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

Danilo Maia Corrêa

Informatização e violação de privacidade:
novas tecnologias e a (in)segurança quanto aos direitos fundamentais.

Assis

2014

Danilo Maia Corrêa

Informatização e violação de privacidade:
novas tecnologias e a (in)segurança quanto aos direitos fundamentais.

Trabalho de Conclusão de Curso, como requisito para receber Certificado de Conclusão em Curso de Graduação em Direito pela Fundação Educacional do Município de Assis – FEMA/IMESA.

Orientador – Lenise Antunes Dias de Almeida.

Área de Concentração – Direito Internacional e Direito Constitucional.

Assis

2014

Ficha Catalográfica

Corrêa, Danilo Maia

Informatização e violação de privacidade: novas tecnologias e a (in)segurança quanto aos direitos fundamentais/Danilo Maia Corrêa. Fundação Educacional do Município de Assis- IMESA, Assis, 2014.
Nº pág.60.
Orientador – Lenise Antunes Dias de Almeida
Trabalho de Conclusão de Curso-IMESA Instituto Municipal de Ensino Superior de Assis.

1.Informatização; 2. Violação de privacidade;

CDD 340
Biblioteca da Fema

Informatização e violação de privacidade:
novas tecnologias e a (in)segurança quanto aos direitos fundamentais.

Danilo Maia Corrêa

Trabalho de Conclusão de Curso, como requisito para receber Certificado de Conclusão em Curso de Graduação em Direito pela Fundação Educacional do Município de Assis – FEMA/IMESA.

Orientador – _____

Analisador – _____

Assis
2014

(Errata)

DEDICATÓRIA

Dedico primeiramente a Deus por estar ao meu lado durante toda essa longa caminha, posteriormente a minha família por sua capacidade de acreditar e investir em mim.

AGRADECIMENTOS

Agradeço aos meus pais João e Marta, que apesar de todas as dificuldades sempre estiveram ao meu lado, apoiando e incentivando nas horas mais difíceis. Ao meu irmão que sempre foi um exemplo a ser seguido por mim.

A minha orientadora Lenise, pela orientação, apoio e confiança.

A todos os professores por me proporcionar conhecimento e sabedoria ao longo dessa jornada de formação profissional.

Agradeço aos amigos que fizeram parte da minha formação.

A Deus por estar ao meu lado durante essa caminhada. E por ele ter coloca em minha vida pessoas e amigos especiais, e ter colocado na minha vida a minha namorada Jéssica.

E a todos que direita ou indiretamente participaram dessa jornada de estudo e aprendizado.

Resumo

Com o recente progresso tecnológico na área de informatização, autodenomina-se a atual sociedade como “digital”, onde serviços estatais, serviços bancários, meios de transmissão e armazenamento de dados, uso livre da internet, em redes sociais, bate-papo, e-mails, aplicativos, *sites* comerciais, blogs, enfim, toda essa informação exposta à fragilidade da segurança, onde civis, *hackers*, *crackers*, como também agências de vigilância ou mesmo empresas, tomam posse de informações preciosas, nos âmbitos públicos e privados, civis e comerciais. No estado que as coisas se encontram o direito à privacidade é, demasiadamente, desrespeitado. Câmeras de vigilância, arquivos (imagens, fotos, textos, dados em geral), espionagem para fins de proteção ao terrorismo, muitas vezes tomando um curso que não condiz com sua natureza primária. Hoje, a pessoa, o Estado e demais representantes internacionais, estão postos a fragilidade. Não se sabe quem está na vigilância, se determinados dados não serão expostos de forma que venha a prejudicar a honra, a dignidade humana, transações comerciais, relações de entes internacionais. É nesse cenário que estão surgindo normas jurídicas, princípios, em todo o mundo, sendo que há países que incluem tal proteção à privacidade diante a rede na própria Constituição. Portanto, pretende-se, através desse trabalho, discorrer sobre o assunto da informatização e a violação de privacidade.

Palavras-chaves: informatização, violação de privacidade, sociedade da informação, segurança, direito digital, direito internacional.

Abstract

With the recent technological progress in the informatization area the present society self-denominated as a digital one, where state services, banking services, broadcasting means and store data, free use of internet in social nets, chats, e-mails, tools commercial sites, blogs, and then all exposed information to the fragility of security, where civilians, hackers, crackers, vigilance agencies and even companies, taking precious information on the range of private and public, civil and commercial. At the real stage where things are, the right on privacy is too disrespected. Watching cameras, images, photos, texts and general data, spying to the terrorism protection, many times carrying to what is not consistent to its primary nature. Today the person, the state other international representative are placed at the fragility. It is not aware who is at the vigilance, if determinate data are not shown at a way it can damage the honor, the human dignity, commercial transaction, international entities relations. It is in this scenery that the juridical and principle rules are coming up in the world, as there are countries that include such privacy protection on the network at own Constitution. Then, the intention through this work is to argue about the information and the violation of privacy.

Keys Words: informatization, violation of privacy, society of information, security, digital law, international law.

Lista de Ilustrações

Figura 1. Privacidade e Intimidade.....22

Lista de Tabelas

Tabela 1. Exemplos da diferença entre Privacidade e Intimidade.....22

Lista de Abreviaturas e siglas

ARPA – Advanced Research Projects Agency.

ARPAnet – Parte da Agência norte-americana voltada a comunicação em rede.

ART – artigo.

CC – Código Civil.

CDC – Código de Direito do Consumidor.

CE – Conselho Europeu.

CF – Constituição Federal.

CGI – Comitê Gestor da Internet no Brasil.

CPC – Código de Processo Civil.

CPP – Código de Processo Penal.

ECA – Estatuto da Criança e do Adolescente.

EUA – Estados Unidos da América.

IP – Código atribuído a aparelho conectado a internet.

ICP-Brasil – Infra-estrutura de Chaves Públicas Brasileira.

LINDB – Lei de Introdução as Normas do Direito Brasileiro.

NSA – Agência Nacional de Segurança dos Estados Unidos da América.

OAB – Ordem dos Advogados do Brasil.

OAB/SP – Ordem dos Advogados do Brasil do Estado de São Paulo.

RPCTV – Rede Paranaense de Comunicação.

WI-FI – Rede de internet sem fio.

Sumário

1.INTRODUÇÃO..... 14
2.CAPÍTULO I – A EVOLUÇÃO DA TECNOLÓGIA VOLTADA À INFORMATIZAÇÃO..... 16
2.1.*Evolução tecnológica da comunicação e a internet*..... 16
2.2.*Uso público das ferramentas da internet*..... 17
2.3.*A fragilidade dos dados contidos em sistemas informatizados*.....18
3.CAPÍTULO II – O DIREITO A PRIVACIDADE E SEUS DESDOBRAMENTOS.....20
3.1.*Considerações acerca da privacidade*.....20
3.2.*Desdobramentos do direito à privacidade e uso da rede mundial de computadores*.....23
4.CAPÍTULO III – INFORMATIZAÇÃO E A VIOLAÇÃO DA PRIVACIDADE.....26
4.1.*Vigilância e privacidade*.....26
4.2.*O argumento da necessidade de expor o privado em razão da "guerra contra o terror"*..... 28
4.3.*Casos de repercussão internacional e violação de privacidade*.....29
4.4.*Preservação da privacidade através de normas legais no Brasil e no mundo*.... 31
5.CONSIDERAÇÕES FINAIS.....34
REFERÊNCIAS 36
ANEXO – A LEI QUE INSTITUIU "O MARCO CIVIL DA INTERNET".....40

1.INTRODUÇÃO

Dada a quantidade de meios tecnológicos de comunicação, uso da rede mundial de computadores para transmissão de informações, dados pessoais, uso público e privado desses mecanismos, ante a questão do direito fundamental à privacidade, é que se posiciona a pesquisa que foi estabelecida.

Há uma diversificação de aplicativos, programas e meios atuais, como rede sociais e portais exclusivamente para relatar dados do cotidiano do usuário.

A internet acelerou o processo de globalização da informação. Seja em *desktop*, *notebook*, *tablet*, *smartphone*, aparelhos eletrônicos com acesso à rede (ex. aparelhos televisores - TV), qualquer pessoa pode acessar a internet, desde que esteja conectado a um provedor.

Desde meados dos anos 90, muitas questões foram surgindo no uso dos serviços de informatização e suas consequências, de tal forma que os direitos que infringidos pelo uso dessa nova tecnologia foram sendo amparados, gradualmente, pelo Direito Internacional e, no mesmo caminho, os países passaram a adotar medidas domésticas de proteção.

O episódio de 11 de Setembro passou legitimar a troca da privacidade pela segurança, pondo o mundo todo num estado de vigilância que tomou grandes proporções.

Este trabalho, cuida do assunto em três capítulos. Primeiro, considera-se a evolução tecnológica e o advento da internet; Segundo, trata do direito fundamental à privacidade, o qual visa proteger a própria dignidade humana. E, terceiro, cuida-se da ameaça a privacidade e a intimidade, como os meios tecnológicos tem limitado esses direitos, como também termina com um apanhado global de normas que pretende a proteção jurídica.

Utiliza-se para esta investigação a doutrina de Direito Internacional e de Direito Pátrio, legislações sobre o assunto e diversas formas de referências, como obras, *e-book*, palestras *on-line*, *sites* governamentais, programa Painel[1] transmitido pela afiliada da Rede Globo, RPCTV.

No decorrer da leitura, encontrar-se-á alusão a fatos atuais de flagrantes de vigilância indevida promovida por órgão governamental a outros países, fato bastante discutido na imprensa global. Como também aquela promovida por empresas com fim mercadológico e segregativo.

O objetivo primeiro ao iniciar o presente trabalho era trazer a análise situações acerca da violação de privacidade através da internet, apresentar soluções e formas de prevenção.

Porém, o que o leitor encontra aqui é à disposição dos meios de vigilância que são executados pelas novas tecnologias e os caminhos legais que se tem tomado no resguardo da privacidade do usuário da internet e outros meios eletrônicos, no mundo e no Brasil.

[1] Havendo interesse em conhecer o conteúdo do programa Painel sobre "Segurança na internet e *Smartphones*", acessar página www.rpctv.com.br/ painel, programa exibido no dia 02/08/2.014.

2.A EVOLUÇÃO DA TECNOLOGIA VOLTADA À INFORMATIZAÇÃO

No período da Segunda Guerra Mundial houve a aquisição de conhecimentos e fundamentos básicos quanto à tecnologia da informação, transformando a maneira que até então se organizava as informações (documento físico), passando-se a processá-las em máquinas eletrônicas. Em pouco tempo, a potência, a forma cada vez menor de apresentação dos computadores, cálculos que demandavam tempos para sua feitura passam a ser resolvidos por processo eletrônico (ROBERTS, 2004, p. 645).

Surgem máquinas com grande potência de processamento, velozes, compactas; *em trinta anos, um microship do tamanho de um cartão de crédito executava tarefas que antes demandavam máquinas do tamanho de uma sala de estar* (ROBERTS, 2004, p. 645-647).

2.1.Evolução tecnológica da comunicação e a internet.

Em 1.901, a primeira mensagem de rádio transpõe os limites do Atlântico e em 1.930 as pessoas já possuíam transmissores sem fio. Imagens e sons disseminados por meio eletrônico. Rádio, cinema, televisão, formato da difusão das informações modificado, os dados são armazenados em forma de dados eletrônicos (ROBERTS, 2004, p. 646).

Segundo Vieira (2007, p 149-154) a internet surge em meio à Guerra-Fria, resultado de estratégia militar, estudo científico e iniciativas na área da tecnologia, período em que os EUA investiram num projeto de sistema de comunicação que fosse impenetrável pelo “inimigo”, operacionalizado pela Agência de Projetos de Pesquisa Avançada (Advanced Research Projects Agency – ARPA) do Departamento de Defesa, denominado como ARPAnet. O objetivo desse projeto era chegar a um sistema de comunicação independente, com dispositivos geridos sem estar ligados a

uma fonte central, onde todos os pontos de conexão fossem autônomos e independentes.

Com base na tecnologia da comunicação de troca de mensagens por pacotes, cria-se um sistema de transmissão de sons, imagens, dados, sem haver um centro de controle, vindo a funcionar em 1.969. Na década de 80, essa tecnologia passou a ser usada por pesquisadores e acadêmicos norte-americanos, e na década de 90 o projeto foi privatizado.

A partir de então, surge à expressão “sociedade da informação”, como Vieira (2007, p. 156) (...) *denominação que se dá ao uso da tecnologia da informação para coleta, produção, processamento, transmissão e armazenamento de informação.* Essa nova tecnologia envolve: microeletrônica; computação (hardware e software); telecomunicações; optoeletrônica; engenharia genética; processos tecnológicos interligados por uma interface e linguagem comum (VIEIRA, 2007, p. 156)

2.2. Uso público das ferramentas da internet.

O espaço virtual é social e inclusivo, pois a todos alcança.

Nessa nova concepção, o progresso da humanidade está refletido na medida da velocidade em que as informações são transmitidas. Num mundo globalizado, as informações são disseminadas com celeridade, causando mudanças de comportamento social e individual (FORTES e BOFF, 2.014, p. 110).

Informações públicas ou privadas, *sites* comerciais, redes socais, serviço de correspondência por e-mails disponíveis onde tiver um computador e acesso a rede, como também pela via móvel, com os *tablets* e os *smartphones*, através da rede sem fio (Wi-Fi).

É comum as pessoas investirem em aparelhos que as conecte com a rede, dado que muitos programas e aplicativos direcionados para uso até mesmo em um celular.

No Brasil, boa parte das escolas tem acesso à internet. O ensino à distância já é uma realidade, rompendo barreiras de acesso ao conhecimento.

Porém, interessante é a observação de Manuel Castells (apud Vieira, 2007, p. 159): que o povo deveria fazer da internet um espaço para uma democracia participativa, fiscalizando, cobrando, e não como ocorre, o governo é quem observa e analisa os dados do que o povo lança na rede.

2.3. A fragilidade dos dados contidos em sistemas informatizados.

Hoje, difícil é viver sem a internet e o processamento de dados, pois serviços públicos, bancários, comerciais, relacionamentos comerciais e privados dependem da informatização.

Os dados referentes à pessoa humana, colhidos e processados pela esfera pública ou privada, como meio social de desenvolvimento, expõe os mesmos dados de forma acessível a civis, agências ou empresas interessadas em utilizar esses dados para fins diversos, mesmo sem o conhecimento do detentor dos dados ou da própria pessoa.

A pessoa por si mesma dispõe seus dados (Fortes e Boff, 2007, p. 115):

> "(...) os próprios usuários são induzidos, ou seduzidos, ao exibicionismo exacerbado, com a renúncia da privacidade e com o fornecimento de dados pessoais tão valiosos, que compensam a oferta de serviços de forma gratuita, como fazem as grandes corporações do Vale do Silício, *Google* e *Facebook*".

Comum numa busca pelo *Google*, a título de exemplo, encontrar dados que levem a determinados entes ou pessoas, seja por fotos, imagens, sons, dados pessoais, sem contar em dados sigilosos que órgãos de várias naturezas detêm sobre alguém, como um simples resultado de exame laboratorial à telefonemas de uma autoridade governamental.

Estar na rede é estar plugado no mundo, mas a que preço?

Em palestra pela OAB/SP de Simão Filho, em relação à privacidade, o palestrante faz menção ao fato de que o criador do *Facebook* disse, que através desta rede social, estar decretado o fim da privacidade. Fotos, imagens, voz, dados, tudo que é posto na rede social, além de ser de fácil acesso a qualquer pessoa, também há o fato de um "dever" de se compartilhar (ou publicar), denominado por Keen como "era do exibicionismo". (apud FORTES e BOFF, 2007, p. 115)

As pessoas estão expostas, na maioria das vezes por informações que são "conduzidas" a fornecer. Um exemplo desse fenômeno é um aplicativo para *smartphones* de localização, onde é possível saber onde a pessoa se encontra naquele exato momento, fazendo da rotina uma informação pública[2].

Aquela sensação de anonimato, de se estar só, como também de que é seguro pelos mecanismos de segurança que se dispõe, no uso da internet, não é real. Há uma fragilidade em que a sociedade não tem consciência e, por isso mesmo, corre sérios riscos.

[2] Palestra de Simão Filho pela OAB/SP, 2014.

3.O DIREITO À PRIVACIDADE E SEUS DESDOBRAMENTOS.

O direito à privacidade é matéria regulada em âmbito nacional e internacional, tal será discorrido no decorrer do conteúdo monográfico. Ter sua intimidade preservada traz ao ser humano a sensação de liberdade interior, onde pode se desenvolver, por em práticas suas convicções e manterem vínculos familiares e sociais sem estar sendo vigiado e/ou controlado.

Nesse capítulo, faz-se um apanhado da definição legal, conteúdo doutrinário e os desdobramentos do direito à privacidade.

3.1. Considerações acerca da privacidade.

No desejo de falar de sobre direito à privacidade, primeiramente tem-se de se referir a "dignidade humana", princípio que se desenvolveu junto com a sociedade humana e hoje está amparado pelo Direito das Gentes[3].

A Constituição Federal em vigor estabelece a dignidade humana, no art. 1º, inciso III, como um dos fundamentos do Estado Democrático de Direito. Sobre o tema, Moraes (2014, p. 53), afirma que a Carta Magna

> "(...) concede a unidade aos direitos e garantias fundamentais, sendo inerente às personalidades humanas. Este fundamento afasta a ideia de predomínio das concepções transpessoalistas de Estado e Nação, em detrimento da liberdade individual. ***A dignidade é um valor espiritual e moral inerente à pessoa que se manifesta singularmente na autodeterminação consciente e responsável da própria vida e que traz consigo a pretensão ao respeito por parte das demais pessoas,***

[3] Para saber mais sobre a evolução histórica do princípio da dignidade humana, recomenda-se: Portela, Paulo H. G. *Direito Internacional Público e Privado*. 6º edição. Editora Juspodvim. Salvador, Bahia, 2014. (pg. 817 a 1.068).

> ***constituindo-se um mínimo invulnerável que todo estatuto jurídico deve assegurar, de modo que somente, excepcionalmente, possam ser feitas limitações ao exercício dos direitos fundamentais, mas sempre sem menosprezar a necessária estima que merecem todas as pessoas enquanto seres humanos e a busca do Direito à Felicidade***". (grifo nosso)

O direito à personalidade, sua previsão legal e instrumentos processuais inerentes, tem por fim proteger a dignidade humana.

No art. 5º, X e XII, da Constituição Federal de 1.988, há a proteção ao direito à vida privada e a intimidade, alude à honra e a imagem, inviolabilidade do sigilo de correspondência (incluí-se aqui todas as formas que hoje são possíveis - dados), de recolhimento residencial, de telefonia, bancários e fiscais, agasalha-se pessoa física ou jurídica, dando a ambos direito a indenização por dano material e moral. (MORAES, 2014, p. 54)

Há de se ressaltar, que por previsão legal, havendo determinação judicial ou algumas das hipóteses previstas em lei, a privacidade dá lugar à tutela de outros direitos.

Em análise doutrinária, Silva (1998, p. 61), diz que

> "(...) a tutela jurisdicional visa proteger a pessoa de dois atentados particulares: a) o segredo da vida privada; b) a liberdade da vida privada. O segredo da vida privada é condição de expansão da personalidade".

Os direitos da personalidade são absolutos, intransmissíveis, indisponíveis, irrenunciáveis, ilimitados, imprescritíveis, impenhoráveis e inexpropriáveis. Direito subjetivo, "*erga omnes*", sobrepõe-se ao direito de imprensa, ao direito de informação ou ao de ser informado e ao de liberdade de expressão. (DINIZ, 2005, 134)

Diniz (2.005, p. 135), discorre sobre a delicada diferenciação entre privacidade e intimidade; elencam-se situações exemplificativas para maior compreensão do que até agora foi explanado, de acordo com a autora.

DIREITOS	**EXEMPLIFICAÇÕES**
Privacidade	Escolha de modo de viver, hábitos, comunicação com as demais pessoas, recolhimento residencial.
Intimidade	Segredo profissional, relacionamento amoroso, situação de nudez em qualquer forma.

Tabela 1. Exemplos da diferença entre Privacidade e Intimidade.

Diante o quadro acima e em acordo com Silva (1998), Moraes (2014) e Diniz (2005), os quais mantêm o mesmo viés doutrinário, considerando a privacidade o todo, do qual a intimidade seria parte. É nesse sentido a figura a seguir:

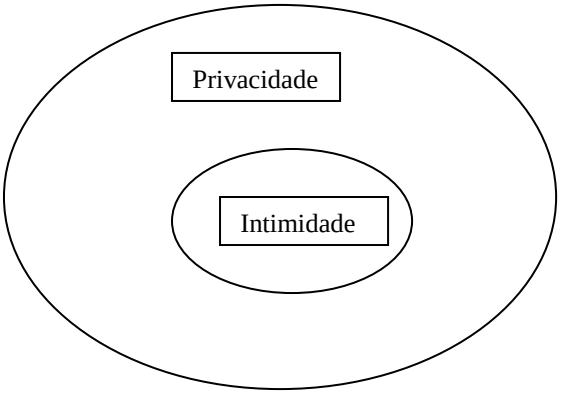

Figura 1. Privacidade e Intimidade

3.2. Desdobramentos do direito à privacidade e uso da rede mundial de computadores.

Moraes, citando Gomes Filho (2014, 54), afirma que

> "*as intromissões na vida familiar não se justificam pelo interesse de obtenção de prova, pois, da mesma forma (...) aos segredos profissionais, deve ser (...) reconhecida a função social de uma vivência conjugal e familiar à margem de restrições e intromissões*".

E, ainda, Moraes (2014, 54), considera dever haver maior amplitude a inviolabilidade referente ao recinto familiar, o qual deve ser protegido de intromissões externas; é nesse sentido:

> "***O preceito que garante o sigilo de dados engloba o uso de informações decorrentes da informática*** (...) necessária em virtude da existência de uma nova forma de armazenamento e transmissão de informações, deve coadunar-se com as garantias de intimidade, honra e dignidade humanas, de forma que se impeçam interceptações ou divulgações por meios ilícitos". (grifo nosso)

Em 1.998, quando a edição da obra utilizada neste conteúdo monográfico foi impressa, Silva (1.998, p. 212) já levantava a questão da possibilidade de cruzamento de dados referente à pessoa, de tal forma a causar-lhe danos à vida privada.

Mecanismos de captura de informações, público, privado, são uma realidade.

Com o advento das redes sociais, *blogs* utilizados como diários, aplicativos, também os antigos conhecidos *Google*, *Youtube, MySpace*, *sites* de recrutamento

empregatício, de relacionamento, como o Par Perfeito, enfim, é quase impossível o anonimato na rede.

Há empresas especializadas em reunir tais dados e depois usá-los mercadologicamente.

A rede faz de anônimos grandes celebridades em pouquíssimas horas.

Buccioli (2.000, pg. 56 e 57), ressalta que nos anos 90 já havia uma preocupação real com os aspectos de segurança e privacidade dos dados na rede Começa-se a utilizar a criptografia assimétrica, a assinatura digital e demais meios no fim de assegurar e dar confiança aos dados constantes na internet.

Evidencia-se, no caso brasileiro, na implantação de Certificado Digital no Brasil (ICP – Brasil), a constatação da necessidade de haver segurança no ambiente virtual. Barra, afirma que a utilização da internet por terroristas fica evidente com o ataque de 11 de Setembro. (BARRA, 2009, 192)

Na obra de Barra (2009, p. 192), há referência aos meios de segurança que o Estado Brasileiro passa a implantar, unindo esforços interdisciplinares

> "Em grande medida, profissionais formados em dois campos de conhecimentos técnicos – engenharia e direito – construíram e implantaram o ICP-Brasil. O caso mostrou grande correlação entre engenheiros e a preocupação com a segurança, o que é consistente com estruturas de dominação que tendem ao modelo racional-legal".

As invasões de privacidade na vida privada, o uso de meios tecnológicos para fins de destruição em massa ou para fins comerciais, forma de obter informações, lucros e objetivos que até então era limitado, inverte-se o fim evolutivo científico da rede para torná-la fonte de acesso a interesses que antes não era possível.

4. INFORMATIZAÇÃO E A VIOLAÇÃO DA PRIVACIDADE.

Como exposto nos capítulos anteriores, na sociedade da informação estamos diante da insegurança quanto aos nossos dados, pois múltiplos tipos de mídias estão sendo utilizadas, pelo público e pelo privado, para exercer vigilância sobre todos.

Não há isenções. Dados de países que são espionados por outros, telefones grampeados de autoridades governamentais, diplomáticas, conteúdos de *e-mails* e demais formas de comunicação, todos vigiados e utilizados para conseguir informações privilegiadas.

Há empresas com o único fim de obter informações sobre dados de pessoas na rede e depois comercializá-los.

A internet tornou inexistente a privacidade de todo cidadão que a ela tenha acesso, que o mesmo tenha conhecimento de que seu sistema pessoal foi assaltado.

Projetos como Echelon e Enfopol, criados por EUA e Reino Unido para fins de monitoramento de comunicação, permanece pós-guerra fria. E o episódio terrível de 11 de Setembro, somente deu fundamento para que houvesse a troca da privacidade pessoal pela segurança contra o "*terror*".

No cenário internacional, os EUA têm papel de destaque ao falar em monitoramento e segurança de dados pessoais. Leite (2013, p. 113), em sua análise aos discursos presidenciais norte-americanos, afirma que estes portam um sentimento de missão em trazer e manter a liberdade no mundo, o que legitima sua ação face aos "*outlaw states*"[4] *motivados por compaixão aos demais povos*,

> "Os Estados Unidos atuam por ordem divina contra o mal que surge na Terra, e por isso não dialogam nem hesitam na hora de atuar, afinal, o contrário significaria a vitória da maldade e

[4] *Outlaw States* é denominação dada aos "Estados fora da lei" pelos estadunidenses. (Leite, 2013, 113).

> a ideia de que não há ninguém que olhe pelos 'bons'". (LEITE, 2013, p. 127)

Essa postura de superioridade é base para atos de vigilância dos EUA sobre os demais Estados nas relações internacionais, e ao serem questionados de sua postura, argumentam a necessidade de segurança e a "guerra ao terror".

4.1. Vigilância e a privacidade.

É interessante o que Simão Filho em sua palestra (anteriormente citada e disposta nas referências), a concepção de vigilância, com o fim de evitar ato lesivo, surge na Idade Moderna com Jeremy Bentham, na figura do panóptico (pan – tudo/ óptico – vê). Modelo de arquitetural para instituições que permite vigilância total e o ser que é vigiado não faz ato lesivo, sem saber quando e por quem se está sendo vigiado.

Ainda que, a ideia é reanalisada por George Orwell em 1.984, com *Sociedade do Futuro,* surge a concepção do *Big Brother*, manifesta, hoje, pelo Big Data, programa que permite realizar vigilância total nos meios eletrônicos de armazenamento de dados, o que permite traçar um perfil psicológico do usuário da rede.

Finalmente, o palestrante, refere-se à obra '*Vigiar e Punir. Vigilância como forma de controle',* de Michel Foucault, onde, novamente, o panóptico é objeto de questionamento. Numa aferição atual, a obra '*Pós panoptismo hoje'*, de Zygmunt Bauman e David Lyon, do ano de 2.013, esse modelo de vigilância é colocado diante a uma sociedade que os autores denominam liquida, visto que se desestrutura com muita agilidade[5], os valores se desfazem, o que é importante hoje, amanhã pode não mais ser.

Quem vigia? A quem vigia? Como vigia?

[5] Palestra pela OAB/SP de Simão Filho em 2.014 (encontra-se em referências).

Call Centers, mecanismos de busca como o *Google*, serviço de *e-mails*, redes sociais, aplicativos, várias portas estão abertas para fins do que Simão Filho (2.014) chama de segregação, onde pessoas com moléstias são identificadas, pessoas com probabilidade de cometer crimes, hábitos religiosos, obesidade, enfim, uma gama de situações a que o indivíduo é exposto. Há uma seleção dos "bons" e dos "maus".

Câmeras nas ruas, em estabelecimentos comerciais e governamentais, nos prédios, nos elevadores; meios tecnológicos de obter todo tipo de mídia (imagem, som, texto); localizadores; drones (captam imagem e som em tempo real, podem carregar tipos de artilharia e atingir uma região somente com uma ordem da central), não tripulados, pequenos, já há pesquisa no Departamento de Defesa norte-americano de drones que simulam insetos. É impossível fugir à vigilância.

Uma questão surge destas constatações: quem vigia aquele que vigia?

4.2. O argumento da necessidade de expor o privado em razão da "guerra contra o terror".

Após os atentados de 11 de Setembro, o argumento de necessidade de expor a privacidade numa forma de segurança na "guerra contra o terror", por muito tempo foi incontestável.

Simão Filho, em palestra on-line pelo Portal da OAB/SP, ressalta que "*a privacidade se tornou moeda de troca: concedo dados privados e recebo segurança ao ponto de considerar normal a vigilância imposta*".

No sentido de terrorismo *versus* privacidade, Vieira (2007, p. 40) ressalta que

> "Todo cidadão deve estar atento para o novo cenário mundial que se descortina quanto à necessidade de se combater com veemência a

> atividade ilícita em referência, que provoca a morte de tantos inocentes; ***entretanto, há que se ter um mínimo de razoabilidade para não descambar para extremismos, numa irreversível aniquilação da privacidade***". (grifo nosso)

É ainda, nessa mesma linha, ao falar de direitos fundamentais, a mesma autora (Vieira, 2014, p. 20) afirma que

> "***Exercer com tranquilidade a liberdade de consciência, de crença e de expressão supõe o exercício do direito que se concede a qualquer pessoa, de dispor de um espaço reservado em que possa voltar-se para si mesma, sem prender-se ao jugo de qualquer censura, sentir-se cativa da observação de outrem (...) para exercer, enfim, o seu direito de autodeterminação***". (grifo nosso)

Assim, vê-se que o direito à privacidade e a proteção do que é íntimo ao indivíduo, ultrapassa a visão que até então havia sobre as relações, públicas e privadas, nacionais e internacionais.

4.3. Casos de repercussão internacional de violação de privacidade.

O episódio mais relevante no ano de 2.013, também, fato que ressaltou a insegurança de dados informatizados, foi o caso de espionagem da NSA (Agência de Segurança Nacional dos Estados Unidos). Um dos funcionários do governo, o qual trabalhou NSA, Edward Snowden, revelou para imprensa mundial, inclusive de posse de documentos probatórios, que os EUA espionam para benefício próprio.

Tornou-se público que os EUA grampearam telefones de autoridades governamentais, teve acesso a dados oficiais, dados de negociações da Petrobrás, no Brasil e em muitos outros países como Argentina, França e Alemanha.

Em recente ação na Alemanha, a chanceler Angela Merkel, teve seu telefone pessoal grampeado por espião que trabalha para os EUA. Descoberta a espionagem, o agente foi detido e o caso está sendo investigado[6].

Tais fatos, de conhecimento público, corroboram a alegação dos EUA utilizar-se de meios tecnológicos para captação, monitoramento e investigação de dados que já não pertencem à alçada da proteção do mundo quanto aos "inimigos".

Como na esfera pública, há a violação de privacidade exercida por empresas especializadas em captura de dados, para fins comerciais e até de segregação, onde pessoas com determinados perfis psicológicos (os quais eles mesmos determinam), são inutilizadas por propensão a moléstia grave ou a cometer delitos, ou ainda, simplesmente, por ser obesa, existir uma mídia que a difama.

Quando há o cruzamento de dados de um grupo ou individual, de forma a estabelecer hábitos, pensamentos, convicção religiosa, sua vida íntima é devastada. É evidente que em determinados casos seja necessário, ao poder público, a violação de privacidade para fins de manter a ordem; há previsões legais sobre as formas que se pode restringir esse direito fundamental.

Norberto Bobbio, (apud Vieira, 2007, p. 65), "*afirma que a história demonstra que os direitos fundamentais são variáveis no tempo e no espaço"*, dadas as circunstâncias atuais da evolução tecnológica e o desvio de intenção na questão da vigilância, o direito à privacidade no tocante ao uso da rede mundial de computadores tem sido matéria prevista no Direito Internacional e em regras do Direito Constitucional e demais do Direito Brasileiro, visto a necessidade urgente de proteção aos atuais direitos fundamentais.

---

[6] Maiores informações disponíveis no site <www1.folha.uol.com.br/dw/2014/07/1492264-governo-alemao-confirma-que-adotara-celulares-criptografados.shtml>. Acesso em 25/08/2014.

4.4. Preservação da privacidade através de normas legais no Brasil e no mundo.

Numa busca de preservar o direito fundamental à vida privada, princípios e normas estão surgindo e adequando o sistema jurídico à necessidade de proteção dos dados diante das novas tecnologias.

A Declaração Universal dos Direitos Humanos prevê o direito à privacidade, a vida familiar, ao recinto familiar, também direito a honra e inviolabilidade de correspondência. No mesmo sentido de proteção ao Direito das Gentes é estabelecido o Pacto Internacional de Direitos Civis e Políticos.

E, ainda, em matéria internacional, sendo a privacidade um direito fundamental à dignidade humana, está protegido por tratados internacionais e de blocos regionais.

Nessa via, a Comunidade Européia estabeleceu institutos de proteção a privacidade e ao tratamento de dados pessoais nas telecomunicações, visto o disposto na Directiva 66 de 1.997 do Conselho da União Européia[7], descrevendo definições, regras, princípios, concernentes ao assunto.

Portugal e Brasil, ante a história desses dois países, um tendo sua raiz no outro, adotando a mesma língua como idioma oficial. Na Constituição da República Portuguesa, encontra-se a seguinte previsão sobre informática e segurança no seu uso:

> **"Artigo 35.º**
>
> **(Utilização da informática)**
>
> **1.**Todos os cidadãos têm o direito de acesso aos dados informatizados que lhes digam respeito, podendo exigir a sua rectificação e actualização, e o direito de conhecer a finalidade a que se destinam, nos termos da lei.

[7] Fonte elencada nas Referências.

> **2.**A lei define o conceito de dados pessoais, bem como as condições aplicáveis ao seu tratamento automatizado, conexão, transmissão e utilização, e garante a sua protecção, designadamente através de entidade administrativa independente.
> **3.**A informática não pode ser utilizada para tratamento de dados referentes a convicções filosóficas ou políticas, filiação partidária ou sindical, fé religiosa, vida privada e origem étnica, salvo mediante consentimento expresso do titular, autorização prevista por lei com garantias de não discriminação ou para processamento de dados estatísticos não individualmente identificáveis.
> **4.**É proibido o acesso a dados pessoais de terceiros, salvo em casos excepcionais previstos na lei.
> **5.**É proibida a atribuição de um número nacional único aos cidadãos.
> **6.**A todos é garantido livre acesso às redes informáticas de uso público, definindo a lei o regime aplicável aos fluxos de dados transfronteiras e as formas adequadas de protecção de dados pessoais e de outros cuja salvaguarda se justifique por razões de interesse nacional.
> **7.**Os dados pessoais constantes de ficheiros manuais gozam de protecção idêntica à prevista nos números anteriores, nos termos da lei. **(...)".**

Nossa Constituição prevê proteção aos direitos fundamentais, em espécie, direito à privacidade e seus desdobramentos no art. 5º, incisos X e XII, somente podendo ser infringido por previsão legal, onde há algumas exceções.

Outra maneira e proteção ao direito a privacidade no ordenamento jurídico brasileiro, é sua participação e acolhimento de Tratados Internacionais e princípios do Direito das Gentes, tal como a matéria é disciplinada pela Constituição Federal de 1.988, como também o estabelecido na Lei de Introdução das Normas do Direito Brasileiro (LINDB). No direito civil, no direito do consumidor, no direito penal e nos direitos processuais pátrios.

O Comitê Gestor da Internet no Brasil já tratava de questões concernentes ao uso da rede mundial desde 1.995[8].

E, agora, há o Marco Civil Regulatório da Internet (Lei nº 12.965/14), norma recente e que depende de maior estudo doutrinário, pois vêm determinando princípios, diretrizes, definições, direitos e deveres no uso da internet e o provimento do serviço. Também tem causado reflexões, de cunho especializado ou leigo, na sociedade como um todo.

O professor e palestrante, Simão Filho (palestra já comentada), faz crítica a inexistência no Marco Civil da Internet do direito de deletar, do direito ao esquecimento, faz menção, para tanto, ao caso espanhol em que a Google foi condenada por não deletar caminhos nos mecanismos de busca em detrimento a imagem de determinada pessoa, pois não fez a retirada quando requisitada.

Rossini, promotor de justiça e palestrante no site da OAB/SP em 2014[9], destaca vantagens do Marco Civil da Internet, como a segurança jurídica que ela traz ao estabelecer conceitos, princípios e garantias, como regrar a atuação de empresas estrangeiras que são direcionadas para o público brasileiro, determinando a competência processual dos tribunais brasileiros para solução de controvérsias.

Ao que parece, esta nova norma, apesar de criticada, é instrumento jurídico de proteção ao brasileiro enquanto usuário da rede mundial, abrindo caminhos para uma legislação que possa trazer segurança aos direitos fundamentais, como o direito à privacidade.

---

[8] Histórico de atos promovidos por esse Órgão Federal está no endereço eletrônico < www.cgi.br>.
[9] Palestra elencada em referências.

5.CONSIDERAÇÕES FINAIS

Após os fatos e situações analisadas anteriormente, percebe-se que o objetivo de trazer as possíveis situações de violação de privacidade por meio da informatização foi alcançado, de forma pontual sobre a questão dos recentes fatos internacionais de espionagem e a insegurança que os meios de armazenamento e transmissão de dados a pessoa está exposta.

No que tange ao fator segurança, no Programa de TV Painel foi feito alerta de evitar uma rede aberta em lugares públicos, pois pode fragilizar os conteúdos do aparelho do portador, proteger *smartphones* com senhas e não deixá-lo em qualquer lugar. Ao notar que seu sistema está muito lento, na dúvida de haver monitoramento, é melhor formatar.

Como dito no trabalho, o usuário é seduzido em expor histórico de sua vida, com acesso de qualquer outra pessoa, tal como fotos, imagens, relatos pessoais, localização, sem perceber que, em razão da emoção, está fragilizando sua vida e relacionamentos.

Ainda, como acima analisado, há situações em que o usuário sente-se no “dever” de compartilhar, é como que o privado não fosse mais um fator relevante, o compartilhamento de informações (de qualquer forma e tema) é postado e disseminado no mundo virtual.

Vive-se num estado de vigilância, onde o que é vigiado não sabe quem é que vigia, porque vigia e como vigia, estando alheio ao que programas e aplicativos podem causar em sua vida, coletando informações, fazendo estudo e utilizando para vários fins, inclusive para a segregação social.

Trocar a privacidade por segurança ou por serviços na rede é o mesmo que se abrir uma porta para o inimigo entrar e devassar o que é íntimo.

Na doutrina e legislação, é voz quase unânime que a vida íntima deve ser preservada, pois doutra forma, põe em risco o próprio desenvolvimento da personalidade da pessoa. Assim, a privacidade residencial, de documentos pessoais, dados em qualquer mídia, contendo o que é íntimo, deve ser preservado, tal como ocorre com a vida amorosa ou mídias que contenham nudez.

Com referência ao âmbito global, que país tem o direito de invadir informações secretas do outro? Há uma deturpação no que se refere promover a segurança com aproveitamento dos dados que foram colhidos para uso próprio. Não existe Estado superior a outro, o Direito Internacional considera a todos com igualdade e detentores de soberania em seu território.

Várias são as formas de vigilância que se aplica ao indivíduo, o problema se encontra no desconhecimento dele sobre esse estado em que foi colocado, privando-o de seu direito fundamental de privacidade e de intimidade.

Exceções são previstas em lei, e devem ser aplicadas de forma não lesiva.

Tendo em vista tudo quanto foi questionado neste trabalho, conclui-se que o caminho primeiro é a informação, sendo necessária uma educação digital, esclarecendo que o comportamento no uso da rede mundial de computadores é fator importante para fins de usufruir os benefícios das novas tecnologias sem perder a segurança.

Que a sociedade da informação se torne consciente do uso adequado das novas tecnologias e que pessoas e Estados sejam tratados com dignidade e respeito, garantindo, assim, segurança que seja efetiva.

E, ainda, que o Brasil possa caminhar, legislativa e juridicamente, para que cybercrimes, violações de privacidade, dano a honra, injúrias, vigilância obscura e com fins de obter vantagens, sejam flagradas e, melhor, impedidas de causar os danos que ora recai sobre os brasileiros.

O Marco Civil Regulatório da Internet, como demais recursos normativos sobre o uso da rede mundial na legislação pátria, são apenas alguns passos em direção a um futuro de respeito para com a pessoa, detentora de dignidade humana, resguardando seus direitos fundamentais, tal como é o direito à privacidade.

REFERÊNCIAS

ALBERTIN, A.; MOURA, R. M. de. Comércio Eletrônico: seus Aspectos de Segurança e Privacidade. Revista de Administração de Empresas, Vol. 38, nº 2, abr/jun, pg. 49-61, 1.998. Disponível em <www.rae.fgv.br/era/vol38-num2-1998/comercio-eletronico-seus-aspectos-segurança-privacidade>. Acesso em 17/07/14.

BARRA, Marcello Cavalcanti. O Leviatã eletrônico. A trama política que colocou o Estado na internet. Editora Edusc. Bauru, São Paulo, 2.009.

BRASIL. *Constituição da República Federativa do Brasil*. Instituída em 05/10/1988.

BUCCIOLI, P. A. F. *Apontamentos sobre aspectos jurídicos do E-commerce*. Revista de Administração de Empresas, vol 40, nº 4. Fundação Getúlio Vargas. Out/Dez 2.000. Disponível <www.rae.fgv.br/sites/rae.fgv.br/files/artigos/10.1590_S0034-75902000000400007.pdf>. Acesso em 17/07/14.

COMITÊ GESTOR DA INTERNET, Histórico da atuação do Comitê Gestor da Internet no Brasil Disponível em <www.cgi.br>. Acesso jun/jul 2.014.

COMUNIDADE EUROPÉIA. Directiva 66 do CE do ano de 1.997. Disponível em <www.umic.pt/images/stories/publicacoes200709/Directiva97_66_CE.pdf>. Acesso em 19/07/14.

DINIZ, Maria Helena. *Código Civil Anotado*. 10º ed, rev. e atual. de acordo com o Novo Código Civil (Lei nº 10.406 de 10/01/2002). Editora Saraiva. São Paulo. 2.004.

_____ *Curso de Direito Civil Brasileiro. Teoria Geral do Direito Civil. 1º Vol.* 22º ed. rev. e atual. de acordo com o Novo Código Civil (Lei nº 10.406 de 10/01/2002) e o Projeto de Lei nº 6.960/2002. Editora Saraiva. São Paulo. 2.005.

FORTES, Vinícius Borges; BOFF, Salete Oro. *A Privacidade e a Proteção dos Dados Pessoais no Ciberespaço como um "Direito Fundamental": perspectivas de construção de um marco regulatório para o Brasil*. Revista Sequência, nº 68, pg. 109-127. Florianópolis, junho de 2.014. Disponível em <www.scielo.br/pdf/seq/n68/06.pdf>. Acesso em 17/07/14.

LEITE, Lucas Amaral Batista. *A construção do Inimigo nos discursos presidenciais norte-americanos do pós-guerra fria*. Cultura Acadêmica. Editora Edunesp. São Paulo. 2.013. Disponível em <www.culturaacadêmica.com.br/catalogo-detalhe.asp?ctl_id=426>. Acesso em 17/07/14.

MORAES, Alexandre de. *Direito Constitucional*. 30º ed. Editora Atlas. São Paulo. 2.014.

PAINEL. *Segurança na internet e smartphones*. Programa Painel do dia 02/08/2.014 da filiada da Rede Globo RPCTV Paraná. Assistido em 02/08/2014.

PEREIRA, Rafael H. M. *Resenha- O Leviatã eletrônico. A trama política que colocou o Estado na internet*. Disponível em <www.scielo.br/scielo.php?script=sci_arttext&pid=S1517-5222010000300013>. Acesso em 17/07/14.

PORTELA, Paulo H. G. *Direito Internacional e Direitos Humanos. Coleção para Exame da OAB – Vol 11*. 2º Ed. Editora Juspodivm. Salvador, Bahia. 2.014.

_____ *Direito Internacional Público e Privado*. 6º ed. Editora Juspodivm. Salvador, Bahia. 2.014.

PORTUGAL, *Constituição da República Portuguesa*. Disponível em <www.parlamento.pt/legislacao/paginas/constituicaorepublicaportuguesa>. Acesso em 17/07/14.

ROBERTS, J. M. *O Livro de Ouro da História do Mundo. Da Pré-História à Idade Contemporânea*. Trad. Laura Alves e Aurélio Rebello. 13º ed. Editora Ediouro, Rio de Janeiro, 2004.

ROSSINI, Augusto Eduardo de Souza. *O Marco Civil da Internet e os Desafios em face dos crimes cibernéticos*. Palestra *on-line* OAB/SP. Disponível em <www.videosoabsp.com.br/Default.aspx>. Acesso em 30/07/14.

SILVA, José Afonso da. Curso de Direito Constitucional Positivo. 15º ed. Editora Malheiros. São Paulo. 1.998.

SIMÃO FILHO, Adalberto. *Princípio da privacidade e da proteção da base de dados em tempos de vigilância liquida*. Palestra *on-line* OAB/SP. Disponível em <www.videosoabsp.com.br/Default.aspx>. Acesso em 31/07/14.

VIEIRA, Tatiana Malta. O *Direito à privacidade na sociedade da informação: efetividade desse direito fundamental diante dos avanços da tecnologia da informação*. Dissertação de Mestrado. Universidade de Brasília. Brasília. 2007. Disponível em <www.repositorio.unb.br/bitstream/10482/3358/1/2007_tatianamaltavieira>. Acesso em 17/07/14.

ANEXO

A LEI QUE INSTITUIU O “MARCO CIVIL DA INTERNET”

LEI Nº 12.965, DE 23 DE ABRIL DE 2014

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

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

CAPÍTULO I

DISPOSIÇÕES PRELIMINARES

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

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

I - o reconhecimento da escala mundial da rede;

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

III - a pluralidade e a diversidade;

IV - a abertura e a colaboração;

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

VI - a finalidade social da rede.

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

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

II - proteção da privacidade;

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

IV - preservação e garantia da neutralidade de rede;

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

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

VII - preservação da natureza participativa da rede;

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

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

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

I - do direito de acesso à internet a todos;

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

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

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

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

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

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

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

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

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

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

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

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

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

CAPÍTULO II

DOS DIREITOS E GARANTIAS DOS USUÁRIOS

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

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

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

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

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

V - manutenção da qualidade contratada da conexão à internet;

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

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

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

a) justifiquem sua coleta;

b) não sejam vedadas pela legislação; e

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

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

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

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

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

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

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

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

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

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

CAPÍTULO III

DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

SEÇÃO I

Da Neutralidade de Rede

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

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

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

II - priorização de serviços de emergência.

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

I - abster-se de causar dano aos usuários, na forma do art. 927 da Lei n 10.406, de 10 de janeiro de 2002 - Código Civil;

II - agir com proporcionalidade, transparência e isonomia;

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

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

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

SEÇÃO II

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

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

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

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

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

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

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

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

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

§ 3º. Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.

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

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

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

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

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

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

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

SUBSEÇÃO I

Da Guarda de Registros de Conexão

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

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

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

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

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

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

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

SUBSEÇÃO II

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

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

SUBSEÇÃO III

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

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

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

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

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

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

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

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

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

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

SEÇÃO III

Da Responsabilidade por Danos Decorrentes de Conteúdo Gerado por Terceiros

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

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

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

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

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

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

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

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

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

Parágrafo único. A notificação prevista no **caput** deverá conter, sob pena de nulidade, elementos que permitam a identificação específica do material apontado

como violador da intimidade do participante e a verificação da legitimidade para apresentação do pedido.

SEÇÃO IV

Da Requisição Judicial de Registros

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

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

I - fundados indícios da ocorrência do ilícito;

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

III - período ao qual se referem os registros.

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

CAPÍTULO IV

DA ATUAÇÃO DO PODER PÚBLICO

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

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

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

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

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

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

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

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

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

IX - promoção da cultura e da cidadania; e

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

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

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

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

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

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

V - fortalecimento da participação social nas políticas públicas.

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

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

I - promover a inclusão digital;

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

III - fomentar a produção e circulação de conteúdo nacional.

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

CAPÍTULO V

DISPOSIÇÕES FINAIS

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

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

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

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

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

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

DILMA ROUSSEFF

José Eduardo Cardozo

Miriam Belchior

Paulo Bernardo Silva

Clélio Campolina Diniz