Sergio Cavaliere. **Programa de Responsabilidade Civil**. 9º Ed. São Paulo: Atlas, 2010.
- GABRIEL, Leonardo. **Dicionário de Termos Técnicos**. Informática para concursos. Disponível em <<http://leonardogabriel.com.br/doc/dicionario.pdf>>. Acesso em 06 set. 2013.
- GRANDINETTI, L.G.; CARVALHO, Castanho de. **Liberdade de Informação e o Direito Difuso à Informação Verdadeira**, Rio de Janeiro: Renovar, 2003.
- IDGNOW. **Pesquisa do Comitê Gestor da Internet no Brasil**. Divulgado aos 02.10.2012. Disponível em: <<http://idgnow.uol.com.br/internet/2012/10/02/jovens-do-brasil-usam-mais-redes-sociais-do-que-adolescentes-europeus/>>. Acesso em: 23 abr. 2013.
- LUCCA, Newton; SIMÃO FILHO, Adalberto. **Direito e Internet. Aspectos Jurídicos Relevantes**. 2ed. São Paulo: Quartier Latin, 2005.
- MAÇULA, Marcelo e FILHO, Pio Armando Benini. **Informática: Conceitos e Aplicações**. São Paulo: Érica, 2005.
- MADEIRA, Carolina Gaspar; GALLUCCI, Laura. **Mídias sociais, redes sociais e sua importância para as empresas no início do século XXI**. Trabalho apresentado XXXII Congresso Brasileiro de Ciências da Comunicação. Escola Superior de Propaganda e Marketing. São Paulo, 2009.
- MENDES, Gilmar Ferreira; BRANCO, Paulo Gustavo Gonet Branco. **Curso de direito constitucional**. 7 Ed. São Paulo: Saraiva: 2012.
- NASCIMENTO, Bárbara Luiza Coutinho do Nascimento. **Liberdade de Expressão, Honra e Privacidade na Internet: A evolução de um conflito entre direitos fundamentais**. Monografia. Escola de Magistratura do Estado do Rio de Janeiro. Rio de Janeiro, 2009.
- NOBRE JÚNIOR., Edilson Pereira. **O direito brasileiro e o princípio da dignidade da pessoa humana**. São Paulo: Juris Síntese, 2000.
- NOGUEIRA, Sandro D' Amato. **Crimes de Informática**. São Paulo: BH Editora, 2008.
- NOVELINO, Marcelo. **Direito Constitucional**. 3ª Ed. São Paulo: Método, 2009.
- OLIVEIRA, Tainá Cristina de. **Privacidade na Internet à luz do direito penal**. Monografia. Universidade Estadual do Norte do Paraná. Jacarezinho, 2012. Disponível em: <<http://www.slideshare.net/TainaOliveira1/monografia-privacidade-na-internet-luz-do-direito-penal>>. Acesso em: 30 ago. 2013.
- OLIVEIRA, Tainá Cristina de. **Privacidade na Internet à luz do direito penal**. Monografia. Universidade Estadual do Norte do Paraná. Jacarezinho, 2012. Disponível em: <<http://www.slideshare.net/TainaOliveira1/monografia-privacidade-na-internet-luz-do-direito-penal>>. Acesso em: 30 ago. 2013.

RECUERO, Raquel. **Redes sociais na Internet**. Porto Alegre: Sulina, 2009. (Coleção Ciber-cultura).

REINALDO FILHO, Demócrito. **Julgados sobre a responsabilidade dos provedores**. 2011. Disponível em: <<http://www.conjur.com.br/2011-fev-20/jurisprudencia-responsabilidade-provedores-internet>>. Acesso em 05 set. 2013.

RODRIGUES JUNIOR, Álvaro. **Liberdade de Expressão e liberdade de informação: limites e formas de controle**. Curitiba: Juruá, 2009.

ROHR, Altieres. Organização AntiSpam sofre maior ataque cibernético da história. **Jornal Online G1. globo.com**. 27 de março de 2013. Disponível em <<http://g1.globo.com/tecnologia/noticia/2013/03/organizacao-antispam-sofre-maior-ataque-cibernetico-da-historia.html>>. Acesso em: 30 ago. 2013.

ROSA, Fabrício. **Crimes de Informática**. 2 ed. Campinas: Bookseller, 2006.

SARLET, Ingo Wolfgang. **A eficácia dos direitos fundamentais**. Porto Alegre: Livraria do Advogado, 2001.

SILVA, José Afonso da. **Curso de Direito Constitucional Positivo**. 30ª Ed. São Paulo: Malheiros, 2008.

THE BRIDGE. **Números e fatos das mídias sociais (2013)**. Disponível em: <<http://www.youtube.com/watch?v=dGeuNF4oUHE>>. Acesso em: 05 ago. 2013.

TRENTIN, Taise Rabelo Dutra. TRENTIN, Sandro Seixas. Internet: Publicações ofensivas em redes sociais e o direito à indenização por danos morais. **Revista Direitos Emergentes na Sociedade Global**. v. 1, n. 1, jan.jun/2012. Universidade Federal de Santa Maria. Disponível em: <<http://cascavel.ufsm.br/revistas/ojs-2.2.2/index.php/REDESG/article/download/626-3/pdf>>. Acesso em: 05 set. 2013.

VALLE, J. D. Lei Carolina Dieckmann entra em vigor nesta terça-feira. **Revista Veja (on line)**. Editora Abril. São Paulo, 2013. Disponível em: <<http://veja.abril.com.br/noticia/vida-digital/lei-carolina-dieckmann-entra-em-vigor-nesta-terca-feira>>. Acesso em: 25 ago. 2013.

VENOSA, Sílvio de Salvo. **Direito Civil: Parte geral**. 5ª ed. São Paulo: Atlas, 2005.

## ANEXOS

## ANEXO A

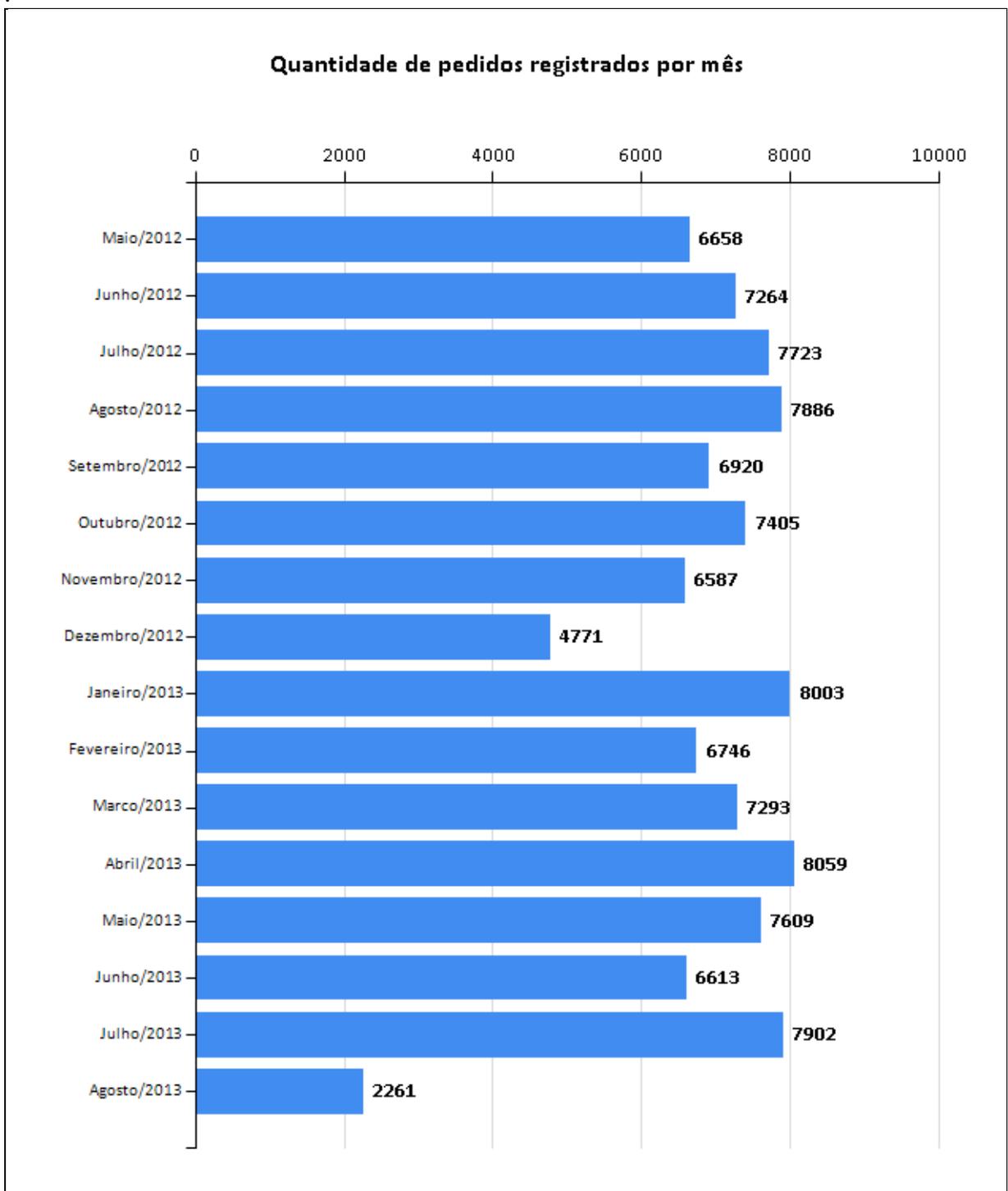


Gráfico 01. Quantidade de pedidos de acesso à informação registrados por mês. 2012/ 2013. Fonte: <http://www.acaoainformacao.gov.br> (e-SIC), ano de 2013

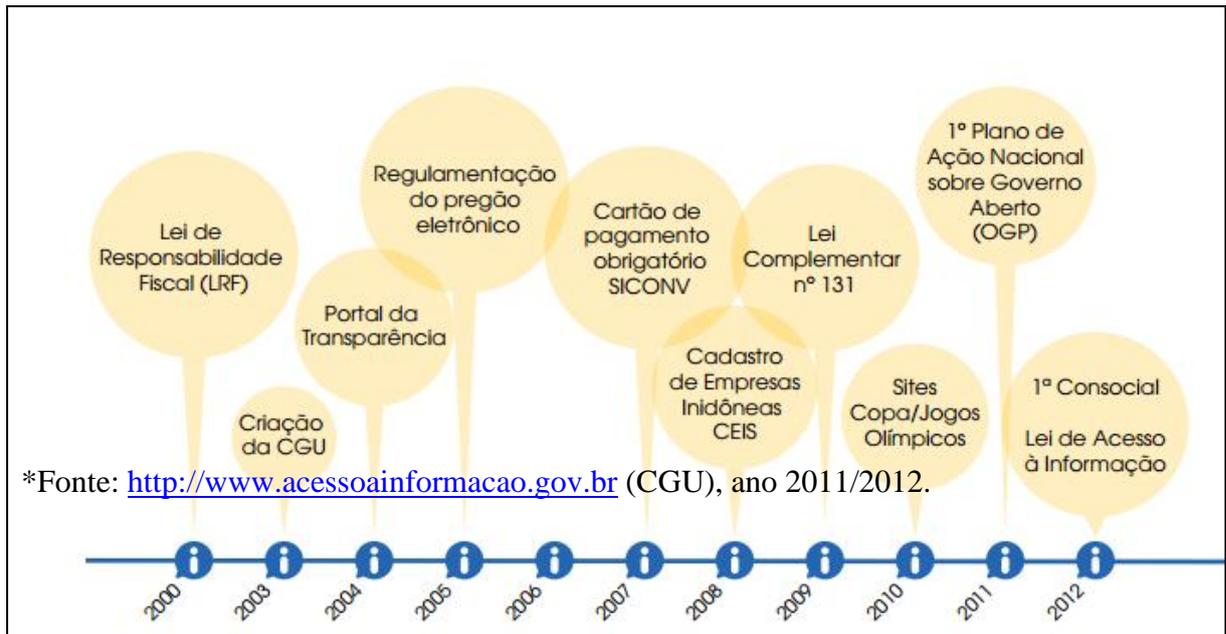


Gráfico 02. Transparência e acesso à informação no Brasil. 2000 /2012.

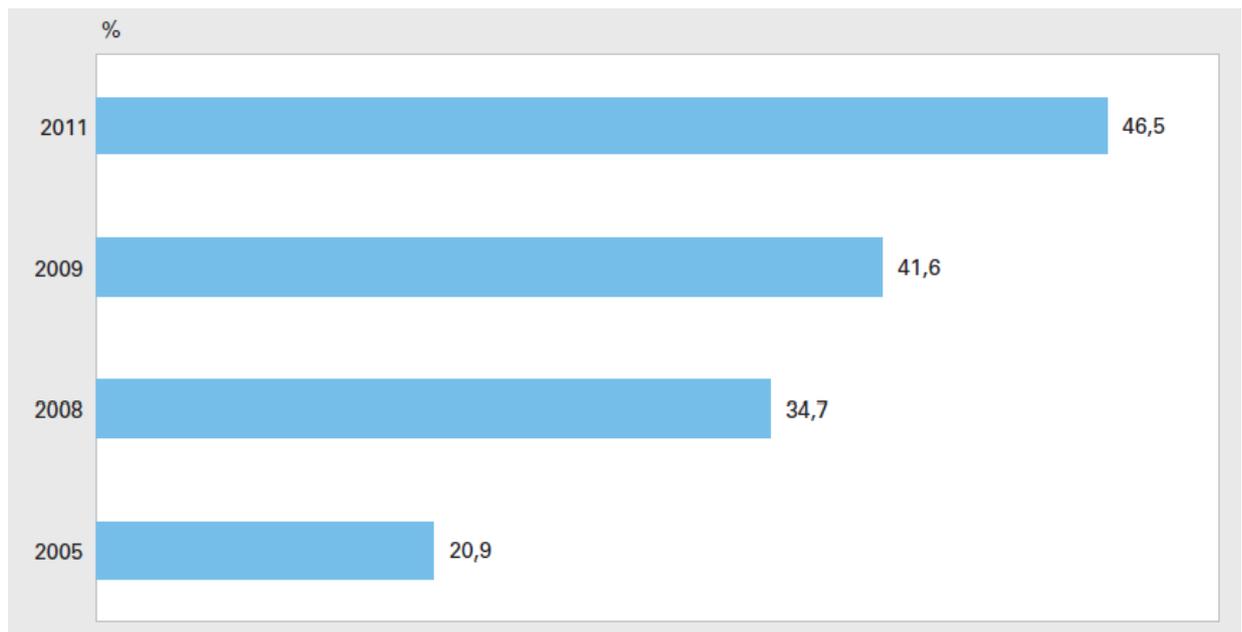


Gráfico 03. Percentual de pessoas que utilizaram a internet, no período de referência dos últimos três meses, na população de 10 anos ou mais de idade no Brasil. 2005/2011.

Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios 2005/2011.

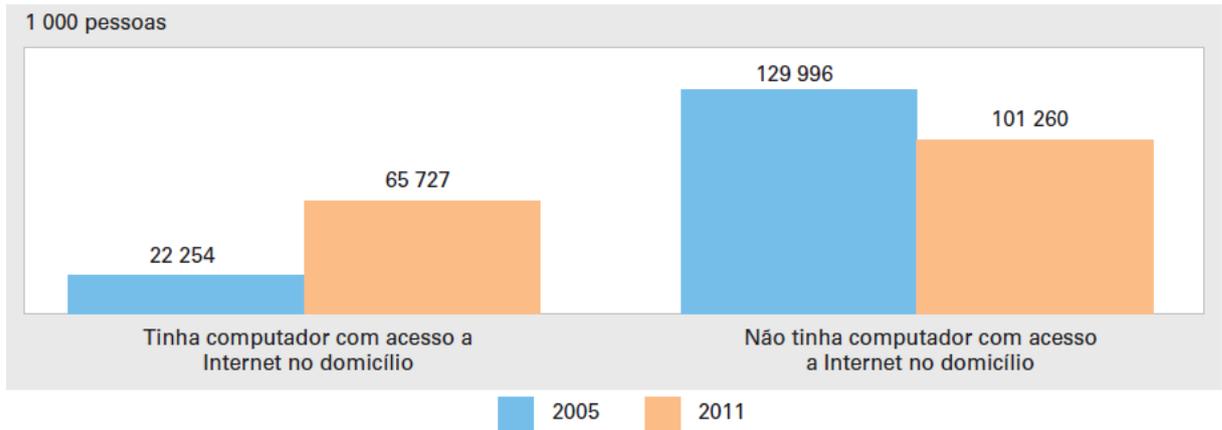


Gráfico 04. Pessoas de 10 anos ou mais de idade, segundo a existência de microcomputador com acesso à internet no domicílio, no período de referência dos últimos três meses no Brasil. 2005/2011.

Fonte: IBGE, Diretoria de Pesquisas, Coordenação de Trabalho e Rendimento, Pesquisa Nacional por Amostra de Domicílios 2005/2011.

## ANEXO B

## PORTARIA INTERMINISTERIAL NÚMERO 147, DE 31 DE MAIO DE 1995

Ministério das Comunicações.  
Gabinete do Ministro.

O Ministro de Estado das Comunicações e o Ministro de Estado da Ciência e Tecnologia, no uso das atribuições que lhes confere o artigo 87, parágrafo único, inciso II, da Constituição, e com o objetivo de assegurar qualidade e eficiência dos serviços ofertados, justa e livre competição entre provedores, e manutenção de padrões de conduta de usuários e provedores, e considerando a necessidade de coordenar e integrar todas as iniciativas de serviços Internet no país, resolvem:

Art. 1º. Criar o Comitê Gestor Internet do Brasil, que terá como atribuições:

I - acompanhar a disponibilização de serviços Internet no país;

II - estabelecer recomendações relativas a: estratégia de implantação e interconexão de redes, análise e seleção de opções tecnológicas, e papéis funcionais de empresas, instituições de educação, pesquisa e desenvolvimento (IEPD);

III - emitir parecer sobre a aplicabilidade de tarifa especial de telecomunicações nos circuitos por linha dedicada, solicitados por IEPDs qualificados;

IV - recomendar padrões, procedimentos técnicos e operacionais e código de ética de uso, para todos os serviços Internet no Brasil;

V - coordenar a atribuição de endereços IP (Internet Protocol) e o registro de nomes de domínios;

VI - recomendar procedimentos operacionais de gerência de redes;

VII - coletar, organizar e disseminar informações sobre o serviço Internet no Brasil; e

VIII - deliberar sobre quaisquer questões a ele encaminhadas.

Art. 2º. O Comitê Gestor será composto pelos seguintes membros, indicados conjuntamente pelo Ministério das Comunicações e Ministério da Ciência e Tecnologia:

I - um representante do Ministério da Ciência e Tecnologia, que o coordenará;

II - um representante do Ministério das Comunicações;

III - um representante do Sistema Telebrás;

IV - um representante do Conselho Nacional de Desenvolvimento Científico e Tecnológico - CNPq;

V - um representante da Rede Nacional de Pesquisa;

VI - um representante da comunidade acadêmica;

VII - um representante de provedores de serviços;

VIII - um representante da comunidade empresarial; e

IX - um representante da comunidade de usuários do serviço Internet.

Art. 3º. O mandato dos membros do Comitê Gestor será de dois anos, a partir da data de nomeação.

Parágrafo único: A nomeação dos membros do Comitê Gestor será mediante portaria conjunta do Ministério das Comunicações e Ministério da Ciência e Tecnologia.

Art. 4º. Esta Portaria entra em vigor na data de sua publicação.

**Sérgio Motta José Israel Vargas**

Fonte: <http://www.cgi.br/regulamentacao/port147.htm>

## ANEXO C

## 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. Inadir 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