

**XXVII CONGRESSO NACIONAL DO
CONPEDI PORTO ALEGRE – RS**

**DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS
II**

JOSÉ RENATO GAZIERO CELLA

JÚLIA FRANCIELI NEVES DE OLIVEIRA

SALETE ORO BOFF

Todos os direitos reservados e protegidos. Nenhuma parte deste anal poderá ser reproduzida ou transmitida sejam quais forem os meios empregados sem prévia autorização dos editores.

Diretoria – CONPEDI

Presidente - Prof. Dr. Orides Mezzaroba - UFSC – Santa Catarina

Vice-presidente **Centro-Oeste** - Prof. Dr. José Querino Tavares Neto - UFG – Goiás

Vice-presidente **Sudeste** - Prof. Dr. César Augusto de Castro Fiuza - UFMG/PUCMG – Minas Gerais

Vice-presidente **Nordeste** - Prof. Dr. Lucas Gonçalves da Silva - UFS – Sergipe

Vice-presidente **Norte** - Prof. Dr. Jean Carlos Dias - Cesupa – Pará

Vice-presidente Sul - Prof. Dr. Leonel Severo Rocha - Unisinos – Rio Grande do Sul

Secretário Executivo - Profa. Dra. Samyra Haydêe Dal Farra Napolini - Unimar/Uninove – São Paulo

Representante Discente – FEPODI

Yuri Nathan da Costa Lannes - Mackenzie – São Paulo

Conselho Fiscal:

Prof. Dr. João Marcelo de Lima Assafim - UCAM – Rio de Janeiro

Prof. Dr. Aires José Rover - UFSC – Santa Catarina

Prof. Dr. Edinilson Donisete Machado - UNIVEM/UENP – São Paulo

Prof. Dr. Marcus Firmino Santiago da Silva - UDF – Distrito Federal (suplente)

Prof. Dr. Ilton Garcia da Costa - UENP – São Paulo (suplente)

Secretarias:

Relações Institucionais

Prof. Dr. Horácio Wanderlei Rodrigues - IMED – Rio Grande do Sul

Prof. Dr. Valter Moura do Carmo - UNIMAR – Ceará

Prof. Dr. José Barroso Filho - UPIS/ENAJUM – Distrito Federal

Relações Internacionais para o Continente Americano

Prof. Dr. Fernando Antônio de Carvalho Dantas - UFG – Goiás

Prof. Dr. Heron José de Santana Gordilho - UFBA – Bahia

Prof. Dr. Paulo Roberto Barbosa Ramos - UFMA – Maranhão

Relações Internacionais para os demais Continentes

Profa. Dra. Viviane Coêlho de Séllos Knoerr - Unicuritiba – Paraná

Prof. Dr. Rubens Beçak - USP – São Paulo

Profa. Dra. Maria Aurea Baroni Cecato - Unipê/UFPB – Paraíba

Eventos:

Prof. Dr. Jerônimo Siqueira Tybusch UFSM – Rio Grande do Sul

Prof. Dr. José Filomeno de Moraes Filho Unifor – Ceará

Prof. Dr. Antônio Carlos Diniz Murta Fumec – Minas Gerais

Comunicação:

Prof. Dr. Matheus Felipe de Castro UNOESC – Santa Catarina

Prof. Dr. Liton Lanes Pilau Sobrinho - UPF/Univali – Rio Grande do Sul

Prof. Dr. Caio Augusto Souza Lara - ESDHC – Minas Gerais

Membro Nato – Presidência anterior Prof. Dr. Raymundo Juliano Feitosa - UNICAP – Pernambuco

E27

Direito, governança e novas tecnologias II [Recurso eletrônico on-line] organização CONPEDI/ UNISINOS

Coordenadores: José Renato Gaziero Cella; Salette Oro Boff; Júlia Francieli Neves de Oliveira. – Florianópolis: CONPEDI, 2018.

Inclui bibliografia

ISBN: 978-85-5505-726-7

Modo de acesso: www.conpedi.org.br em publicações

Tema: Tecnologia, Comunicação e Inovação no Direito

1. Direito – Estudo e ensino (Pós-graduação) – Encontros Nacionais. 2. Assistência. 3. Isonomia. XXVII Encontro Nacional do CONPEDI (27 : 2018 : Porto Alegre, Brasil).

CDU: 34



XXVII CONGRESSO NACIONAL DO CONPEDI PORTO ALEGRE – RS

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS II

Apresentação

No XXVII Congresso Nacional do CONPEDI, realizado de 14 a 16 de novembro de 2018, que teve lugar na Universidade do Vale do Rio dos Sinos - UNISINOS, em Porto Alegre-RS, o grupo de trabalho “Direito, Governança e Novas Tecnologias II” se destacou no evento não apenas pela qualidade dos trabalhos apresentados, mas pelo numeroso público, composto por pesquisadores-expositores e interessados, que deixou a sala repleta até o término das atividades. Foram apresentados 19 artigos objeto de um intenso debate presidido pelos coordenadores e acompanhado pela participação instigante do público presente.

Esse fato demonstra a inquietude que o tema desperta na seara jurídica. Cientes desse fato, os programas de pós-graduação em Direito empreendem um diálogo que suscita a interdisciplinaridade na pesquisa e se propõe a enfrentar os desafios que as novas tecnologias impõem ao Direito. Pode-se agrupar os trabalhos apresentados em quatro grandes temáticas, que se congregam nesta coletânea.

Houve enfoque nas possibilidades e contingências democráticas das novas tecnologias, tanto no âmbito teórico quanto no âmbito prático, com apresentações e debates dos seguintes artigos:

1. POLÍTICAS PÚBLICAS E NEUTRALIDADE DA REDE NO BRASIL;
2. OS DEPARTAMENTOS JURÍDICOS E AS EMPRESAS MULTINACIONAIS DE TECNOLOGIA DA INFORMAÇÃO (TI) QUE ATUAM EM PAÍSES EMERGENTES: A GERAÇÃO DE VANTAGENS COMPETITIVAS À LUZ DAS CAPACIDADES DINÂMICAS;
3. PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO: UMA VISÃO SOB O ASPECTO DOS DIREITOS DA PERSONALIDADE NO BRASIL E NA UNIÃO EUROPEIA;
4. “CORPO ELETTRONICO” COMO VÍTIMA EM MATÉRIA DE TRATAMENTO DE DADOS PESSOAIS: RESPONSABILIDADE CIVIL POR DANOS À LUZ DA LEI DE PROTEÇÃO DE DADOS BRASILEIRA E DANO ESTÉTICO NO MUNDO DIGITAL;

5. O VOTO DISSIDENTE DE SOCIO MINORITARIO COMO FORMA DE GESTAO DO RISCO NANOTECNOLOGICO;
6. DEMOCRACIA E TECNOLOGIA: A ELABORAÇÃO DE NOVOS INSTRUMENTOS PARTICIPATIVOS NOS MUNICÍPIOS;
7. PARTICIPAÇÃO DA SOCIEDADE CIVIL NO CONTEXTO DA UNIÃO EUROPEIA: UM ESTUDO DE CASO DA FERRAMENTA EU-PILOT;
8. DIREITO E MEDICINA: UMA VISÃO INTERDISCIPLINAR FRENTE AOS APLICATIVOS PARA MARCAÇÃO DE CONSULTAS MÉDICAS E O POSICIONAMENTO DOS CONSELHOS PROFISSIONAIS;
9. AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: NATUREZA JURÍDICA E A LEI Nº 13.079/2018;
10. GESTÃO DOS ASPECTOS JURÍDICOS DA INOVAÇÃO DISRUPTIVA;
11. REFLEXÕES SOBRE A AUTOMAÇÃO NO DIREITO: LAW TECHS;
12. POLÍTICA REGULATÓRIA PARA TECNOLOGIAS DISRUPTIVAS NO BRASIL: O CASO DA TECNOLOGIA BLOCKCHAIN E TECNOLOGIAS DE REGISTRO DISTRIBUÍDAS;
13. O PRINCÍPIO DA PUBLICIDADE E DA FUNDAMENTAÇÃO DAS DECISÕES JUDICIAIS FRENTE A UTILIZAÇÃO DE ALGORITMOS NO DESEMPENHO DA ATIVIDADE JURISDICIONAL E DOS ATOS PROCESSUAIS;
14. ACCOUNTABILITY DE FAKE NEWS: BUSCANDO A VERDADE DA NOTÍCIA FALSA;
15. DIGITALIZAÇÃO NA ERA DA SOCIEDADE DA INFORMAÇÃO – VIRTUALIZAÇÃO E DESMATERIALIZAÇÃO. SATISFAÇÃO DO INTERESSE PÚBLICO – GOVERNO ELETRÔNICO;
16. O DIREITO HUMANO À INTIMIDADE NA CONTEMPORANEIDADE E SEUS DESAFIOS NA SOCIEDADE GLOBALIZADA EM REDE;

17. EFETIVIDADE DO DIREITO À INFORMAÇÃO: DIAGNÓSTICO DA POLÍTICA ESTADUAL DE DADOS ABERTOS GOVERNAMENTAIS NO RIO GRANDE DO SUL;

18. A INCORPORAÇÃO DE DRONES PARA VIGILÂNCIA DE ESPAÇOS URBANOS BRASILEIROS: O USO PELAS FORÇAS ARMADAS E ÓRGÃOS DE SEGURANÇA PÚBLICA DA UNIÃO E DO ESTADO DE SANTA CATARINA; e

19. AUTOCOMUNICAÇÃO E CONTRAPODER: A ARQUITETURA DAS TIC COMO INSTRUMENTOS DE DIFUSÃO INFORMATIVA E O IMPACTO NA AGENDA POLÍTICA

Os artigos que ora são apresentados ao público têm a finalidade de fomentar a pesquisa e fortalecer o diálogo interdisciplinar em torno do tema “direito, governança e novas tecnologias”, que trazem consigo, ainda, a expectativa de contribuir para os avanços do estudo desse tema no âmbito da pós-graduação em Direito brasileira, apresentando respostas para uma realidade que se mostra em constante transformação.

Os Coordenadores:

Prof. Dr. José Renato Gaziero Cella – IMED

Prof. Dr. Felipe Chiarello de Souza Pinto – UPM

Profa. Dra. Salete Oro Boff - IMED / IESA / UFFS

Nota Técnica: Os artigos que não constam nestes Anais foram selecionados para publicação na Plataforma Index Law Journals, conforme previsto no artigo 8.1 do edital do evento. Equipe Editorial Index Law Journal - publicacao@conpedi.org.br.

PROTEÇÃO DE DADOS PESSOAIS NA SOCIEDADE DA INFORMAÇÃO: UMA VISÃO SOB O ASPECTO DOS DIREITOS DA PERSONALIDADE NO BRASIL E NA UNIÃO EUROPEIA.

PROTECTION OF PERSONAL DATA IN THE INFORMATION SOCIETY: A POINT OF VIEW ABOUT PERSONALITY RIGHTS IN BRAZIL AND EUROPEAN UNION.

Victor Augusto Tateoki ¹

Ana Elizabeth Lapa Wanderley Cavalcanti ²

Resumo

O presente trabalho tem como objetivo fazer uma análise da proteção de dados pessoais na sociedade da informação, mais precisamente tratando-se de um estudo da proteção no Brasil e na União Europeia, já que as duas possuem proteção com vieses semelhantes baseados em direitos da personalidade. Deste modo, o artigo científico, utiliza-se dos métodos dedutivos e indutivos para sua abordagem. Para tanto foi realizado uma pesquisa normativa, doutrinária e prática, buscando compreender a sociedade da informação e a importância da proteção dos dados pessoais nos dias atuais e o impacto da manipulação de dados pessoais nos chamados direitos da personalidade.

Palavras-chave: Sociedade da informação, Proteção de dados pessoais, Privacidade, Direitos da personalidade

Abstract/Resumen/Résumé

The objective of this study is to analyze the protection of personal data in the information society, more precisely a study of protection of personal data in Brazil and the European Union, since both have very similar protection based on rights of personality. Thus, this article uses the deductive and inductive methods for its development. For this, a normative, doctrinal and practical research was carried out, seeking to understand the information society and the importance of the protection of personal data in present days and the impact of the personal data's manipulation on the personality rights.

Keywords/Palabras-claves/Mots-clés: Information society, Personal data protection, Privacy, Personality rights

¹ Mestrando em Direito da Sociedade da Informação - FMU. Graduado em Direito e História pela UNITOLEDO. Membro da Comissão de Direito Digital e Compliance da OAB/SP. Professor e Advogado.

² Doutora e Mestre em Direito pela PUC/SP. Professora da graduação em Direito das Faculdades Metropolitanas Unidas - FMU e do Mestrado em Direito da Sociedade da Informação das FMU.

INTRODUÇÃO

O presente artigo científico tem como objetivo discutir e analisar a proteção de dados pessoais na sociedade da informação, mais especificamente no Brasil e na União Europeia, pois estes dois países possuem características semelhantes voltados ao direito da personalidade. Deste modo, o presente trabalho analisará no Brasil as leis esparsas e o projeto de lei de proteção de dados pessoais, (PL 53/2018) que está em fase de sanção pelo Presidente da República, após aprovado na Câmara dos Deputados e no Senado, e em relação a União Europeia será analisado o Regulamento Geral de Proteção de Dados Pessoais (RGPD), em vigência.

O trabalho ainda visa discutir as mudanças tecnológicas dos últimos anos e como elas transformaram diretamente a sociedade, surgindo assim, a sociedade da informação, além de como o direito encara tais dilemas. Com o barateamento e evolução das tecnologias da comunicação, como, por exemplo, a internet, os telefones celulares e os computadores cada vez mais se tornarão populares, aumentando o seu tempo de uso. Assim, mais dados pessoais são gerados para coleta, uso, armazenamento e tratamento, tornando visível de forma mais precisa e específica a vida privada e a intimidade de qualquer pessoa. Deste modo, fica evidente a necessidade da proteção dos dados pessoais com os avanços tecnológicos e da sociedade da informação, como forma de respeito aos direitos da personalidade e da dignidade da pessoa humana.

Em primeiro momento, o artigo abordará a sociedade da informação, os avanços das tecnologias e o impacto no direito. No momento seguinte, trabalho tratará dos direitos da personalidade - mais especificamente a privacidade e a proteção de dados pessoais. Em sequência, falará sobre a proteção de dados pessoais no Brasil e, logo após, a proteção dos dados pessoais na União Europeia.

Deste modo, o trabalho valeu-se dos métodos dedutivos e indutivos para sua análise e produção. Utilizou-se ainda pesquisas bibliográficas, doutrinárias, normativas e práticas, buscando aperfeiçoar e fomentar as discussões a respeito da temática, que se torna atual conforme o uso e o avanço das tecnologias da comunicação.

1 SOCIEDADE DA INFORMAÇÃO

A revolução da informática nos últimos anos modificou as bases estruturais do convívio em sociedade, da cultura, da política e da economia. Assim, o direito também

foi diretamente afetado. Na verdade, quase toda e qualquer transformação tecnológica faz com que o direito acabe enfrentando diversos dilemas, e a informática acentuou ainda mais essas questões.

Leonardi (2012) aponta que os avanços das tecnologias criam novos dilemas jurídicos, além de tornar outros obsoletos, como os avanços do exame de DNA nas investigações de paternidade, gravações de conversas telefônicas para investigações criminais e diversos outros, além de ressaltar que a tecnologia também deve ser modulada pelo sistema jurídico como foi o caso do carro, armas de fogo, aeronaves, imprensa, telecomunicações e todas as suas legislações específicas e correspondentes.

A sociedade da informação surge segundo Castells (2011) após a Segunda Guerra Mundial e a Revolução Industrial. Mas foi somente na década de 1970, com surgimento da microeletrônica, que as tecnologias da comunicação começaram a se tornar mais populares. Destarte que a sociedade da informação não cuida somente da evolução do *hardware* e do *software*, ou seja, das tecnologias propriamente ditas, e sim de como toda a sociedade foi transformada ou se atualizada por elas, como explica Lisboa (2007, p. 125): “A revolução informacional reflete-se sobre todas as relações sociais, tal como ocorreu com a Revolução Industrial, no passado”.

O trabalho utiliza o termo sociedade da informação pois foi assim que o governo brasileiro adotou, em documento oficial, denominado como Livro Verde da Sociedade da Informação. Lembrando que tal expressão não é unânime entre os acadêmicos. Por exemplo, Ascensão (2002) usa o termo sociedade da comunicação, pois o destaque é a comunicação em si. Já Lèvy (1999) utiliza o termo sociedade do conhecimento, uma vez que o autor destaca a diferença entre conhecimento e informação.

Deste modo, o meio de comunicação que mais alavancou a sociedade da informação inegavelmente é a internet, que possibilitou que fronteiras entre países se diluíssem, que transações financeiras e comunicações se tornassem instantâneas, ampliou o compartilhamento de informações e conhecimento em larga escala, dentre outros diversos avanços.

Assim informações sobre a intimidade e a vida privada de qualquer pessoa podem ser compartilhadas e armazenadas em larga escala e de fácil acesso com a internet, por diversos setores da sociedade, comércio, publicidade, educação, saúde, segurança, financeira, dentre outros, desta forma iniciaram-se as primeiras discussões sobre a proteção da privacidade e proteção de dados pessoais dos usuários, que serão abordados adiante neste trabalho.

2 DIREITOS DA PERSONALIDADE, PRIVACIDADE E PROTEÇÃO DE DADOS PESSOAIS

Os direitos da personalidade são aqueles que são considerados inerentes ao próprio ser humano. Ou seja, são os direitos que possuem como valor basilar a construção da própria pessoa ou do ser humano, como é o caso ao direito à vida, que advém antes mesmo do ideal jurídico de tutela ou proteção. É através da personalidade que os outros direitos são construídos e entre eles podem ser considerados os princípios que fundamentam o direito.

Assim os direitos da personalidade, segundo Bittar (1995, p 11), são “direitos inatos (originários), absolutos, extrapatrimoniais, intransmissíveis, imprescritíveis, impenhoráveis, vitalícios, necessários e oponíveis erga omnes”. Deste modo, os direitos da personalidade possuem certas características que, segundo Diniz (2012), são absolutas por possuírem o dever geral de abstenção, ou seja, erga omnes. Eles são extrapatrimoniais por não ser possível valorizá-los economicamente; intransmissíveis por não ser possível a sua transferência para outra pessoa; indisponíveis, não podendo ser utilizados como bem entender, mas podem ser objetos de contrato como, por exemplo, a concessão do uso da própria imagem; irrenunciáveis já que não se pode negar seu direito; ilimitados pois não existe uma numeração aos direitos da personalidade; imprescritíveis, impenhoráveis e inexpropriáveis pois não se extinguem e não podem ser penhorados.

Para França (1983, p. 07) são considerados como direitos da personalidade “as faculdades jurídicas cujo objeto são os diversos aspectos da própria pessoa do sujeito, bem assim as suas emanações e prolongamentos”.

No mesmo sentido, Cupis (2004, p.23) ressalta que:

Todos os direitos, na medida em que destinados a dar conteúdo à personalidade, poderiam chamar-se "direitos da personalidade". No entanto, na linguagem jurídica, esta designação é reservada aos direitos subjetivos, cuja função, relativamente à personalidade, é especial, constituindo o *minimum* necessário e imprescindível ao seu conteúdo.

Verifica-se, portanto, que os direitos da personalidade consistem naqueles direitos subjetivos das pessoas, que têm em vista a tutela da pessoa humana e sua dignidade. Trata-se, portanto, de direitos com aspectos extrapatrimoniais, que tem por objeto os diversos aspectos da pessoa humana, constituindo a sua individualidade e que definem e garantem a sua dignidade.

O maior passo para evolução dos direitos da personalidade no Brasil foi o advento da Constituição Federal de 1988, segundo Gonçalves (2012), que previu expressamente em seu artigo 5º, inciso X, a inviolabilidade da intimidade, vida privada e a honra e a imagem das pessoas. Importante ressaltar que, caso esses direitos sejam violados, cabe indenização por danos morais e/ou materiais. Na questão da intimidade e vida privada, importa salientar o direito à privacidade e à proteção dos dados pessoais, por serem objeto principal de estudo neste artigo acadêmico.

A privacidade historicamente nas palavras de Silva Neto (2001) foi inicialmente citada pelo juiz norte americano Thomas Cololey, o qual se referiu a expressão em 1888. Dois anos mais tarde, o termo direito à privacidade foi claramente trabalhado por dois advogados: Samuel Warren e Luis D. Bradeis, os quais publicaram um artigo chamado *The right to privacy*, no qual discutiram o direito de não se ter imagens fotográficas utilizadas sem consentimento.

No mais, o conceito de privacidade foi se desenvolvendo ao longo dos anos, conforme o desenvolvimento das tecnologias de captação das expressões da personalidade, entre elas a gravação de som e imagem, a capacidade de armazenamento de informações pessoais e dados relativos à pessoa, dentre outros. Assim, cada vez mais a privacidade começou a ser cerceada e seu conceito e proteção necessitou ser atualizado e discutido.

Nas palavras de Leonardi (2012), existiram diversos conceitos unitários de privacidade, como o direito a ser deixado só, o resguardo de interferências alheias, segredo ou sigilo, e o controle de informações. O maior problema é que esses conceitos são muito restritivos e também não conseguem representar a privacidade nos dias atuais. Necessitamos um conceito plural de privacidade que apresente diversas proteções contra uma pluralidade de problemas entre si.

Entendemos, portanto, que deve a privacidade ser tratada como um conceito plural que pode abarcar diversos aspectos da vida privada como a honra, a imagem, intimidade, a própria moradia, o sigilo das comunicações e correspondência, dentre diversas outras, assim, como preceitua Silva (2005, p. 206), “(...) preferimos usar a expressão direito à privacidade, num sentido genérico e amplo, de modo a abarcar todas as manifestações da esfera íntima, privada da personalidade, que o texto constitucional consagrou”

Cabe ainda mencionar que a privacidade está prevista em diversos documentos legais que fazem parte do nosso sistema jurídico, como na Constituição Federal de 1988

(no já citado o artigo 5, inciso X), na Declaração Universal dos Direitos Humanos, no Código Civil, e no próprio Marco Civil da Internet, Lei 12.965/2014.

Após verificarmos o conceito de privacidade, passamos a analisar a questão da proteção dos dados pessoais como forma de proteção da intimidade e privacidade e, por consequência, dos direitos da personalidade.

A proteção de dados pessoais, como já falado anteriormente, é uma consequência do direito à privacidade, pois os dados pessoais revelam informações sobre os indivíduos, sobre a sua intimidade e a sua vida privada, que muitas vezes nem mesmo as próprias pessoas sabem. Por exemplo, com dados pessoais médicos ou farmacêuticos é possível identificar quais tipos de doenças uma pessoa pode possuir futuramente, ou também pode revelar seu modo de vida, suas características físicas e genéticas. Além disso, a proteção de dados pessoais constitui um direito fundamental para a manutenção democrática do estado de direito, como afirma Rodotà (2008, p. 21):

A proteção de dados pessoais constitui não apenas um direito fundamental entre outros: é o mais expressivo da condição humana contemporânea. Relembrar isso a cada momento não é verbosidade, pois toda mudança que afeta a proteção de dados tem impacto sobre o grau de democracia que nós podemos experimentar

Na atual sociedade da informação, segundo Barreto Junior (2007), a informação passou a ter o valor de mercadoria. Com a possibilidade de coleta e tratamento da informação, cada vez mais os produtos se tornaram mais específicos para atender a um público consumidor mais individualizado e os dados pessoais são importantes para personalizar o tratamento ao consumidor.

Consequentemente, com o avanço e o barateamento dos custos das tecnologias de captação de dados pessoais, maior é a necessidade de sua proteção, uma vez que a maior parte dos serviços oferecidos pelos provedores de aplicações ou conteúdo na internet são oferecidos em troca dos dados e a privacidade do indivíduo. Com a capacidade cada vez mais aumentada de cruzamentos de dados, um perfil ou uma personalidade de uma pessoa poderão ser montados como alerta Tapscott (2010, p.89):

À medida que a internet se torna base para o comércio, o trabalho, a mídia, o entretenimento, a assistência média, o aprendizado e a maioria das formas de discurso humano, a nossa vida privada se torna cada vez menos privada. Quando compramos livros ou música na internet, essas comprar são registradas e inseridas em bancos de dados gigantescos. Quando compramos medicamentos ou mantimentos em loja, e usamos nosso cartão de crédito para pagar, um registro é gerado e armazenado. A pesquisa de uma criança para um projeto escolar, o leitor de cartões em um estacionamento, as interações do seu carro com um banco de dados via satélite, as publicações on-line que você lê, a camisa que você compra com seu cartão da loja de

departamentos, os remédios que você compra e as centenas de outras transações em rede em uma semana comum: todas essas informações são gravadas em vários bancos de dados. Os computadores podem, com um custo baixo, conectar e cruzar esses bancos de dados para fragmentar e reorganizar as informações sobre indivíduos em centenas de maneiras diferentes. Podem criar seu perfil com base no que você compra e no que faz on-line.

Desta forma, com o avanço da utilização da internet em todas as formas na sociedade, mais e mais dados serão cedidos, armazenados e perfilados, diminuindo cada vez mais a privacidade, conseqüentemente, passa a ser necessária a proteção efetiva dos dados pessoais, situação que será objeto de discussão adiante.

3 PROTEÇÃO DE DADOS PESSOAIS NO BRASIL

A proteção de dados pessoais, apesar de ser um tema de extrema importância, demorou no Brasil para ser implementada. Somente no dia 29 de maio de 2018, o Projeto de Lei de Proteção de Dados Pessoais de número de origem 4060/2012 foi aprovado na Câmara dos Deputados. Após isso, o Projeto de Lei foi encaminhado para o Senado Federal, sob o número 53/2018, e aprovado pelos senadores no dia 10 de julho de 2018, indo para sanção presidencial (até o momento da elaboração do presente trabalho, o Projeto ainda não tinha sido sancionado pelo Presidente da República)

Antes a esse fato, o Brasil nunca teve lei ou qualquer tipo de norma para regulamentasse exclusivamente esta questão, ou seja, o Brasil nunca teve uma Lei Geral de Proteção de Dados Pessoais, somente algumas leis esparsas e setoriais que tratavam da matéria brevemente e não de forma aprofundada e específica, como por exemplo a Lei do Habeas Data (Lei n. 9507/97), no Código de Defesa do Consumidor (Lei n. 8078/90), Resolução CFM n. 1821/07 que dispõe sobre prontuário eletrônico e prontuário de dados médicos; a Lei 12.414/2011 que disciplinou o cadastro positivo e certos aspectos sobre proteção de dados pessoais em ambiente creditício; o Marco Civil da Internet (Lei n. 12.965/2014), que estabelece princípios, garantias, direitos e deveres para o uso da internet no Brasil e o seu próprio Decreto Regulamentador (Decreto n. 8771/2016). Daí a importância da sanção presidencial para o Projeto de Lei n. 53/2018 para a criação da Lei Geral Brasileira de Proteção de Dados Pessoais!

Mesmo não havendo uma lei de proteção de dados pessoais no Brasil, a doutrina já discutia amplamente as questões referentes a dados pessoais, fundamentando-se bastante na antiga Diretiva n. 95/46/CE de proteção de dados europeia, recentemente

alterada pelo Regulamento Geral de Proteção de Dados da União Europeia n. 2016/679.

Sobre a legislação europeia, Danilo Doneda (2006) apresenta os princípios norteadores encontrados já nas primeiras leis de proteção de dados pessoais na Europa. São eles resumidamente: 1) o princípio da publicidade, também conhecido como da transparência, o qual revela que deve ser de conhecimento público se existe algum banco de dado; 2) princípio da exatidão, de acordo com o qual os dados devem ser fieis à realidade, podendo ser corrigidos se não estiver condizente com ela; 3) princípio da finalidade, conforme o qual os dados pessoais devem ter uma finalidade para sua coleta, não podendo ser desviados para outros uso se não pela finalidade para qual ele foi coletado; 4) princípio do livre acesso, no qual o indivíduo tem o acesso ao banco de dados sobre suas informações, inclusive para controle e cópia; 5) princípio da segurança física e lógica, segundo o qual os dados devem ser protegidos, para não haver alguma adulteração, ou extravio.

Por outro lado, no Brasil, mesmo não havendo uma Lei Geral de Proteção de Dados Pessoais, o Marco Civil da Internet, Lei 12.965/2014, que estabeleceu princípios, garantias, direitos e deveres para o uso da internet no Brasil, apresentou em seu texto, ainda que de forma indireta, alguns princípios de proteção de dados, como é o caso da transparência e da publicidade, no artigo 7º VIII, o qual obriga haver informações claras e precisas da coleta, armazenamento, uso e do tratamento de dados pessoais, também o princípio da finalidade no artigo 7º, VIII, “a” o qual apresenta que deve haver a finalidade e a sua justificção para sua coleta, uso, tratamento e armazenamento de dados pessoais, e o da do princípio da segurança física e lógica previsto no artigo 3º, III, que o prevê na forma da lei.

Mesmo assim a mencionada Lei 12.965/2014, não estabeleceu ou definiu em seu texto o que é dado pessoal e tratamento de dados pessoais. Somente com seu Decreto Regulamentador (Decreto n. 8771/2016) restou evidenciado o que é dado pessoal e tratamento de dados pessoais no nosso país. Assim, segundo o artigo 14 do Decreto:

Art. 14. Para os fins do disposto neste Decreto, considera-se:

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

II - tratamento de dados pessoais - 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. (Decreto Lei n. 8771/2016)

Mesmo assim, vemos a importância de o Brasil ter uma Lei Geral de Proteção de Dados pessoais, pois atualmente temos apenas leis setoriais de proteção de dados que não conseguem abarcar, com a complexidade econômica do uso de dados pessoais na atual sociedade da informação para uma maior segurança jurídica, tanto o setor empresarial que se utiliza na economia de dados pessoais, quanto as pessoas comuns que necessitam da proteção de dados pessoais.

Nesse sentido, o Projeto de Lei de Proteção de Dados Pessoais que está para sanção do Presidente da República toca em pontos importantes, além de se aplicar a todas as formas de operação de coleta e tratamento de dados pessoais, seja para os setores públicos e privados, como pessoas naturais e jurídicas, como consta no artigo 3º do PL 54/2018. Além disso o PL define também em seu artigo 5º conceitos que antes não existiam em nenhum tipo de legislação no país, como: dado pessoal, dado pessoal sensível, dado anonimizado, banco de dados, titular, controlador, operador, agentes, tratamento, anonimização, consentimento, bloqueio, eliminação, transferência internacional de dados, uso compartilhado dos dados e relatório de impacto.

Também o Projeto de Lei firmou e deixou expressos os princípios de proteção de dados pessoais descritos anteriormente que já eram apontados na doutrina e nas legislações dos outros países, como os da finalidade, adequação, necessidade, livre acesso, qualidade dos dados, transparência, segurança, prevenção, não discriminação, responsabilização e prestação de contas.

Outro ponto de destaque é que o PL 54/2018 definiu que toda a pessoa natural é titular de seus dados pessoais, garantindo uma série de controle de seus dados. Além do mais, tornou mais rígido o tratamento de dados pessoais, exigindo diversos requisitos e destacando um tratamento diferenciado aos dados sensíveis e o tratamento de dados de crianças e adolescentes e estabeleceu uma série de garantias ao término do tratamento de dados.

No mais, estabeleceu regras e responsabilidade específicas ao poder público no tratamento de dados pessoais, no capítulo IV; no capítulo V, abordou a transferência internacional de dados, no VI, tratou os agentes de tratamento de dados pessoais, como do controlador e operador, do encarregado, da responsabilidade e do ressarcimento e dos danos causados; no VII, estabeleceu regras de segurança e das boas práticas, da segurança e dos sigilos de dados, das boas práticas de governança.

Outrossim, no capítulo VIII, estabelece regras de sanções administrativa, caso ocorram infrações, podendo gerar até mesmo advertências, como multa até dois por

cento do faturamento econômico da empresa ou 50 milhões de reais, e até mesmo a suspensão do exercício das atividades; no capítulo IX, determina a autoridade nacional de proteção de dados pessoais (ANPD) e do conselho nacional de proteção de dados pessoais e da privacidade, demonstrando ser multisetorial para não privilegiar somente uma camada da sociedade; e no final estabelece regras transitórias como alteração do Marco Civil da Internet e um período de *vacatio legis* de 18 meses.

Destaque que a autoridade autárquica especial, da administração pública indireta vinculada ao Ministério da Justiça de proteção de dados pessoais é necessária para aplicação da lei e sua fiscalização, uma vez que sem ela a lei será inócua, pois não existe na administração pública direta ou indireta, com prerrogativas similares para atuar nestes casos.

4 PROTEÇÃO DE DADOS PESSOAIS NA UNIÃO EUROPEIA

O continente europeu sempre esteve em passos adiantados na discussão e na implementação da proteção dos dados pessoais, tanto é assim que o projeto de se baseou no sistema europeu. Exemplo disso é a via dupla de controle dos dados pessoais, na qual segundo Drummond (2003), é necessária uma via de atuação dos órgãos governamentais e a outra via a legislativa. No Brasil, como anteriormente citado, a própria lei previu uma autoridade administrativa para aplicar a própria lei.

Na Europa, segundo Mendes (2014), as primeiras leis de proteção de dados pessoais se deram nos anos 1970, como no caso da Alemanha e Suécia, conforme houve a centralização dos bancos de dados nacionais. As primeiras leis visavam controlar a tecnologia, ou seja, buscavam o procedimento do tratamento dos dados e não o direito, com o avanço da tecnologia as unidades governamentais, e a iniciativa privada poderia gerir dados de forma descentralizada, aumentando cada vez mais o número de bancos de dados. Desse modo, surgiu a segunda geração de proteção de dados que visava ligar a proteção de dados pessoais a direitos fundamentais, como privacidade e a liberdade individual, como foram os casos das constituições Portugal, Espanha e Àustria. A terceira geração é marcada pela decisão do Tribunal Constitucional alemão, declarando o direito à autodeterminação informática em 1983, ou seja, a ideia de controle da pessoa sobre os seus dados pessoais. A quarta geração visava fortalecer o autocontrole dos dados pessoais por parte dos indivíduos, como é o caso da antiga Diretiva n. 95/56/CE do Parlamento Europeu e do Conselho, de 24 de outubro de 1995:

Isso porque está no seu cerne a participação dos indivíduo no processo de tratamento de dados pessoais. Além disso, em caso de tratamento de dados sensíveis, a Diretiva determina que ele está condicionado ao consento expresse e informado do indivíduo (MENDES, 2014, p. 44)

A Diretiva n. 95/56/CE da União Europeia foi importante pois, segundo Saldanha (2018, p. 04), “tornar equivalente em todos os Estados Membros o nível de proteção dos direitos e liberdades das pessoas no que diz respeito ao tratamento de dados pessoais”. Assim sendo, a diretiva unificava e obrigava um padrão legislativo dos países pertencentes na União Europeia

A Diretiva também foi importante por muito tempo para servir de exemplo e modelo para diversos outros países de como deveria se legislar sobre a proteção de dados pessoais, até mesmo o Marco Civil da Internet, possui resquícios de inspiração da Diretiva. Para Miranda (2018, p. 100):

A Diretiva 95/46/CE foi claramente um instrumento normativo com dois vieses: o primeiro protetivo, pois visava proteger a privacidade do cidadão europeu no processo de coleta, tratamento e transmissão de dados; e o segundo, a notória preocupação de que a proteção conferida ao cidadão não criasse barreiras demasiadas à transmissão de dados, inviabilizando o desenvolvimento científico e econômico, buscando equilibrar com regras claras a proteção e o fomento ao comércio

Mesmo a União Europeia tendo uma legislação atualizada de proteção de dados pessoais, com o desenvolvimento das novas tecnologias de comunicação e captação de dados, existiram ainda alguns conflitos entre as legislações nacionais entre os países membros da UE, sendo agravados com escândalos de espionagem do governo americano.

Assim, em 27 de abril em 2016, o Parlamento Europeu e o Conselho promulgaram o Regulamento Geral sobre a Proteção de Dados conhecido como GDPR, Regulamento de n. 2016/679 da União Europeia que é relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e a livre circulação desses dados pessoais, e revoga, a Diretiva 95/46/CE. Uma das principais diferenças entre a Diretiva e o Regulamento segundo Miranda (2018), é que a primeira tem como objetivo direcionar as legislações nacionais a seguir um mesmo caminho, adaptando conforme sua realidade social, cultura e econômica. Já o segundo tem força vinculante, é um ato legislativo aplicável para todos os países da União Europeia sem distinção, já que a antiga Diretiva era bastante fragmentada a respeito da proteção de dados pessoais.

A GDPR teve um período de *vacatio legis* de vinte quatro meses, ou seja, de dois anos, pois a implementação dela alcança diversos setores da sociedade europeia

que se utilizam de dados pessoais. Assim, somente em 25 de maio de 2018 começou a entrar em vigor a lei. Neste dia, foi marcado que os provedores de conteúdo, aplicações, serviços atualizariam seus termos de uso em suas políticas de privacidade para estar em conformidade legal, mandando diversos e-mails aos seus usuários avisando da atualização.

Não tendo o objetivo de exaurir todas as modificações e todo Regulamento Geral de Proteção de Dados Pessoais da União Europeia, este artigo tratará de alguns pontos mais importantes, já que os dois possuem pontos similares, com algumas modificações.

O Regulamento n. 2016/679 estabelece, segundo Saldanha (2018, p. 19) “que todas as pessoas singulares, independentemente da sua nacionalidade e do seu local de residência, relativamente ao tratamento de dados pessoais”, o artigo 1º da referida legislação ainda diz que:

2. O presente regulamento não se aplica ao tratamento de dados pessoais:
 - a) Efetuado no exercício de atividades não sujeitas à aplicação do direito da União;
 - b) Efetuado pelos Estados-Membros no exercício de atividades abrangidas pelo âmbito de aplicação do título V, capítulo 2, do TUE;
 - c) Efetuado por uma pessoa singular no exercício de atividades exclusivamente pessoais ou domésticas;
 - d) Efetuado pelas autoridades competentes para efeitos de prevenção, investigação, deteção e repressão de infrações penais ou da execução de sanções penais, incluindo a salvaguarda e a prevenção de ameaças à segurança pública. (PARLAMENTO EUROPEU E DO CONSELHO, online)

Ainda também a lei demonstra seus aspectos de aplicação material e territorial em seus artigos 2º e 3º; em seu artigo 4º define e conceitua, dados pessoais, tratamento, limitações do tratamento, definição de perfil, pseudonimização, ficheiro, responsável pelo tratamento, subcontratante, destinatário, terceiro, consentimento, violação de dados pessoais, dados genéticos, dados biométricos, dados relativos a saúde, estabelecimento principal, representante, empresa, grupo empresarial, regras vinculativas aplicáveis às empresas, autoridade de controle, autoridade de controle interessada, tratamento transfronteiriço, objetivação pertinente e fundamentada, serviços da sociedade da informação, organização internacional.

No artigo 5º, define os princípios que já eram previsto na antiga diretiva, da transparência e licitude, finalidade, adequação e pertinência, exatidão, da segurança. A inovação trazida pelo GDPR segundo Raposo (2018) é o princípio da responsabilidade proativa, o qual exige que as organizações que tratam dados pessoais atuem de uma

forma proativa, consciente e diligente a todos os tratamentos de dados pessoais que realizam.

Além disso, o regulamento trata as causas de licitude de tratamento de dados pessoais, bem como as condições do consentimento da sua coleta, dando uma atenção específica ao consentimento das crianças no artigo 8, e ainda nos artigos 9 a 11 mostram outros tipos especiais de tratamento de dados. No mais, a lei especifica as informações sobre o tratamento, coleta, armazenamento de dados, como também ao direito ao acesso, a limitação, além do direito ao apagamento dos dados no artigo 17.

Enfim, a lei também inclui sanções; responsabilidade; questões de ação judicial, da formação do comitê europeu de proteção de dados pessoais e das autoridades de controle independentes; a cooperação internacional no domínio da proteção de dados pessoais; códigos de conduta e certificação; avaliação de impacto sobre a proteção de dados pessoais; questões referentes a segurança de dados.

CONCLUSÃO

A sociedade da informação tem evoluído muito, atualmente as tecnologias da informação e comunicação tem feito parte da vida das pessoas com muito mais frequência e importância. Praticamente não fazemos mais nada no nosso cotidiano sem utilizar ao menos uma forma dessas tecnologias. Assim, com esse avanço tecnológico, gradativamente mais dados pessoais serão produzidos pela sociedade e poderão ser coletados, manipulados, armazenados, utilizados e tratados de maneiras e finalidades diversas que podem ser positivas ou mesmo negativas. Deste modo, a proteção de dados pessoais deve existir seja para proteger o cidadão de uma interferência ou vigilância severa, seja para manutenção da vida privada e a intimidade das pessoas. A privacidade tem um papel de importância para o desenvolvimento intelectual e da personalidade humana, devendo ser protegida. Trata-se, sem dúvida, de uma questão importante tanto no aspecto ético como no aspecto jurídico e que, devemos nos debruçar para que nossos direitos fundamentais e da personalidade sejam respeitados, tendo como fundamento principal a dignidade da pessoa humana.

O Regulamento Geral de Proteção sobre a Proteção de Dados Pessoais (GDPR), ou seja, a lei europeia de proteção dos Dados Pessoais, é um documento importante para nosso ordenamento jurídico, pois, além de nos afetar diretamente, posto que qualquer relação comercial internacional traçada com qualquer pessoa ou empresa que esteja no território europeu deverá respeitar suas determinações, serve também de exemplo para

que possamos criar uma cultura e legislação sobre a importância da proteção de dados na sociedade contemporânea. Tanto é assim, que percebemos a influência das posições europeias sobre o tema, no Projeto de Lei brasileiro aprovado na Câmara e que segue para sanção presidencial. Importante também ressaltar que o GDPR possui uma sofisticação jurídica de aplicabilidade e tutela da proteção dos dados pessoais, da proteção dos direitos da personalidade, em especial da privacidade e, além disso, busca enfrentar a realidade da atual sociedade da informação e a defesa dos direitos pessoais.

O projeto de lei de proteção de dados pessoais do Brasil que está em fase de sanção possui diversos pontos de contato com o GDPR e, entendemos, que este é um ponto bastante positivo para o direito brasileiro.

No mais, para que exista aplicabilidade e eficácia da proteção de dados pessoais, defendemos também, como consta no projeto de lei de proteção de dados pessoais, a criação da autoridade autárquica fiscalizadora, pois, sem ela, a lei pode tornar-se ineficaz e inaplicável, de tal modo que não existe, na administração pública direta e indireta, uma entidade que tenha prerrogativas para tal, já que a lei aplica-se a todos aqueles que tratam de dados pessoais, não sendo setorial.

Assim, as legislações apresentadas, tanto a brasileira, quanto a europeia, estão de acordo com a proteção necessária, buscando sempre uma equidade entre as relações individuais, do estado e do terceiro setor, lembrando, entretanto, que as normas deverão sempre ser atualizadas de acordo com a necessidade da sociedade e a evolução tecnológica. Somente assim será possível realmente a proteção dos dados pessoais como forma de defesa aos direitos fundamentais e da personalidade.

REFERÊNCIAS

ASCENSÃO, José de Oliveira. Direito da internet e da sociedade da informação: estudos. Rio de Janeiro: Forense, 2002.

BARRETO JUNIOR, Irineu Francisco. A relevância do conceito Sociedade da Informação para a pesquisa jurídica. In: PAESANI, Liliana Minardi. Direito na Sociedade da Informação. São Paulo: Atlas, 2007.

BITTAR, Carlos Alberto. Os direitos da personalidade. 2.a ed. Rio de Janeiro: Forense Universitária, 1995.

BRASIL, Decreto n. 8771, de 11 de maio de 2016. Regulamenta a Lei no 12.965, de 23 de abril de 2014, para tratar das hipóteses admitidas de discriminação de pacotes de dados na internet e de degradação de tráfego, indicar procedimentos para guarda e proteção de dados por provedores de conexão e de aplicações, apontar medidas de

transparência na requisição de dados cadastrais pela administração pública e estabelecer parâmetros para fiscalização e apuração de infrações. Disponível em <http://www.planalto.gov.br/ccivil_03/_Ato2015-2018/2016/Decreto/D8771.htm>. Acesso em: 20 jul. 2018.

CASTELLS, Manuel. A era da informação: economia, sociedade e cultura. V. I. A sociedade em rede. 14. ed. São Paulo: Paz e Terra, 2011.

CUPIS, Adriano de. **Os direitos da personalidade**. Campinas, Romana Editora, 2004.

DINIZ, Maria Helena. Curso de direito civil brasileiro, vol 1: teoria geral do direito civil. 29. ed. São Paulo: Saraiva, 2012.

DONEDA, Danilo. Da privacidade à proteção de dados pessoais. Rio de Janeiro: Renovar, 2006.

DRUMMOND, Victor. Internet, privacidade e proteção de dados pessoais. Rio de Janeiro: Lumen Juris, 2003.

FRANÇA, Rubens Limongi. Direitos da personalidade. **Revista dos Tribunais**. São Paulo, n.º 567, p. 09-16, jan. 1983.

GONÇALVES, Carlos Roberto. Direito civil brasileiro, volume 1: parte geral. 10. ed. São Paulo: Saraiva, 2012.

LEONARDI, Marcel. Tutela e privacidade na internet. São Paulo: Saraiva, 2012.

LISBOA, Roberto Senise. O consumidor na sociedade da informação. In: PAESANI, Lilana Minardi (coord.). O direito na sociedade da informação. São Paulo: Atlas, 2007.

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

MENDES, Laura Schertel. Privacidade e proteção de dados e defesa do consumidor: linhas gerais de um novo direito fundamental. São Paulo: Saraiva, 2014.

MIRANDA, Leandro Alvarenga. A proteção de dados pessoais e o paradigma da privacidade. São Paulo: All Print Editora, 2018.

PARLAMENTO EUROPEU E DO CONSELHO. Regulamento geral de proteção de dados pessoais. Disponível: <<https://protecao-dados.pt/wp-content/uploads/2017/07/Regulamento-Geral-Prote%C3%A7%C3%A3o-Dados.pdf>>. Acesso em: 20 jul. 2018.

RAPOSO, Jorge Nunes. Guia prático do regulamento geral sobre proteção de dados pessoais. Lisboa: Edição do autor, 2018.

RODOTÀ, Stefano. A vida na sociedade da vigilância. Rio de Janeiro: Renovar, 2008.

SALDANHA, Nuno. Novo regulamento geral de proteção de dado: o que é? a quem se aplica? como implementar?. Lisboa: FCA, 2018.

SILVA NETO, Amaro Moraes e. Privacidade na internet: um enfoque jurídico. Bauru: Edipro, 2001.

SILVA, José Afonso da. Curso de direito constitucional positivo. 25.ed. São Paulo: Malheiros, 2005.

TAPSCOTT, Don. A hora da geração digital: como os jovens que cresceram usando a internet estão mudando tudo, das empresas aos governos. Rio de Janeiro: Agir Negócios, 2010.