UNIVERSIDADE BEIRA INTERIOR

Faculdade de Artes e Letras

Direito Fundamental à Privacidade na Sociedade da Informação

Whana Fechine Sobreira

Dissertação para obtenção do Grau de Mestre em

Ciência Política

(2º ciclo de estudos)

Orientadora: Doutora Maria João Cabrita

Covilhã, Setembro de 2017

Dedicatória

Dedico este estudo a Deus(s.)
é o que cada um guarda no coração. é quando
o universo te abraça. é cais em tempestade. é
a gratidão em meio ao ódio. é o pai da
esperança. é sobre caminhos que fortalecem.
é ser morada. é saber ser respeito e respeitar.
é abraçar meus pais. é o todo bom. é saber
que somos passageiros.

“do crente ao ateu, ninguém explica Deus”.
(João DoeDerlein)

Agradecimentos

Encontrar as palavras certas para agradecer a todos aqueles que têm contribuído para o meu desenvolvimento enquanto pessoa, estudante e profissional não constitui uma tarefa fácil. Tendo em vista que se trata, sem dúvida, do término de uma importante etapa, torna-se crucial relembrar aqueles que a tornaram possível.

Desta forma, expresso o meu mais sincero agradecimento a minha mãe Teresa Neuma por ter me acompanhado e apoiado ao longo de toda a minha vida e a minha querida vovó Antônia pelo seu amor infinito, como eu amo vocês.

Ao meu Marido Germanno Teles – "Xuxu" pelo apoio de sempre e sem ele os estudos Além-Mar não teriam acontecido. Xuxu você é o melhor de mim, obrigada por me acompanhar nos piores e melhores momentos e agora com o aumento da família não somos mais 3, seremos 4 com a graça de Deus, vem "Kiwi" nós já te amamos.

Agradeço a minha querida orientadora, a Professora Doutora Maria João Cabrita, pelo tempo despendido, conselhos fornecidos e palavras de incentivo. A sua sabedoria e disponibilidade foram cruciais para o desenvolvimento desta dissertação, meu sincero, Obrigada.

Aos amigos da "Galera do Mal" – Luciana, Lucas e Ivana, foi com vocês que aprendi a amar e respeitar o direito, as descobertas e experiências desse mundo foram cruciais para chegar até aqui. Vocês foram grandes incentivadores do término desse ciclo, Obrigada.

Aos novos amigos feitos na Covilhã em especial Simone por seu meu ombro amigo, e pelas palavras de incentivo e carinho nessa experiência além-mar. À Heliene "LN" que me abraçou e se tornou uma peça chave para descobrirmos juntas experiências fantásticas tanto na UBI quanto na Mobilidade da USP. Com certeza, vocês foram presentes de Deus na minha vida, levarei vocês para sempre no meu coração.

Agradeço também a todos os meus amigos que me acompanharam ao nível pessoal, académico e profissional.

A todos aqueles que sempre acreditaram em mim, meu sincero obrigada.

Resumo

Esta dissertação aborda a questão da privacidade na nova era tecnológica, sendo apresentadas e discutidas, em primeiro lugar, as definições existentes de privacidade, assim como uma reflexão sobre as necessidades regulatórias da Internet e os seus limites. No seu seguimento, falaremos da vigilância global e do modo como os usuários estão sendo vigiados por programas de monitoramento *online*. Por último, faremos uma breve análise comparativa das legislações de proteção de dados pessoais brasileira e portuguesa, bem como referência à nova proteção de dados pessoais no Brasil e à nova regulamentação que vai abranger todo o continente europeu sobre proteção de dados pessoais, sendo uma lei única para todos os estados-membros. Conclui-se ser necessária uma nova legislação que acompanhe essa revolução tecnológica, pois de outro modo os direitos de privacidade ficam desprotegidos.

Palavras-chave

Monitoramento online, Proteção de Dados Pessoais, Privacidade, Revolução Tecnológica, Vigilância Global

Abstract

This dissertation addresses the issue of privacy in the new technological era, with the presentation and discussion of the existing privacy definitions as well as a reflection on the regulatory needs of the Internet and its limits. In the following, we will talk about global surveillance and how users are being monitored by online monitoring programs. Finally, we will make a brief comparative analysis of personal data protection laws between Brazil and Portugal, as well as a reference to the new protection of personal data in Brazil and the new regulations that will cover the entire European continent on personal data protection being one law for all member states. It is concluded that new legislation is needed to accompany this technological revolution, since otherwise the rights of privacy are unprotected.

Keywords

Online monitoring, Personal Data Protection, Privacy, Technological Revolution, Global Surveillance

ÍNDICE

Lista de Acrónimos

BOPE – Batalhão de Operações Policiais Especiais

CC – Código Civil

CF – Constituição Federal

CP – Código Penal

CNPD – Comissão Nacional de Proteção de Dados

EUA – Estados Unidos da América

IP – Protocolo de Internet (*Internet Protocol*)

NSA – Agência de Segurança Nacional (*National Security Agency*)

OAB – Ordem dos Advogados do Brasil

PL – Projeto de Lei

PT-RJ – Partido dos Trabalhadores do Rio de Janeiro

STF – Superior Tribunal Federal

STJ – Superior Tribunal de Justiça

UE – União Européia

URSS – União das Repúblicas Socialistas Soviéticas

Introdução

A análise sobre o modo como a sociedade pode ver os seus direitos de privacidade preservados num espaço público em que os seus dados são disponibilizados na *Internet* exige, em primeira instância, que nos detenhamos, ainda que brevemente, no surgimento da *polis*, juntamente com a esfera pública e privada na visão de Aristóteles e Hannah Arendt. Onde a *polis* era uma forma de organização social que buscava o bem-estar e a justiça para todos. Os homens buscavam com os seus discursos na *Ágora* demonstrar que tinham conhecimentos necessários para debater a visão política da *polis*, visto que todos que pertenciam à esfera pública eram iguais e livres. Na esfera privada surge a ideia de privacidade e de poder paternal, pois o chefe de família mandava em todos os seus dependentes, garantindo moradia, alimentação e segurança.

Antigamente a sociedade vivia sem nenhuma forma de regulação, seja de direitos, deveres ou privacidade. Com o passar dos séculos e a evolução da civilização surgiu a necessidade de cada pessoa ter seu espaço individual, visto que os religiosos e, depois, a burguesia já tinham esse espaço reservado. O modelo arquitetónico das cidades mudou à medida em que as classes sociais foram reivindicando o seu espaço próprio.

Nos finais do séc. XIX, *Warren e Brandeis*, incomodados com a invasão de privacidade dos jornalistas que ficavam expondo assuntos íntimos de pessoas famosas, introduziram o direito à privacidade, o direito de ser deixado só que é utilizado nos dias de hoje. Depois de ser reconhecido o direito de se estar só, o direito à privacidade ganhou *status* internacional, em 1948 foi reconhecido na *Declaração Universal dos Direitos do Homem* e em 1950 na *Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais*. No seu longo processo histórico de desenvolvimento o direito foi aprimorando as suas normas para atender a toda a sociedade sem distinção.

É importante preservar o usuário da observação alheia, garantindo um direito à invisibilidade, um direito de não ser notado, de não ter a sua presença detectada e divulgada. Com a existência da Sociedade da Informação, e das inúmeras inovações tecnológicas, qualquer usuário passa a ser um observador dos que o cercam, quando provido de dispositivos eletrónicos e equipamentos cada vez mais potentes e invasivos, como por exemplo: celulares com câmaras de alta resolução, *tablets*, etc.

Com a evolução das sociedades, novos tipos de relações sociais e de conflitos foram criados, obrigando o direito a acompanhar as mudanças e a responder às novas questões que lhe eram propostas, inclusive questões ligadas aos crimes ou delitos cibernéticos que estão presente no mundo todo, devido a crescente utilização da internet.

A disseminação do uso de computadores fez com que, nos dias de hoje, não somente empresas públicas, que tradicionalmente coletavam dados pessoais, mas também todas as empresas privadas adquirissem os meios para coletar, manipular, armazenar e transmitir dados de uma forma simples e a um custo relativamente baixo. O interesse tanto do setor público como do privado em incrementar a utilização de sistemas de informação em diversas áreas como comércio, administração, educação, saúde, praticamente em todas as outras áreas, pode ser explicado pela circunstância de transformação da informação num recurso valioso. Na era dos mercados globais e da concorrência sem fronteiras territoriais, as tecnologias que possibilitam a manipulação, gerenciamento e uso de informações transformaram-se em ferramentas de poder.

O contínuo desenvolvimento das novas tecnologias facilita a captação dos dados e imagens pessoais e a sua transformação para a forma eletrónica dá-se através de telefones celulares, televisão a cabo, câmaras de vídeo e máquinas fotográficas digitais e vários outros tipos de tecnologia. Com o uso adequado dessas ferramentas tecnológicas, as empresas privadas e públicas conseguem registrar praticamente todos os atos de nossas vidas. Exemplificando: os nossos prontuários médicos ficam arquivados nos hospitais e são manipulados por médicos; as companhias telefónicas registam todos os números que discamos e as chamadas que recebemos; as companhias aéreas e de transporte guardam os registos de nossas viagens; os sistemas de informação dos bancos armazenam todas as nossas movimentações financeiras; a Receita Federal no Brasil, ou a Autoridade Tributária em Portugal, detém todas as informações sobre nosso património; as companhias de cartão de crédito sabem o que compramos e onde compramos; as mensagens de e-mails são armazenadas nos servidores dos provedores de acesso à Internet; a nossa movimentação *online* é capturada pelos *cookies*; se estamos num *hall* de um prédio, num *shopping center*, num elevador, no centro das ruas, nossas imagens são registadas por câmaras - praticamente, nenhum movimento escapa à intrusão dos dispositivos eletrónicos.

É evidente esta invasão de privacidade, seja pelo governo para controlar o terrorismo, desenvolvendo um sistema *online* que monotoriza todas as pessoas do mundo, ou também pelos próprios usuários a colocarem os seus próprios dados na *Internet*. Observando essa exposição da privacidade, *Snowden* decidiu publicar documentos que comprovam que vários governos observam a sua população; dividindo opiniões, sentimentos e até mesmo governos, abriu os olhos do mundo com suas declarações e com a exibição de milhões de documentos.

Essas interações electrónicas e virtuais acarretam o surgimento de novos problemas jurídicos que face à atual legislação, seja brasileira ou internacional, são irresoluveis. Consequentemente, é premente estabelecer leis que permitam conter a invasão da privacidade decorrente dos avanços tecnológicos e aos tribunais resolver os conflitos emergentes nessa nova realidade.

Os países membros da União Européia, que hoje experimentam uma grande centralização e coordenação governamental, num nível supranacional, já editaram várias diretivas e resoluções diretamente ou relacionadas à proteção da privacidade - em Maio de 2018 entra em vigor um novo regulamento UE 679/2016 relativo a proteção de dados pessoais que abrange toda a Europa.

Por sua vez, no Brasil existe o Marco Civil na Internet que regulamenta a sua utilização e estabelece a relação com a privacidade dos dados pessoais dos seus usuários. Mais recentemente, surgiu uma proposta de regulamentação que complementa a Lei do Marco Civil, o Projeto de Lei 5276/16, concernente ao tratamento de dados especiais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa humana. Enquanto o Marco Civil propõe garantias constitucionais, como a liberdade de expressão e a neutralidade da rede, este Projeto de Lei estabelece disposições mais específicas quanto à forma como dados pessoais coletados podem ser tratados, armazenados e dispostos, tanto por entidades públicas quanto por entidades privadas. Num caso ou noutro é evidente a urgência da Lei se colocar a par do desenvolvimento tecnológico, de modo a garantir a privacidade das pessoas na sociedade coeva.

Em termos metodológicos este trabalho não se restringiu à pesquisa e análise de textos de autores de referência das áreas social, do direito e da tecnologia; apoiando-se, simultaneamente, no levantamento e análise da legislação doutrina/jurisprudência existentes. Pois, de outra forma seria impossível elucidar o modo como proteger a privacidade na sociedade da informação.

Capítulo 1 – Direito Fundamental à Privacidade

1.1. Evolução histórica da Polis

> "Sabemos que toda cidade é uma espécie de associação, e que toda associação se forma tendo por alvo algum bem; porque o homem só trabalha pelo que ele tem em conta de um bem. Todas as sociedades, pois, se propõem qualquer bem – sobretudo a mais importante delas, pois que visa a um bem maior, envolvendo todas as demais: a cidade ou sociedade política" (ARISTÓTELES, 2010, p. 13).

Polis em grego significa cidade-estado - as *poleis* da Antiga Grécia constituem a origem e base do desenvolvimento do conceito de cidade que conhecemos hoje. A *polis* é uma comunidade bem estruturada de acordo com o bem comum, constituída por cidadãos livres que discutiam e elaboravam as leis relativas a sua comunidade. Cada *polis* teve a sua moeda, seus sistemas linguísticos e sociais. Se o homem age dentro das normas sociais, vigentes, procurando o bem, o homem será bem recompensado. Viver numa polis é viver numa comunidade justa, onde idealmente impera a justiça, o bem-estar de todos.

A polis é o ambiente natural do antropos, do homem racional - dentro da *polis*, o homem pode alcançar a sua racionalidade, o seu bem comum. Neste sentido, Aristóteles diz que: "o homem é um animal político, porque o homem é o único que tem linguagem e que se permite fazer política" (ARISTÓTELES, 2010, p. 35).

Hannah Arendt (1906 - 1975), ao descrever o bem comum na *polis*, na sua obra *Condição Humana*, percebeu que não foi por viverem em comunidade que os homens iriam abrir mão da sua individualidade para aplicar-se aos assuntos referentes à cidade (ARENDT, 2007, p. 64).

Os homens tinham suas divergências de opiniões e posições políticas, mas o que lhes garantia a união era o interesse comum: a busca por uma vida justa e ideal, segundo os padrões gregos.

Nas condições de um mundo comum, a realidade não é garantida pela "natureza comum" de todos os homens que o constituem, mas sobretudo pelo fato de que, a despeito de diferenças de posição e da resultante variedade de perspectivas, todos estão sempre interessados no mesmo objeto (ARENDT, 2007, p. 67).

1.2. Considerações Iniciais sobre Esfera Pública

Para Aristóteles o homem comum é o homem que tem posses. O homem que estuda, que busca compreender a realidade e que pode participar da atividade política. Para falar na *Ágora* – que era uma praça pública, onde os cidadãos se reuniam para atividades comerciais, discussões políticas, manifestações cívicas e religiosas - o homem precisava ter conhecimento e isso só era adquirido com o estudo.

O homem comum só pode se desenvolver, mostrar as suas virtudes dentro da *polis*. Ele precisava de ter conhecimento para saber os seus direitos perante a coletividade. Aristóteles afirmava: "quem não vive em coletividade ou é um Deus ou uma fera selvagem e quem vive numa coletividade e não vive em uma *polis* é um ser inferior". (ARISTÓTELES, 2010, p. 55).

Para Hannah Arendt o labor, o trabalho e a ação são as atividades da "vida activa", pois cada uma delas corresponde a uma das condições básicas mediante as quais a vida foi dada ao homem na terra. Como escreve a teórica política, "o labor é um processo biológico necessário para a sobrevivência do indivíduo e da espécie humana" (ARENDT, 2007, p. 78); "o trabalho é atividade de transformar coisas naturais em coisas artificiais (…) uma atividade que o homem impôs à sua própria espécie" (*Idem* p. 88); e "a ação é a necessidade do homem em viver entre seus semelhantes, sua natureza é eminentemente social. O homem quando nasce precisa de cuidados, precisa aprender e apreender, para sobreviver". (Idem, p. 93).

A vida na *polis*, segundo Arendt, dividia-se em dois domínios básicos: de um lado, havia a vida privada, do lar, local das atividades, do labor e do trabalho, e de outro, a vida pública que se realizava na Ágora, onde se reunia os cidadãos para discutir os assuntos de interesse da *polis*. Na esfera pública todos os homens são iguais, permitindo-lhes o exercício de sua liberdade e espontaneidade, ou seja, de sua cidadania. Enquanto o produto realizado na vida privada era um artefato ou um bem de consumo, a atividade da vida pública formava o ser humano. Na esfera privada era a necessidade que reinava sobre todas as atividades exercidas no lar.

A igualdade dos homens na política deve-se ao fato de todos serem da mesma espécie, possibilitando a comunicação e o entendimento mútuo. É a partir do discurso que os homens públicos falam de si, exibindo a sua forma de agir, a sua existência. É por meio do discurso e da ação que o homem pode distinguir-se dos demais, pois são atividades cuja a existência depende de iniciativa própria de cada indivíduo. A ação é a atividade que mais caracteriza o homem, sem a ação deixa de ser humano.

No decorrer dos tempos a esfera pública deixou de ser a esfera do político, da ação e a da virtude e passou a ser a esfera do comerciante, do trabalho e dos bens fabricados. O homem que se

relaciona na esfera política passa a ser valorizado não pela suas ações, mas pelos bens que possui e que sustentam a sociedade moderna. Concomitantemente, o direito passa a ser um bem do comércio, a servir aos interesses da sociedade e a ser valorizado conforme sua serventia.

Na concepção de Hannah Arendt, o poder e a política estão relacionados com a liberdade, com a cooperação e com a ética. Eles manifestam-se no bem comum na relação entre pessoas, nas organizações, em garantir a vida e a sinergia do ser humano com o meio ambiente. Esta teórica mostra que podemos ter direitos relacionados com o poder e a política, direitos que vão gerar leis e princípios relacionados com a coletividade, com o bem comum. Só podemos falar em democracia quando existir poder e política, pois a partir do momento em que estes são substituídos pela força e violência, elimina-se qualquer possibilidade de existir uma colaboração e - através dessas violência e força - surge leis autoritárias que prejudicam a existência de um povo.

1.3. Surgimento da Esfera Privada

Para Aristóteles o núcleo da esfera privada está na casa (*oikos*), onde as atividades relativas ao modo de vida e de gestão são realizadas. A autoridade máxima da casa pertencia ao chefe de família - era ele que mandava em tudo, tratando com violência quem o enfrentasse. O chefe de família exercia o poder arbitrário sobre os seus membros: mulher, filhos e escravos e aos quais não era permitido qualquer tipo de discussão livre e racional. As relações entre o chefe de família e seus dependentes eram apenas relacionadas com a alimentação, o lar e a segurança. Assim, no lar decorria a transferência da liberdade dos subordinados ao chefe, em troca de proteção, asilo e sustento. A mulher era tratada como objeto, sua função restringia-se à procriação e cuidado dos filhos. Os escravos, por sua vez, ajudavam o chefe de família nas atividades domésticas que geralmente envolviam força física.

No âmbito privado, a desigualdade era condição de existência, pois o chefe de família comandava e os seus dependentes obedeciam. Não existia nenhum tipo de limitações jurídicas sobre o comportamento e autoridade do chefe de família. O chefe de família garantia a segurança do lar e o poder total sobre vida e morte.

O homem na esfera privada não exercia a sua principal capacidade que era a ação política. Enquanto ser humano, ele tinha que ultrapassar o domínio instintivo e natural da vida privada, para só assim participar da vida pública. Consequentemente, para participar numa esfera de igualdade e liberdade, que era a esfera pública acabaria por desvalorizar a vida privada.

1.4. Aspectos gerais da Privacidade

Durante a Idade Média, ainda não era possível estabelecer a ideia de privacidade – como por exemplo, o vulgo não usufruía de quarto privado e banho privado - pois prevalecia os espaços coletivos e tudo era compartilhado entre todos. Tempos mais tarde, constatou-se que por causa dos enclausuramentos monásticos, onde os religiosos/místicos tinham o seu espaço inviolável, surgiu a ideia de romper com o espaço coletivo e cada pessoa do alto clero começava a ter o seu espaço privado.

O feudalismo foi um modo de organização político e social baseado no regime de servidão, onde o trabalhador rural era o servo do grande proprietário de terra, o senhor feudal. Os senhores feudais cediam parte das suas terras aos vassalos, em troca eles trabalhavam de graça alguns dias na semana e toda a produção do sistema feudal - plantar, colher, produzir o vinho, azeite, farinha, pão, criação de gado, fabricação de queijo, manteiga - dependia desta mão de obra. O senhor feudal podia-se isolar na sua propriedade repleta de vassalos que cumpriam as suas ordens e regras, mas que não detinham de espaço privado. Eles continuavam a viver num espaço coletivo só que, desde então, dentro da propriedade do senhor feudal.

O termo "privacidade" está ligado ao termo "privado", que vem do latim *privatus*, que significa "separado de". O conceito de privacidade vem da Antiguidade clássica, onde a definição de Aristóteles distinguia a esfera privada ("*oikos*") da esfera pública ("*polis*").

No século XVI iniciou-se um processo de transformação de culturas no que se refere à vida cotidiana, surgindo uma nova disposição arquitetónica das casas e cidades, tornando-se mais propícias à separação de classes e categorias, bem como mais favorável ao isolamento.

A origem do direito à privacidade faz referência às teses filosóficas de John Locke (1632 –1704) e John Stuart Mill (1806 –1873). Locke, no *Ensaio sobre o Governo Civil*, desenvolveu sua ideia de liberdade como: "autonomia para dispor, como bem lhe pareça de sua pessoa, de seus atos, de seus bens e de tudo quanto lhe pertença, submetendo-se ao que ordenam as leis sobre as quais vive"; e afirmava que "a exclusão de toda submissão a vontade arbitrário de outro, para poder seguir livremente a sua" (LOCKE, 1999, p.51).

Mill, em sua obra *On Liberty* (1859), afirmava que: "os únicos aspectos da conduta humana que produziam deveres e responsabilidades sociais seriam aqueles que afetassem os demais" (MILL, 2000, p.123). Para este filósofo, "os aspectos que só dizem respeito ao indivíduo são absolutamente independentes, sendo o indivíduo soberano sobre si, seu corpo e sua mente" (*Ibidem*).

É importante destacar que, não obstante ambos os filósofos fazerem referência a uma liberdade que propõe uma autonomia, sem interferência de terceiros, à época não se utilizavam as expressões "privacidade", "intimidade" e "vida privada".

O marco inaugural do direito à privacidade, surgiu de um trabalho chamado *The Right to Privacy*, de Samuel D. Warren e Louis D. Brandeis, publicado na *Harvard Law Review*, em 15 de dezembro de 1890. O objetivo do trabalho era de estabelecer limites para que a imprensa não invadisse a vida privada, pois os jornalistas estavam publicando assuntos íntimos de homens públicos e de pessoas famosas e não existia nada, à época, que proibisse tal publicação.

Esse artigo firmou as bases técnico-jurídicas da noção de *privacy*, configurando-a como um direito à solidão, que pode ser traduzido como "o direito a que nos deixem em paz" ou, mais literalmente, "o direito de ser deixado só". Direito que começa por ser reivindicado pela burguesia, classe com características individualistas e que, pela privacidade, se isola dentro de si.

Warren e Brandeis afirmam:

> "Que o indivíduo deva receber plena proteção de sua pessoa e de sua propriedade é um princípio antigo como o *common law*. Não obstante, tem sido necessário, de tempos em tempos, redefinir a natureza exata e a extensão dessa proteção. As transformações políticas, sociais e econômicas exigem o reconhecimento de novos direitos e o *common law*, com sua eterna juventude, cresce para satisfazer as demandas da sociedade" (1890, p.5).

Exercer com tranquilidade a liberdade de crença, de religião e de expressão é o exercício do direito que se concede a qualquer pessoa de ter um espaço reservado sem que haja qualquer censura ou observação de outrem. Neste sentido, a privacidade proporciona ao indivíduo a oportunidade de tirar todas as máscaras que a sociedade lhe impõe no seio do seu lar.

Após o avanço doutrinário e jurisprudencial, o direito à privacidade ganhou *status* internacional ao ser reconhecido na *Declaração Universal dos Direitos Humanos*, aprovada em 10 de dezembro de 1948, conforme dispõe o artigo 12º: "Ninguém será objeto de ingerências arbitrárias em sua vida privada, sua família, seu domicílio ou sua correspondência, nem de ataques a sua honra ou a sua reputação. Toda pessoa tem direito à proteção da lei contra tais ingerências e ataques" (ONU, 1948).

No mesmo sentido, na *Convenção para a Proteção dos Direitos Humanos e das Liberdades Fundamentais*, de 1950, destaca-se o art. 8º, que diz:

> "Qualquer pessoa tem direito ao respeito da sua vida privada e familiar,

> do seu domicílio e da sua correspondência; não pode haver ingerência de autoridade pública no exercício desse direito senão quando esta ingerência estiver prevista na lei e constituir uma providência que, numa sociedade democrática, seja necessária para a segurança nacional, para a segurança pública, para o bem-estar econômico do país, a defesa da ordem e prevenção das infrações penais, a proteção da saúde ou da moral e a proteção dos direitos e liberdades de terceiros" (CONSELHOS DA EUROPA, 1950);

1.5. Direito à Privacidade

A Constituição Federal Brasileira de 1988 - CF em seu art. 5° no inciso X dispõe que: "são invioláveis a intimidade, a vida privada, a honra e a imagem das pessoas, assegurado o direito a indenização pelo dano material ou moral decorrente de sua violação" (CF, 1988). A preocupação do texto constitucional é a de preservar o indivíduo, a sua intimidade, a sua vida privada, a respectiva honra e imagem das pessoas. A função principal da Constituição Federal é proteger o cidadão frente ao arbítrio do Estado, mas também a proteção perante outros cidadãos, a proteção do direito à privacidade.

A intimidade, a vida privada das pessoas não pode ser arbitrariamente exposta. A honra e a imagem das pessoas podem ter prejuízos por conta dessa exposição. É preciso que se respeite a inviolabilidade das pessoas.

Atualmente, as modernas tecnologias informáticas não só permitem que as pessoas se observem à distância através de câmaras sofisticadas, mas sobretudo permitem que essas informações sejam gravadas e posteriormente publicadas nos meios de comunicação de massa.

Segundo Celso Bastos, a privacidade é:

> "[a] faculdade que tem cada indivíduo de obstar a intromissão de estranhos em sua vida privada e familiar, assim como de impedir-lhes o acesso a informações sobre a privacidade de cada um, e também impedir que sejam divulgadas informações sobre esta área da manifestação existencial do ser humano" (BASTOS, 1989, P. 63)

Os grandes avanços tecnológicos nos meios de comunicação tornaram possíveis novas e infinitas oportunidades de interagir e compartilhar informações. Os perfis em redes sociais que possuem informações particulares, de lugares que frequentamos, lugares de trabalho, compartilhamento de fotos e muitas outras informações que antes eram consideradas pessoais e que hoje podemos

dizer que são públicas. Blogs, vídeos, páginas online mudaram a percepção que tínhamos sobre a privacidade, tornando possíveis novas formas de interação. Hoje em dia, todos vivem como celebridades, suas atividades são observadas, sujeitas a comentários maldosos, a perguntas indiscretas. É preciso que se faça uma reeducação do uso adequado da internet e ético da privacidade e a sua utilização nos meios de comunicação, sendo o principal ponto a preservação da privacidade pessoal.

Atualmente, existem muitos processos em andamento por conta da exposição inadequada da intimidade das pessoas em virtude da internet. Não se respeita mais a privacidade e, com isso, a vida privada que era para ser desfrutada somente em família ou entre amigos, está sendo compartilhada com outras pessoas do mundo.

A violação da privacidade pessoal é um caso importante devido às suas graves consequências. É preciso que cada cidadão compreenda que o direito à privacidade é muito mais que a simples garantia de estar só, consistindo principalmente na garantia de agir livremente sem o jugo alheio.

Os direitos de personalidade, como o direito à imagem, à honra, à intimidade e à privacidade são naturais dos indivíduos e vitalícios, pois acompanham cada pessoa desde seu nascimento até sua morte. Os direitos da personalidade caracterizam-se como: absolutos – porque não sofrem nenhum tipo de limitação; irrenunciáveis – o titular não pode renunciar ao seu direito; intransmissíveis – o titular não pode transmitir o seu direito para terceiros; indisponíveis – o titular do direito não pode cedê-los a terceiros, conquanto possa autorizar o uso da sua imagem por tempo determinado; e imprescritíveis – os direitos não prescrevem, não têm data limite para o seu fim, dada a sua condição de direito fundamental, esses direitos não podem ser desvinculados de cada pessoa.

Em seguida iremos falar sobre esses direitos – Direito à intimidade, à vida privada, à honra e a imagem das pessoas que são protegidos pela Constituição Federal.

1.5.1 Direito à Intimidade e a Vida Privada

A proteção dos direitos à intimidade e à vida privada foi necessária devido à transformação do homem e sua busca pela dignidade, representando a luta contra a opressão e o arbítrio. A jurista e especialista em Direito Civil no Brasil Maria Helena Diniz afirma que intimidade é "[a] zona espiritual reservada de uma pessoa ou de um grupo de indivíduos, constituindo um direito da personalidade, daí o interesse jurídico pelo respeito à esfera privada (Diniz, 2000, p.132). Essa zona espiritual é representada pela sua casa, seu domicílio, espaço inviolável, onde só se pode

entrar com autorização. É a vida secreta do indivíduo, que tenta separar do espaço público, o local da sua intimidade e de relacionamento com a sua família.

Como o direito de intimidade é um direito de personalidade, o indivíduo não pode renunciar a esse direito, conquanto possa autorizar a sua divulgação - como é o caso do programa de televisão *Big Brother*, em que indivíduos confinados num determinado espaço autorizam a divulgação da sua intimidade, mas sem poderem renunciar a esse direito.

O desrespeito à intimidade pode configurar os crimes de violação de domicílio, violação de correspondência e comunicação telefónica e violação de correspondência comercial previstos no Código Penal.

A violação de domicílio está prevista no art.150 do Código Penal do Brasil – CP, dispõe que: "Entrar ou permanecer, clandestina ou astuciosamente, ou contra a vontade expressa ou tácita de quem de direito, em casa alheia ou em suas dependências"(CP, 1988, art. 150). A violação de domicílio só é admissível com ordem judicial durante o dia ou então em caso de desastre ou para prestar socorro sem consentimento do morador.

A violação de correspondência está prevista no art. 151 do Código Penal do Brasil e dispõe que: "Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem". Segundo o Superior Tribunal Federal - STF o diretor do presídio pode abrir e ler a correspondência dos presos, para garantir a segurança do estabelecimento criminal.

A violação de comunicação telefónica está prevista no art. 151 incisos II, III e IV do Código Penal dispondo que, inciso II: "quem indevidamente divulga, transmite a outrem ou utiliza abusivamente comunicação telegráfica ou radioelétrica dirigida a terceiro, ou conversação telefônica entre outras pessoas"; inciso III: "quem impede a comunicação ou a conversação referidas no número anterior"; inciso IV: "quem instala ou utiliza estação ou aparelho radioelétrico, sem observância de disposição legal." A violação de comunicação telefónica é permitida apenas quando haja ordem judicial e ocorra dentro um processo penal uma investigação criminal.

A vida privada tem a ver com as relações familiares, bem como as alegrias, as tristezas, as lembranças da infância. E cada indivíduo tem o poder de compartilhar as suas relações, lembranças, estórias da sua vida privada com terceiros.

José Afonso da Silva conceitua vida privada como:

> "O conjunto de informações acerca do indivíduo que ele pode decidir manter sob seu exclusivo controle, ou comunicar, decidindo a quem, quando, onde e em que condições, sem a isso poder ser legalmente sujeito. A esfera de inviolabilidade é ampla, abrange o modo de vida doméstico, nas relações familiares e afetivas em geral, fatos, hábitos, local, nome, imagem, pensamentos, segredos, e, bem assim, as origens e planos futuros do indivíduo" (SILVA, 2001, p.45).

1.5.2 Direito à Honra

A honra está inserida no direito da personalidade que é objeto de proteção jurídica na Constituição Federal de 1988, e também no âmbito civil e na seara penal. É um bem imaterial inerente para aqueles que possuem personalidade, ou seja, a honra pode ser atribuída tanto a pessoa física quanto a pessoa jurídica.

Segundo o filósofo Schopenhauer (1788 –1860) a honra possui 2 vertentes:

- Honra subjetiva: diz respeito ao sentimento de autoestima, amor próprio, dignidade;
- Honra objetiva: diz respeito ao apreço social, a reputação e boa fama; (Schopenhauer, 2001.)

Independentemente desta distinção, o que a legislação brasileira busca é a proteção do respeito à honra da pessoa. A honra está vinculada à reputação, ao que a sociedade entende a respeito daquela pessoa. Não existem pessoas desonradas, a Constituição Federal prevê que essa desonra provocaria uma grave violação da dignidade humana.

O Código Civil do Brasil, em seu art. 20, diz que:

> "Salvo se autorizadas, ou se necessárias à administração da justiça ou à manutenção da ordem pública, a divulgação de escritos, a transmissão da palavra, ou a publicação, a exposição ou a utilização da imagem de uma pessoa poderão ser proibidas, a seu requerimento e sem prejuízo da indenização que couber, se lhe atingirem a honra, a boa fama ou a respeitabilidade, ou se destinarem a fins comerciais" (CC, 1988, art. 20).

Em um mesmo dispositivo, no caso o art. 20, do código civil tutelou sobre o direito à imagem e à honra.

Comprometer a honra de outrem é ofender o indivíduo podendo causar danos físicos ou até mesmo danos psíquicos, dependendo da agressão, a pessoa pode ficar emocionalmente desequilibrada, precisando de tratamento médicos para voltar a viver em sociedade.

O pacto de São José da Costa Rica, vigente no Brasil, reconhece a proteção à honra no art. 11, dispondo que: "toda pessoa tem direito ao respeito de sua honra e ao reconhecimento de sua dignidade". (Organização dos Estados Americanos, 1969).

O desrespeito à honra alheia pode entrar na seara penal e configurar os crimes de calúnia, difamação e injúria previstos no Código Penal Brasileiro. Nos termos deste código:

- "Caluniar alguém, imputando-lhe falsamente fato definido como crime. " Por exemplo: O pai esta espancando o filho; (art.138, CP).
- "Difamar alguém, imputando-lhe fato ofensivo à sua reputação. Por exemplo: Esse professor é um farsa, ele copia as aulas de outro professor;" (art. 139, CP).
- "Injuriar alguém, ofendendo-lhe a dignidade ou o decoro. Por exemplo: esse professor é um corno;" (art. 140, CP).

Estes tipos de crimes são investigados pela delegacia civil, não envolvendo Ministério Público ou Polícia Federal, a não ser que esses crimes sejam de repercussão nacional; sendo assim, o Ministério Público pode ser acionado para investigar esses tipos de crimes.

O processo que decorreu no Brasil contra o filme *Tropa de Elite* é um exemplo da denúncia de crime de honra. Alguns policiais militares do BOPE – Batalhão de Operações Policiais Especiais - pretendiam suspender por meio legal a comercialização, divulgação e exibição do filme. Eles argumentaram que o filme violava a sua honra, dignidade e trazia riscos à integridade física do grupo de elite da polícia militar do Rio de Janeiro. A juíza analisou o processo e indeferiu o pedido, alegando o caráter ficcional do filme ao qual se vinculava o direito de livre expressão, cabendo aos espectadores acreditar ou não naquilo que o filme retrata.

Nos últimos anos, houve um aumento de ações de reparação por dano moral nos tribunais de todo país, causando um verdadeiro caos para a celeridade da tutela jurisdicional. A grande maioria dessas ações são transtornos diários inerentes do cotidiano de uma sociedade.

1.5.3 Direito à Imagem

O Direito à imagem é um direito fundamental e esse direito estende-se a todas as pessoas de imediata exigibilidade; ou seja, todos nós temos o direito sobre a nossa imagem e o dever de

proteger ou o de não violar o direito de imagem de outras pessoas. Quando, por exemplo, um namorado com raiva divulga fotos íntimas da sua namorada na internet, essa exposição pode causar sérios danos à sua imagem, problemas na família, com os amigos e, inclusive, no trabalho.

A imagem é um direito da personalidade e esse direito preocupa-se em defender a imagem ou, quando esta tenha sido atingida, tenta minimizar os efeitos negativos dessa exposição.

Sob a tutela do direito básico das pessoas à segurança, hoje as câmaras de vigilância estão por toda parte, em *shoppings*, em repartições públicas, em escolas e além disso qualquer pessoa tem um celular com uma câmara que utiliza para registar situações reais – registos que, com menor ou maior frequência, são compartilhados na Internet.

A imagem é o cartão de visita de cada pessoa, o direito tem que proteger a imagem das pessoas, pois esse direito é inerente a cada cidadão. O direito à imagem é um direito absoluto, consequentemente o seu titular não pode renunciá-lo, conquanto possa autorizar a utilização da sua imagem para fins comerciais. Eu posso abrir mão do direito a imagem de forma momentânea, mas não definitiva.

Com frequência o circuito de câmaras de vigilância flagram delitos e as suas imagens são cada vez mais usadas na justiça como prova de crime, mas a gravação não pode violar a intimidade da pessoa e ser usada sem autorização da justiça.

Para o Supremo Tribunal Federal – STF, a gravação de conversas telefónicas de alguém pode ser usada mesmo que tenha sido feito sem autorização da justiça ou de quem estava do outro lado da linha, principalmente se for em defesa própria ou investigação criminal. A previsão legal para esses gravações está na Constituição Federal, art. 5, inciso 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 que a lei estabelecer para fins de investigação criminal ou instrução processual penal". O mesmo vale para vídeos onde uma das partes envolvidas é o responsável pela gravação, mas o entendimento muda em conversas protegidas pelo sigilo constitucional, como por exemplo, entre advogados e clientes.

Na Constituição Federal, inciso XIV, o sigilo de advogados e clientes é enunciado nos seguintes termos: "é assegurado a todos o acesso à informação e resguardado o sigilo da fonte, quando necessário ao exercício profissional". No Código de Ética e Disciplina da Ordem dos Advogados do Brasil, OAB art.26, lê-se:

> "O advogado deve guardar sigilo, mesmo em depoimento judicial, sobre o que saiba em razão de seu ofício, cabendo-lhe recusar-se a depor como testemunha em processo no qual funcionou ou deva funcionar, ou

> sobre fato relacionado com pessoa de quem seja ou tenha sido advogado, mesmo que autorizado ou solicitado pelo constituinte".

Mesmo que o cliente autorize o advogado a revelar o sigilo das informações, o mesmo não poderá fazê-lo, visto que a assistência jurídica não pode ser colocada em risco. Por exemplo, o dono de um estabelecimento comercial pode-se recusar a mostrar as imagens de segurança a um cliente que foi furtado, visto o estabelecimento não ter a obrigação de fazê-lo. Neste caso, a parte lesada deve-se deslocar à delegacia mais próxima para registar um boletim de ocorrência, depois disso o delegado de polícia vai instaurar um inquérito policial e requisitar as imagens com o intuito de chegar à autoria do delito cometido no estabelecimento. Há previsão legal pela Lei 12.830/13 que trata da investigação criminal conduzida pelo delegado de polícia.

É permitido instalar câmaras de segurança em locais públicos como por exemplo em escolas, repartições públicas, *shoppings*, restaurantes, presídios e na própria residência da pessoa - a câmara é um instrumento de defesa, para se proteger de algum tipo de delito que venha a ocorrer. Por outro lado, é proibido a instalação de câmaras dentro da casa de banho e não é recomendado dentro do quarto, pois viola o direito de intimidade da pessoa.

Para o Superior Tribunal de Justiça – STJ o direito à imagem reveste-se de um duplo conteúdo. Primeiro de um conteúdo moral, porque é um direito da personalidade, e também de um conteúdo patrimonial, porque assente no princípio segundo o qual a ninguém é facultado enriquecer a custa de terceiros (Resp 74. 473, STJ). O segundo parâmetro para o STJ, diz respeito a imagem do cidadão sem a sua devida autorização, no sentido de constituir um enriquecimento indevido. Um terceiro parâmetro para o STJ, é no sentido em que no direito da imagem a obrigação de reparação decorre do próprio uso indevido da imagem sem a respectiva autorização da pessoa, não importando se foi com fins comercias ou não, visto não haver a necessidade de prova do dano – é suficiente a não autorização. Um quarto parâmetro para o STJ, é no sentido de que o direito à imagem, o direito de retratação, deve sempre obedecer a uma sistemática prevista pela jurisprudência brasileira.

Exposto isto, o uso da imagem precisa ser autorizado pelo titular - se alguém utiliza a imagem de outrem sem autorização, pode ensejar uma eventual reparação por danos, seja material ou moral. Com base nisso o STJ publicou a Súmula 403, que diz: "Independe de prova do prejuízo a indenização pela publicação não autorizada de imagem de pessoa com fins econômicos ou comerciais ".

As imagens gravadas para fins de segurança pública não podem ser expostas na internet, pois trata-se de garantir a segurança das pessoas interessadas. Diversamente, uma imagem gravada no celular de amigos pode ser colocada na internet, desde que não exponha pessoas ao ridículo e

não traga nenhum prejuízo à honra e à imagem dessa pessoa. O grande problema de colocar as imagens na internet, em sites de busca ou em redes sociais é que a pessoa não tem direito ao esquecimento, pois aquelas permanecem expostas por tempo indeterminado. Por sua vez, os conteúdos postados na internet, e-mails e em redes sociais são aceites como prova, conquanto a dificuldade em comprovar a autenticidade do material.

Com o advento da internet, o direito não acompanhou essas transformações e com isso as leis ficaram desfasadas. É urgente o STF e outros tribunais em todo o mundo acompanharem essas transformações e implementarem novas leis que atendam às necessidades da sociedade nos dias de hoje.

É preciso que a sociedade tenha cuidado com o conteúdo que está sendo gravado e com o que se expõe na internet, sob penas de responsabilidade tanto civil como criminal, até porque não existem julgados para tratar esse tipo de assunto e é algo que está sendo construído para os próximos anos.

A publicação de imagens na internet deve decorrer conforme as seguintes regras:

- Ninguém pode falar em teu nome sem a tua autorização;
- Ninguém pode-te citar sem a tua autorização;
- Ninguém pode usar fotos tuas sem a tua autorização;
- Ninguém pode-te adicionar a grupos sem a tua autorização;
- Ninguém pode anunciar algo em teu nome.

As redes sociais, por exemplo, quando cadastram um novo usuário no Facebook, Instagram, Youtube, obrigam-no a aceitar os termos de condições. Nos termos de condições do Facebook, fica explícito a utilização, quando necessária, dos dados do usuário, que autoriza os outros usuários a compartilharem as suas fotos, a marcarem-no. O usuário pode modificar a sua privacidade, limitando quem pode visualizar as suas publicações, bloqueando, excluindo usuários indesejados, etc. Ou seja, o Facebook dá liberdade ao seu usuário, pois quanto se sinta incomodado pode fazer essas alterações; mas regra geral, ao aceitar as condições de uso o usuário coloca à disposição desta plataforma as suas informações, como fotos, vídeos, publicações.

1.5.4 Privacidade Digital

Com a revolução tecnológica, a Internet trouxe uma série de benefícios para a sociedade, desde a facilidade de comunicação com pessoas do outro lado do mundo, ao acesso e compartilhamento de todo tipo de informações. Mas além de todos os benefícios, trouxe alguns riscos à sociedade, com relação à segurança do usuário que utiliza a rede de computadores.

Hackers estão a toda hora invadindo contas de e-mails, perfis de redes sociais, contas de banco, tudo isso porque a segurança falha. Devemos tomar todos os cuidados para evitar possíveis fraudes nas nossas contas.

As relações pessoais estão deixando de existir e estão se tornando cada vez mais relações virtuais, com isso o excesso de exposição nas redes sociais está fazendo com que os usuários compartilhem a sua privacidade com o mundo, não só as suas opiniões, gosto musicais, em relação a filmes, fotos, vídeos, dentre tantas outras coisas. Os novos meios de comunicação chamam a atenção da sociedade de como a vida privada está sendo invadida constantemente.

Aplicativos como Facebook e Gmail têm um sistema de mecanismo que grava tudo o que o seu usuário procura e mostra para ele através de publicidade. Com isso a sua privacidade, a individualidade dos usuários torna-se altamente vulnerável, pois hoje em dia é muito fácil rastrear um banco de dados que revela a vida dos seus usuários, sem que ao menos saibam e sem nenhum tipo de autorização dos mesmos.

O direito à privacidade no Brasil é um direito fundamental assegurado na Constituição Federal do Brasil. O art. 5º da CFB no inciso X diz: "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".

No inciso seguinte deste mesmo artigo enuncia-se: "a casa é asilo inviolável do indivíduo, ninguém nela podendo penetrar sem consentimento do morador, salvo em caso de flagrante delito ou desastre, ou para prestar socorro, ou, durante o dia, por determinação judicial". No seu prosseguimento, o inciso XII determina:

> "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 que a lei estabelecer para fins de investigação criminal ou instrução processual penal".

O dano cometido à imagem de uma pessoa, seja ela pública ou não, torna-se muito mais grave quando o conteúdo danoso é compartilhado no meio eletrónico, pois em poucos horas o mundo inteiro pode aceder-lhe.

As leis e jurisprudências brasileiras foram criadas para tentar proteger mais o usuário contra crimes ou delitos informáticos que a legislação não previa. Uma lei que ficou muito conhecida no Brasil foi a Lei 12.737/2012 ou Lei Carolina Dieckman, que foi criada no decorrer do processo instalado por essa atriz brasileira, como vítima de divulgação das suas fotos íntimas pela internet, e que pretende combater o crime cibernético cometido no Brasil.

Não é possível reparar completamente o dano, por mais que se busque alternativas, que se busque a esfera criminal, que se busque uma reparação por um dano moral, identificando quem foi o responsável, mas apenas tentar reparar o dano ocorrido, pois o sofrimento já foi experimentado pela vítima.

Capítulo 2 – Sociedade da Informação

2.1 Aspectos Gerais sobre a Internet

O ambiente virtual, em razão da evolução tecnológica, passou a cercar o cotidiano humano nas últimas décadas. De forma gradativa, as relações sociais passaram a interagir eletronicamente e a internet afirmou-se como um meio de comunicação de notável eficiência e baixo custo. Interação à qual a dinâmica do mercado de capitais não pôde furtar-se. As relações comerciais via internet são cada vez mais cómodas e facilitadas - hoje é possível realizar negócios, transações financeiras, pagamentos, emissão de notas fiscais, bem como a compra e venda de produtos por meio eletrónico.

A vida moderna exige maior agilidade por parte dos indivíduos, fator que conduz a uma constante necessidade de conexão ao ambiente virtual por meio de computadores, celulares, *smartphones*, *tablets*, e demais insumos eletrónicos. Considerando a era tecnológica experimentada pela sociedade atual, é imperiosa a inovação de normas para regulamentar as novas formas de transações comerciais.

O termo internet é popularmente conhecido como rede mundial de computadores, pois de entre as suas principais funções pode ser destacado a interação, em tempo real, entre pessoas em diferentes localidades do planeta. Modernamente, essa rede de sistemas possibilita o acesso imediato aos mais diversos tipos de serviços, informações, transferências de dados, e transações comerciais.

A Internet, para Rosa (2005, p. 03), pode ser entendida como:

> "Uma rede transnacional de computadores interligados com a finalidade de trocar informações diversas e na qual o usuário ingressa, por vários meios, mas sempre acaba por realizar fato jurídico, gerando consequências inúmeras nas mais diversas localidades".

Coadunando com esse entendimento, Willing (1997, p. 30) define Internet como: "Uma rede mundial, não regulamentada, de sistemas de computadores, conectados por comunicações de fio de alta velocidade e compartilhando um protocolo comum que lhes permite comunicar-se".

Retomando a análise da definição de Rosa, temos que a rede é transnacional, ou seja, não existe fronteiras físicas para sua comunicação e, consequentemente, para as trocas de arquivos, desde o entretenimento até o uso comercial da informação.

A arquitetura da rede eletrónica deve conceder proteção aos usuários do sistema virtual, mormente, em relação ao trânsito de informações. Além da tutela jurídica de seus interesses, o consumidor também é digno da proteção por meio da utilização de códigos-fontes matemáticos de acesso, para proteger as informações e disciplinar as condutas e relacionamentos adotados pelos internautas.

Os usuários devem utilizar a Internet com responsabilidade, pois hoje em dia é muito comum colocarmos nossos dados pessoais em qualquer transação feita na Internet e com isso ficamos expostos em todo o mundo. Segundo pesquisas de empresas especializadas, o mercado virtual movimenta bilhões e tornou-se um instrumento hábil a alavancar a economia.

2.2 A Internet e o Ciberespaço

O termo "Ciber" decorre da palavra grega *kybernan* que significa navegar ou controlar. O ciberespaço é definido como o "espaço de comunicação aberto pela interconexão mundial dos computadores e das memórias dos computadores" (LÊVY, 2002, p. 34).

Segundo a definição da UNESCO:

> "O ciberespaço é um novo ambiente humano e tecnológico de expressão, informação e transações econômicas. Consiste em pessoas de todos os países, de todas as culturas e línguas, de todas as idades e profissões fornecendo e requisitando informações; uma rede mundial de computadores interconectada pela infraestrutura de telecomunicações que permite a informação em trânsito ser processada e transmitida digitalmente."(Unesco, 2012)

O Ciberespaço é um mundo sem territórios, sem fronteiras e com regulação normativa própria de comunicação (HESPANHA, 2002, p.45). Neste sentido, Silva (2003, p.46) define o Ciberespaço como um ambiente virtual e desconhecido para o Direito, apresentando novas definições de tempo e espaço. É a própria geografia, como salienta Pinheiro (2006, p. 10), que muda no Ciberespaço:

> "Com o ciberespaço, a geografia como conhecemos (física) desaparece, surge uma nova geografia, algo que não é material, mas real. O Ciberespaço é um não lugar, ou um lugar imaginário, que só temos acesso pelo computador, mesmo assim ele está ligado a realidade pelo uso que temos feito dele nos dias atuais, transformando-o em um espaço intermediário entre duas realidade."

A Internet foi concebida para ser livre e insubordinada a autoridades governamentais, ultrapassando o espaço tridimensional a que o homem está habituado. Mostra-nos a existência de um espaço virtual onde circulam informações com valor económico, onde se comercializam bens corpóreos e não corpóreos, onde o ser humano deixa o traço da sua própria existência e genialidade. A absoluta falta de controle, ou "quase anarquia", tem criado espaços exclusivos de disseminação de atividade criminosa (OLIVEIRA, 2001; CASTRO, 2003).

É precisamente neste sentido que Abreu (2001, p. 60 – 62) esclarece:

> "Na internet impera a liberdade virtual de caráter ilimitado; é justamente na falta de limites territoriais que se criam os problemas éticos e jurídicos e residem as maiores dificuldades para a aplicação do direito nas áreas de civil e penal".

Deste modo, Internet e Ciberespaço fundem-se. A Internet promove o acesso à rede, enquanto o Ciberespaço permite a interação entre os milhões de usuários (KAMINSKI *apud* GARCIA, 2008). Lêvy afirma que: "as expressões ciberespaço e internet operam em todas as dimensões sem limites de tempo e de lugar" (2002, p. 13). A Internet modifica a nossa relação virtual com o mundo real mais radicalmente que todos os instrumentos ou veículos anteriores de comunicação criados pela inteligência coletiva dos homens (CADOZ, 2002, p. 34).

Na Comunidade Europeia a Internet é identificada como "a rede das redes", um novo ramo do Direito, frequentemente denominado de Direito do Ciberespaço, Direito da Informática ou até mesmo Direito Virtual ou eletrónico, tendo em vista a grande proporção que tem tomado e conquanto não desfrute de uma autonomia efetivamente reconhecida.

Passando para a análise da natureza jurídica da Internet, os pensamentos doutrinários divergem quanto ao facto de ser um meio ou um lugar. Sobre esta matéria, Garcia (2002, p. 43) defende:

> "[...] se entendermos que a Internet é um lugar, muitas das questões já previamente definidas pelo Direito, tais como o foro competente, deveriam ser redesenhadas. Imagine um contrato celebrado entre uma empresa alemã e outra brasileira. Se a Internet é um lugar, onde seria assinado o contrato? A resposta, então, é nem no Brasil e nem na Alemanha, mas na Internet. A proposta e a aceitação também seriam realizadas na Internet."

Diversos serviços, como a declaração de impostos via Internet, o oferecimento de denúncias nos sites do Procon e do Ministério Público e o fornecimento, pela Procuradoria-Geral da Fazenda Nacional, da certidão negativa da dívida ativa da União pela Internet, têm sido criados no sentido

de apaziguar a burocracia, evitando que o cidadão gaste horas perambulando por repartições públicas. Garcia (2002, p. 12) afirma que:

> "Através da Internet, tem-se acesso direto a diversos órgãos estatais, possibilitando o acompanhamento de processos e a pesquisa, bem como pode-se, nas centenas de *home-pages* jurídicas, pesquisar leis, doutrinas e jurisprudências; consultar escritórios de todo o Brasil e do mundo; realizar conferências e discussões virtuais com operadores do Direito, visitar bibliotecas, autores; trocar informações; e permanecer informados sobre as mais recentes novidades do mundo jurídico."

Por exemplo, um usuário pode consultar a sua situação de quitação eleitoral na Internet no site do Tribunal Superior Eleitoral, evitando ter que se deslocar até o cartório eleitoral para saber se a sua situação de voto está regularizada.

2.3 Internet das Coisas

Algumas coisas precisam de um manual de instruções para sabermos como devemos usá-las, diferentemente das ferramentas e objetos úteis que, resolvendo os nossos problemas, dispensam qualquer manual. Hoje ninguém precisa de um manual para usar a internet no seu tablet, smartphone ou computador.

A internet nasceu na ARPANET, uma rede de computadores experimental financiada pelo militares dos EUA, tendo por objectivo interligar grandes universidades e centros de pesquisas e permitindo aos investigadores universitários compartilharem informações nessas redes. Com o tempo muitas redes de computadores foram se interligando até dar origem à grande rede mundial que temos atualmente. Várias aplicações foram criadas para interligar pessoas do mundo todo e houve diversos avanços na tecnologia, como por exemplo a criação do email, os notebooks, a web(www), o comércio eletrónico(amazon), os buscadores(google), a tecnologia de rede sem fio(wifi), as músicas online(iTunes), a tecnologia de voz sobre ip(skype), os vídeos online(youtube), os smartphones, as redes sociais(Facebook), etc. Hoje, muito mais que uma rede de computadores, a internet é uma rede de pessoas e comunidades.

Notável cientista da computação, Mark Weiser criou, no findar da década de 80 do século passado, o conceito de computação ubíqua. Neste sentido, escreve:

> "A computação ubíqua é a terceira onda da computação que está apenas começando. Primeiro tivemos os mainframes compartilhados por várias pessoas. A segunda onda é a era da computação pessoal, com

> pessoas e máquinas se estranhando umas às outras. A seguir vem a computação ubíqua a era da tecnologia calma quando a tecnologia recua para o pano de fundo de nossas vidas. As tecnologias mais importantes são aqueles que desaparecem. Elas se integram ao dia a dia, ao nosso cotidiano, até serem indistinguíveis". (Weiser, 2012)

Assim, a computação ubíqua, mais conhecida como a internet das coisas, passa a interligar vários tipos de objetos e dispositivos inteligentes que interagem entre si e conosco, tornando a nossa vida mais fácil. A internet e os computadores estão desaparecendo, mas estão cada vez mais presente em tudo e nem damos por isso - por exemplo, hoje já se pode comprar uma TV que tenha embutido um sistema wifi e que tenha acesso a internet.
O físico e escritor contemporâneo Michio Kaku afirma que:

> "Computadores, silenciosamente lendo nossos pensamentos serão capazes de realizar nossos desejos. Nós poderemos mover objetos apenas com a força da mente. Com o poder da nanotecnologia, poderemos pegar um objeto e transformá-lo em alguma coisa diferente. Embora coisas assim possam parecer inimaginavelmente avançadas, as sementes dessas tecnologias estão sendo plantadas nesse momento. É a ciência moderna e a tecnologia e não mágicas e encantos que nos darão esse tipo de poder". (Kaku, 2015)

Atualmente, já é possível automatizar a nossa casa e controlá-la pelo *tablet*. Eventualmente não é necessário controlar os objetos, eles podem reagir à nossa presença. Cidades podem espalhar sensores para monitorar a temperatura, a velocidade do vento, a humidade e a qualidade do ar, podendo ajudar na previsão do tempo. Um automóvel pode-se comunicar com outro, avisando de um engarrafamento, ou mesmo de um acidente, tal como os relógios que controlam a pulsação dos pacientes podem alertar os médicos em casos problemáticos, geladeiras podem alertar para a falta de produtos em stock, e por aí adiante. Essa evolução da internet tem muitas novidades promissoras e é muito bem vinda. Todavia, é necessário tomar cuidado em relação à segurança dos dispositivos, perante invasões, ataques, *spam*, vírus – na *net* alguns destes vírus ocorrem por problemas nos *softwares* dos nossos computadores. Ao embutir um pequeno computador num dispositivo qualquer não se deve deixar a segurança para segundo plano, pois há que evitar que o controle nos nossos aparelhos seja invadido por *hackers*. A estes é extremamente fácil, por exemplo, invadir o nosso automóvel e acionar os freios na hora indevida.

Outro ponto importante é a privacidade, quem terá acesso aos dados disponíveis sobre determinada pessoa. Por exemplo, que um usuário partilhe com os seus médicos os dados sobre o seu estado de saúde, avaliados por sensores, não significa que deseje compartilhá-los com os

intervenientes de outras instituições sociais. É desejável que o seu gestor de conta bancária tenha acesso a esses dados? A resposta provável é "não".

Recentemente, houve uma denuncia de que a NSA (National Security Agency), um órgão do governo americano, está coletando dados de todos nós. Certamente, não queremos que o futuro torne real o cenário ficcionado por George Orwell em 1984, onde o ditador, chamado de *Big Brother*, vigiava e controlava tudo e todos. A informação sobre os limites e privacidades da internet já é pauta importante em todo o mundo.

É necessário lembrar a relevância da infraestrutura da internet e que, com o surgimento da internet das coisas, os endereços ip's que identificam esses dispositivos de forma única não têm estrutura para receber essa quantidade de equipamentos na rede. Por isso mesmo, tecnologicamente a internet está em transição do Ipv4 para o Ipv6; e conquanto esta transição esteja muito atrasada, já não existem mais endereços disponíveis de Ipv4. Muitos provedores estão começando a compartilhar endereços entre vários usuários simultâneos usando técnicas de compartilhamento. A implantação do Ipv6 é necessária para a continuidade da internet e para sua evolução.

2.4 Conceito de Sociedade da Informação

Sociedade é a associação de indivíduos vivendo sob as mesmas regras, trabalhando, estudando, se divertindo, influenciando seus rumos, mas também sendo influenciados - sobretudo os jovens, que recebem e aprimoram em sociedade as suas formações.

Segundo Luís Gouveia:

> "A sociedade da informação está baseada nas tecnologias de informação e comunicação que envolvem a aquisição, o armazenamento, o processamento e a distribuição da informação por meios eletrônicos como rádio, a televisão, telefone e computadores, entre outros. Estas tecnologias não transformam a sociedade por si só, mas são utilizadas pelas pessoas em seus contextos sociais, econômicos e políticos, criando uma nova comunidade local e global: a sociedade da informação." (Gouveia, 2013)

Foi por conta dos grandes avanços tecnológicos permitidos pelo moderno uso da inteligência humana, através de um intenso esforço intelectual que a economia do capitalismo ocidental deu seus grandes saltos, materializando através dos inventos, das máquinas, da criação artificial, cujo

objetivo geral visou o ganho, a acumulação de lucro - e isso concretizou-se através da produção em escala da sociedade industrial.

A "informação" é o acto de comunicar algo a uma ou mais pessoas. Quando alguém assiste a um filme, lê um livro ou conversa com outros obtém informações – as quais podem ser interessantes ou úteis. Mas nem todos os indivíduos sabem dar uso à informação. A partir do momento que o indivíduo consegue expressar esse conjunto de informações, tanto na forma escrita quanto na verbal, ensinando um grupo de pessoas, transformando esse conhecimento em produtos e serviços, dominando esse conjunto de informações, constrói conhecimento. Nunca a informação circulou de uma forma tão intensa e rápida como na era da internet. Um turbilhão de novos textos, vídeos e músicas que, provavelmente, alguns usuários compartilharam recentemente.

Os meios tradicionais de informação como rádio, jornal e televisão tentam-se adaptar a esta revolução tecnológica, procurando identificar a informação relevante num mundo em que, minuto a minuto, emerge uma quantidade imensa e variada de informação - esta é, de resto, uma tarefa complicada para todos os meios de comunicação.

Segundo Pekka Himane (2012, pág.132): "[a] tecnologia é uma dimensão fundamental da mudança social. As sociedades evoluem e transformam-se através de uma completa interação de fatores culturais, econômicos, políticos e tecnológicos."

A sociedade da informação substancia a possibilidade da humanidade aceder ao conteúdo por ela produzido. Com a era da informação o jornal deixou de constituir a única e segura fonte de informação – hoje o conhecimento está na rede. A rede se tornou essa grande plataforma de interação, de compartilhamento de informações.

Com a rede social o mundo empresarial tem um banco de dados disponível nas novas mídias e pessoas ao vivo a discutir questões que vão do meio ambiente à política. Hoje, a sociedade da informação passou a ser chamada sociedade do conhecimento, pois produz conhecimento em tempo real e pode ser acessada de qualquer *smartphone*. Segundo Pekka Himane (2012, pág 135): "Conhecimento e informação foram fatores centrais em muitas, senão em todas, sociedades historicamente conhecidas".

Com uma convergência midiática e com a popularização dos *smartphones*, houve um aumento de compartilhamento e produção de conteúdo. De acordo com a Revista *Exame,* o Brasil é o quarto país com mais smartphones possui cerca de 70 milhões de aparelhos e, entre 2008 e 2012, foi o oitavo em termos de maior número de internautas. Neste período surgiram 27 milhões de novos usuários e em 2103 o país reunia cerca de 88 milhões de usuários na rede, o que representa a conexão de cerca de 45% da população do Brasil. Segundo Pekka Himane (2012): "Não existem

revoluções tecnológicas sem transformação cultural. Tecnologias revolucionárias tem de ser pensadas."

Hoje, a continuidade do nosso corpo são os *smartphones* não é preciso ter um *smartphone* topo de gama, desde que permita tirar fotos e publicá-las na rede social. Não conseguimos mais pensar na nossa vida sem um *smartphone,* num mundo em que as pessoas estão trocando as relações pessoais para ter relações virtuais - o lazer, a família, o trabalho, tudo isso fica comprometido. O grande questionamento é como fazer para que a tecnologia não distancie as pessoas dentro de casa - é necessário delimitar-se a sua utilização no espaço familiar e os pais devem ser responsáveis por essa mudança.

2.5 Coleta de Informações

A coleta de informações é a captura e recolha dos dados necessários à conclusão do processamento de transações. Com a criação de um ambiente virtual, essa coleta de dados ficou mais fácil. No caso dos sites, os administradores colocam um arquivo chamado *cookies* toda vez que um usuário acede a um site, um pequeno arquivo de texto é colocado dentro do próprio computador, *tablet*, *smartphone* do usuário. Com isso, sempre que o usuário aceda ao mesmo site o arquivo de texto manda informações para o seu servidor, permitindo uma melhor navegação, de acordo com as suas preferências ou, então, lembrando senhas gravadas em alguma etapa de compra.

Recentemente, a Google oficializou o escaneamento das mensagens de e-mail; ou seja, todos as mensagens que entram e saem da plataforma gmail são lidas automaticamente pelo seu sistema, com o objetivo de oferecer anúncios personalizados aos seus usuários. A empresa também argumenta que com essa prática é possível detectar as possíveis invasões como vírus, *spams*, etc.

2.6 Digitalização de Informações

Vivemos uma grande mudança de uso e costumes e a forma documental por escrito remonta ao tempo da pedra - os desenhos feitos nas pedras mostravam como os homens pensavam e se organizavam; com o passar do tempo veio o papiro e depois papel, uma grande invenção usada até nos dias de hoje. Depois do papel surgiram várias outras formas de guardar informações, primeiramente o e-mail, que é um comunicador instantâneo, depois o envio de mensagens pelo celular – SMS, e as redes sociais que podem guardar informações.

A digitalização de documentos funciona com *softwares* e *hardwares* específicos, os documentos são preparados para serem digitalizados em escâneres especiais, depois de digitalizados, são conferidos e guardados em servidores. A sua finalidade é a otimizar e racionalizar a gestão documental de forma mais ágil, mais rápida. Com esse processo as empresas começaram a substituir o papel físico pelo suporte digital.

Nos EUA o Presidente Barack Obama mandou digitalizar cerca de 80% de todos os registros médicos até 2014. No Chile está sendo implementada a criação de prontuários eletrônicos. No Brasil, o prontuário era registado em papel e com isso surgiam inúmeras dificuldades, principalmente em relação à letra ilegível dos médicos e à incompletude das informações dos pacientes. Todavia, com a resolução do Conselho Federal de Medicina nº 1.821/2007 foram aprovadas as normas técnicas concernentes à digitalização e uso dos sistemas informatizados para a guarda e manuseio dos documentos dos prontuários dos pacientes, autorizando a eliminação do papel. No prontuário eletrónico, o sistema gera uma base de dados, melhora o controle de toda a documentação do paciente e os farmacêuticos já conseguem entender qual remédio prescrito pelo médico.

Os países do mundo inteiro estão investindo cada vez mais em dados eletrónicos em substituição do papel - esta substituição representa uma melhoria de governança, de controle. Diferentemente do meio eletrónico, o papel não gera rastros, sendo elevada a possibilidade de vazar um documento ou de perdê-lo - isso acontece em muitos casos, principalmente em desastres naturais.

A sociedade digital é mais formal, guarda mais os documentos e usa menos papel. Por exemplo, antigamente no Brasil um resultado de exame laboratorial era entregue em papel, enquanto hoje o usuário recebe uma senha do exame, acessa o site do laboratório e pode visualizar o resultado dos exames, e o resultado pode ser visualizado pelo médico ou por qualquer outra pessoa autorizada a fazê-lo. O usuário tem mais acesso à informação porque ela não está aprisionada em papel. Algumas certidões brasileiras podem ser emitidas pela Internet, como é o caso da Certidão de Quitação Eleitoral, que garante o cumprimento das obrigações eleitorais por parte do eleitor – no Brasil o voto é obrigatório.

Outro grande marco da digitalização de documentos foi a informatização do processo judicial no Brasil e em outros países. No Brasil, antigamente, para dar entrada num processo era preciso que o advogado fosse ao protocolo do fórum; e o acompanhamento do andamento do processo exigia mais deslocações, por parte do advogado, ao forúm. Hoje, toda a informação do processo é digitalizada. O processo é enviado via sistema e toda a visualização do mesmo se dá pela internet - a distribuição, processamento e julgamento são mais céleres. O judiciário brasileiro já aceita o documento eletrónico como indícios de prova.

Na sociedade da informação se alguém inserir/alterar os dados já existem meios de provar a sua ocorrência, pois fica registada no sistema.

2.7 Armazenamento de Informações

Cada vez que o usuário entra num site e coloca no carrinho de compras determinado produto ou quando publica algo numa rede social, todas as informações sobre a sua navegação estão sendo armazenadas. Hoje, as informações são tratadas pela *Big Data*; ou seja, são submetidas a um tratamento de dados de modo a se tornarem compreensíveis e a serem colocadas em algum sistema de informação. Estas informações são comercializadas de acordo com a navegação do usuário. São sistemas que trabalham com algoritmos que vão estudando e desenhando o perfil do usuário para que as empresas possam oferecer produtos de acordo com a sua navegação.

Na grande maioria das vezes, o usuário não sabe que a sua navegação está sendo monitorada. Grandes empresas como a Google, o Facebook, o Twitter e o WhatsApp não cobram aos usuários a utilização dos seus serviços, mas monotorizam esses serviços de modo a financiarem as suas infraestruturas – a venda de informações sobre os milhões de usuários cadastrados em seus serviços constitui o seu meio de financiamento. Seja através de *banners*, anúncios, estas empresas comercializam a informação deixada pelo usuário ao longo da sua navegação. Toda a internet trabalha no sentido de facilitar e dar utilidade ao conteúdo da navegação do usuário.

2.8 Segurança da informação

A análise do tópico "segurança de informação" exige, primeiramente, que se clarifique o que se entende por "informação". Neste sentido, tomamos por base a ideia de que é um conjunto de dados inseridos dentro de um contexto para ter significado dentro de uma organização. Esses dados contextualizados podem representar: informações financeiras, segredos ou arquivos confidenciais, ou inúmeros outros tipos de informação. Hoje a informação é considerado um ativo importante tanto para as pessoas quanto para as organizações, sendo muitas vezes o bem de maior valor de empresas privadas e órgãos públicos. Estas informações são tão valiosas que são empregues inúmeros recursos para protegê-las. Porém, enquanto alguns querem proteger as suas informações, outros querem acessá-las de qualquer maneira para fins ilícitos.

Para a informação ser acessada precisa ser transmitida, seja em tempo real - em uma conversa, por exemplo - ou a longo prazo - em um livro, por exemplo. Esse processo de transmissão ou

troca de informações é chamado de comunicação e pode ocorrer de diversas maneiras: diálogo, gestual, escrita por meio eletrónico, carta ou outro meio de suporte. Qualquer processo de comunicação é composto pelos seguintes elementos: em primeiro lugar, temos a mensagem que vem do emissor e é organizada através de um código que pode ser conhecido por uma língua comum ou então por uma linguagem binária de computadores ou código criptografado - a mensagem criptografada é enviada por um canal que garante a sua recepção ao destinatário -, além do código em comum, pressupõe o contexto ou situação referencial da mensagem. Para evitar problemas que possam atrapalhar este processo de comunicação e garantir a eficácia e segurança da informação, existem atributos básicos conhecidos como os 5 pilares da segurança da informação: confidencialidade - é a garantia de que somente pessoas autorizadas terão acesso a informação; integridade – é a garantia de que a informação mantém características originais estabelecidas pelo seu proprietário, de que não foi modificada ou alterada de forma indevida; disponibilidade – é a garantia de que a informação estará pronta para o uso; autenticidade – é a garantia de que a informação vem da fonte anunciada, ou seja, de que o autor da informação é realmente quem diz ser; e irretratabilidade – é a garantia de que a pessoa não negue ter assinado ou criado a informação.

Pelo Supremo Tribunal de Justiça brasileiro passa todos os dias milhares de informações, as quais são importantes para o tribunal e para milhões de cidadãos que nele confiam para julgar seus processos e manter em sigilo todas essas informações. É preciso que essas informações sejam protegidas no nosso ambiente de trabalho. Não bastando que se tome cuidado com o tráfico de informações na rede, é necessário não deixar em cima da mesa documentos sigilosos, *pendrive* com arquivos, *cd's* com informações importantes, ou dentro de gavetas destrancadas. Os documentos sigilosos devem ser destruídos antes de serem jogados no lixo.

Empresas especializadas em segurança da informação fazem sugestões de como evitar-se o vazamento de informações. Sugerem, por exemplo, que se bloqueie ou desligue o computador sempre que nos afastemos da mesa de trabalho, evitando-se, assim, a possibilidade de alguém aceder indevidamente a informações sigilosas com a nossa senha; que não devemos escrever a nossa senha nem divulgá-la a outras pessoas, pois de outro modo corremos o risco de sermos responsabilizados por possíveis atos cometidos por essas pessoas; que troquemos de senha assim que desconfiamos que alguém a conhece, a fim de evitarmos problemas futuros; que evitemos conversas em locais públicos, pois pessoas mal intencionadas podem utilizar tais informações para prejudicar-nos pessoal ou profissionalmente; que tenhamos cuidado com as informações passadas pelo telefone, especialmente a desconhecidos, pois grande parte da quebra de informação ocorre através de ligações telefónicas; e que informações importantes devem ser trocadas por vias formais, como o *email* da organização, pois nunca se sabe quem ouve a nossa conversa.

A segurança de informação é da responsabilidade de todas as áreas e de todos os colaboradores da organização, todos sem exceção possuem deveres e responsabilidades na segurança da informação. A maior parte do vazamento de informação é realizado por pessoas sem conhecimentos na área da informática. As informações deixadas sobre a mesa, impressoras ou gavetas destrancadas são tão perigosas quanto a arquivos confidenciais.

2.9 O papel do governo brasileiro na sociedade da informação

O grande desafio do governo brasileiro é o de como melhorar o alcance de informações de toda a população brasileira. As informações não podem estar totalmente no meio digital porque nem toda a população tem acesso a esse tipo de tecnologia, mesmo havendo no Brasil 90% de domicílios com aparelhos celulares. Trata-se, aqui, de um acesso sistemático, onde qualquer cidadão pode entrar nos sites do governo - municipal, estadual ou federal - e de conhecer quais políticas públicas oferecidas pelo mesmo à sua população. O governo precisa falar a língua da população para promover a formação de hábito, o engajamento e não vai trazê-la para a esfera pública.

A utilização da tecnologia permite aumentar a visibilidade do governo, fazendo propaganda em escolas, em postos de saúde, na assistência técnica que chega até a propriedade do agricultor familiar. Por exemplo, quanto à questão de saber qual o tipo de cor da população brasileira, se antigamente o governo contratava vários pesquisadores para colectar nas ruas essa informação, hoje pode recorrer à tecnologia, dado que cadastrou a população. O sistema envia vários SMS simultâneos ou chamadas de vozes com uma voz conhecida na região em estudo e com isso aumenta a qualidade de dados, pois deste modo a amostra de população entrevistada é maior que nas entrevistas diretas e o seu custo é menor – por celular o preço é o mesmo para qualquer local do país. Deste modo, pode-se concluir que o uso da tecnologia pode melhorar progressivamente o tipo de serviços públicos.

O servidor público não está preparado para a inovação tecnológica, sendo necessário inseri-la na vida do servidor. A cultura organizacional da administração pública, tendencialmente conservadora e estagnada, paralisa o processo. Inovar é preciso, e aquilo que é novo para a administração pública não é permitido e portanto é ilegal, pois a novidade não é contemplada pela lei. Todavia, existe sempre um certo grau de discricionariedade, leis e decretos que são interpretados consoante os casos concretos e é justamente nessa interpretação de busca de novas formas que se pode ser inserida a inovação. O projecto GENOVA do laboratório de inovação e governo tem por objetivo ajudar órgãos públicos a inovarem, a partir de metodologias e novas tecnologias, mas sobretudo tentando entender quais os problemas que têm de ser solucionados e

quais experimentos que podem ser usados para resolver os problemas de forma rápida. O GENOVA procura constantemente novas formas ou um novo jeito de fazer novas políticas, de forma a resolver problemas crónicos; ou seja, assume que pensar-se de forma diferente pode ser o caminho adequado para a sua resolução.

O Brasil é um país muito heterogéneo e, por isso mesmo, uma determinada tecnologia pode ser insuficiente ao seu território. Para que não haja uma segregação de regiões é necessário a promoção de múltiplos canais, sejam analógicos ou digitais.

Capítulo 3 – Privacidade na Sociedade da Informação

3.1 Direito ao Esquecimento

Em 1931, num julgamento realizado no Tribunal da Califórnia definiu-se que uma ex-prostituta, que havia constituído família e abandonado a prostituição, tinha direito ao esquecimento em relação ao seu passado. Enquanto prostituta envolveu-se num homicídio, do qual foi ilibada em tribunal. Com o passar do tempo casou-se e, justamente, o seu marido pleiteou na corte o direito da sua mulher a esquecer aqueles fatos e que a comunidade não tomasse mais conhecimento desse caso, pois à época estava a ser divulgado um filme que citava o seu verdadeiro nome, a sua profissão e o seu envolvimento no caso criminal. Tendo em vista que a vida dela tinha tomado um rumo positivo, o tribunal concedeu-lhe o direito a ser deixada em paz, à verdade daqueles fatos serem esquecidos e, deste modo, a divulgação do filme foi proibida.

O direito ao esquecimento, ou de ser esquecido, é a possibilidade de se impedir a divulgação de informações que apesar de verídicas causem prejuízos a determinadas pessoas e, concomitantemente, pode-se afirmar que se trata do direito que tem como fundamento preservar a honra, a intimidade e a vida privada, dentre outros direitos da personalidade, das pessoas face, essencialmente, a exposições midiáticas e cibernéticas.

A sociedade está inserida num contexto de informações sem precedentes, onde o sentido da informação se perde na sua própria essência, ou seja, é o informar pelo informar. Não existe o cuidado com a imagem, privacidade, honra e intimidade do próximo, não há a capacidade de se colocar no lugar do outro. O informante não vislumbra o informado como sujeito de direitos, ele é tratado apenas como objeto da informação, tampouco se preocupa com a veiculação de notícias que possam acarretar inúmeros prejuízos à vida da pessoa humana.

No Brasil o direito ao esquecimento foi apresentado na VI Jornada de Direito Civil - no Enunciado 531, lê-se: “A tutela da dignidade da pessoa humana na sociedade da informação inclui o direito ao esquecimento“. No mesmo Enunciado é exposto que

> “Os danos provocados pelas novas tecnologias de informação vêm-se acumulando nos dias atuais. O direito ao esquecimento tem sua origem histórica no campo das condenações criminais. Surge como parcela importante do direito do ex-detento à ressocialização. Não atribui a ninguém o direito de apagar fatos ou reescrever a própria história, mas apenas assegura a possibilidade de discutir o uso que é dado aos fatos

> pretéritos, mais especificamente o modo e a finalidade com que são lembrados."

Em 2013, o STJ julgou dois casos envolvendo o direito ao esquecimento. O primeiro caso foi a chacina da candelária. O STJ definiu que gera dano moral a veiculação de programa televisivo sobre fatos ocorridos a longa data com ostensiva identificação de pessoa que tenha sido investigada, denunciada, e posteriormente inocentada. Nesse caso, um policial viu-se envolvido de forma inequívoca neste episódio, tendo sido preso e posteriormente inocentado. O programa de televisão Linha Direta da rede Globo trouxe à tona novamente esses fatos, exibindo fotos e o nome do policial após ter sido inocentado. Todavia, como acentuado pelo Ministro Luís Filipe, neste caso o STJ julgou uma tese do direito ao esquecimento em relação à televisão, mas não em relação à internet. E quando se trate do julgar o direito ao esquecimento neste âmbito os seus entendimentos jurídicos poderão ser outros.

O segundo caso foi referente a Aida Cury, uma jovem assassinada no ano de 1958. Ela foi estuprada e atirada do alto de um prédio, sob o intuito de parecer um suicídio. O caso foi repercutido em todo o Brasil. Os irmãos da vítima buscaram o direito ao esquecimento pela morte da irmã, pois o caso dela foi explorado pelo programa Linha Direta da rede Globo, e o seu pedido foi julgado improcedente. Apesar da improcedência do pedido dever-se à exibição de uma única foto de Aida, o STJ entendeu não diferir o direito ao esquecimento, dado o lapso temporal entre a sua morte e a apresentação do programa. O Ministro afirmou: "Relembrar um fato trágico a depender do tempo transcorrido, embora possa gerar um desconforto não causa o mesmo abalo de antes" (Recurso Especial, n. 1.335.153 - RJ). O programa foi exibido no final da década de 1990.

Mendes e Branco (2011, p. 321-322) explicam a questão sobre o direito ao esquecimento nos seguintes termos:

> "Por vezes, diz-se que o homem público, i. é, aquele que se pôs sob a luz da observação do público, abre mão da sua privacidade pelo só fato do seu modo de viver. Essa questão é incorreta. O que ocorre é que, vivendo ele do crédito público, estando constantemente envolvido em negócios que afetam a coletividade, é natural que em torno dele se avolume um verdadeiro interesse público, que não existiria com reação ao pacato cidadão comum. (...) Fatos desvinculados do papel social da figura pública não podem ser considerados de interesse público, não ensejando que a imprensa invada a privacidade do indivíduo".

Assim, nos espaços públicos da Sociedade da Informação todas as pessoas precisam ser protegidas, famosas ou não, para que possam ter uma vida tranquila, passageira e sem vestígios para à posteridade.

3.2 Programas de Vigilância Global

Os programas de vigilância em massa foram descobertos em 1972, quando o Analista da NSA, Perry Fellwock, revelou informações sobre fatos e organizações relacionados com a prática de espionagem e vigilância globalizada com capacidade de interceptar meios de comunicações em todo o mundo. No seguimento do 11 de Setembro e em prol da segurança nacional, o Presidente George Bush autorizou a escuta das ligações telefónicas dos americanos por parte da NSA.

Com o passar dos anos, os programas de vigilância em massa têm ficado cada vez mais robustos. Com o advento da Internet, milhões de informações são publicadas diariamente; e por conta dessa quantidade de informações produzida diariamente, foram desenvolvidos softwares capazes de processá-las de forma a proteger o mundo das possíveis ameaças terroristas.

Em 2006, o jornal *USA Today* divulgou que a NSA produzida um banco de dados das ligações telefónicas dos americanos. Os dados dessa coleta foram fornecidos pelas principais companhias telefónicas dos EUA, dentre as quais: AT&T, Verizon, etc.

Em junho de 2013, o mundo foi surpreendido com revelações acerca de um sistema de vigilância global organizado pelos EUA, através da NSA. Os documentos oficiais divulgados pelo americano Edward Snowden mostraram detalhes da atividades de vigilância da NSA sobre a privacidade dos indivíduos de todo o mundo.

3.3 Espionagem Governamental

Em *1984* George Orwell retrata uma sociedade governada por um regime político totalitário e repressivo. O enfoque recai sobre a ausência de privacidade dos cidadãos que compõem a sociedade. Nesta obra as teletelas funcionam como ecrãs de divulgação de propaganda para a assistência e, simultaneamente, como captadores de imagem ou instrumentos de espionagem. O *Big Brother* é, por sua vez, a entidade que está por trás de toda a espionagem - "Grande Irmão" é a metáfora que retrata o controlo do governo sobre a população. Um dos lemas contidos no livro é o seguinte: quem controla o passado, controla o futuro e quem controla o presente controla o passado. Já que algumas personagens do livro passam o dia a modificar os registos

históricos de jornais e livros e, com isso, a reescrever a história A história não pode ser modificada, é ela que guia os passos da humanidade - alterar fatos históricos tem consequências profundas e importantes para todo o desenvolvimento da humanidade. Por exemplo, se daqui a 100 anos os professores de história ensinarem às crianças que a Alemanha Nazista venceu a IIª Guerra Mundial, a superioridade ariana será confirmada para estas crianças.

Nós somos o que somos hoje, por tudo que acreditamos, tudo isso se deve a história que nos foi contada nos livros ou nas escolas. Hoje o grande problema é a internet, onde qualquer um pode colocar um conteúdo mentiroso e quem lê, caso seja pouco culto e acrítico, facilmente é enganado por esse tipo de conteúdo. Com isso, existe o perigo de daqui a alguns anos ninguém saber o que é verdade ou o que é mentira. O *Wikipedia* é um grande exemplo disso, pois qualquer pessoa pode editar os artigos do site e muita gente tem esse site como referência, sem procurar mais fontes de informação.

Na sociedade descrita em *1984* algumas pessoas têm as suas compras limitadas, podendo dispor somente de alguns bens de extrema necessidade e descartando os supérfluos. No mundo real a ingerência do governo na vida das pessoas através da monitoração das suas compras foi facilitada pela disseminação do uso de cartões de crédito. Hoje grande parte das transações são realizadas por meio virtual e dessa forma é mais fácil monitorar-se tudo o que o cidadão compra e vende. Os nossos dados pessoais, que antes eram confidenciais, estão cada vez mais expostos.

Estamos todos a ser controlados, como se o "Grande Irmão" soubesse tudo o que nós fazemos, e sabe. Se cada cidadão possuir alguma rede social, como por exemplo, *Facebook*, *Instagram* ou o um *email* da Google, não se engane, pois todas essas empresas gravam suas preferências, tendências, hábitos. A população está sendo vigiada constantemente.

3.3.1. Máquina Enigma

Em 1918 o engenheiro alemão Arthur Scherbius criou a Enigma. As suas primeiras aparições deram-se no Congresso da União Universal Postal de 1923 e 1924, tratando-se de uma máquina parecida à máquina de escrever e pesando pouco mais de seis quilos. O propósito inicial desta máquina era apenas comercial, mas os militares das forças armadas alemãs viram a sua utilidade no ramo militar. Em 1926 a marinha alemã comprou alguns exemplares para serem estudados e adaptados, logo em seguida o exército e a aeronáutica também adquiriram essa máquina. Após essas aquisições, a Enigma tornou-se o principal meio de comunicação secreta dos alemães, de uma nação que, reemergindo orgulhosamente após a humilhação do desfecho da Iª Guerra Mundial, dava os primeiros passos para se tornar uma grande potência no cenário mundial.

A máquina tinha uma engrenagem que gerava milhares de combinações - haviam 5 rotores numerados de 1 a 5, sendo que dentro da máquina sempre ficavam 3 rotores, cada rotor tinha 26 posições. Sempre que um botão era pressionado, cada rotor girava independentemente, recodificando cada letra de forma diferente. Usando os 3 rotores cada 1 com 26 posições, a Enigma dava 16.576 posições. Porém, a máquina ia além dos rotores, dado ter um painel de *pluges* que permitia a troca das letras criando assim uma camada extra de codificação. As combinações dos 3 rotores associados aos plugues operavam 1 sextilhão de possibilidades. Os operadoras da Enigma tinham um livro que continha uma tabela diferente para cada dia do mês e que indicava qual dos 3 rotores deveria estar na máquina naquele dia e as suas devidas posições, como também o posicionamento dos plugues. Desta forma, diariamente os operadores alteravam a configuração da Enigma. O livro era trocado mensalmente para que não houvesse repetição da criptografia. Para trocar mensagem um oficial passava a mensagem para um operador da Enigma que a digitava, uma segunda pessoa anotava as letras que apareciam no painel luminoso; por sua vez, a mensagem criptografada era passada para um operador de rádio que transcrevia a mensagem já criptografada em código *Morse*, do outro lado o receptor ouvia a mensagem e descodificava-a letra a letra e, seguidamente, digitalizava-a na máquina que, agora, iria mostrar no painel luminoso a mensagem original. O livro que recebiam era importante para que todas as máquinas tivessem a mesma encriptação ao mesmo tempo, sendo esta alterada todos os dias; assim, só sabiam os seus segredos quem estivesse autorizado a manipular a Enigma.

O matemático inglês Alan Turing trabalhava no setor de decodificação e de criptoanálise do Serviço de Inteligência Britânico quando, em sequência da declaração de guerra do Reino Unido à Alemanha Nazista, foi para a Base *Bletchley Park*, à data o Quartel-General de Comunicações Governamentais. Alan Turing e sua equipa tiveram por missão quebrar o indecifrável código da Enigma. Com esse objectivo, em 1943 projetou o Colossus, um computador que foi utilizado na IIª Guerra Mundial – esta máquina usava símbolos perfurados em fita de papel, processando a informação a uma velocidade de 25.000 caracteres por segundo. Como os códigos alemães mudavam frequentemente, o Colossus devia se adaptar constantemente de modo a tornar a decifração rápida. Depois do sucesso do Colossus em descriptografar a Enigma, os britânicos mantiveram a sua descoberta em segredo - mesmo no seio do governo, poucos foram aqueles que acederam a esta informação. Todas as mensagens descobertas pela Colossus saiam do Quartel de Comunicações com o codinome ULTRA. O serviço de inteligência britânico sabia onde e quando os nazistas iriam atacar, para não levantar muitas suspeitas, nem todos os ataques eram interceptados.

Os matemáticos passaram a influenciar quase todos os aspectos da guerra. Batalhas da Grã-Bretanha foram vencidas graças ao esforço de Turing e da sua equipa. Assustado com as repentinas baixas em algumas regiões da Europa, o alto comando nazista preferiu crer que as

suas tropas estavam a enfrentar grandes frotas, pelotões e esquadrilhas; recusando encarar a hipótese da máquina Enigma ter sido descriptografada. Quando na verdade seus passos estavam sendo vigiados pela equipa de Turing, que descriptografava cerca de 90 mil mensagens por mês. Fechada dentro de uma sala a decifrar mensagens, esta equipa mudou o rumo de inúmeras batalhas nos últimos anos da guerra.

Com o fim da IIª Guerra Mundial, o serviço de inteligência britânico recomendou a destruição de todos os arquivos e que Turing e os membros da sua equipa se separassem para sempre. A grande descoberta de Alan Turing permaneceu em segredo por mais de 50 anos, segredo que foi considerado o mais bem guardado de toda a história. Turing não recebeu nenhum tipo de homenagem pela sua descoberta, nem foi reconhecido pelo seu país como herói de guerra, pois não sobreviveu ao desvelar do segredo – morreu em 1954, dois anos após ter sido condenado por homossexualidade e submetido a castração química. Estima-se que, graças a quebra do código da Enigma, a guerra foi encurtada em 2 a 3 anos, poupando mais de 14 milhões de vida. Somente em 1975 o governo britânico reconheceu os feitos de Alan Turing e pediu desculpas públicas por tê-lo condenado.

3.3.2. Caso Edward Snowden

Especialista Análise de Sistemas, Edward Snowden (1983) trabalhou, inicialmente, numa base militar americana no Japão, onde recebeu treino como soldado das forças especiais americanas – não tendo concluído o curso devido a uma lesão. Em seguida trabalhou numa base da NSA e, posteriormente, ingressou na CIA como administrador de sistemas e técnico na área tecnologia da informação. Após alguns anos, deixou a CIA e foi contratado pela BOOZ ALLEN HAMILTON, empresa privada americana que presta serviços de consultoria para centrais de inteligência e departamentos de defesa, incluindo a NSA.

Snowden tornou público detalhes de vários programas de espionagem que constituem o Sistema de Vigilância Global. Enquanto agente que trabalhou na Dell, a *EC-Council - Council of E-Commerce Consultants* concedeu-lhe o certificado de *Hacker* Ético. Um *Hacker* Ético é alguém que testa segurança das redes e os sistemas de computadores para encontrar vulnerabilidade e fragilidades para comunicar às empresas a fim destas repararem as suas fragilidades. Nos anos iniciais da CIA e da NSA, Snowden trabalhou como *hacker* de defesa barrando possíveis ameaças aos sistemas.

Durante o período em que trabalhou na NSA, *Snowden* conseguiu gravar numa *pendrive* centenas de arquivos e resolveu compartilhá-los com o jornalista Gleen GreenWald, conhecido pelo seu trabalho de defesa das liberdades civis e respeitado como comentador político. GreenWald

morava no Rio de Janeiro e trabalhava para o jornal britânico *The Guardian*. Snowden contactou GreenWald por intermédio da cineasta Laura Power, revelando centenas de documentos e pondo a descoberto um programa de vigilância intenso sobre governos, líderes mundiais e, principalmente, usuários de toda internet. Em 2013 o jornal *The Guardian* publicou os documentos do ex-agente da NSA - entre vários documentos divulgados, os relativos ao *Prism*, projeto de vigilância global da NSA, descrevendo as suas capacidades, foram os mais detalhados. O programa *Prism* permite que os funcionários da NSA coletem dados de usuários que estão nos servidores dos serviços na internet, como históricos de pesquisas, conteúdo de e-mails, transferências de arquivos, vídeos, fotos, chamadas de voz e vídeo, detalhes de rede sociais, *login* e quaisquer outros existentes tudo é mostrado de maneira explícita e detalhada. Entre as empresas que trabalham com a NSA estão as Microsoft, Google, Yahoo, Apple, *Youtube*. Todas elas emitiram comunicados na imprensa negando qualquer envolvimento com a NSA no seu projeto *Prism*.

Sabendo dos riscos que corria após vazar documentos secretos da NSA, Snowden emitiu um comunicado, onde dizia: "estou disposto a me sacrificar porque eu não posso em sã consciência deixar que o governo dos EUA destrua a privacidade, a liberdade de internet e os direitos básicos das pessoas de todo o mundo, tudo em nome de um grande programa de vigilância que eles estão desenvolvendo."(GreenWald, 2013). Com isso Snowden tornou-se um herói, iniciando-se um série de movimentos ativistas na internet.

Muitos países foram espionados, como foram os casos da Europa Ocidental, México, Turquia, Japão, Brasil, dentre outros. No caso do Brasil, o jornal *O Globo* publicou em julho de 2013 dados coletados por Snowden que mostravam como milhões de e-mails e ligações de brasileiros e estrangeiros em trânsitos no país haviam sido monitorados. Segundo estes documentos, houve em Brasília uma estação de espionagem da NSA até 2002. Os documentos apontavam, ainda, para a possibilidade da embaixada do país em Washington e a representação do país na ONU, em Nova Iorque, terem sido monitoradas. Em setembro de 2013 foram revelados documentos de caráter exclusivo, classificados de ultra secretos, revelando que a Presidente Dilma Roussef e seus principais assessores foram alvos direto de espionagem da agência. O Brasil recebeu com grave preocupação a notícia de espionagem e, ainda em 2013, Antônio Patriota solicitou esclarecimentos aos EUA e ao embaixador americano no Brasil. O governo americano afirmou que não discutiria essas questões publicamente, mas somente através de estrutura diplomática no país. Por conta dos acontecimentos, foi instalado uma CPI – Comissão Parlamentar de Inquérito - no senado que investigaria as denúncias de espionagem pelos EUA de e-mails, telefonemas e dados digitais no Brasil. Na leitura da Presidente Dilma Roussef, os atos de espionagem dos EUA feriram o Direito Internacional e afrontaram os princípios e acordos que regem a relação dos dois países, colocando a autonomia do Brasil em risco.

A NSA emitiu um comunicado com base nas acusações de espionagem, onde sublinhou ter agido totalmente dentro da lei, mas 80 fundações e ONGs lançaram uma campanha para protestar contra o programa de vigilância online *Prism*. Elas criaram o site: http://rally.stopwatching.us - em tradução livre, "Parem de nos vigiar" - e pediram ao governo que divulgasse mais informações sobre o programa de vigilância. O Presidente Barack Obama fez questão de ressalvar que os cidadãos americanos não estavam sendo monitorados, que suas conversas telefónicas mantinham-se privadas e que pelejaria para que as medidas relativas ao monitoramento da privacidade fossem mudadas; mostrando-se, assim, preocupado com a transparência e privacidade.

Os EUA continuam a afirmar que tiveram um enorme prejuízo com o vazamento de dados e que isso colocou em risco ações contra os inimigos da América. Foram anunciadas medidas protetivas para evitar futuros vazamentos. Preventivamente, o Presidente Barak Obama ordenou que a NSA parasse de espionar ocasionalmente a sede do FMI e do Banco Mundial, mas a principal medida foi comunicada apenas em 2014, quando anunciou que as agências de inteligência iriam interromper a prática de espionar as comunicações de dezenas de líderes internacionais considerados amigos e aliados dos EUA.

3.3.3. Caso Echelon e a espionagem americana na Europa

O projeto Echelon é tão ultra-secreto que nenhum governo nele envolvido assume a sua existência. Este projeto envolve cinco países - EUA, Grã-Bretanha, Canadá, Austrália e Nova Zelândia e é liderada pela NSA. Juntos, estes países vigiam todo o mundo, ouvindo chamadas, lendo fax, e-mails, monitorando até operações de saques. Echelon foi fruto da IIª Guerra Mundial, altura em que os cinco países se reuniram para interceptar as comunicações do Japão, Alemanha e de outros inimigos, para trocarem informações e decifrar os códigos das mensagens interceptadas. Juntos decifraram códigos importantes como o PURPURA, código japonês utilizado durante a guerra.

Logo após o fim da IIª Guerra Mundial houve uma vontade de aproveitar esses conhecimentos e capacidades. A relação entre os cinco países foi formalizada em 1948, através da assinatura de um acordo sobre a partilha das informações recolhidas pelos seus serviços secretos sobre a URSS, à data o seu principal inimigo. Durante 40 anos, a URSS foi o principal alvo deste acordo. Os 5 países reuniam-se anualmente a fim de escolherem quem deveria ser investigado. Eles dividiam o mundo em blocos e cada país membro vigiava determinado bloco - por exemplo, pela sua localização, a Grã-Bretanha vigiava a Europa.

Durante anos concentraram-se em vigiar os sinais de alta frequência, como os sinais de rádio e tv, e era a NSA que interceptava essas comunicações. A captação desta informação foi facilitada

quando, na década de 70, os satélites começaram a ser usados para a comunicação de voz. Todavia, com o aumento da quantidade de informação houve a necessidade de ser mais criterioso quanto à informação relevante. Esta necessidade esteve na origem do sistema Echelon, que compartilhado pelos cinco países permitia a troca de informações secretas - analisadas pelos super computadores da época. Cada país estabelecia uma palavra chave no sistema para especificar o que era do seu interesse.

Com o fim da guerra fria, o Echelon assumiu como interesse principal a captura de informações acerca do terrorismo. Todavia, não detectou informações relativas aos atentados do 11 de setembro, nem indícios do ataque às embaixadas americanas na África oriental. O sucesso do projeto Echelon em razão do terrorismo tem sido relativo. Por muitos anos a NSA foi considerada a melhor agência de segurança nacional do mundo no ramo de interceptação - durante a guerra fria foi bem sucedida, pois conseguia vigia a URSS bem de perto e sempre que um avião descolava de uma base secreta sabia o seu destino. Contudo, esse sucesso não foi verificado contra o terrorismo. Não sendo um alvo fixo, a Al-Qaeda era diferente da URSS e os seus membros, movendo-se em várias partes do mundo, usavam meios de comunicação diversos – o email, conversas por voz, vídeo, chamadas telefónicas. Diferentemente, na época da guerra fria o único equipamento usado pela URSS foi o telefone. A NSA já vigiava o grupo Al-Qaeda desde 1990, sem grandes sucessos desde 1996, quando Osama Bin Laden resolveu mudar-se para Jerusalém, utilizando o telefone por satélite a única forma de comunicar com o mundo exterior. A NSA começou a interceptar as suas chamadas telefónicas, sabendo os número dos telefone de Bin Laden e de seus aliados ao redor do mundo. Por sua vez, os terroristas sabiam que estavam sendo gravados e começaram a falar por códigos e, consequentemente, o plano de ataque às Torres gémeas desenvolveu-se sem a NSA ter obtido qualquer informação sobre o mesmo.

No dia anterior ao 11 de setembro, duas mensagens foram interceptadas – diziam “o jogo começa amanhã” e “amanhã hora zero”. Duas frases que fora do contexto do 11 de setembro não permitiram determinar onde o atentado iria ocorrer. Depois do 11 de setembro começou uma caçada implacável a Bin Laden. A agência descobriu os esconderijos de vários aliados da Al-Qaeda e salvaram muitas vidas. O procedimento natural de proteger os informantes, as fontes e os métodos é importante para o sucesso da agência, tanto é que a população não sabe quando um ataque foi desmantelado com sucesso. Quando as informações são reveladas sobre um possível ataque, as fontes desaparecem impedindo o sucesso da operação.

Em março de 2013, o Secretário de Estado Colin Powell revelou no Congresso uma conversa telefónica de Saddam Hussein em que este ameaçava matar a próxima pessoa que falasse coisas importantes numa linha de telefone aberta - isso mostrou ao mundo o quanto a agência americana capta as informações de todo o mundo. A necessidade de se proteger as fontes dos

informantes teve uma repercussão negativa, visto que uma grande parte das comunicações interceptadas pelo projeto Echelon vem de satélites comercias que as pessoas presumem serem privadas. As conversas de pessoas inocentes acabam sendo ouvidas por algum analista da NSA.

No seguimento das primeiras informações que surgiram sobre o projeto Echelon na imprensa europeia, em meados dos anos 90, o Parlamento Europeu criou uma comissão para analisar esse projeto. Esta comissão viria a concluir que os EUA utilizava o Echelon para fazer espionagem Industrial em prol das empresas americanas. Nos relatórios do Parlamento Europeu alega-se que a NSA interceptou todos os fax e chamadas telefónicas do fabricante europeu de aviões da Airbus Linhas Aéreas da Arábia Saudita e que essa informação ajudou duas empresas americanas a assinar um contrato milionário. O que se revelou problemático não foi o sistema Echelon, mas a forma como foi utilizado. Uma coisa é proteger a população contra o terrorismo, o que faz dele um sistema válido; outra coisa é utilizá-lo para fazer espionagem industrial para favorecer as indústrias dos que nele participam, o que não é correcto e deve ser combatido. O diretor da NSA à época admitiu que interceptava informações sob o intuito económico. O Parlamento Europeu suspendeu a comissão que investigava a espionagem industrial, mas recomendou que a União Europeia criptografasse suas comunicações para que o Echelon não tivesse acesso a elas. Logo após essa recomendação, os EUA tentaram convencer as empresas europeias a fornecerem os seus códigos de segurança à NSA por motivos de segurança nacional, mas fracassaram.

O maior problema que a NSA enfrenta tem origem na revolução tecnológica marcada pelo aumento do uso de celulares e cabos de fibra ótica que servem de suporte à internet e outros meios de comunicação. A NSA foi concebida como reação a uma guerra que, à data, tinha uma único inimigo, a URSS, um estado oligárquico que evoluía lentamente. A nível mundial a quantidade de informações aumentou cerca de 800% entre os anos 1990-2000.

Após o 11 de setembro a NSA reformulou-se e passou a contar com os computadores mais rápidos do mundo, juntamente com uma equipa de profissionais altamente qualificados para ajudar a transformar milhões de metadados diários em informações relevante para o mundo. O projeto Echelon capta tudo o que no mundo é transmitido diariamente, milhões de dados são lidos através de programas de inteligência artificial, matemática avançada que é capaz de transformar milhões de informações em informações relevantes para a proteção global contra o terrorismo. Atualmente as comunicações dos inimigos baseiam-se numa evolução e indústria global que progridem com a velocidade da luz.

Capítulo 4 – Proteção de Dados Pessoais na Sociedade da Informação

4.1. Rede Social e a Proteção de Dados Pessoais

A tecnologia tem sido usada cada vez mais para violar a intimidade e dar lucro às empresas que divulgam dados pessoais. Vamos relembrar, aqui, algumas situações em que os próprios usuários colocam a sua intimidade na internet. Quantas vezes o usuário já colocou suas informações pessoais na internet sem ter controle no que, *a posteriori*, vai acontecer com elas? Quando os clientes vão a uma loja e fazem um cadastro, participam de uma promoção, utilizam um aplicativo grátis, estão automaticamente fornecendo dados pessoais, e na maioria das vezes fazem isso sem pensar. Atualmente os dados pessoais estão sendo processados e compartilhados, muitos deles sem a nossa permissão e o nosso conhecimento. As empresas descobriram que os dados dos usuários são muito lucrativos. Dados demográficos sobre tendências de compras ou preferências pessoais tornaram-se valiosos para as organizações que tentam vender seus produtos em um mercado altamente competitivo, por esta razão a indústria de dados é extremamente lucrativa.

Quando o usuário está navegando pela internet aparecem propagandas relacionadas com a sua pesquisa no mundo virtual, lugares que frequentou e o seu consumo. São esses dados pessoais que estão ajudando a personalizar as propagandas, mas resta saber se o usuário autorizou este tipo de uso ou se sabia que os seus dados viriam a ser vendidos.

O *facebook*, a rede social mais usada em todo o mundo, utiliza as informações do seu usuário - quando faz o cadastro nesta rede social, automaticamente autoriza o uso dos seus dados pessoais, pois antes de fazer o *login*, tem uma série de termos de aceitação que, uma vez anuídos pelo mesmo, autorizam esta rede social a compartilhar todas as suas informações.

Os usuários da internet precisam tomar cuidado ao exporem os seus dados, pois uma vez compartilhados ficam expostos para sempre; ou seja, os usuários não têm o direito ao esquecimento.

4.2 Legislação Europeia - Diretiva 95/46/CE

A Diretiva 95/46/CE entrou em vigor em 24 de Outubro de 1995, sendo um marco nos anos 90, onde foi estabelecido um regime geral de proteção de dados pessoais no que diz respeito ao tratamento dos dados pessoais e à livre circulação desses dados.

O objetivo da Diretiva 95/46/CE visava:

- Proteger o direito fundamental à proteção de dados;
- Assegurar a livre circulação de dados pessoais entre os Estados-Membros.

Esta Diretiva determina normas gerais sobre a legitimidade do tratamento de dados pessoais, estabelece os direitos das pessoas a quem se referem os dados e prevê a supervisão e interpretação de leis independentes; ou seja, cada Estado-membro pode usar a sua legislação nacional associada com a Diretiva 95/46 sobre a proteção de dados pessoais. A Diretiva estabelece, igualmente, que "os dados pessoais só podem ser tratados com o consentimento da pessoa em causa e caso seja informada da operação de tratamento desses dados"(Diretiva 96/46/CE, artigo 7).

A evolução tecnológica e a globalização alteraram a forma como os dados são recolhidos, acessíveis e utilizados, havendo uma necessidade de estabelecer novas disposições e matérias mais atuais referentes a proteção de dados. Além de toda essa mudança tecnológica, nos Estados-Membros da UE aplicaram as normas da Diretiva 95/46/CE de formas diferentes. Uma legislação única resolveria a atual fragmentação e os dispendiosos encargos administrativos.

No dia 25 de janeiro de 2012, a Comissão do Parlamento Europeu propôs uma reforma global da legislação relativa à proteção de dados pessoais da UE. Essa reforma visou proteger os dados pessoais na UE, aumentando o controle dos usuários sobre os seus próprios dados e reduzindo os custos para as empresas.

A Comissão do Parlamento Europeu (2012, p.171) afirmou que:

> "Uma sociedade globalizada, caracterizada por uma evolução tecnológica rápida em que o intercâmbio de informações não conhece fronteiras, é particularmente importante respeitar a esfera privada dos cidadãos. A União deve assegurar que à proteção de dados é aplicado de forma sistemática. É necessário reforçar a posição da UE em matéria de proteção dos dados pessoais no contexto de todas as políticas da União Europeia, incluindo nos domínios da aplicação da lei e da prevenção da criminalidade, bem como nas nossas relações internacionais".

4.3 Legislação Europeia - Regulamento (UE) 2016/679

Em janeiro de 2012 foi criada uma nova Proposta de Regulamento Geral sobre a Proteção de Dados Europeia visando reformar a proteção de dados na União Europeia. Ao longo de quatro anos estas medidas protetoras da sociedade europeia foram debatidas e analisadas, questionando-se, essencialmente, a sua eficiência.

Foi aprovado em fevereiro de 2016 e publicado em 27 de abril de 2016 o novo Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho Geral relativo à proteção de dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE – que é o Regulamento Geral sobre a Proteção de Dados, com aplicação em todos os Estados Membros, a partir de maio de 2018. As empresas sediadas fora da União Europeia terão de seguir o novo regulamento para serviços que prestarem à UE, onde em 2018 irá existir uma lei para a proteção de dados pessoais.

A diferença da Diretiva 95/46/CE para o Regulamento (UE) 679/2016 é que a Diretiva é adaptada para a legislação nacional – como supramencionado, cada país tem a sua própria legislação referente a proteção de dados; já com a aplicação do novo regulamento todos os países membros da UE passarão a ter uma única lei vigente em todo o território europeu.

O Regulamento (UE) 2016/679 é composto por 99 artigos – analisaremos, em seguida, apenas as principais alterações que ganharam maior visibilidade no novo regulamento:

a) Novo conceito de Dados Pessoais – "informação relativa a uma pessoa singular identificada ou identificável (titular de dados); é considerada identificável uma pessoa singular que possa ser identificada, direta ou indiretamente, em especial por referência a um identificador, como por exemplo, um nome, um número de identificação, dados de localização, identificadores por via eletrônica ou a um ou mais elementos específicos da identidade física, fisiológica, genética, mental, econômica, cultural ou social dessa pessoa singular " (Art.4 "definições" al.1), incluindo:

a.1) Definição de perfis – qualquer forma de tratamento automatizado de dados pessoais para analisar ou prever aspectos relacionados com o seu desempenho profissional, sua situação econômica, saúde, preferências pessoais, fiabilidade, comportamento, localização ou deslocações (Art.4 "definições" al.4);

a.2) Pseudo-anonimização – é o tratamento de dados pessoais que não podem ser atribuídos a uma pessoa singular identificada ou identificável (Art.4 "definições" al.7) ;

a.3) Dados biométricos – dados pessoais de um tratamento técnico específico relativo às características físicas, fisiológicas ou comportamentais de uma pessoa singular que permitam a identificação única por imagens faciais ou dados dactiloscópicos (Art.4 "definições" al.14);

a.4) Pessoa singular - pode ser associada a identificadores por via eletrônica, fornecidos pelos aparelhos, aplicações, ferramentas e protocolos, tais como: endereços IP (*internet protocol*), *cookies* ou identificação por radiofrequência (Deliberação [30]);

b) Consentimento de crianças em relação aos serviços da sociedade da informação - todos os menores de 16 anos de idade têm que ter o consentimento autorizado pelos responsáveis parentais (Art.8 "definições" al.1), podendo dispor os Estados-membros de uma idade inferior aos 16 anos, desde que não seja inferior aos 13 anos;

c) Direitos do titular dos dados - a pessoa cujo dados sejam objeto de tratamento saí com direitos reforçados que lhe conferem maior controle sobre os seus dados pessoais, mediante (Art.12 "definições" al.1)/ (Deliberação [59]) :

- exigência de um claro consentimento ao processamento de dados pessoais;
- transparência aos respectivos dados pessoais;
- direito de retificação, de apagamento e o direito de ser esquecido;
- direito de oposição, para efeitos de definição de perfis;
- direito de portabilidade dos dados de um prestador de serviço para outro;

d) Obrigações do Responsável e Subcontratante sobre os direitos do titular:

- obter previamente e provar o consentimento do titular – a necessidade de provar o consentimento do titular dos dados pessoais em todas as atividades sejam, públicas ou privadas;
- tratamento desenvolvido na pseudo-anonimização – tratamento da big Data;
- garantir o direito a ser esquecido;
- garantir o direito à portabilidade dos dados;
- garantir a privacidade por defeito (privacity by default);
- garantir a privacidade por desígnio (privacity by design);
- efetuar avaliações de impacto sobre a proteção de dados;
- garantir a proteção dos dados;
- notificar e registrar as violações de dados pessoais;

e) Notificação da Violação de Dados às autoridades e aos titulares dos dados (Art.33 e Art.40 "definições" al.j)/ (Deliberação [85]) :

- Será obrigatório comunicar as violações de dados à autoridade de controle a menos que seja improvável que apresentem riscos para os direitos e liberdades dos titulares em causa;
- A notificação deve ser feita até 72 horas após a verificação/confirmação da

falha, a menos que existam circunstâncias excepcionais justificadas;

- Se o risco for alto, os titulares em causa devem ser notificados;
- Revisões regulares e auditorias para garantir que todos os envolvidos estão aptos;

f) Direito à Portabilidade de Dados (Art.20)/(Deliberação [68]) : a portabilidade dos dados permitirá que um utilizador/cliente possa solicitar uma cópia dos seus dados pessoais, num formato utilizável por ele, e que seja transmissível por via eletrónica para outro sistema de tratamento;

g) Proteção de Dados desde a Concepção e Proteção de Dados por Defeito (Art.25)/(Deliberação [4] [78]):

- Requisitos para sistemas e processos no cumprimento e conformidade com os princípios de proteção de dados, buscando medidas técnicas e organizativas;
- A privacidade na concepção, seja no produto ou serviço, é levada em conta não só na entrega final, mas desde o início;
- Os dados só devem ser recolhidos quando necessários para cumprir os propósitos específicos do tratamento, descartando-os quando eles forem desnecessários, para proteger os direitos do titular;
- Os tratamento de dados devem ser concebidos para servir as pessoas;

h) Avaliação do impacto sobre a proteção de dados (Art.35)/(Deliberação [84]) ocorre sempre que o tratamento:

- Utilize novas tecnologias e pela sua natureza, âmbito, contexto e finalidades, for suscetível de implicar elevado risco para os direitos e liberdades dos titulares;
- For automatizado e de avaliação sistemática e completa dos aspectos pessoais, incluindo a definição de perfis;
- Seja sobre dados sensíveis ou relacionados com condenações penais e infrações;
- De controle sistemático de zonas acessíveis ao público em grande escala;

i) Avaliação do Impacto sobre a privacidade (Art.35)/(Deliberação [84]):

- Identificar a necessidade de uma avaliação de impacto sobre a privacidade;
- Descrever os fluxos de informação;
- Identificar os fluxos de privacidade e afins;
- Identificar e avaliar soluções;

- Arquivar e registrar os resultados da avaliação de impacto sobre a privacidade;
- Integrar os resultados da avaliação de impacto sobre a privacidade na revisão dos planos de projeto;

j) Responsável pela Proteção de Dados existe quando (Art.37)/(Deliberação [77]):

- Se tratem de Autoridades ou Organismos públicos;
- Todas as empresas que tenham atividades principais que consistam em operações de tratamento que, devido à sua natureza, âmbito e/ou finalidade, exijam um controle regular e sistemático dos titulares dos dados em grande escala;
- Todas as entidades que tenham operações de tratamento em grande escala de categorias especiais de dados – dados pessoais sensíveis e dados relacionados com condenações penais e infrações;

l) Funções do Encarregado da Proteção de Dados existem quando (Art.39):

- Aconselhar o responsável, subcontratante e trabalhadores a respeito das obrigações;
- Controlar a avaliação e a realização de impacto sobre a proteção de dados;
- Cooperar com as autoridades de controle – ponto de contato;
- Avaliar os riscos associados ao tratamento (natureza, âmbito, contexto e finalidades);
- Não pode ser destituído, nem penalizado internamente e tem que ter apoio e recursos;
- O regulamento não especifica as credenciais necessárias para as funções do encarregado da proteção de dados, mas exige que tenha qualidades profissionais e especialmente conhecimentos especializados de legislação e práticas de proteção de dados;

m) Conformidades (Art.37)/(Deliberação [77]):

- Especificar as obrigações gerais dos responsáveis pelo tratamento dos dados pessoais e dos que efetuam esse tratamento (subcontratantes);
- Obrigação de aplicar medidas de segurança adequadas, em função dos riscos inerentes às operações de tratamento de dados efetuadas por esses responsáveis e subcontratantes;
- Alguns casos exigem aos responsáveis pelo tratamento de dados a notificação

das violações de dados pessoais;

- Autoridades públicas e empresas que desempenhem certas operações sensíveis de tratamento de dados terão de designar o responsável pela proteção de dados;

n) Responsável e Subcontratados (Art.37)/(Deliberação [77]):

- Cooresponsabilidade;
- Conformidade interna/externa – cláusulas contratuais;
- Acordos entre clientes e fornecedores – controle mútuo;
- Maior controle e gestão de tratamento de dados com terceiros – necessidade de auditorias de conformidade;
- Transferência internacional de dados – as organizações devem estar cientes do risco de transferência de dados para países que não fazem parte da UE; Os controladores não pertencentes à UE podem precisar de nomear representantes nos casos de transferência de dados para fora do território da UE;

o) Consentimento (Art.7, "definições" al.1-4)/(Deliberação [32]):

- O consentimento do titular dos dados para o tratamento deve ser livre, específico, informado e inequívoco, e demonstrado, quer através de uma declaração ou de uma ação afirmativa e clara que significa acordo para o processamento;
- O consentimento pode ser retirado;
- O consentimento deve ser explícito para dados sensíveis;
- Ao controlador de dados é obrigatório ser capaz de demonstrar que o consentimento foi dado exigindo prova física ou digital;
- Transferência internacional de dados – as organizações devem estar cientes do risco de transferência de dados para países que não fazem parte da UE; os controladores não pertencentes à UE podem precisar de nomear representantes nos casos de transferência de dados para fora do território da UE;

p) Proteção relativa a medidas baseadas nos perfis (Art.22]): direito de não ficar sujeito às medidas que produzam efeitos na sua esfera jurídica ou que a afetem de modo significativo, tomada exclusivamente com base num tratamento automatizado de dados destinado a avaliar determinados aspectos da sua personalidade, ou de analisar ou prever, em especial, a sua capacidade profissional, situação financeira, localização, saúde, preferências pessoais,

fiabilidade e comportamentos;

q) Licitude dos Tratamentos, necessários o(a) (Art.5 e 6)/(Deliberação [50]):

- Consentimento dos titular dos dados;
- Execução de um contrato no qual o titular dos dados é parte;
- Cumprimento de uma obrigação jurídica a que o responsável pelo tratamento está sujeito;
- Defesa de interesses vitais do titular dos dados ou de outra pessoa singular;
- Exercício de funções de interesse público ou ao exercício da autoridade pública;
- Efeito de interesses legítimos prosseguidos pelo responsável pelo tratamento ou por terceiros;

r) Segurança dos Dados Pessoais (Art.32)/(Deliberação [50]):

- Registro de todas as atividades do tratamento e suporte documental, seja físico ou digital;
- Pseudo-anonimização e Cifragem;
- Capacidade de assegurar a confidencialidade, integridade, disponibilidade e resiliência permanentes dos sistemas e dos serviços de tratamento;
- Capacidade de restabelecer a disponibilidade e o acesso aos dados pessoais de forma atempada no caso de um incidente físico ou técnico;
- Processo para testar, apreciar e avaliar o regulamento e a eficácia das medidas técnicas e organizativas para garantir a segurança do tratamento;
- Avaliar o nível de segurança adequado face aos riscos de destruição, perda e alteração acidentais ou ilícitas, e a divulgação ou ao acesso não autorizados, na transmissão, conservação ou qualquer outra operação;

s) Coimas (Art. 83)/(Deliberação [148]):

- Caso de incumprimento das medidas, sejam em atividades públicas ou privadas, as sanções são elevadas : até 20.000.000,00 Euros ou, em caso de empresas até 4% da faturação anual;
- Fundamental a preparação e implementação da estratégia de segurança e proteção de dados pessoais, de modo a garantir a conformidade com o regulamento;

t) Indemnização (Art. 47 “definições” al.1.3)/(Deliberação [143] [145]):
o regulamento reconhece o direito do titular de apresentar queixa à autoridade de controle e

ação judicial contra a autoridade de controle, bem como o direito de reclamar indemnização e responsabilização do responsável pelo tratamento e subcontratante junto dos tribunais nacionais;

u) Transferência para fora da UE (Art. 83)/(Deliberação [148]):

- Estabelecimento principal (sede) – uma empresa estabelecida fora do espaço da UE e sem presença na UE, se oferecer serviços e fizer negócios que envolvam algum género de tratamento de dados pessoais – o regulamento é aplicável a esse tipo de empresa;
- Centralização (decisão única de controle para a proteção de dados) – nos casos de transfronteiras, em que haja o envolvimento de várias autoridades nacionais de controle, é tomada uma decisão única de controle que é chamada de balcão único – significa que uma empresa que tenha filiais em vários Estados-Membros só terá de tratar com a autoridade nacional responsável pela proteção de dados do Estado-Membro do seu estabelecimento principal, no caso, a sede da empresa;
- O regulamento abrange igualmente a transferência de dados pessoais para países terceiros e organizações internacionais;
- Propõe-se que a Comissão Europeia fique encarregue de avaliar o nível de proteção assegurado num determinado território ou setor de um país terceiro;
- Na ausência de uma decisão adequada da Comissão Europeia relativa a um território ou setor, a transferência de dados pessoais poderá ocorrer em casos específicos ou quando existam garantias adequadas.

Com o novo regulamento de proteção de dados da UE tem como principal objetivo atualizar e modernizar os princípios estabelecidos na Diretiva 95/46/CE, bem como reforçar os direitos dos cidadãos, proporcionando-lhes um maior controle sobre os seus dados e a garantia de que a sua vida privada continua sendo protegida na era digital.

4.4 Legislação Portuguesa sobre a Proteção de Dados Pessoais

Em Portugal o regime jurídico de proteção de dados pessoais encontra-se fundamentado na Lei n. 67/98, de 26 de outubro - Lei de Proteção de Dados Pessoais, que veio a ser substituída pela Diretiva n. 95/46/CE. Cada país europeu segue esta Diretiva, mas tem a sua própria legislação para a proteção de dados pessoais e em Portugal não é diferente - existe uma legislação

específica para determinadas áreas, como é o caso da lei que regula o tratamento de dados pessoais no contexto das redes e serviços de comunicações eletrónicas acessíveis ao público, a Lei n. 46/2012, de 29 de agosto.

O responsável por tratar questões ligadas a proteção de dados pessoais é a Comissão Nacional de Proteção de Dados (CNPD) - autoridade nacional portuguesa que controla e fiscaliza o cumprimento das disposições legais e regulamentares em matéria de proteção de dados pessoais, competindo-lhe, em especial, autorizar ou registar os tratamentos de dados pessoais e emitir pareceres sobre disposições legais ou legislação sobre a proteção de dados pessoais"(*Comissão Nacional de Proteção de Dados*).

Antes de qualquer tratamento de dados, as entidades precisam obter o consentimento do titular dos dados, exceto quando não estiver regulado em lei. As entidades podem ser pessoa física ou jurídica que registe, organize, conserve, adapte, altere, recupere, consulte, transmita ou realize qualquer tipo de operação que envolva dados pessoais. Todas as entidades públicas e privadas que tratem de dados pessoais estão sujeitas ao cumprimento de várias obrigações em matéria de privacidade, principalmente, se estes dados forem sensíveis, ou seja, se forem dados referentes ao nome, morada, email, idade, estado civil, ou então dados referentes à imagem, gravação de chamadas eletrónicas, endereços de Ip's, dados de localização ou até dados referentes a convicções religiosas, políticas e filosóficas. Todos estes dados são considerados como dados sensíveis e a sua utilização tem que ser autorizada pelo usuário. As entidades que residam ou tenham o seu estabelecimento no território português estão sujeitas às lei de proteção de dados pessoais.

Com a aprovação do novo Regulamento (UE) 2016/679 relativo à proteção de dados singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados, revogando a Diretiva 95/46/CE – que é o Regulamento Geral sobre a Proteção de Dados – e cuja aplicação nos Estados-Membros da EU entra em vigor a partir de maio de 2018, as empresas em Portugal já começaram a implementar essas novas alterações.

4.5 Regime Legal de Proteção de Dados Pessoais no Brasil

No Brasil existe o Marco Civil na Internet que regulamenta a sua utilização e estabelece a relação com a privacidade dos dados pessoais das pessoas que a utilizam. Quando o usuário baixa um aplicativo e no final da instalação aceita os termos e as condições de uso, autoriza automaticamente a utilização dos seus dados pessoais para fins comerciais.

Hoje em dia é irreversível que empresas de qualquer segmento utilizem as redes sociais e a internet como fatores de vendas, mas também as pessoas que utilizam a internet têm que consciencializar-se de que não estão sós e de que tudo o que nela façam é do conhecimento dessas empresas que estão capturando todos os seus dados, com o objetivo de redirecionar os usuários para determinados tipos de produtos que haviam pesquisados. Um dos maiores exemplos que podemos citar na atualidade é o *Facebook*, rede social que tem total acesso aos dados dos seus usuários, sejam estes fotos, vídeos, textos e etc. Os Bancos de dados de vários aplicativos estão todos interligados e conversam entre si - por exemplo, o *Uber* sabe qual o trajeto mais comum que o usuário faz e qual o melhor caminho para percorrê-lo em menos tempo.

Quando uma pessoa compra um *Smartphone*, este traz instalado uma série de aplicativos básicos que o proprietário não poderá desinstalar e que acedem às suas informações uma vez que sejam iniciados. O *Google*, o maior provedor de pesquisa do mundo, possui uma grande quantidade de aplicativos, que vão desde o entretenimento como é o caso *Youtube*, o *Maps* que é um aplicativo de navegação, o *Gmail* que é provedor de email, o Tradutor que é um aplicativo que permite a tradução em tempo real de palavras e etc; e todos os seus dados vão ser compartilhados com todos os aplicativos da *Google*.

Com todos esses aplicativos instalados no seu *Smartphone*, o usuário autoriza a utilização dos seus dados e, frequentemente, nem sabe com que tipo de aplicativos estão a ser compartilhados. Com isso uma área que está crescendo muito é a do marketing de permissão, onde parte-se da premissa que o cliente tem que começar o contrato de acordo com o que deseja e, dessa forma, evita-se o seu constrangimento em relação a determinados tipos de produto indesejáveis. No Brasil não existe qualquer tipo de punição judicial para as empresas que enviam *spams* sem permissão dos clientes.

4.5.1 Marco Civil da Internet no Brasil – Lei 12.965/14

A criação da internet provocou a ruptura em relação às limitações negociais a que as transações comerciais estavam sujeitas. Em razão disso, foi gerada uma nova forma de estruturação económica. Neste sentido, Wald (2001, p. 09) enfatiza que

> A grande ruptura do terceiro milênio consiste na criação, no reconhecimento e na generalização, no mundo inteiro, da nova economia, baseada no desenvolvimento tecnológico e na competição, mas também na globalização e na desmaterialização parcial da riqueza. E esta nova concepção da economia tem reflexos em todos os aspectos da sociedade e inclusive no direito.

Entende-se por Marco Civil da internet uma iniciativa legislativa surgida em 2009, a qual possui como principal objetivo realizar a regulamentação sobre o uso da internet no direito brasileiro, constatando-se assim uma política de Estado que deverá obedecer aos princípios e garantias expressas no texto constitucional.

A inspiração para a criação do Marco Civil da internet foi a Constituição Federal Brasileira de 1988, as convenções internacionais de direitos humanos, principalmente, o Pacto de São José da Costa Rica de 1969, as recomendações do Comité Gestor da Internet no Brasil – CGI.br e a Diretiva 95/46/CE do Parlamento Europeu, relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados.

O Marco Civil da internet foi apresentado em Agosto de 2011 pelo deputado Alessandro Molon (PT–RJ) e sancionado pela Presidente Dilma Roussef em 23 de abril de 2014, tornando a Lei de n 12.965/14, como é possível verificar no Anexo 1.

Os principais temas tratados na lei são:

a) a neutralidade da rede, princípio pelo qual o provedor de internet não poderá conceder tratamento diferenciado aos clientes que contrataram exatamente o mesmo tipo de dados, respeito ao limite de velocidade, etc - como descrito no art. 9º ao estabelecer que: "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 ". Tal princípio está previsto como diretriz a ser seguida para a utilização da internet no Brasil, tendo como diretriz a força vinculante e normativa. Segundo Oliveira (2013, *online*):

> "A princípio, o tema mais fervoroso do Marco Civil é a "neutralidade da rede", que defende a ideia de que nenhum provedor de internet poderá exercer influência no conteúdo do usuário. Por exemplo, o provedor X não poderá bloquear conteúdos da concorrência ou armazenar dados dos usuários para estratégias próprias – é permitido coletar apenas dados de conexão, e esses deverão ser apagados em um ano";

b) A proteção à vida privada dos usuários, este princípio remonta a CF no seu art.5º. A ideia no Marco Civil é a de reforçar a inviolabilidade dos dados pessoais - o que inclui os dados de conexão (números IP e que indicam o horário UTC) e os dados de acesso a aplicações de Internet, como, por exemplo, que sites têm sido visitados, que aplicativos tem sido usados, qual sua frequência, quais foram os programas e arquivos baixados, com quem o usuário interagiu;

c) A responsabilidade civil, penal e administrativa dos provedores. O Marco Civil da internet prevê essa responsabilidade no art. 12, que estabelece:

> "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, com direito a advertência; multa de 10% do faturamento do grupo econômico no Brasil no seu último exercício; suspensão temporária das atividades; proibição de exercício das atividades".

A responsabilidade civil dos provedores depende da provocação de uma das parte – neste caso, ou das vítimas ou do Poder Público, onde podemos incluir os advogados privados ou públicos, ou dos membros do Ministério Público. Os réus podem ser os próprios provedores, pessoas jurídicas, ou seus administradores. A aplicação das penas dependerá de uma decisão judicial, respeitado o devido processo legal, previsto no Código de Processo Civil.

A responsabilidade criminal é regida pelas leis penais como estabelece no Código Penal e no Código de Processo Penal. Só se admite a responsabilidade pessoal e subjetiva dos administradores de provedores que pratiquem condutas tipificadas nas leis penais, agindo como autores, coautores ou participantes.

A responsabilidade administrativa dos provedores que violam o Marco Civil está prevista no artigo 12 o qual estabelece que os provedores estão sujeitos a uma série de medidas repressivas (advertência, multas, suspensão e até proibição das atividades no território brasileiro) aplicadas pela autoridade administrativa federal competente;

d) Função social que a rede precisará de cumprir de modo a garantir a liberdade de expressão e a transmissão do conhecimento, além de impor obrigações de responsabilidade civil aos usuários e provedores. Isto dará segurança jurídica sobre a utilização da internet no direito pátrio, demonstrando-se tal fato pela imputação de responsabilidade por condutas utilizando como ferramenta a rede mundial de computadores. Como argumenta Araújo (2012, *online*):

> "As diretrizes que permeiam a atuação do Poder Público no desenvolvimento da Internet no Brasil são dispostas ao longo de nove incisos do artigo 24. Prevê a participação de vários setores da sociedade brasileira na criação de "mecanismos de governança transparentes" e a integração tecnológica dos vários "Poderes e níveis da federação" com a finalidade de acelerar a troca de informações e procedimentos. O inciso IV do referido artigo discorre sobre a recomendação de preferencialmente ser utilizado, por parte da União, Estados, Distrito Federal e Municípios, tecnologias e padrões abertos e livres. De acordo com site do PLANALTO (2011), a intenção do Capítulo IV do Marco Civil da Internet é "dar mais transparência e acessibilidade a informações públicas, de modo a estimular a participação social nas políticas públicas", e em conformidade com o inciso I, II e III do artigo 27, "promover a inclusão digital, buscar reduzir as desigualdades no acesso e uso das tecnologias da informação e comunicação e fomentar a produção e circulação de conteúdo nacional".

Sendo assim, pode-se dizer que existe uma grande preocupação estatal quanto à forma de utilização da rede mundial no Brasil, fato que pretendemos demonstrar ao longo deste capítulo e

que é sublinhado na análise de Araújo ao artigo 7º inciso XII da Lei nº 12.965/14, na qual se lê: "reforça o caráter inclusivo das tecnologias utilizadas nos portais do Poder Público, objetivando atingir o maior número de pessoas oferecendo acessibilidade independente das "capacidades físico-motoras, perceptivas, culturais e sociais", tornando simples e fácil a utilização de tais portais (Araújo, 2012, *online*).

As políticas públicas deverão ser adotadas tanto para permitir o acesso a internet como um direito próprio do exercício da cidadania, bem como o Estado deverá possibilitar a utilização da internet de forma consciente, segura e responsável conforme dicção do art. 26 da Lei em análise.

Segundo Araújo (2012, *online*), "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", conforme relatado no art. 28 da Lei n 12.965/14.

O Marco Civil da Internet soma-se ao Código Civil de 2002 (especialmente nos temas de direito da personalidade), ao Código de Defesa do Consumidor (Lei 8.078/1990), ao Estatuto da Criança e do Adolescente (Lei 8.069/1990), à Lei Anti-Racismo (Lei 7.716/1989), à Lei de Direitos Autorais (Lei 9.610/1999), à Lei de Propriedade Industrial (Lei 9.279/1996), à Lei do Sistema Brasileiro de Defesa da Concorrência (Lei 12.529/2011) e, no campo processual, à Lei de Ação Civil Pública, à Lei do Habeas Data (Lei 9.507/1997) e ao Código de Processo Civil, garantindo a tutela de direitos individuais, coletivos e difusos. Podemos dizer, assim, que o Marco Civil da Internet é uma construção social com base na necessidade de se estabelecer direitos e deveres nos assuntos referentes à mesma.

4.5.2 Projeto de Lei 5276/16

O Projeto de Lei – PL 5276/16 – *v.* anexo 2 - é resultado de uma consulta pública promovida pelo Ministério da Justiça no espaço virtual, onde a população apresentou as suas opiniões e participou no debate – consulta que ficou aberta durante 6 meses, recebendo mais de 50 mil visitas e obtendo mais de 1.100 contribuições de todo o Brasil.

Este Projeto estabelece sobre o tratamento de dados especiais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural. Essa proposta de regulamentação é considerada um complemento à Lei do Marco Civil na internet. Enquanto o Marco Civil propõe garantias constitucionais, como à liberdade de expressão, neutralidade da rede, o Projeto de Lei estabelece disposições mais específicas quanto à forma como os dados pessoais coletados podem ser tratados, armazenados e dispostos, tanto por entidades públicas quanto por entidades privadas.

Foi criada na Câmara dos Deputados uma Comissão Especial sobre Tratamento e Proteção de Dados Pessoais para tratar das suas alterações, bem como para tentar acelerar a aprovação desse projeto junto ao Congresso Nacional. Nos termos do Projeto de Lei enviado para Comissão Especial são dados sensíveis aqueles que identificam a orientação sexual, a opinião pública e religião de alguém, não podendo ser tratados. No entanto, é comum as redes sociais – onde as pessoas tendem a relacionar-se com as suas áreas de interesse e, por isso mesmo, estes dados sensíveis precisam ser preservados – fazerem essa depuração de dados.

O Projeto de Lei é composto por 56 artigos, divididos em 9 capítulos – abordaremos, seguidamente, os tópicos que dizem respeito:

a) À definição de dados sensíveis - o PL, estabelece que: "dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação, a sindicatos ou organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos" (Art. 5, inciso III, PL 5276/14). Esses dados só podem ser revelados pelo seu titular, mediante consentimento livre, informado e inequívoco (Art. 7, inciso I, PL 5276/14), ou então para o cumprimento de uma obrigação legal pelo responsável (Art. 7, inciso II, PL 5276/14), ou fornecidos pela administração pública, para o tratamento ou uso compartilhados de dados necessários à execução de políticas públicas (Art. 7, inciso III, PL 5276/14), ou para o exercício regular de direitos em processo judicial ou administrativo (Art. 7, inciso VI, PL 5276/14), ou para a proteção da vida ou da incolumidade física do titular ou de terceiro (Art. 7, inciso VII, PL 5276/14);

b) Às informações financeiras de crédito - o PL, estabelece que: "o titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos da sua personalidade". (Art. 20, PL 5276/14) - existe uma disposição similar na Diretiva Europeia de 95, no seu Art.15.1;

c) Ao tratamento de dados de crianças e adolescentes - no PL estabelece-se que: "o tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos da legislação pertinente" (Art. 14, PL 5276/14). Porém, o PL não estabelece uma regra, podendo o juiz aplicar a regra que mais se adeque às situações particulares.

A Lei norte-americana conhecida como *COPPA - Children's Online Privacy Protection Act*, de 1998 - dispõe que o tratamento da proteção de dados pessoais de crianças/adolescentes na internet tem como regra geral proibição da coleta de dados de menores de 13 anos de idade, sempre que não haja o consentimento dos pais;

d) À criação de autoridade específica para a proteção de dados – o PL estabelece que seja um Conselho Nacional vinculado ao Ministério da Justiça com poder consultivo e nacional composto por 15 membros, especializados em áreas diversas e capazes de acompanhar as mudanças da tecnologia e implementar a lei.

Com a regulamentação da privacidade, do acesso aos dados pessoais, as empresas irão ter que se adequar a essa nova regulamentação. Quando não siga estas normas, uma empresa pode sofrer diversos tipos de penalidades, inclusive, multas, suspensão ou até mesmo ter a sua licença cassada.

Uma vez aprovado, o Projeto de Lei 5276/16 trará uma legislação eficaz – simples na compreensão e na aplicação da Lei – baseada nas necessidades da sociedade contemporânea, protegendo-a efetivamente.

Considerações Finais

A privacidade é um conceito de difícil definição, pois na generalidade as diversas acepções sobre os seus limites não são unânimes, e que flui através da sociedade, sendo circunscrito pelos acontecimentos históricos. O surgimento, na jurisprudência, da privacidade coincide com momentos históricos em que houve explosão tecnológica, através da facilitação de mecanismos que permitiram um aumento dos riscos de invasão a esse direito, como aconteceu, por exemplo, com a massificação de mídia impressa, com a criação de aparelhos de escuta telefónica, com câmaras de vigilância e, mais recentemente, com as tecnologias da comunicação informática.

Mesmo que a privacidade seja protegida pelo direito jurisprudencial, é necessário criar novas leis condizentes com a realidade da sociedade tecnológica. Por exemplo, no caso do Brasil essa necessidade foi premente, visto as normas constitucionais e legais, da Constituição Federal Brasileira, estarem desfasadas da realidade encontrada nos meios tecnológicos.

O problema do Brasil, no que tange à proteção dos dados pessoais, não é a ausência de leis. Com a aprovação do Marco Civil da Internet e com o novo Projeto de Lei que o complementa, pretende-se criar leis que regulamentem tanto a Internet quanto a proteção de dados pessoais. A Constituição Federal Brasileira consagra a proteção da intimidade e da vida privada e a inviolabilidade do domicílio dentre os direitos e garantias individuais. Algumas leis disciplinam certos aspectos da proteção das informações pessoais (como são os casos, por exemplo, do Código de Defesa do Consumidor - CDC, que contém algumas regras sobre cadastros de consumo; da Lei Complementar n. 105/2001, que protege o sigilo bancário; do Código Tributário Nacional - CTN, que protege o sigilo fiscal; e da Lei 9296/96, que regula a interceptação de comunicações), embora não disponhamos de uma estrutura sistematizada e encadeada. O mais grave, no entanto, é que não há uma cultura da proteção de dados pessoais e, consequentemente, esta não é tida como relevante para o desenvolvimento da sociedade.

A preocupação dos países membros da União Europeia relativamente à protecção do direito à privacidade remonta aos anos 70, época em que começaram a editar leis e princípios de proteção a dados pessoais e, concomitantemente, criaram comissões e autoridades supervisoras para garantir efetividade a essas leis. Com a aprovação do novo Regulamento que abrange à Europa (UE) 2016/679 relativo à proteção de dados singulares no que diz respeito ao seu tratamento e à sua livre circulação, a sua aplicação será integral nos Estados-Membros da UE a partir de maio de 2018.

O novo regulamento de proteção de dados da UE tem por principal objetivo atualizar e modernizar os princípios estabelecidos na Diretiva 95/46/CE, bem como reforçar os direitos dos cidadãos, proporcionando-lhes um maior controle sobre os seus dados e a garantia de que a vida privada mantém-se protegida na era digital.

O regulamento (UE) 2016/679 traz vários desafios sobre a proteção de dados tanto para as empresas públicas ou privadas, quanto para os cidadãos. Pretende contribuir para a realização de um espaço de liberdade, segurança e justiça e de uma união económica, para o progresso económico e social. Com as principais alterações introduzidas no regulamento - como a previsão de regras para menores de 16 anos, o direito à transparência e o direito de informação e acesso a dados pessoais, o direito ao esquecimento, à portabilidade dos dados e a instituição de coimas com montantes elevados - é expectável que todas as regras sejam aplicadas e cumpridas para que o usuário tenha os seus direitos preservados.

Os profissionais de informação devem colocar um conjunto de questões éticas relacionados com a proteção de dados pessoais: até onde deve ser cumprida a Constituição em matéria de proteção da vida privada? Até onde deve ir o direito à privacidade daqueles que compram um livro, ou acessa suas redes sociais? Deve ser defendido o anonimato? A privacidade de uma pessoa é vendável? A discussão destes tópicos tem de ser considerada importante agora, e não deixada para o futuro.

As autoridades mundiais precisam passar a tratar a questão da proteção da privacidade com mais seriedade, dimensionando os direitos individuais relacionados à proteção de dados pessoais. Nesse contexto, surge um movimento maior formado por indivíduos, grupos organizados e instituições reclamando o direito de definir, segundo sua livre escolha, quando, como e em que extensão podem ser divulgadas as informações a eles referentes. Num futuro próximo, é previsível que a proteção da privacidade aumente; ou seja, que se trave uma intensa luta pelo direito de controle sobre a informação entre indivíduos, o Estado e as empresas privadas.

Constata-se que a efetividade do direito à privacidade – em especial do direito à privacidade informacional - depende de uma ação positiva por parte do Estado; ou seja, o poder público tem o dever de implementar medidas administrativas e legislativas necessárias à concretização desse direito fundamental.

A proteção da intimidade e da vida privada impõe-se como um pressuposto para o exercício da liberdade de consciência, de crença e de expressão, configura-se como uma proteção contra "ingerências alheias" que perturbem o livre desenvolvimento da personalidade, o que não veda a auto-exposição a critério do próprio titular. Sob tal aspecto, a privacidade abrange, em seu âmbito de proteção, a liberdade de divulgação de fatos íntimos, cabendo apenas à própria pessoa

o livre-arbítrio de se expor ou de não se expor e, ainda mais importante, até que limite deseja se expor, não se admitindo qualquer interferência estatal, sob pena de violação do direito do indivíduo de se autodeterminar e de tomar suas próprias decisões.

No cenário da sociedade da informação, cresce o interesse tanto dos governos quanto da iniciativa privada na privacidade das pessoas. O mercado impõe como um dos critérios para avaliação do valor de venda de corporações a quantidade de informações pessoais de que essas entidades dispõem a respeito de seus clientes; o Estado investe em poderosos bancos de dados para interconexão e processamento de informações pessoais, a fim de traçar o perfil dos cidadãos; o comportamento das pessoas torna-se cada vez mais controlado por meio de câmaras de vigilância instaladas por toda parte; as empresas incrementam os procedimentos de monitoramento das comunicações dos empregados; surgem companhias especializadas na coleta e no processamento de dados pessoais para fins de marketing e de publicidade; as agências de inteligência firmam acordos, a fim de interceptar comunicações ao redor de todo o mundo; enfim, a sociedade assume contornos de permanente controle e vigilância dos indivíduos por meio dos novos artefatos tecnológicos.

Além da exagerada coleta de informações pessoais, a intromissão na intimidade e na vida privada dos indivíduos se consuma por meio da espionagem operada pelos sistemas de inteligência. Hoje, agências de inteligência interceptam comunicações realizadas por meio de telefone, rádio e até internet; o que suscita preocupações em relação ao direito à privacidade. Os programas operados pelos EUA/UE são utilizados por agentes policiais e agentes de inteligência, escondem seus objetivos sob alegações ancoradas à necessidade de se combater a corrupção, o terrorismo, o tráfico de entorpecentes e a lavagem de dinheiro, mas o que se observa é a tentativa de se ampliar o já desmesurado poder económico dos países que os controlam, e que livremente coletam informações privilegiadas sobre transações comerciais e negociações políticas de todos os povos.

O Marco Civil da Internet no Brasil foi pioneiro na garantia de diversos direitos relacionados a internet - como a privacidade, o desenvolvimento, o acesso à internet e a neutralidade da rede. Dentro da privacidade destacam-se questões como: cláusulas contratuais claras e transparentes; consentimento prévio de uso e fornecimento de dados; quebra de sigilo das comunicações; procedimento de retirada de materiais contendo cenas de nudez e atos sexuais; mecanismos e instâncias de defesa; etc. No desenvolvimento e acesso à internet aparecem a essencialidade e qualidade do serviço de internet; suspensão de conexão; ações e programas de capacitação para o uso da internet, de forma segura, consciente e responsável; estudos e planos relacionados ao desenvolvimento e uso da internet no país, etc. Já a neutralidade da rede concerne a questões técnicas como requisitos indispensáveis para a prestação dos serviços e aplicações; a definição do

que significa dano ao usuário, etc. Constata-se, assim, uma política de Estado que, sob a alçada dos princípios e garantias expressos no texto constitucional, propõe-se beneficiar a população brasileira com melhores serviços e garantindo melhores condições de uso da internet.

Como suplemento do Marco Civil, o Projeto de Lei 5276/16 visa dar resposta às necessidades da sociedade contemporânea, protegendo-a efetivamente. As novas medidas de segurança pretendem evitar acessos não autorizados a essas informações e a garantia de que todo cidadão tenha o direito a inviolabilidade da intimidade, da vida privada, da honra e da imagem e trazendo uma legislação eficaz, simples na compreensão e na aplicação da Lei.

Referências Bibliográficas

ARENDT, Hannah. *A condição humana*. 11 ed. Rio de Janeiro: Forense Universitária, 2007.

ARISTÓTELES. *A Política*. Folha de São Paulo, 2010.

BASTOS, Celso Ribeiro; MARTINS, Ives Gandra. *Comentários à Constituição do Brasil*. São Paulo: Saraiva, 1989, vol. 2, p. 63.

BELLO, Cíntia Dal (2011). *Visibilidade, vigilância, identidade e indexação: a questão da privacidade nas redes sociais digitais, Revista LOGOS - Dossiê - O estatuto da Cibercultura no Brasil, 18* (1).

BOYD, Danah (2008). *Facebook's privacy trainwreck: Exposure, invasion and social convergence, Convergence*, 14 (1), 13-20.

CARDOSO, Gustavo *et al*. (2012). *Sociedade em Rede. A Internet em Portugal*. Lisboa: OberCom – Observatório da Comunicação.

CASTEL, Robert (1991). From Dangerious to Risk. i*n* G. Bruchell, C. Gordon e P. Miller (ed.) *The Foucault Effect: Studies in Gouvernamentality with Two Lectures and Interview with Michel Foucault* (pp. 281-298). Chicago: University of Chicago Press.

CASTELLS, Manuel. *A sociedade em rede*. A era da informação: economia, sociedade e cultura. Tradução de Roneide Venâncio Majer. 7 ed. São Paulo: Paz e Terra, 2003.

COHEN, Nicole S. (2008). *The valorization of surveillance: Towards a political economy of Facebook, Democratic Communiqué*, 22 (1), 5-22.

CONSELHO DA EUROPA. *Convenção para a Proteção dos Direitos do Homem e das Liberdades Fundamentais*. Roma. 4 de novembro de 1950. Disponível em <http://www.hrea.org/erc/Library/hrdocs/coe/echr _pt.pdf>. Acesso em: 16 de maio de 2017.

CONTI, G. e Sobiesk, E. (2007). *An honest man has nothing to fear: user perceptions on Web-based information disclosure. in Cranor LF (Ed.), Proceedings of the 3rd symposium on usable privacy and security* (pp.112-121). Pittsburgh: PA. ACM, New York.

DINIZ, Maria Helena. *Liberdade de Pensamento e Direito à Vida Privada: conflitos entre direitos da personalidade*. São Paulo: Editora Revista dos Tribunais, 2000.

DINIZ, Maria Helena. *Curso de Direito Civil brasileiro: teoria geral do direito civil*. v. 1. 25 ed. São Paulo: Saraiva, 2008.

DONEDA, Danilo Cesar Maganhoto. *Considerações iniciais sobre bancos de dados informatizados e o direito à privacidade*. In: TEPEDINO, Gustavo (org.) *Problemas de direito civil-constitucional*. Rio de Janeiro: Renovar, 2000, pp. 111-136.

DONEDA, Danilo. (2006). *Da privacidade à proteção de dados pessoais*. Rio de Janeiro, Renovar. FARIAS, Edilsom Pereira de. (1996). *Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação*. Porto Alegre, Sérgio Antônio Fabris.

DOTTI, René Ariel. *Proteção da Vida Privada e Liberdade de Informação*. São Paulo: Ed. RT, 1980.

FACEBOOK. *Facebook Q1 2016 Results*, 2016. Disponível em: <https://s21.q4cdn.com/399680738/files/doc_financials/2016/FB_Q116_Earnings_Slides.pdf>. Acesso em: 17 jun. 2017

FARIAS, Edilsom Pereira. *Colisão de direitos: a honra, a intimidade, a vida privada e a imagem versus a liberdade de expressão e informação*. 2 ed. Porto Alegre: Sérgio Antônio Fabris Editor, 2000.

GREENWALD, Glenn; MAcASKILL, Ewen; Poitras, Laura (9 de junho de 2013). *Edward Snowden: the whistleblower behind the NSA surveillance revelations. The Guardian*. London. Consultado em 6 de agosto de 201

GONÇALVES, Savigny; BARBOSA, Isabel (2011). *A privacidade da era do Facebook, ERA (Ética e Realidade Atual)*. Acessado em 2 de dezembro de 2016, de http://era.org.br/wp-content/uploads/A-Privacidade-na-era-do-*Facebook*.pdf.

HABERMAS, Jürgen. *Direito e democracia: entre facticidade e validade*. v. II. 2 ed. Rio de Janeiro: Tempo Brasileiro, 2003.

HAINZENREDER JUNIOR, Eugênio. (2007). *O direito à intimidade e à vida privada do empregado frente ao poder diretivo do empregador: o monitoramento do correio eletrônico no ambiente de trabalho*. 157f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre.

HAMMERSCHMIDT, Denise. (2008). *Intimidade genética & direito da personalidade*. Curitiba, Juruá.

JABUR, Gilberto Haddad. *Liberdade de pensamento e direito à vida privada: conflito entre direitos da personalidade*. São Paulo: RT, 2000, p. 260

LÉVY, Pierre. *Cibercultura*. Tradução de Carlos Irineu da Costa. São Paulo: 34, 1999.

LIMBERGER, Têmis. (2007). *O direito à intimidade na era da informática: a necessidade de proteção de dados pessoais*. Porto Alegre, Livraria do Advogado.

LOCKE, John. *Segundo tratado sobre o governo civil: ensaio sobre a origem, os limites e os fins verdadeiros do governo*. Petrópolis: Vozes, 1999.

LUCAS, Doglas Cesar. *Direitos Humanos e interculturalidade: um diálogo entre a igualdade e a diferença*. Unijuí: Unijuí, 2010.

MARTINS, Moisés de Lemos. *Espaço público e vida privada*. Revista Filosófica de Coimbra, 2005. p. 172. Disponível em: <www.uc.pt/fluc/dfci/publicacoes/espaco_publico_e_vida_privada>. Acesso em: 07.03.2017.

MENDES, Gilmar Ferreira. (1994). *Colisão de Direitos Fundamentais: liberdade de eexpressão e de comunicação e direito á honra e à imagem*. *Revista da Informação Legislativa*. n. 31, maio/ junho. 297-301.

MENDES, Gilmar; BRANCO, Paulo Gustavo Gonet. *Curso de Direito Constitucional*. 7 ed. São Paulo: Saraiva, 2012.

MILLER, Arhur R. (1971). *The assault in privacy: computers, data banks and dossiers*. s.l.: The University of Michigan Press.

MILL, J. S. *A liberdade/utilitarismo*. 1. ed. Martins Fontes, 2000.

NEVES, Clarissa Baeta; SAMIOS, Eva Machado Barbosa (Orgs.) *Niklas Luhmann: a nova teoria dos sistemas*. Porto Alegre: UFRGS, Goethe-Institut / ICBA, 1997.

ORWELL, George. *1984*. ed. Companhia das Letras, 2009.

ONU. *Declaração Universal dos Direitos Humanos. Resolução n. 217A (III) da Assembléia Geral das Nações Unidas*. 10 de dezembro de 1948. Disponível em <http://www.mj.gov.br /sedh/ct/legis_intern/ddh_bib_inter_universal.htm>. Acesso em: 16 de maio de 2017.

Organização dos Estados Americanos, *Convenção Americana de Direitos Humanos ("Pacto de San José de Costa Rica")*, 1969.

PANITZ, João Vicente Pandolfo. (2007). *Proteção de dados pessoais: a intimidade como núcleo do direito fundamental à privacidade e a garantia constitucional à dignidade*. 115 f. Dissertação (Mestrado em Direito) – Faculdade de Direito, Pontifícia Universidade Católica do Rio Grande do Sul, Porto Alegre.

PASQUALINI, Alexandre. (1999**).** *Hermenêutica e sistema jurídico*. Porto Alegre, Livraria do Advogado.

PIÑAR MAÑAS, José Luis. (2005). "El derecho fundamental a la protección de datos personales, algunos retos de presente y futuro". *Revista Parlamentária de La Asamblea de Madrid,* n. 13. Madri.

PIÑAR MAÑAS, José Luis. (2006). "El derecho fundamental a la protección de datos personales".

Protección de datos de caráter personal en Iberoamérica. Valencia, Tirant lo Blanch.

RAMIRO, Mônica Arenas. (2006). *El derecho fundamental a la protección de datos personales em Europa*. Valencia, Tirant to Blanch. RODOTÁ, Stefano. (2008). *A vida na sociedade de vigilância: a privacidade hoje*. Rio de Janeiro, Renovar.

RECURSO ESPECIAL No 1.335.153 - RJ (2011/0057428-0)

ROCHA, F. *Espionagem e Internet*. Caderno Aslegis, v. 49, 2015.

RUARO, Regina Linden. (2007), *O conteúdo essencial dos direitos fundamentais à intimidade e à vida privada na relação de emprego: o monitoramento do correio eletrônico pelo empregador*. In: SARLET, I.W. (Org.). *Direitos fundamentais, informática e comunicação: algumas aproximações*. Porto Alegre, Livraria do Advogado. v. 1, cap. 9.

RUARO, Regina Linden. (2007). *Responsabilidade Civil do estado por dano Moral em Caso de Má Utilização de Dados Pessoais. Direitos Fundamentais e Justiça*, n. 1 – out./dez.

ROUSSEAU, Jean-Jacques. *Do contrato social: princípios do direito político*. Trad. Antonio de Pádua Danesi. 4 ed. São Paulo: Martins Fontes, 2006.

SARLET, Ingo Wolfgang. (2010). *A eficácia dos direitos fundamentais*. Porto Alegre, Livraria do Globo.

SCHOPENHAUER, Arthur. *O Mundo como Vontade e Representação*. Rio de Janeiro: Contraponto, 2001.

SILVA, José Afonso da. *Curso de direito constitucional positivo*. 35. ed. São Paulo: Malheiros, 2012.

Superior Tribunal de Justiça - 4ª Turma - Resp. 74.473 - Rel. Min. Sálvio de Figueiredo Teixeira - j. 23.02.1999 - RSTJ 122/303.

TOFFLER, Alvin. *A terceira onda*. 23 ed. São Paulo: Record, 1998.

UNIÃO EUROPÉIA. Diretiva 2002/58 CE, de 12 de dezembro de 2002. *Relativa ao tratamento de dados pessoais e à protecção da privacidade no sector das comunicações electrónicas (Directiva relativa à privacidade e às comunicações electrónicas)*. Diário Oficial das Comunidades Europeias, Bruxelas, 31 jul. 2002. Disponível em: <http://eur- lex.europa.eu/pt/index.htm>. Acesso em: 07.03.2017.

WARREN; BRANDEIS. *The Right to Privacy*. In Havard Law Review, Vol IV, Dezembro 15, 1890, Nº 5.

Anexos

Anexo 1 – Marco Civil da Internet

LEI Nº 12.965, DE 23 DE ABRIL DE 2014[20]

(Marco Civil da Internet)

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;

20 Publicada no *Diário Oficial da União*, Seção 1, de 24 de abril de 2014, p. 1.

V – preservação da estabilidade, segurança e funcionalidade da rede, por meio de medidas técnicas compatíveis com os padrões internacionais e pelo estímulo ao uso de boas práticas;
VI – responsabilização dos agentes de acordo com suas atividades, nos termos da lei;
VII – preservação da natureza participativa da rede;
VIII – liberdade dos modelos de negócios promovidos na internet, desde que não conflitem com os demais princípios estabelecidos nesta lei.
Parágrafo único. Os princípios expressos nesta lei não excluem outros previstos no ordenamento jurídico pátrio relacionados à matéria ou nos tratados internacionais em que a República Federativa do Brasil seja parte.

Art. 4º A disciplina do uso da internet no Brasil tem por objetivo a promoção:
I – do direito de acesso à internet a todos;
II – do acesso à informação, ao conhecimento e à participação na vida cultural e na condução dos assuntos públicos;
III – da inovação e do fomento à ampla difusão de novas tecnologias e modelos de uso e acesso; e
IV – da adesão a padrões tecnológicos abertos que permitam a comunicação, a acessibilidade e a interoperabilidade entre aplicações e bases de dados.

Art. 5º Para os efeitos desta lei, considera-se:
I – internet: o sistema constituído do conjunto de protocolos lógicos, estruturado em escala mundial para uso público e irrestrito, com a finalidade de possibilitar a comunicação de dados entre terminais por meio de diferentes redes;
II – terminal: o computador ou qualquer dispositivo que se conecte à internet;
III – endereço de protocolo de internet (endereço IP): o código atribuído a um terminal de uma rede para permitir sua identificação, definido segundo parâmetros internacionais;
IV – administrador de sistema autônomo: a pessoa física ou jurídica que administra blocos de endereço IP específicos e o respectivo sistema autônomo de roteamento, devidamente cadastrada no ente nacional responsável pelo registro e distribuição de endereços IP geograficamente referentes ao país;
V – conexão à internet: a habilitação de um terminal para envio e recebimento de pacotes de dados pela internet, mediante a atribuição ou autenticação de um endereço IP;

VI – registro de conexão: o conjunto de informações referentes à data e hora de início e término de uma conexão à internet, sua duração e o endereço IP utilizado pelo terminal para o envio e recebimento de pacotes de dados;
VII – aplicações de internet: o conjunto de funcionalidades que podem ser acessadas por meio de um terminal conectado à internet; e
VIII – registros de acesso a aplicações de internet: o conjunto de informações referentes à data e hora de uso de uma determinada aplicação de internet a partir de um determinado endereço IP.

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

CAPÍTULO II
DOS DIREITOS E GARANTIAS DOS USUÁRIOS

Art. 7º O acesso à internet é essencial ao exercício da cidadania, e ao usuário são assegurados os seguintes direitos:
I – inviolabilidade da intimidade e da vida privada, sua proteção e indenização pelo dano material ou moral decorrente de sua violação;
II – inviolabilidade e sigilo do fluxo de suas comunicações pela internet, salvo por ordem judicial, na forma da lei;
III – inviolabilidade e sigilo de suas comunicações privadas armazenadas, salvo por ordem judicial;
IV – não suspensão da conexão à internet, salvo por débito diretamente decorrente de sua utilização;
V – manutenção da qualidade contratada da conexão à internet;
VI – informações claras e completas constantes dos contratos de prestação de serviços, com detalhamento sobre o regime de proteção aos registros de conexão e aos registros de acesso a aplicações de internet, bem como sobre práticas de gerenciamento da rede que possam afetar sua qualidade;
VII – não fornecimento a terceiros de seus dados pessoais, inclusive registros de conexão, e de acesso a aplicações de internet, salvo mediante consentimento livre, expresso e informado ou nas hipóteses previstas em lei;
VIII – informações claras e completas sobre coleta, uso, armazenamento, tratamento e proteção de seus dados pessoais, que somente poderão ser utilizados para finalidades que:

a) justifiquem sua coleta;
b) não sejam vedadas pela legislação; e
c) estejam especificadas nos contratos de prestação de serviços ou em termos de uso de aplicações de internet;

IX – consentimento expresso sobre coleta, uso, armazenamento e tratamento de dados pessoais, que deverá ocorrer de forma destacada das demais cláusulas contratuais;
X – exclusão definitiva dos dados pessoais que tiver fornecido a determinada aplicação de internet, a seu requerimento, ao término da relação entre as partes, ressalvadas as hipóteses de guarda obrigatória de registros previstas nesta lei;
XI – publicidade e clareza de eventuais políticas de uso dos provedores de conexão à internet e de aplicações de internet;
XII – acessibilidade, consideradas as características físico-motoras, perceptivas, sensoriais, intelectuais e mentais do usuário, nos termos da lei; e
XIII – aplicação das normas de proteção e defesa do consumidor nas relações de consumo realizadas na internet.

Art. 8º A garantia do direito à privacidade e à liberdade de expressão nas comunicações é condição para o pleno exercício do direito de acesso à internet.
Parágrafo único. São nulas de pleno direito as cláusulas contratuais que violem o disposto no *caput*, tais como aquelas que:
I – impliquem ofensa à inviolabilidade e ao sigilo das comunicações privadas, pela internet; ou
II – em contrato de adesão, não ofereçam como alternativa ao contratante a adoção do foro brasileiro para solução de controvérsias decorrentes de serviços prestados no Brasil.

CAPÍTULO III
DA PROVISÃO DE CONEXÃO E DE APLICAÇÕES DE INTERNET

Seção I
Da Neutralidade de Rede

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

§ 1º A discriminação ou degradação do tráfego será regulamentada nos termos das atribuições privativas do presidente da República previstas no inciso IV do art. 84 da Constituição Federal, para a fiel execução desta lei, ouvidos o Comitê Gestor da Internet e a Agência Nacional de Telecomunicações, e somente poderá decorrer de:
I – requisitos técnicos indispensáveis à prestação adequada dos serviços e aplicações; e
II – priorização de serviços de emergência.
§ 2º Na hipótese de discriminação ou degradação do tráfego prevista no § 1º, o responsável mencionado no *caput* deve:
I – abster-se de causar dano aos usuários, na forma do art. 927 da Lei nº 10.406, de 10 de janeiro de 2002 (Código Civil);
II – agir com proporcionalidade, transparência e isonomia;
III – informar previamente de modo transparente, claro e suficientemente descritivo aos seus usuários sobre as práticas de gerenciamento e mitigação de tráfego adotadas, inclusive as relacionadas à segurança da rede; e
IV – oferecer serviços em condições comerciais não discriminatórias e abster-se de praticar condutas anticoncorrenciais.
§ 3º Na provisão de conexão à internet, onerosa ou gratuita, bem como na transmissão, comutação ou roteamento, é vedado bloquear, monitorar, filtrar ou analisar o conteúdo dos pacotes de dados, respeitado o disposto neste artigo.

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

Art. 10. A guarda e a disponibilização dos registros de conexão e de acesso a aplicações de internet de que trata esta lei, bem como de dados pessoais e do conteúdo de comunicações privadas, devem atender à preservação da intimidade, da vida privada, da honra e da imagem das partes direta ou indiretamente envolvidas.
§ 1º O provedor responsável pela guarda somente será obrigado a disponibilizar os registros mencionados no *caput*, de forma autônoma ou associados a dados pessoais ou a outras informações que possam contribuir para a identificação do usuário ou do terminal, mediante ordem judicial, na forma do disposto na Seção IV deste capítulo, respeitado o disposto no art. 7º.

§ 2º O conteúdo das comunicações privadas somente poderá ser disponibilizado mediante ordem judicial, nas hipóteses e na forma que a lei estabelecer, respeitado o disposto nos incisos II e III do art. 7º.
§ 3º O disposto no *caput* não impede o acesso aos dados cadastrais que informem qualificação pessoal, filiação e endereço, na forma da lei, pelas autoridades administrativas que detenham competência legal para a sua requisição.
§ 4º As medidas e os procedimentos de segurança e de sigilo devem ser informados pelo responsável pela provisão de serviços de forma clara e atender a padrões definidos em regulamento, respeitado seu direito de confidencialidade quanto a segredos empresariais.

Art. 11. Em qualquer operação de coleta, armazenamento, guarda e tratamento de registros, de dados pessoais ou de comunicações por provedores de conexão e de aplicações de internet em que pelo menos um desses atos ocorra em território nacional, deverão ser obrigatoriamente respeitados a legislação brasileira e os direitos à privacidade, à proteção dos dados pessoais e ao sigilo das comunicações privadas e dos registros.
§ 1º O disposto no *caput* aplica-se aos dados coletados em território nacional e ao conteúdo das comunicações, desde que pelo menos um dos terminais esteja localizado no Brasil.
§ 2º O disposto no *caput* aplica-se mesmo que as atividades sejam realizadas por pessoa jurídica sediada no exterior, desde que oferte serviço ao público brasileiro ou pelo menos uma integrante do mesmo grupo econômico possua estabelecimento no Brasil.
§ 3º Os provedores de conexão e de aplicações de internet deverão prestar, na forma da regulamentação, informações que permitam a verificação quanto ao cumprimento da legislação brasileira referente à coleta, à guarda, ao armazenamento ou ao tratamento de dados, bem como quanto ao respeito à privacidade e ao sigilo de comunicações.
§ 4º Decreto regulamentará o procedimento para apuração de infrações ao disposto neste artigo.

Art. 12. Sem prejuízo das demais sanções cíveis, criminais ou administrativas, as infrações às normas previstas nos arts. 10 e 11 ficam sujeitas, conforme o caso, às seguintes sanções, aplicadas de forma isolada ou cumulativa:
I – advertência, com indicação de prazo para adoção de medidas corretivas;
II – multa de até 10% (dez por cento) do faturamento do grupo econômico no Brasil no seu último exercício, excluídos os tributos, considerados a

condição econômica do infrator e o princípio da proporcionalidade entre a gravidade da falta e a intensidade da sanção;
III – suspensão temporária das atividades que envolvam os atos previstos no art. 11; ou
IV – proibição de exercício das atividades que envolvam os atos previstos no art. 11.
Parágrafo único. Tratando-se de empresa estrangeira, responde solidariamente pelo pagamento da multa de que trata o *caput* sua filial, sucursal, escritório ou estabelecimento situado no país.

Subseção I
Da Guarda de Registros de Conexão

Art. 13. Na provisão de conexão à internet, cabe ao administrador de sistema autônomo respectivo o dever de manter os registros de conexão, sob sigilo, em ambiente controlado e de segurança, pelo prazo de um ano, nos termos do regulamento.
§ 1º A responsabilidade pela manutenção dos registros de conexão não poderá ser transferida a terceiros.
§ 2º A autoridade policial ou administrativa ou o Ministério Público poderá requerer cautelarmente que os registros de conexão sejam guardados por prazo superior ao previsto no *caput*.
§ 3º Na hipótese do § 2º, a autoridade requerente terá o prazo de 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 seis meses, nos termos do regulamento.
§ 1º Ordem judicial poderá obrigar, por tempo certo, os provedores de aplicações de internet que não estão sujeitos ao disposto no *caput* a guardarem registros de acesso a aplicações de internet, desde que se trate de registros relativos a fatos específicos em período determinado.
§ 2º A autoridade policial ou administrativa ou o Ministério Público poderão requerer cautelarmente a qualquer provedor de aplicações de internet que os registros de acesso a aplicações de internet sejam guardados, inclusive por prazo superior ao previsto no *caput*, observado o disposto nos §§ 3º e 4º do art. 13.
§ 3º Em qualquer hipótese, a disponibilização ao requerente dos registros de que trata este artigo deverá ser precedida de autorização judicial, conforme disposto na Seção IV deste capítulo.
§ 4º Na aplicação de sanções pelo descumprimento ao disposto neste artigo, serão considerados a natureza e a gravidade da infração, os danos dela resultantes, eventual vantagem auferida pelo infrator, as circunstâncias agravantes, os antecedentes do infrator e a reincidência.

Art. 16. Na provisão de aplicações de internet, onerosa ou gratuita, é vedada a guarda:
I – dos registros de acesso a outras aplicações de internet sem que o titular dos dados tenha consentido previamente, respeitado o disposto no art. 7º; ou
II – de dados pessoais que sejam excessivos em relação à finalidade para a qual foi dado consentimento pelo seu titular.

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

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

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

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

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

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

vistos 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 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

Anexo 2 – Projeto de Lei 5276/2016

CÂMARA DOS DEPUTADOS

*PROJETO DE LEI N.º 5.276-A, DE 2016

(Do Poder Executivo)

Mensagem nº 255/2016
Aviso nº 291/2016 - C. Civil

Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

DESPACHO:
ÀS COMISSÕES DE:
CIÊNCIA E TECNOLOGIA, COMUNICAÇÃO E INFORMÁTICA; TRABALHO, DE ADMINISTRAÇÃO E SERVIÇO PÚBLICO; E CONSTITUIÇÃO E JUSTIÇA E DE CIDADANIA (MÉRITO E ART. 54 DO RICD).

APRECIAÇÃO:
Proposição Sujeita à Apreciação do Plenário

S U M Á R I O

(*) Atualizado em 06/07/2016 em virtude da apresentação da MSC 372/16

PROJETO DE LEI 5276/2016

Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

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 dispõe sobre o tratamento de dados pessoais por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Art. 2º A disciplina da proteção de dados pessoais tem como fundamento o respeito à privacidade e:

I - a autodeterminação informativa;

II - a liberdade de expressão, de comunicação e de opinião;

III - a inviolabilidade da intimidade, da vida privada, da honra e da imagem;

IV - o desenvolvimento econômico e tecnológico; e

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

Art. 3º Esta Lei aplica-se a qualquer operação de tratamento realizada por pessoa natural ou por pessoa jurídica de direito público ou privado, independentemente do país de sua sede ou do país onde estejam localizados os dados, desde que:

I - a operação de tratamento seja realizada no território nacional;

II - a atividade de tratamento tenha por objetivo a oferta ou o fornecimento de bens ou serviços ou o tratamento de dados de indivíduos localizados no território nacional; ou

III - os dados pessoais objeto do tratamento tenham sido coletados no território nacional.

Parágrafo único. Consideram-se coletados no território nacional os dados pessoais cujo titular nele se encontre no momento da coleta.

Art. 4º Esta Lei não se aplica ao tratamento de dados:

I - realizado por pessoa natural para fins exclusivamente pessoais;

II - realizado para fins exclusivamente jornalísticos, artísticos, literários ou acadêmicos; ou

III - realizado para fins exclusivos de segurança pública, de defesa nacional, de segurança do Estado ou de atividades de investigação e repressão de infrações penais.

§ 1º O tratamento de dados pessoais previsto no inciso III será regido por legislação específica, observados os princípios gerais de proteção e os direitos do titular previstos nesta Lei.

§ 2º É vedado o tratamento dos dados a que se refere o inciso III por pessoa de direito privado, exceto em procedimentos sob tutela de pessoa jurídica de direito público, que serão objeto de informe específico ao órgão competente.

§ 3º O órgão competente emitirá opiniões técnicas ou recomendações referentes às exceções previstas nos incisos II e III e poderá solicitar aos responsáveis relatórios de impacto à privacidade.

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

I - dado pessoal: dado relacionado à pessoa natural identificada ou identificável, inclusive números identificativos, dados locacionais ou identificadores eletrônicos quando estes estiverem relacionados a uma pessoa;

II - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento, armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração;

III - dados sensíveis: dados pessoais sobre a origem racial ou étnica, as convicções religiosas, as opiniões políticas, a filiação a sindicatos ou a organizações de caráter religioso, filosófico ou político, dados referentes à saúde ou à vida sexual e dados genéticos ou biométricos;

IV - dados anonimizados: dados relativos a um titular que não possa ser identificado;

V - banco de dados: conjunto estruturado de dados pessoais, localizado em um ou em vários locais, em suporte eletrônico ou físico;

VI - titular: a pessoa natural a quem se referem os dados pessoais que são objeto de tratamento;

VII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada;

VIII - responsável: a pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais;

IX - operador: a pessoa natural ou jurídica, de direito público ou privado, que realiza tratamento de dados pessoais em nome do responsável;

X - encarregado: pessoa natural, indicada pelo responsável, que atua como canal de comunicação perante os titulares e o órgão competente;

XI - transferência internacional de dados: transferência de dados pessoais para um país

estrangeiro;

XII - anonimização: qualquer procedimento por meio do qual um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo;

XIII - bloqueio: guarda do dado pessoal ou do banco de dados com a suspensão temporária de qualquer operação de tratamento;

XIV - eliminação: exclusão definitiva de dado ou de conjunto de dados armazenados em banco de dados, independente do procedimento empregado; e

XV - uso compartilhado de dados: a comunicação, a difusão, a transferência internacional, a interconexão de dados pessoais ou o tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos, no cumprimento de suas competências legais, ou entre órgãos e entidades públicos e entes privados, com autorização específica, para uma ou mais modalidades de tratamento delegados por esses entes públicos.

Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:

I - finalidade: pelo qual o tratamento deve ser realizado para finalidades legítimas, específicas, explícitas e informadas ao titular, não podendo ser tratados posteriormente de forma incompatível com essas finalidades;

II - adequação: pelo qual o tratamento deve ser compatível com as suas finalidades e com as legítimas expectativas do titular, de acordo com o contexto do tratamento;

III - necessidade: pelo qual o tratamento deve se limitar ao mínimo necessário para a realização das suas finalidades, abrangendo dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;

IV - livre acesso: pelo qual deve ser garantida aos titulares consulta facilitada e gratuita sobre as modalidades de tratamento e sobre a integralidade dos seus dados pessoais;

V - qualidade dos dados: pelo qual devem ser garantidas aos titulares a exatidão, a clareza, relevância e a atualização dos dados, de acordo com a periodicidade necessária para o cumprimento da finalidade de seu tratamento;

VI - transparência: pelo qual devem ser garantidas aos titulares informações claras, adequadas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento;

VII - segurança: pelo qual devem ser utilizadas medidas técnicas e administrativas constantemente atualizadas, proporcionais à natureza das informações tratadas e aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;

VIII - prevenção: pelo qual devem ser adotadas medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais; e

IX - não discriminação: pelo qual o tratamento não pode ser realizado para fins discriminatórios.

CAPÍTULO II

REQUISITOS PARA O TRATAMENTO DE DADOS PESSOAIS

Seção I

Requisitos para o tratamento

Art 7º O tratamento de dados pessoais somente poderá ser realizado nas seguintes hipóteses:

I - mediante o fornecimento pelo titular de consentimento livre, informado e inequívoco;

II - para o cumprimento de uma obrigação legal pelo responsável;

III - pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis ou regulamentos;

IV - para a realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais;

V - quando necessário para a execução de um contrato ou de procedimentos preliminares relacionados a um contrato do qual é parte o titular, a pedido do titular dos dados;

VI - para o exercício regular de direitos em processo judicial ou administrativo;

VII - para a proteção da vida ou da incolumidade física do titular ou de terceiro;

VIII - para a tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias;

IX - quando necessário para atender aos interesses legítimos do responsável ou de terceiro, exceto no caso de prevalecerem interesses ou direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais, em especial se o titular for menor de idade.

§ 1º Nos casos de aplicação do disposto nos incisos II e III, o responsável deverá informar ao titular as hipóteses em que será admitido o tratamento de seus dados.

§ 2º A forma de disponibilização das informações previstas no parágrafo anterior e no art. 24 poderá ser especificada pelo órgão competente.

§ 3º No caso de descumprimento do disposto no § 1º, o operador ou o responsável pelo tratamento de dados poderá ser responsabilizado.

§ 4º O tratamento de dados pessoais cujo acesso é público deve ser realizado de acordo com esta Lei, considerados a finalidade, a boa-fé e o interesse público que justificaram a sua disponibilização.

Art. 8º O titular deverá ter acesso facilitado às informações sobre o tratamento de seus dados, que deverão ser disponibilizadas de forma clara, adequada e ostensiva sobre, entre outros:

I - finalidade específica do tratamento;

II - forma e duração do tratamento;

III - identificação do responsável;

IV - informações de contato do responsável;

V - sujeitos ou categorias de sujeitos para os quais os dados podem ser comunicados e o âmbito de sua difusão;

VI - responsabilidades dos agentes que realizarão o tratamento; e

VII - direitos do titular, com menção explícita à possibilidade de:

a) acessar os dados, retificá-los ou revogar o consentimento, por procedimento gratuito e facilitado;

b) denunciar ao órgão competente o descumprimento de disposições desta Lei; e

c) não fornecer o consentimento, na hipótese em que o consentimento é requerido, mediante o fornecimento de informações sobre as consequências da negativa.

§ 1º Na hipótese em que o consentimento é requerido, este será considerado nulo caso as informações fornecidas ao titular tenham conteúdo enganoso ou não tenham sido apresentadas previamente de forma clara, adequada e ostensiva.

§ 2º Em caso de alteração de informação referida no inciso IV do **caput**, o responsável deverá comunicar ao titular as informações de contato atualizadas.

§ 3º Nas atividades que importem em coleta continuada de dados pessoais, o titular deverá ser informado periodicamente sobre as principais características do tratamento, nos termos definidos pelo órgão competente.

§ 4º Quando o consentimento para o tratamento de dados pessoais for condição para o fornecimento de produto ou de serviço ou para o exercício de direito, o titular será informado com destaque sobre tal fato e sobre os meios pelos quais poderá exercer controle sobre o tratamento de seus dados.

§ 5º O órgão competente poderá dispor sobre os meios referidos no § 4º.

Art. 9º O consentimento previsto no art. 7º, inciso I, deverá ser livre, informado e inequívoco e fornecido por escrito ou por qualquer outro meio que o certifique.

§ 1º Caso o consentimento seja fornecido por escrito, este deverá ser fornecido em cláusula destacada das demais cláusulas contratuais.

§ 2º Cabe ao responsável o ônus da prova de que o consentimento foi obtido em conformidade com o disposto nesta Lei.

§ 3º É vedado o tratamento de dados pessoais quando o consentimento tenha sido obtido mediante erro, dolo, coação, estado de perigo ou simulação.

§ 4º O consentimento deverá se referir a finalidades determinadas, sendo nulas as autorizações genéricas para o tratamento de dados pessoais.

§ 5º O consentimento pode ser revogado a qualquer momento, mediante manifestação expressa do titular.

§ 6º Em caso de alteração de informação referida nos incisos I, II, III ou V do art. 8º, o responsável deverá obter novo consentimento do titular, após destacar de forma específica o teor das alterações.

§ 7º O órgão competente poderá adequar os requisitos para o consentimento, considerado o contexto em que é fornecido e a natureza dos dados pessoais fornecidos.

Art. 10. O legítimo interesse do responsável somente poderá fundamentar um tratamento de dados pessoais quando necessário e baseado em uma situação concreta, respeitados os direitos e liberdades fundamentais do titular.

§ 1º O legítimo interesse deverá contemplar as legítimas expectativas do titular quanto ao tratamento de seus dados, de acordo com o disposto no art. 6º, inciso II.

§ 2º O responsável deverá adotar medidas para garantir a transparência do tratamento de dados baseado no seu legítimo interesse, devendo fornecer aos titulares mecanismos eficazes para que possam manifestar sua oposição ao tratamento de dados pessoais.

§ 3º Quando o tratamento for baseado no legítimo interesse do responsável, somente os dados pessoais estritamente necessários para a finalidade pretendida poderão ser tratados, devendo ser anonimizados sempre que compatível com a finalidade do tratamento.

§ 4º O órgão competente poderá solicitar ao responsável relatório de impacto à privacidade quando o tratamento tiver como fundamento o seu interesse legítimo.

Art. 11. É vedado o tratamento de dados pessoais sensíveis, exceto:

I - com fornecimento de consentimento livre, inequívoco, informado, expresso e específico pelo titular:

a) mediante manifestação própria, distinta da manifestação de consentimento relativa a outros dados pessoais; e

b) com informação prévia e específica sobre a natureza sensível dos dados a serem tratados, com alerta quanto aos riscos envolvidos no seu tratamento.

II - sem fornecimento de consentimento do titular, nas hipóteses em que for indispensável para:

a) cumprimento de uma obrigação legal pelo responsável;

b) tratamento e uso compartilhado de dados necessários à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos;

c) realização de pesquisa histórica, científica ou estatística, garantida, sempre que possível, a anonimização dos dados pessoais sensíveis;

d) exercício regular de direitos em processo judicial ou administrativo;

e) proteção da vida ou da incolumidade física do titular ou de terceiro; ou

f) tutela da saúde, com procedimento realizado por profissionais da área da saúde ou por entidades sanitárias.

§ 1º Aplica-se o disposto neste artigo a qualquer tratamento de dados pessoais capaz de revelar dados pessoais sensíveis.

§ 2º O tratamento de dados pessoais sensíveis não poderá ser realizado em detrimento do titular, ressalvado o disposto em legislação específica.

§ 3º O disposto na alínea "c" do inciso II não se aplica caso as atividades de pesquisa estejam vinculadas a qualquer das seguintes atividades:

I - comercial;

II - de administração pública, quando a pesquisa não for a atividade principal ou legalmente estabelecida do órgão; ou

III - relativa à investigação criminal ou inteligência,

§ 4º Nas hipóteses do parágrafo anterior, sempre que possível, será garantida a anonimização dos dados pessoais.

§ 5º Nos casos de aplicação do disposto nas alíneas "a" e "b" do inciso II pelos órgãos e pelas entidades públicas, será dada publicidade à referida dispensa de consentimento, nos termos do art. 24.

Art. 12. O órgão competente poderá estabelecer medidas adicionais de segurança e de proteção aos dados pessoais sensíveis, que deverão ser adotadas pelo responsável ou por outros agentes do tratamento, ou solicitar a apresentação de relatório de impacto à privacidade.

Art. 13. Os dados anonimizados serão considerados dados pessoais, para os fins desta Lei, quando o processo de anonimização ao qual foram submetidos for revertido ou quando, com esforços razoáveis, puder ser revertido.

§ 1º Poderão ser igualmente considerados como dados pessoais, para os fins desta Lei, dados utilizados para a formação do perfil comportamental de uma determinada pessoa natural, ainda que não identificada.

§ 2º O órgão competente poderá dispor sobre padrões e técnicas utilizadas em processos de anonimização e realizar verificações acerca de sua segurança.

§ 3º O compartilhamento e o uso que se faz de dados anonimizados deve ser objeto de publicidade e de transparência, sem prejuízo do órgão competente poder solicitar ao responsável relatório de impacto à privacidade referente aos riscos de reversão do processo de anonimização e demais aspectos de seu tratamento.

Art. 14. O tratamento de dados pessoais de crianças e de adolescentes deverá ser realizado no seu melhor interesse, nos termos da legislação pertinente.

Seção II

Término do tratamento

Art. 15. O término do tratamento de dados pessoais ocorrerá nas seguintes hipóteses:

I - verificação de que a finalidade foi alcançada ou de que os dados deixaram de ser necessários ou pertinentes ao alcance da finalidade específica almejada;

II - fim do período de tratamento;

III - comunicação do titular, inclusive no exercício do seu direito de revogação do consentimento conforme disposto no art. 9º, § 5º; ou

IV - determinação do órgão competente, quando houver violação da legislação em vigor a respeito.

Parágrafo único. O órgão competente estabelecerá os períodos máximos para o tratamento de dados pessoais, ressalvado o disposto em legislação específica.

Art. 16. Os dados pessoais serão eliminados após o término de seu tratamento, autorizada a conservação para as seguintes finalidades:

I - cumprimento de obrigação legal do responsável;

II - pesquisa histórica, científica ou estatística, garantida, quando possível, a anonimização dos dados pessoais; ou

III - transferência a terceiros, desde que respeitados os requisitos de tratamento de dados dispostos nesta Lei.

Parágrafo único. O órgão competente poderá estabelecer hipóteses específicas de conservação de dados pessoais, garantidos os direitos do titular, ressalvado o disposto em legislação específica.

CAPÍTULO III

DOS DIREITOS DO TITULAR

Art. 17. Toda pessoa natural tem assegurada a titularidade de seus dados pessoais, garantidos os direitos fundamentais de liberdade, intimidade e privacidade, nos termos desta Lei.

Art. 18. O titular dos dados pessoais tem direito a obter, em relação aos seus dados:

I - confirmação da existência de tratamento;

II - acesso aos dados;

III - correção de dados incompletos, inexatos ou desatualizados;

IV - anonimização, bloqueio ou eliminação de dados desnecessários, excessivos ou tratados em desconformidade com o disposto nesta Lei;

V - portabilidade, mediante requisição, de seus dados pessoais a outro fornecedor de serviço ou produto;

VI - eliminação, a qualquer momento, de dados pessoais com cujo tratamento o titular tenha consentido; e

VII - aplicação das normas de defesa do consumidor, quando for o caso, na tutela da proteção de dados pessoais.

§ 1º O titular pode se opor a tratamento realizado com fundamento em uma das hipóteses de dispensa de consentimento, em caso de descumprimento ao disposto nesta Lei.

§ 2º Os direitos previstos neste artigo serão exercidos mediante requerimento do titular a um dos agentes de tratamento, que adotará imediata providência para seu atendimento.

§ 3º Em caso de impossibilidade de adoção imediata da providência de que trata o § 2º, o responsável enviará ao titular, em até sete dias, contados da data do recebimento do requerimento, resposta em que poderá:

I - comunicar que não é agente de tratamento dos dados, indicando, sempre que possível, o agente; ou

II - indicar as razões de fato ou de direito que impedem a adoção imediata da providência.

§ 4º A providência de que trata o § 2º será realizada sem custos para o titular.

§ 5º O responsável deverá informar aos terceiros a quem os dados tenham sido comunicados sobre a realização de correção, eliminação, anonimização ou bloqueio dos dados, para que repitam idêntico procedimento.

Art. 19. A confirmação de existência ou o acesso a dados pessoais serão providenciados, a critério do titular:

I - em formato simplificado, imediatamente; ou

II - por meio de declaração clara e completa, que indique a origem dos dados, a data de registro, os critérios utilizados e a finalidade do tratamento, fornecida no prazo de até sete dias, contado da data do requerimento do titular.

§ 1º Os dados pessoais serão armazenados em formato que favoreça o exercício do direito de acesso.

§ 2º As informações e os dados poderão ser fornecidos, a critério do titular:

I - por meio eletrônico, seguro e idôneo para tal fim; ou

II - sob forma impressa, situação em que poderá ser cobrado exclusivamente o valor necessário ao ressarcimento do custo dos serviços e dos materiais utilizados.

§ 3º Quando o tratamento tiver origem no consentimento do titular ou em um contrato, o titular poderá solicitar cópia eletrônica integral dos seus dados pessoais em formato que permita a sua utilização subsequente, inclusive em outras operações de tratamento.

§ 4º O órgão competente poderá dispor sobre os formatos em que serão fornecidas as informações e os dados ao titular.

§ 5º O órgão competente poderá dispor de forma diferenciada acerca dos prazos dos incisos I e II do **caput** para os setores específicos.

Art. 20. O titular dos dados tem direito a solicitar revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, inclusive as decisões destinadas a definir o seu perfil ou avaliar aspectos de sua personalidade.

Parágrafo único. O responsável deverá fornecer, sempre que solicitadas, informações claras e adequadas a respeito dos critérios e dos procedimentos utilizados para a decisão automatizada, respeitados os segredos comercial e industrial.

Art. 21. Os dados pessoais referentes ao exercício regular de direitos pelo titular não podem ser utilizados em seu prejuízo.

Art. 22. A defesa dos interesses e dos direitos dos titulares de dados poderá ser exercida em juízo individual ou coletivamente, na forma do disposto na Lei nº 9.507, de 12 de novembro de 1997, nos art. 81 e art. 82 da Lei nº 8.078, de 11 de setembro de 1990, na Lei nº 7.347, de 24 de julho de 1985, e nos demais instrumentos de tutela individual e coletiva.

CAPITULO IV

DO TRATAMENTO DE DADOS PESSOAIS PELO PODER PÚBLICO

Seção I

Tratamento de Dados Pessoais pelo Poder Público

Art. 23. O tratamento de dados pessoais pelas pessoas jurídicas de direito público referenciadas no parágrafo único do art. 1º da Lei 12.527, de 18 de novembro de 2011, deverá ser realizado para o atendimento de sua finalidade pública, na persecução de um interesse público, tendo por objetivo a execução de competências legais ou o cumprimento de atribuição legal pelo serviço público.

Art. 24. Os órgãos do Poder Público deverão informar as hipóteses em que, no exercício de suas competências, realizam o tratamento de dados pessoais, fornecendo informações claras e atualizadas sobre essas atividades em veículos de fácil acesso, preferencialmente em seus sítios eletrônicos.

§ 1º Os órgãos do Poder Público que realizarem operações de tratamento de dados pessoais deverão indicar um encarregado, nos termos do art. 40.

§ 2º O órgão competente poderá dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento.

Art. 25. As empresas públicas e as sociedades de economia mista que atuem em regime de concorrência, sujeitas ao disposto no art. 173 da Constituição Federal, terão o mesmo tratamento dispensado às pessoas jurídicas de direito privado particulares, nos termos desta Lei.

Parágrafo único. As empresas públicas e as sociedades de economia mista, quando estiverem operacionalizando políticas públicas e não estiverem atuando em regime de concorrência, terão o mesmo tratamento dispensado aos órgãos e às entidades do Poder Público, nos termos desse Capítulo.

Art. 26. O uso compartilhado de dados pessoais pelo Poder Público deve atender a finalidades específicas de execução de políticas públicas e atribuição legal pelos órgãos e pelas entidades públicas, respeitados os princípios da proteção de dados pessoais elencados no art. 6º desta Lei.

Parágrafo único. É vedado ao Poder Público transferir a entidades privadas dados pessoais constantes de bases de dados a que tenha acesso, exceto em casos de execução descentralizada de atividade pública que o exija e exclusivamente para este fim específico e determinado, observado o disposto na Lei nº 12.527, de 2011.

Art. 27. A comunicação e a transferência de dados pessoais de pessoa jurídica de direito público a pessoa de direito privado será informada ao órgão competente e dependerá de consentimento do titular, exceto:

I - nas hipóteses de dispensa do consentimento previstas nesta Lei; ou:

II - nos casos de uso compartilhado de dados, em que será dada publicidade nos termos do art. 24.

Art. 28. A comunicação de dados pessoais entre órgãos e entidades de direito público será objeto de publicidade, nos termos art. 24.

Art. 29. O órgão competente poderá solicitar, a qualquer momento, às entidades do Poder Público a realização de operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei.

Art. 30. O órgão competente poderá estabelecer normas complementares para as atividades de comunicação de dados pessoais.

Seção II

Responsabilidade

Art. 31. Quando houver infração a esta Lei em decorrência do tratamento de dados pessoais por órgãos públicos, o órgão competente poderá enviar informe com medidas cabíveis para fazer cessar a violação.

Parágrafo único. As punições cabíveis a agente público no âmbito desta Lei serão aplicadas pessoalmente aos operadores de órgãos públicos, conforme disposto na Lei nº 8.112, de 11 de dezembro de 1990, e na Lei nº 8.429, de 2 de junho de 1992.

Art. 32. O órgão competente poderá solicitar a agentes do poder público a publicação de relatórios de impacto de privacidade e poderá sugerir a adoção de padrões e boas práticas aos tratamentos de dados pessoais pelo poder público.

CAPÍTULO V

DA TRANSFERÊNCIA INTERNACIONAL DE DADOS

Art. 33. A transferência internacional de dados pessoais somente é permitida nos seguintes casos:

I - para países que proporcionem nível de proteção de dados pessoais ao menos equiparável ao desta Lei;

II - quando a transferência for necessária para a cooperação judicial internacional entre órgãos públicos de inteligência e de investigação, de acordo com os instrumentos de direito internacional;

III - quando a transferência for necessária para a proteção da vida ou da incolumidade física do titular ou de terceiro;

IV - quando o órgão competente autorizar a transferência;

V - quando a transferência resultar em compromisso assumido em acordo de cooperação internacional;

VI - quando a transferência for necessária para execução de política pública ou atribuição legal do serviço público, sendo dada publicidade nos termos do art. 24; ou

VII - quando o titular tiver fornecido o seu consentimento para a transferência, com

informação prévia e específica sobre o caráter internacional da operação, com alerta quanto aos riscos envolvidos.

Parágrafo único. O nível de proteção de dados do país estrangeiro será avaliado pelo órgão competente, que levará em conta:

I - as normas gerais e setoriais da legislação em vigor no país de destino;

II - a natureza dos dados;

III - a observância dos princípios gerais de proteção de dados pessoais previstos nesta Lei;

IV - a adoção de medidas de segurança previstas em regulamento; e

V - as outras circunstâncias específicas relativas à transferência.

Art. 34. A autorização referida no inciso IV do **caput** do art. 33 será concedida quando o responsável pelo tratamento apresentar garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular, apresentadas em cláusulas contratuais aprovadas pelo órgão competente para uma transferência específica, em cláusulas contratuais padrão ou em normas corporativas globais, nos termos do regulamento.

§ 1º O órgão competente poderá elaborar cláusulas contratuais padrão ou homologar dispositivos constantes em documentos que fundamentem a transferência internacional de dados, que deverão observar os princípios gerais de proteção de dados e os direitos do titular, garantida a responsabilidade solidária do cedente e do cessionário, independentemente de culpa.

§ 2º Os responsáveis pelo tratamento que fizerem parte de um mesmo grupo econômico ou conglomerado multinacional poderão submeter normas corporativas globais à aprovação do órgão competente, obrigatórias para todas as empresas integrantes do grupo ou do conglomerado, a fim de obter permissão para transferências internacionais de dados dentro do grupo ou do conglomerado sem necessidade de autorizações específicas, observados os princípios gerais de proteção e os direitos do titular.

§ 3º Na análise de cláusulas contratuais, de documentos ou de normas corporativas globais submetidas à aprovação do órgão competente, poderão ser requeridas informações suplementares ou realizadas diligências de verificação quanto às operações de tratamento.

§ 4º As garantias suficientes de observância dos princípios gerais de proteção e dos direitos do titular referidas no **caput** serão, também, analisadas de acordo com as medidas técnicas e organizacionais adotadas pelo operador, de acordo com o previsto nos § 1º e § 2º do art. 45.

Art. 35. O cedente e o cessionário respondem solidária e objetivamente pelo tratamento de dados, independentemente do local onde estes se localizem, em qualquer hipótese.

CAPÍTULO VI

DOS AGENTES DO TRATAMENTO DE DADOS PESSOAIS

Seção I

Responsável e operador

Art. 36. São agentes do tratamento de dados pessoais o responsável e o operador.

Art. 37. O responsável e o operador devem manter registro das operações de tratamento de dados pessoais que realizarem.

Parágrafo único. O órgão competente poderá dispor sobre o formato, a estrutura e o tempo de guarda do registro.

Art. 38. O operador deverá realizar o tratamento segundo as instruções fornecidas pelo responsável, que verificará a observância das próprias instruções e das normas sobre a matéria.

Art. 39. O órgão competente poderá determinar ao responsável que elabore relatório de impacto à privacidade referente às suas operações de tratamento de dados, nos termos do regulamento.

Art. 40. A comunicação de dados pessoais entre responsáveis ou operadores de direito privado dependerá do consentimento do titular, ressalvadas as hipóteses de dispensa do consentimento previstas nesta Lei.

Seção II

Encarregado pelo tratamento de dados pessoais

Art. 41. O responsável deverá indicar um encarregado pelo tratamento de dados pessoais.

§ 1º A identidade e as informações de contato do encarregado deverão ser divulgadas publicamente de forma clara e objetiva, preferencialmente no sítio eletrônico do responsável.

§ 2º As atividades do encarregado consistem em:

I - receber reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providências;

II - receber comunicações do órgão competente e adotar providências;

III - orientar os funcionários e os contratados da entidade a respeito das práticas a serem tomadas em relação à proteção de dados pessoais; e

IV - demais atribuições determinadas pelo responsável ou estabelecidas em normas complementares.

§ 3º O órgão competente poderá estabelecer normas complementares sobre a definição e

as atribuições do encarregado, inclusive hipóteses de dispensa da necessidade de sua indicação, conforme a natureza e o porte da entidade ou o volume de operações de tratamento de dados.

Seção III

Responsabilidade e ressarcimento de danos

Art. 42. Todo aquele que, em razão do exercício de atividade de tratamento de dados pessoais, causar a outrem dano patrimonial, moral, individual ou coletivo, é obrigado a repará-lo.

Parágrafo único. O juiz, no processo civil, poderá inverter o ônus da prova a favor do titular dos dados quando, a seu juízo, for verossímil a alegação ou quando a produção de prova pelo titular resultar-lhe excessivamente onerosa.

Art. 43. A eventual dispensa da exigência do consentimento não desobriga os agentes do tratamento das demais obrigações previstas nesta Lei, especialmente da observância dos princípios gerais e da garantia dos direitos do titular.

Art. 44. Nos casos que envolvem a transferência de dados pessoais, o cessionário ficará sujeito às mesmas obrigações legais e regulamentares do cedente, com quem terá responsabilidade solidária pelos danos eventualmente causados.

Parágrafo único. A responsabilidade solidária não se aplica aos casos de tratamento realizado no exercício dos deveres de que trata a Lei nº 12.527, de 2011, relativos à garantia do acesso a informações públicas.

CAPÍTULO VII

DA SEGURANÇA E DAS BOAS PRÁTICAS

Seção I

Segurança e sigilo de dados

Art. 45. O operador deve adotar medidas de segurança técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou qualquer forma de tratamento inadequado ou ilícito.

§ 1º O órgão competente poderá dispor sobre padrões técnicos e organizacionais para tornar aplicável o disposto no **caput**, levando-se em consideração a natureza das informações tratadas, características específicas do tratamento e o estado atual da tecnologia, em particular no caso de dados sensíveis.

§ 2º As medidas de segurança deverão ser observadas desde a fase de concepção do produto ou do serviço até a sua execução.

Art. 46. Os agentes de tratamento ou qualquer outra pessoa que intervenha em uma das fases do tratamento obriga-se ao dever de sigilo em relação aos dados pessoais, mesmo após o seu término.

Art. 47. O responsável deverá comunicar ao órgão competente a ocorrência de qualquer incidente de segurança que possa acarretar risco ou prejuízo relevante aos titulares.

Parágrafo único. A comunicação será feita em prazo razoável, conforme definido pelo órgão competente, e deverá mencionar, no mínimo:

I - a descrição da natureza dos dados pessoais afetados;

II - as informações sobre os titulares envolvidos;

III - a indicação das medidas de segurança utilizadas para a proteção dos dados, inclusive procedimentos de encriptação;

IV - os riscos relacionados ao incidente;

V - os motivos da demora, no caso da comunicação não ter sido imediata; e

VI - as medidas que foram ou que serão adotadas para reverter ou mitigar os efeitos de prejuízo.

Art. 48. O órgão competente verificará a gravidade do incidente e poderá, caso necessário para a salvaguarda dos direitos dos titulares, determinar ao responsável a adoção de outras providências, como:

I - pronta comunicação aos titulares;

II - ampla divulgação do fato em meios de comunicação; e

III - medidas para reverter ou mitigar os efeitos do incidente.

§ 1º No juízo de gravidade do incidente, será avaliada eventual comprovação de que foram adotadas medidas técnicas adequadas que tornem os dados pessoais afetados ininteligíveis para terceiros não autorizados a acessá-los.

§ 2º A pronta comunicação aos titulares afetados pelo incidente de segurança será obrigatória, independente de determinação do órgão competente, nos casos em que for possível identificar que o incidente coloque em risco a segurança pessoal dos titulares ou lhes possa causar danos.

Art. 49. Os sistemas utilizados para o tratamento de dados pessoais devem ser estruturados de forma a atender aos requisitos de segurança, aos princípios gerais previstos nesta Lei e às demais normas regulamentares.

Seção II

Boas práticas

Art. 50. Os responsáveis pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e outros aspectos relacionados ao tratamento de dados pessoais.

§ 1º Ao estabelecer regras de boas práticas, o responsável pelo tratamento e o operador levarão em consideração a natureza, o escopo e a finalidade do tratamento e dos dados e a probabilidade e a gravidade dos riscos de danos aos indivíduos.

§ 2º As regras de boas práticas serão disponibilizadas publicamente e atualizadas e poderão ser reconhecidas e divulgadas pelo órgão competente.

Art. 51. O órgão competente estimulará a adoção de padrões técnicos que facilitem o controle dos titulares sobre seus dados pessoais.

CAPÍTULO VIII
DA FISCALIZAÇÃO

Seção I
Sanções administrativas

Art. 52. As infrações realizadas por pessoas jurídicas de direito privado às normas previstas nesta Lei ficam sujeitas às seguintes sanções administrativas aplicáveis pelo órgão competente:

I - multa simples ou diária;

II - publicização da infração;

III - anonimização dos dados pessoais;

IV - bloqueio dos dados pessoais;

V - suspensão de operação de tratamento de dados pessoais;

VI - cancelamento dos dados pessoais; e

VII - suspensão de funcionamento de banco de dados.

§ 1º As sanções serão aplicadas fundamentadamente, isolada ou cumulativamente, de acordo com as peculiaridades do caso concreto e com a gravidade e a natureza das infrações, à natureza dos direitos pessoais afetados, à existência de reincidência, à situação econômica do infrator e aos prejuízos causados.

§ 2º O disposto neste artigo não substitui a aplicação de sanções administrativas, civis ou penais definidas em legislação específica.

§ 3º O disposto nos incisos III a VII do **caput** deste artigo poderá ser aplicado às entidades e aos órgãos públicos, sem prejuízo do disposto na Lei nº 8.112, de 1990, e na Lei nº 8.429, de 1992.

Seção II

Órgão competente e Conselho Nacional de Proteção de Dados e da Privacidade

Art. 53. O órgão competente designado para zelar pela implementação e pela fiscalização desta Lei terá as seguintes atribuições:

I - zelar pela proteção dos dados pessoais, nos termos da legislação;

II - elaborar diretrizes para uma Política Nacional de Proteção de Dados Pessoais e Privacidade;

III - realizar auditoria nos tratamentos de dados pessoais e processos envolvidos com dados pessoais visando garantir a sua conformidade aos princípios e regras desta Lei;

IV - promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais e as medidas de segurança;

V - promover estudos sobre as práticas nacionais e internacionais de proteção de dados pessoais e privacidade;

VI - estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais;

VII - promover ações de cooperação com autoridades de proteção de dados pessoais de outros países, de natureza internacional ou transacional;

VIII - dispor sobre as formas pelas quais se dará a publicidade das operações de tratamento;

IX - solicitar, a qualquer momento, às entidades do Poder Público que realizem operações de tratamento de dados pessoais, informe específico sobre o âmbito, natureza dos dados e demais detalhes do tratamento realizado, podendo emitir parecer técnico complementar para garantir o cumprimento desta Lei;

X - estabelecer normas complementares para as atividades de comunicação de dados pessoais;

XI - elaborar relatórios anuais acerca de suas atividades;

XII - editar normas sobre proteção de dados pessoais e privacidade; e

XIII - realizar demais ações dentro de sua esfera de competência, inclusive as previstas nesta Lei e em legislação específica.

Art. 54. O Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será composto por quinze representantes titulares, e seus respectivos suplentes, dos seguintes órgãos:

I - sete representantes do Poder Executivo federal;

II - um representante indicado pelo Congresso Nacional;

III - um representante indicado pelo Conselho Nacional de Justiça;

IV - um representante indicado pelo Conselho Nacional do Ministério Público;

V - um representante indicado pelo Comitê Gestor da Internet no Brasil;

VI - um representante da sociedade civil;

VII - um representante da academia; e

VIII - dois representantes do setor privado.

§ 1º Os representantes serão designados por ato do Ministro de Estado da Justiça e terão mandato de dois anos, permitida uma recondução.

§ 2º A participação no Conselho Nacional de Proteção de Dados Pessoais e da Privacidade será considerada atividade de relevante interesse público, não remunerada.

§ 3º Os representantes referidos no inciso I a V do **caput** e seus respectivos suplentes serão indicados pelos titulares dos respectivos órgãos e entidades.

§ 4º Os representantes referidos nos incisos VI a VIII do **caput** e seus respectivos suplentes serão indicados na forma do regulamento.

Art. 55. Compete ao Conselho Nacional de Proteção de Dados Pessoais e da Privacidade:

I - fornecer subsídios para a elaboração da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

II - elaborar relatórios anuais de avaliação da execução das ações da Política Nacional de Proteção de Dados Pessoais e da Privacidade;

III - sugerir ações a serem realizadas pelo órgão competente;

IV - realizar estudos e debates sobre a proteção de dados pessoais e da privacidade; e

V - disseminar o conhecimento sobre proteção de dados pessoais e privacidade à população em geral.

CAPÍTULO IX
DISPOSIÇÕES FINAIS E TRANSITÓRIAS

Art. 56. Esta Lei entra em vigor cento e oitenta dias após a data de sua publicação.

Parágrafo único. O órgão competente estabelecerá normas sobre a adequação progressiva de bancos de dados constituídos até a data de entrada em vigor desta Lei, considerada a complexidade das operações de tratamento e a natureza dos dados.

Brasília,

EMI nº 00073/2016 MJ MP

Brasília, 29 de Abril de 2016

Excelentíssima Senhora Presidenta da República,

1. Submetemos à elevada consideração de Vossa Excelência a minuta de Projeto de Lei que dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural.

2. O Anteprojeto é resultado de um amplo debate público promovido pelo Ministério da Justiça, que teve duração de quase seis meses, recebendo mais de 50 mil visitas e obtendo mais de 1.100 contribuições. Esses subsídios foram analisados e consolidados no texto ora apresentado pelo Ministério da Justiça em parceria com o Centro de Estudos sobre Tecnologias Web (Ceweb), vinculado ao Núcleo de Informação e Coordenação do Ponto BR (Nic.br) e com o Instituto Nacional de Ciência e Tecnologia para a Web (InWeb), da Universidade Federal de Minas Gerais.

3. A proposta visa assegurar ao cidadão o controle e a titularidade sobre suas informações pessoais, com fundamento na inviolabilidade da intimidade e da vida privada, na liberdade de expressão, comunicação e opinião, na autodeterminação informativa, no desenvolvimento econômico e tecnológico, bem como na livre iniciativa, livre concorrência e defesa do consumidor. O avanço da tecnologia da informação amplia enormemente o potencial de coleta, processamento e utilização de dados pessoais, o que representa, por um lado, uma oportunidade de geração de novos conhecimentos e serviços mas, por outro, pode acarretar graves riscos aos direitos da personalidade do cidadão, ao acesso a serviços e bens, além de uma grande insegurança jurídica para o ambiente de negócios de tecnologia da informação existente no país, bem como para o comércio exterior, por conta da desconformidade da legislação brasileira atual aos padrões internacionais existentes neste tema.

4. É relevante apontar que o debate sobre privacidade e dados pessoais de que trata este Anteprojeto de Lei também foi fortemente influenciado pelo contexto internacional, consubstanciado, por exemplo, pela Resolução da ONU de 25 de novembro de 2013 sobre "Direito à Privacidade na Era Digital". Nessa manifestação, o governo brasileiro se empenhou para criar medidas que reiterassem também "online" os direitos que os cidadãos possuem "offline". Ocorre, no entanto, que apesar dos esforços diplomáticos realizados pelo país nesse sentido, o Brasil encontra-se defasado em relação ao resto do mundo no que toca à regulamentação do tema, na medida em que ainda não possui qualquer lei específica que diga respeito à proteção de dados pessoais, enquanto cerca de 109 países possuem normas nesse sentido e mais de 90 destes têm uma autoridade pública específica especializada no tema.

5. Não é apenas pela defasagem em comparação a outros países que urge a necessidade de promulgação desta norma legal. A utilização, cada vez mais intensa, de dados pessoais na sociedade da informação cria um desequilíbrio entre os poderes dos indivíduos, titulares de seus próprios dados pessoais, e os dos utilizadores de tais dados, justamente pela quantidade de informações pessoais que as novas tecnologias são capazes de agregar e utilizar. Para que esses dados possam ser utilizados com fins transparentes e legítimos, ao mesmo tempo em que sejam garantidos os direitos de seus titulares, são

necessárias normas e mecanismos institucionais que estabeleçam os parâmetros e limites deste tratamento, até mesmo no momento de término dessa relação. Além disso, tendo em vista o caráter transnacional do fluxo dessas informações, cumpre indicar que este Projeto abrange tanto as operações de tratamento de dados pessoais realizadas no Brasil, como aquelas realizadas no exterior, mas cuja coleta tenha ocorrido em território nacional.

6. A minuta proposta abarca o tratamento de informações pessoais processadas tanto pelo setor público como pelo setor privado. Estão excluídos do âmbito de proteção da norma, no entanto, aqueles tratamentos de dados pessoais realizados para fins exclusivamente pessoais, bem como aqueles que tem por objeto o exercício regular da atividade jornalística, artística, literária ou acadêmica. Quanto à regulação referente à segurança pública, esta deverá respeitar os princípios gerais estabelecidos no texto, porém contará com legislação específica posterior a esta proposta.

7. Os direitos do titular, por sua vez, são explicitados, em particular com relação ao acesso, correção, dissociação e oposição ao tratamento de seus dados. Ademais, o anteprojeto estabelece normas específicas para o tratamento de dados cujo tratamento possa ensejar discriminação ao titular (os chamados "dados sensíveis", por se referirem a orientação sexual, convicções religiosas, filosóficas ou morais, ou opiniões políticas, por exemplo), prevendo como regra geral que esses dados não devem ser tratados e que ninguém pode ser obrigado a fornecer informações de tal natureza a seu respeito, ressalvadas as hipóteses previstas em lei, assim como um regramento mais rígido quando o tratamento desses dados for permitido.

8. Diante do exposto, fica claro que os dados pessoais merecem uma tutela forte e específica do ordenamento jurídico. O processamento dessas informações influencia diretamente a vida das pessoas, afetando oportunidades, escolhas e interações sociais, elementos que compõem o livre desenvolvimento da sua própria personalidade. Tendo isso em vista, é imperativo que haja um conjunto de princípios que norteiem o tratamento desses dados por terceiros, entre os quais podem ser destacados sua utilização somente para finalidades específicas, adequadas e necessárias, além da regra de que o responsável pela coleta desses dados deva mantê-los em segurança, e que não os utilize para discriminação e permita o acesso facilitado ao titular.

9. Além disso, são elencados uma série de requisitos para o tratamento dos dados pessoais, sem os quais este não pode se reputar legítimo. Um destes requisitos é o do consentimento livre e inequívoco do titular. Para garantir os direitos do titular, a decisão sobre o consentimento deve ser sempre livre e incontroversa para cada pessoa, sempre com base na boa-fé, de modo a preservar a sua autodeterminação e proteger a sua personalidade. Há, ainda, outros casos específicos para a legitimação do tratamento, como nos casos em que há legítimo interesse do titular. Essa exceção, por outro lado, não deve ser compreendida como uma escusa genérica à demanda do consentimento, mas sim deve estar atrelada a uma tutela específica, que não pode jamais reduzir direitos fundamentais do titular.

10. O estabelecimento de regras sobre a proteção de dados pessoais possui, portanto, duas funções: proteger o titular dos dados e, ao mesmo tempo, favorecer a sua utilização dentro de um patamar de segurança, transparência e boa-fé. Dessa forma, a utilização lícita de dados será incentivada pela delimitação de um espaço de segurança jurídica, favorecendo o fluxo de dados por agentes responsáveis e o desenvolvimento de setores econômicos ligados, por exemplo, às tecnologias de informação. Nesse sentido, a proposta também trata da transferência internacional de dados e o condicionamento de sua ocorrência para determinadas circunstâncias, entre elas, para países que tenham nível de proteção equiparável ao brasileiro. Essa disposição implica que a partir da promulgação da lei brasileira de proteção de dados pessoais, o país estará apto a entrar no rol de Estados com os quais as empresas europeias podem realizar negócios que envolvam o tratamento de dados pessoais, sendo um importante avanço para o comércio exterior e, portanto, para o desenvolvimento econômico do Brasil.

11. Com esse mesmo objetivo de garantir segurança jurídica nas relações entre titulares e usuários

de dados, a proposta inclui sanções administrativas para coibir abusos neste tratamento, indicando quais condutas são vedadas aos atores envolvidos nessa relação.

12. Não escapa também ao escopo do Anteprojeto de Lei, a necessidade de regulamentação da forma como o poder público deve tratar os dados pessoais da população. Nesses casos, as diretrizes gerais devem decorrer sempre de competências legais, e a transparência ativa sobre como são usados os dados por meio de sites públicos deve ser a regra.

13. É relevante indicar que este anteprojeto se constituirá no marco geral para a regulação da proteção e uso dos dados pessoais no país e se harmoniza com os instrumentos legais que atualmente tratam do tema de forma setorial ou específica no ordenamento jurídico brasileiro.

14. A aplicação efetiva do direito individual fundamental à privacidade depende, em grande medida, das respostas coletivas que serão apresentadas para implementá-lo, motivo pelo qual é necessário empenhar-se na construção de uma democracia da informação que proteja tanto a autodeterminação e a liberdade de controle das informações pessoais pelo cidadão, como também a tutela contra a utilização discriminatória dos dados. Nesse contexto, a minuta ora apresentada visa possibilitar que a sociedade brasileira obtenha os benefícios econômicos e sociais potencializados pela tecnologia da informação, ao criar no país uma arquitetura regulatória capaz de fazer emergir o tema da proteção de dados pessoais como um verdadeiro vetor de políticas públicas, composto por instrumentos estatutários, sancionatórios, bem como por um órgão administrativo, responsável pela implementação e aplicação da legislação.

15. Ainda, o texto abre espaço para que categorias profissionais e segmentos empresariais estabeleçam regras comuns, a título de boas práticas, outorgando ao mercado um grau necessário de autorregulamentação, sem prejuízo da observância aos princípios gerais da lei.

16. Com o objetivo de dar efetividade à regulamentação sugerida, a proposta prevê um órgão competente para a proteção de dados pessoais no país. Será sua responsabilidade elaborar diretrizes de uma Política Nacional de Proteção de Dados Pessoais e Privacidade, promover entre a população o conhecimento das normas e das políticas públicas sobre proteção de dados pessoais, bem como das medidas de segurança, estimular a adoção de padrões para serviços e produtos que facilitem o exercício de controle dos titulares sobre seus dados pessoais, entre outras medidas.

17. Como auxiliar deste órgão, propõe-se a criação de um Conselho Nacional de Proteção de Dados Pessoais e Privacidade, composto por representantes do poder público, setor privado, academia, comunidade técnica e organizações não-governamentais.

18. A consolidação de um regime integrado de proteção de dados no Brasil mostra-se, assim, fundamental no ordenamento jurídico pátrio, de modo a possibilitar uma regulação integral do tema e a coesão de diversas iniciativas na área. Somente uma regulação geral assegurará a instituição de princípios harmônicos sobre o tema, proporcionando o controle dos riscos envolvidos no processamento de dados e assegurando o controle do cidadão em relação às suas próprias informações pessoais e, assim, garantindo a necessária segurança jurídica para a atividade empresarial e para a administração pública no tratamento de dados pessoais.

19. Essas, Senhora Presidenta, são as razões que justificam a apresentação do Anteprojeto de Lei que ora submetemos à elevada apreciação de Vossa Excelência.

Respeitosamente,

Assinado eletronicamente por: Eugênio José Guilherme de Aragão, Francisco Gaetani

Mensagem nº 255

Senhores Membros do Congresso Nacional,

Nos termos do § 1º do art. 64 da Constituição, submeto à elevada deliberação de Vossas Excelências o texto do projeto de lei que "Dispõe sobre o tratamento de dados pessoais para a garantia do livre desenvolvimento da personalidade e da dignidade da pessoa natural".

Brasília, 11 de maio de 2016.