XXVII ENCONTRO NACIONAL DO CONPEDI SALVADOR – BA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

JOSÉ RENATO GAZIERO CELLA

AIRES JOSE ROVER

FERNANDO GALINDO AYUDA

Copyright © 2018 Conselho Nacional de Pesquisa e Pós-Graduação em Direito

Todos os direitos reservados e protegidos. Nenhuma parte destes anais poderá ser reproduzida ou transmitida sejamquaisforemosmeiosempregadossemprévia 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 Naspolini - 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 – Santa Catarina
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 – Goías
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

---

D597

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

Coordenadores: José Renato Gaziero Cella; Aires Jose Rover; Fernando Galindo Ayuda – Florianópolis: CONPEDI, 2018.

Inclui bibliografia
ISBN: 978-85-5505-610-9
Modo de acesso: www.conpedi.org.br em publicações
Tema: Direito, Cidade Sustentável e Diversidade Cultural

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

CDU: 34

Conselho Nacional de Pesquisa
e Pós-Graduação em Direito Florianópolis
Santa Catarina – Brasil
www.conpedi.org.br

Universidade Federal da Bahia - UFBA
Salvador – Bahia - Brasil
https://www.ufba.br/

XXVII ENCONTRO NACIONAL DO CONPEDI SALVADOR – BA

DIREITO, GOVERNANÇA E NOVAS TECNOLOGIAS

Apresentação

Os encontros nacionais do Conselho Nacional de Pesquisa e Pós-graduação em Direito (Conpedi) têm se consolidado como referência na disseminação de pesquisas que abordam os novos fenômenos envolvendo o direito e o Grupo de Trabalho Direito, Governança e Novas Tecnologias é exemplo de pesquisas desse tipo.

Nesta edição houve uma diversidade muito grande de temas e tópicos, diferentemente de edições passadas em que se concentravam em um ou dois temas. Numa tentativa de dar certa unidade temática, ainda assim podemos organizar os artigos em quatro grupos.

O primeiro com temas bem diversos de direito privado envolvendo compliance, inovação em micro e pequenas empresas, responsabilidade civil em situações de uso de veículos autônomos, fintech e o direito do consumidor, novas alternativas de resolução de conflitos e os influencers digitais e a publicidade oculta nas redes sociais.

Outro grupo sempre presente é o da democracia e governança digital. Assim, tópicos como ciberdemocracia e as redes sociais, governança dos sistemas judiciais, populismo e pós-verdade na sociedade da informação e os desafios à neutralidade da rede foram discutidos e aqui publicados.

O grupo de artigos que segue tem um tema que sempre está presente de alguma forma, os dados pessoais e sua proteção. A hiperexposição pessoal nas redes sociais, os dados pessoais sensíveis e os e-mails corporativos, e o direito ao esquecimento na internet foram tópicos tratados.

Por fim, um tema que muito foi tratado na edição passada, a inteligência artificial no direito, teve apenas um artigo, o mesmo ocorrendo com a questão do teletrabalho, artigo com o qual fechamos esta publicação do Conpedi.

Enfim, os coordenadores do GT convidam a todos a ler o teor integral dos artigos, agradecendo a participação dos autores pesquisadores desta edição.

Prof. Dr. Aires José Rover – UFSC

Prof. Dr. Fernando Galindo Ayuda – UNIZAR

Prof. Dr. José Renato Gaziero Cella – IMED

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.

A SEGURANÇA DOS DADOS PESSOAIS NO BRASIL E O DOCUMENTO NACIONAL DE IDENTIDADE

THE SECURITY OF PERSONAL DATA IN BRAZIL AND THE NATIONAL IDENTITY DOCUMENT

Rafael Copetti [1]
José Renato Gaziero Cella [2]

Resumo

O estudo analisa o regime jurídico da Identificação Civil Nacional e da proteção de dados pessoais no Brasil e tem como objetivo, por meio do método hipotético-dedutivo, diante da previsão de centralização e compartilhamento dos bancos de dados entre diferentes entes governamentais e de ausência de legislação protetiva, a potencial violação ao direito constitucional à privacidade. Percebe-se, ao final, a necessidade de regramento específico à efetiva proteção dos indivíduos.

Palavras-chave: Identificação civil nacional, Documento nacional de identidade, Proteção de dados pessoais, Privacidade, Justiça eleitoral

Abstract/Resumen/Résumé

The study analyzes the legal regime of the National Civil Identification and of the personal data protection in Brazil and aims to demonstrate, through the hypothetical-deductive method, in view of centralization and sharing of databases between different government entities and absence of protection legislation, the potential violation of the constitutional right to privacy. At last, it is possible to notice the need of a specific instrument to effective protection of individuals.

Keywords/Palabras-claves/Mots-clés: Nacional civil identification, National identity document, Personal data protection, Privacy, Electoral justice

[1] Mestre em Direito, Democracia e Sustentabilidade da Faculdade Meridional – IMED de Passo Fundo/RS. Especialista em Direito Público pela Faculdade Meridional - IMED/ESMAFE. Servidor Público Federal do TRE-RS.

[2] Doutor em Filosofia e Teoria do Direito pela UFSC. Mestre em Direito do Estado pela UFPR. Professor do Programa de Pós-Graduação Stricto Sensu em Direito da Faculdade Meridional - PPGD/IMED

1. INTRODUÇÃO

A sociedade contemporânea, permeada por dispositivos informáticos que permitem o processamento de milhares de informações, quase que de forma instantânea, a partir de apenas um *click,* tem entre as suas características a celeridade com que a informação circula ao redor do mundo e o volume de dados disponíveis na rede mundial de computadores.

As pessoas estão cada vez mais expostas nas suas relações, sejam elas privadas ou públicas. As informações são coletadas de diferentes formas, na navegação ou cadastros em páginas da internet, fornecidas diretamente pelo usuário, em bancos de dados de diversas fontes ou como requisitos para a obtenção de determinado serviço ou documento perante o Poder Público.

Não obstante, não se observa uma preocupação efetiva com a proteção dos dados pessoais dos cidadãos. O tema é recorrente e ganha relevo com a criação do Documento Nacional de Identidade (DNI) instituído por meio da Lei n° 13.444, de 11 de maio de 2017, a qual dispõe sobre a Identificação Civil Nacional (ICN).

Entre outros aspectos a serem abordados, o novel regramento permite o compartilhamento aduz que o Tribunal Superior Eleitoral irá garantir aos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios acesso à base de dados do ICN, de forma gratuita, excetuando-se apenas questões atinentes às informações eleitorais.

Assim, como problema do presente estudo, surge o questionamento se a Lei que institui a Identificação Civil Nacional traz elementos que asseguram a proteção de dados pessoais no Brasil, notadamente, diante da previsão de compartilhamento dos bancos de dados entre diferentes entes governamentais.

A partir dessa perspectiva, busca-se confirmar a hipótese que a legislação brasileira preserva de forma mitigada as informações do acesso e tratamento dos dados indiscriminado, não estabelecendo limites que respeitem a privacidade dos indivíduos.

Especificamente é objetivo analisar a legislação que institui o documento de identificação único, averiguar a garantia constitucional da privacidade diante do mundo permeado pelas tecnologias de informação e comunicação e o contexto jurídico normativo de proteção de dados pessoais.

A pesquisa utiliza o método de abordagem hipotético-dedutivo, partindo da análise da Lei 13.444/2017, contextualizando a privacidade e o regime jurídico de proteção de dados no Brasil, voltando-se a análise de instrumentos à salvaguarda desses direitos.

Ao final, percebe-se ser necessário uma análise mais pormenorizada à implantação de documentos ou outras iniciativas que demandem a manejo de dados pessoais. Torna-se essencial a utilização de institutos eficazes à proteção de dados pessoais, além de implantação de legislação protetiva desses dados, na qual se defina responsabilidades, meios de controle e de processamento das informações armazenadas.

2. IDENTIFICAÇÃO CIVIL NACIONAL – ICN

A Lei n° 13.444, publicada no Diário Oficial da União em 12 de maio de 2017, é a legislação que institui a Identificação Civil Nacional no território brasileiro com o objetivo de identificar o brasileiro nas relações com a sociedade e com os órgãos e entidades governamentais e privados.

No mesmo texto legislativo é criado o Documento Nacional de Identidade (DNI), o qual "faz prova de todos os dados nele incluídos, dispensando a apresentação dos documentos que lhe deram origem ou que nele tenham sido mencionados" (BRASIL, 2017x).

A emissão do DNI será emitido tanto pela Justiça Eleitoral quanto pelos institutos de identificação civil dos Estados e do Distrito Federal, com certificação pela Justiça Eleitoral, e também emitido por outros órgãos, mediante delegação do Tribunal Superior Eleitoral (TSE).

Haverá uma concentração das informações e guarda das informações no âmbito da Justiça Eleitoral, responsável, por meio do seu órgão superior (TSE), pela gestão do trabalho. Foi criado o Comitê Gestor da ICN, com responsabilidade de recomendações no estabelecimento de critérios e padrões do novo documento, como o padrão biométrico, formação do número. Cabe, ainda, ao Comitê Gestor a orientação e implementação da interoperabilidade entre os sistemas eletrônicos do Poder Executivo federal e da Justiça Eleitoral.

O Comitê Gestor possui, nos termos do artigo 5° (BRASIL, 2017x), uma composição híbrida, sendo formado por 3 (três) representantes do Poder Executivo federal, 3 (três) do Tribunal Superior Eleitoral, 1(um) da Câmara dos Deputados, 1 (um) do Senado Federal e 1 (um) do Conselho Nacional de Justiça.

Entre os objetivos da criação da ICN está a reunião em um único documento as informações de identificação do cidadão e, por conseguinte, praticamente a totalidade dos documentos utilizados atualmente pelos brasileiros, hoje em torno de 20 (vinte) documentos (por exemplo, identidade civil – RG, CPF, título de eleitor, PIS/PASEP, carteiras funcionais,

carteira de trabalho, certidão de nascimento e casamento, certificado de reservista, cadastro em programas governamentais).

Inicialmente já foi previsto na lei instituidora do ICN que o DNI poderá substituir o título de eleitor e que o número de inscrição no Cadastro de Pessoas Físicas (CPF) será incorporado pelo novel documento de identidade.

A ideia de simplificação e desburocratização nas relações do Estado e as pessoas físicas e jurídicas, assim como nas interações entre estas últimas, é de grande valia e iniciativa esperada por parcela significativa da sociedade. Um documento único, além de limitar a quantidade de números e códigos que são necessários numa relação entre as partes citadas, facilita a identificação das pessoas e centraliza as operações em um órgão específico e dificulta fraudes.

Todavia, é preciso analisar se os direitos fundamentais do cidadão, notadamente a privacidade, serão preservados. Como sabido, a Justiça Eleitoral administra o maior cadastro de cidadãos de toda América Latina, atualmente com cerca de 146 milhões e 500 mil de eleitores, sendo mais 82 milhões registrados biometricamente, representando 56% do eleitorado total (TRIBUNAL SUPERIOR ELEITORAL, 2018a).

As referidas observações e informações ganham mais destaque especialmente porque há expressa previsão acerca da integração e utilização do banco de dados por outros entes da Administração Pública. De acordo com a legislação aprovada, nos termos do art. 3º, §1º, da Lei 13.444/2017, "O Poder Executivo dos entes federados poderá integrar aos seus próprios bancos de dados as informações da base de dados da ICN, com exceção dos dados biométricos" (BRASIL, 2017).

Ademais, o acesso à base de dados da ICN deverá, nos termos do art. 3º do diploma legal, ser garantida aos Poderes Executivo e Legislativo da União, dos Estados, do Distrito Federal e dos Municípios, de forma gratuita, excetuando-se quanto às informações eleitorais.

Ainda, a lei não definiu, transferindo essa responsabilidade para ato do TSE, acerca da integração dos registros biométricos pelas Polícias Federal e Civil.

A comunicabilidade entre os diferentes bancos está igualmente assegurada quando no texto legal há referência expressa que o poder público deverá oferecer mecanismos que tornem possível o cruzamento de informações constantes de bases de dados oficiais, a partir do número de inscrição no CPF do solicitante, com intuito, nos termos do art. 11, de "verificação do cumprimento de requisitos de elegibilidade para a concessão e a manutenção de benefícios sociais" (BRASIL, 2017) pelo órgão concedente.

Importante salientar que a ICN utilizará, nos termos do art. 2º (BRASIL, 2017):

> I - a base de dados biométricos da Justiça Eleitoral;
> II - a base de dados do Sistema Nacional de Informações de Registro Civil (Sirc), criado pelo Poder Executivo federal e da Central Nacional de Informações do Registro Civil (CRC Nacional), instituída pelo Conselho Nacional de Justiça (...);
> III – outras informações, não disponíveis no Sirc, contidas em bases de dados da Justiça Eleitoral, dos institutos de identificação dos Estados e do Distrito Federal ou do Instituto Nacional de Identificação, ou disponibilizados por outros órgãos, conforme definido pelo Comitê Gestor da ICN.

Resta clara, portanto, a intenção legislativa de transferência de dados e informações entre os diferentes bancos de dados estatais. O procedimento de como isso se dará não fica regulado pela Lei, mencionando apenas que cabe ao TSE a manutenção do banco de dados, a autenticidade deste e a confidencialidade do seu conteúdo, além da já mencionada interoperabilidade entre os sistemas eletrônicos governamentais. Quanto a este último aspecto, há remissão de que será observada a legislação aplicável e as recomendações técnicas da arquitetura dos Padrões de interoperabilidade entre os sistemas eletrônicos governamentais.

O banco de dados a ser formado trará informações de relevância cujo conteúdo versa acerca de aspectos individuais dos cidadãos. Um exemplo são as informações repassadas por todas as pessoas que solicitam o alistamento eleitoral e que realizam movimentação cadastral no âmbito da Justiça Eleitoral.

Para que o indivíduo possa realizar a sua inscrição eleitoral, transferir seu domicilio eleitoral ou atualizar dados cadastrais é necessário que compareça pessoalmente ao Cartório Eleitoral do seu domicílio eleitoral.

Entre os dados obrigatórios para o expedição do título de eleitor é possível destacar: nome, data de nascimento, nome da mãe, nome do pai, documento de identificação (com número e órgão expedidor), estado civil, sexo (masculino e feminino), Unidade da Federação (UF) e município de nascimento, grau de instrução, ocupação principal, informar se possui ou não irmão(ã) gêmeo(a). (TRIBUNAL SUPERIOR ELEITORAL, 2018b).

Ainda, deve ser informado se o indivíduo é portador de necessidade especial (informando se essa deficiência é visual, de locomoção, outros, visual e locomoção, visual e outros, locomoção e outros, visual, locomoção e outros), código endereçamento postal (CEP), UF e município de residência, logradouro, tempo (anos e meses) de domicílio no município em que esta realizando a operação e, por fim, escolher o respectivo local de votação. (TRIBUNAL SUPERIOR ELEITORAL, 2018b).

Não aparecerem como campos obrigatórios, embora disponíveis para preenchimento, o CPF, número da residência, complemento deste último campo e dois números de telefone. (TRIBUNAL SUPERIOR ELEITORAL, 2018b).

Juntamente com a coleta dessas informações, a Justiça Eleitoral atualiza o cadastro de eleitores com informações biométricas. Em outras palavras, como requisito para a confecção do título de eleitor será preciso que o eleitor, além de assinar em um aparelho eletrônico, tenha uma fotografia e as digitais dos dez dedos coletadas.

Portanto, é preciso refletir acerca controle desses dados relativos à personalidade do indivíduo (sexo, escolaridade, residência, data de nascimento, filiação, entre outros), assim como os biométricos (assinatura digital, foto e impressões digitais dos dedos de ambas as mãos) por órgão do Poder Judiciário. Em especial no ordenamento jurídico brasileiro que não possuí disciplina específica acerca do tema.

A centralização de informações em um único banco de dados facilita o acesso a detalhes privados da vida dos cidadãos. Ainda mais na sociedade atual, permeada por dispositivos informáticos que permitem o processamento de milhares de informações a partir de apenas um *click* e possibilita que a informação circule ao redor do mundo com celeridade impressionante.

As tecnologias utilizadas, combinadas com outras informações, como, por exemplo, a utilização de senhas de acesso e dados biométricos, fazem com que se individualize o usuário e seja possível traçar um perfil baseado nas suas atividades diárias e movimentações financeiras.

Dados cujo interesse é de grande relevância e valor imensurável, tanto na iniciativa privada quanto pública. Na primeira, é possível citar (apenas a título exemplificativo) o interesse de empresas que vender produtos aos usuários baseadas em atividades recentes ou um perfil construído pelo conjunto de dados tratadas. Ao poder público para utilização em programas assistenciais e controles de acesso e circulação em diversos locais.

A ausência de uma legislação protetiva dos dados pessoais auxilia a tornar temerária uma centralização de dados. É preciso a observância dos princípios protetivos na coleta, tratamento e armazenamento. Além disso, uma definição clara de responsabilidades e funções, em outras palavras, um sistema de salvaguardas ao direito constitucional da privacidade.

Reunir todas as informações em um único documento tem um grande potencial de fragilizar os sistemas de proteção de dados pessoais passíveis de ser implementados, na medida em que uma possível vulneração do documento único permitirá o acesso indevido a

todos os dados relevantes, inclusive dados sensíveis, do cidadão. Ainda, são disponibilizadas às autoridades estatais informações que não lhes seria legítimo aceder, com a elevação de exercício de controles nem sempre utilizados de forma adequada. (CELLA, ARNS DE OLIVEIRA, 2015).

Não que tange à imposição de sanções em caso de eventual transgressão aos limites objetivamente definidos na legislação, cabe destacar que não basta apenas a aplicação de sanções pecuniárias e cujo arbitramento fique ao alvitre do julgador. É preciso que sejam estabelecidos balizas na própria lei de forma proporcional à gravidade da norma violada, de forma que tanto quem irá concretizar a norma ou aquele que a viola tenha possibilidade de saber o que se espera e as consequências dos atos. Do contrário, corre-se o risco de patrimonializar o direito à privacidade, o qual, na realidade, está diretamente relacionado à personalidade do indivíduo.

3. REGIME JURÍDICO E A PRIVACIDADE NA LEGISLAÇÃO BRASILEIRA

Ao falar sobre a proteção jurídica da privacidade, da vida privada ou da intimidade, Doneda (2006, p. 101), assevera acerca da definição do tema:

> Ao se tratar da privacidade, há de se fazer antes de tudo um esclarecimentoinicial sobre a terminologia utilizada. A profusão de termos utilizados pela doutrina brasileira para representa-la , propriamente ou não, é considerável; além de 'privacidade' propriamente dito, podem ser lembrados os termos: vida privada, intimidade, segredo, sigilo, recato, reserva, intimidade da vida privada, e outros menos utilizados, como 'privatividade' e 'privaticidade', por exemplo. O fato da doutrina estrangeira apontar igualmente para uma multiplicidade de alternativas certamente contribui, induzindo juristas brasileiros a experimentar diversas destas.

De acordo com Limberger (2007, p. 116), a intimidade como direito fundamental tem sua gênese na "[…] dignidade humana e está vinculado à própria personalidade, sendo seu núcleo central. Como direito que é da expressão da própria pessoa, desfruta da mais alta proteção constitucional". Para a autora, "[…] As exigências do mundo tecnológico atual fizeram com que o direito tutelasse essa nova face da intimidade. A intimidade deriva da dignidade humana, é um direito fundamental que integra a personalidade. Das relações da informática e a intimidade se desenvolve a autodeterminação informativa. […]" (LIMBERGER, 2007, p. 119).

Para Rodotá (1995, p. 122), a privacidade é "[…] o direito de manter o controle sobre as próprias informações e de determinar as modalidades de construção da própria esfera privada […]".

No direito brasileiro, o direito à privacidade pode ser entendido como um direito da personalidade de matiz constitucional, com expressa previsão no artigo 5º, inciso X, da Constituição da República.

Infraconstitucionalmente, a proteção da privacidade se consubstancia na cláusula geral estabelecida no artigo 21 do Código Civil. Ainda, destaca-se que as previsões legislativas específicas para a proteção de dados são escassas. Tem-se, na Lei 8.078/90 – Código de Defesa do Consumidor, a regulamentação dos bancos de dados e cadastros de consumidores em único dispositivo, o artigo 43. Além disso, há a regulamentação do chamado cadastro positivo pela Lei 12.414/2011, que disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito.

No presente estudo, a privacidade é concebida

> [...] como um direito fundamental, em sentido amplo, capaz de recepcionar em seu bojo a proteção da vida privada, da intimidade, da imagem, da honra e dos direitos-base vinculados ao conceito de direitos de privacidade na internet, significa dizer que, na contemporaneidade, o direito de navegar na internet com privacidade, o direito de monitorar quem monitora, o direito de deletar dados pessoais e o direito de proteger a identidade online devem ser tutelados, explícita e expressamente, como um dos pilares de garantia da eficácia do direito fundamental à privacidade em sentido amplo. (FORTES, 2015, p. 188).

A proteção dos dados no sistema normativo da União Europeia (UE) é tratada por meio de um sistema de regulamentos e diretivas, na qual é possível encontrar aspectos pioneiros no regramento da matéria. Há registro de legislações, por exemplo, na Alemanha e Suécia desde a década de 70. Portugal, em 1976, e, posteriormente, Espanha, 1978, foram os primeiros países a elevar a proteção em nível constitucional, trazendo previsões expressas nas respectivas Cartas.

Atualmente, as Diretivas 95/46/CE e 2002/58/CE, e Regulamento 45/2001, trazem diretrizes aos países integrantes da UE. Ganham destaque também os Relatórios e Comunicações de acompanhamento da implantação e eficiência das normativas (FORTES, 2015, p. 132-133).

Cabe mencionar que desde o início de 2012 foi formada a Comissão Europeia para regulamentação sobre a proteção de dados pessoais. Entre os objetivos expostos há referência que

> *La Comisión europea quiere modernizar la legislación europea de protección de datos para garantizar la intimidad de los consumidores y hacerla compatible con la libre circulación de datos en la UE . [...]*
> *Las empresas sólo estarán autorizadas a enviar información personal fuera de la UE a países con un nivel similar en sus sistemas de protección de datos. Se trata además de mejorar y simplificar los mecanismos de transferencia internacional de datos. [...]*
> *El objetivo de la nueva estrategia es consolidar un enfoque común en toda la UE. Las divergencias actuales no permiten determinar con nitidez la legislación aplicable en cada caso. Por eso es necesario armonizar las normas y reforzar el poder de las autoridades de protección de datos con el principio de cooperación y coordinación. (COMISIÓN EUROPEA, 2010).*

Referidas premissas servem ao mesmo tempo de alerta à constante mutação e evolução da tecnologia e da forma com os dados podem ser armazenados e manipulados. É importante, ainda, considerar a facilidade do intercâmbio de informações e procurar meios para que essa circulação atenda requisitos de segurança e preservação da privacidade.

A utilização dos recursos tecnológicos alterou significativamente a circulação, a forma de compartilhamento e o armazenamento de dados. A digitalização de documentos e o arquivamento de informações em bancos de dados digitais é cada vez mais significativo.

Nesse contexto, a proteção de dados pessoais nos sistemas jurídicos em geral necessita uma análise mais criteriosa, principalmente no sistema jurídico brasileiro, no qual não se tem uma legislação específica acerca da proteção dos dados pessoais.

Ao contrário da legislação encontrada em países da Europa, não há no sistema jurídico brasileiro, por exemplo, uma autoridade responsável e independente, dedicada a preservar o consentimento e o uso de dados pessoais mediante a supervisão do cumprimento das obrigações dos responsáveis pelo tratamento de dados, as quais possuem previsão específica. (GALINDO, 2013, p. 136).

De acordo com a normativa europeia, em caso de descumprimento, qualquer cidadão pode reclamar à autoridade de proteção dos dados, a qual estará apta a instaurar procedimento administrativo e aplicar sanções ao responsável. Referida característica, conforme Galindo (2013, p. 137), é relevante, pois:

> *se completó este cuadro de derechos y obligaciones con la atribución legal a la autoridad de protección de datos de su obligación de velar por el cumplimiento de las medidas conducentes a evitar la modificación de los datos personales por la*

utilización de las técnicas de seguridad de las TIC consideradas más adecuadas en cada momento.

A existência de autoridade responsável pela proteção dos dados, com atribuições claras e voltadas a não transgressão dos dados pessoais afigura-se, portanto, um relevante mecanismo.

4. ELEMENTOS PARA UMA PROTEÇÃO DE DADOS PESSOAIS

A autodeterminação informativa é um direito que orienta até hoje a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistsema jurídico romano-germânico. "Concebido como um direito fundamental (...), o direito à autodeterminação informativa proporciona ao indivíduo o controle sobre suas informações" (DONEDA, 2006, p. 196-197).

Um julgamento (*BverfGE 65,1*) emblamático do Tribunal Constitucional Federal da Alemanha, em 15 de dezembro de 1983, foi o qual se averiguou a constitucionalidade da lei que ordenava o recenseamento geral da população, com dados sobre a profissão, moradia e local de trabalho para fins estatísticos.

Segundo o Tribunal Constitucional Federal da Alemanha, em virtude das condições do moderno processamento de dados, o direito geral da personalidade contido no artigo 2 *I GG*, em conjugação com o artigo 1 *I GG*, passa a abranger a proteção do indivíduo contra levantamento, armazenagem, uso e transmissão irrestritos de seus dados pessoais, que somente podem ser utilizados, em princípio, com sua autorização. Essa norma consubstancia um direito geral à autodeterminação sobre a informação, que somente é restringível se houver a contraposição de um interesse predominante da coletividade (SCHWABE, 2005, p. 233-235).

Na construção dessa norma concreta, o Tribunal Constitucional Federal da Alemanha considerou que o direito ao livre desenvolvimento da personalidade abrange o poder do indivíduo de decidir, por si próprio, quando, quais e em que limites os fatos pessoais serão revelados, poder que, diante da evolução tecnológica atinente ao processamento automático de dados, depende de uma proteção especialmente intensa. (SCHWABE, 2005, p. 237).

A faculdade contemporânea e futura de armazenamento ilimitado, transmissão instantânea e consulta irrestrita de dados atentaria contra a autodeterminação individual, uma vez que não mais possibilitaria a determinação, com segurança, de quais informações sobre a

sua pessoa são conhecidas nem por quem são acessadas, inibindo substancialmente a liberdade de planejar ou decidir com autodeterminação. (SCHWABE, 2005, p. 237).

Esse direito à autodeterminação informativa, porém, não é absoluto, mas restrito quanto às informações de interesse geral predominante, quer dizer, limitável excepcionalmente quando imprescindível para a consecução de um interesse público. Tais restrições exigem uma base constitucional que possibilite o conhecimento pelo cidadão, de forma clara e reconhecível, dos pressupostos e da extensão das limitações, atendendo ao princípio da transparência (ou clareza normativa) do Estado de Direito. (SCHWABE, 2005, p. 237-239).

Entre a importância da decisão citada, na qual se concebe o autodeterminação informativa como direito fundamental, aponta Mario Panebianco (*apud* DONEDA, 2006, p. 197), há que se destacar que assertiva que "Os direitos fundamentais não são concedidos ao cidadão para que deles disponha livremente, porém na sua condição de membro da comunidade e também no interesse público".

Na espanha, a tema igualmente tem acolhida, sendo que a sentença 254/93 do Tribunal Constitucional Espanhol é considerada uma referência na matéria. É a partir dela que se acentuam as discussões acerca do surgimento de um novo direito fundamental (da autodeterminação informativa) ou uma evolução do que seria o direito à intimidade.

Murillo (2009, p. 34) menciona que na STC 292/2000 há várias referências ao direito fundamental da proteção de dados, diferenciando-o da intimidade. Pois se compartilham o objetivo de oferecer uma eficaz proteção constitucional da vida privada pessoal e familiar, aquele atribui ao titular a faculdade a seu titular uma séria de faculdades que consiste em sua maior parte no poder jurídico de impor a terceiros a realização ou omissão de determinados comportamentoscuja concreta regulação debe estabelecer a lei.

O núcleo da autodeterminação informativa, enquanto relacionada ao aspecto básico do direito à intimidade, constitui-se na faculdade que a pessoa detém de escolher sobre a divulgação, revelação, ou não de informações que diretamente a ela se referem. Isso porque a intimidade, mais que um estado de autoconfinamento, supõe uma qualidade na interação entre os indivíduos: trata-se de uma condição ou qualidade social da pessoa, que é objeto de tutela constitucional na medida em que esta pode ter o legítimo direito a não revelar aos demais determinados aspectos de suas relacões com outras pessoas, que o titular do direito julga devam permanecer em um plano reservado ao privado. (PODLECH *apud* PERÉZ LUÑO, 2012, p. 93).

Para Doneda (2006, p. 201) a terminologia mais adequada (e simples) é tão somente "proteção de dados pessoais", pois estaria englobada tanto a problemática da privacidade quanto a da informação, que teria como ponto de referência os direitos da personalidade e estaria isenta de uma acepção patrimonialista ou contratual, ao mesmo tempo em que não remonta ao direito à liberdade em uma acapção demasiado ampla.

A critíca do jurista citado reside basicamente em três fatores. O primeiro é acerca da correta definiçaõdo que seja autodeterminação, pois em determinado sentido poderia dar ao indivíduo a oportunidade de controlar as informações que lhe digam respetio, dentro de parâmatetros de ampla informação solidariedade (DONEDA, 2006, p. 198).

Já para uma leitura em chave liberal a autodeterminação concentrar-se-ia no ato do consentimento da pessoa para o tratamento de seus dados pessoais e assumiria contornos negociais, afastando a matéria do âmbito dos direitos da personalidade. (DONEDA, 2006, p. 198).

Por fim, outro problema é a possibilidade de ter a impressão de que as pessoas teriam um direito de propriedade sobre suas informações, o que as transportaria para o campo das situações patrimoniais. (DONEDA, 2006, p. 198-1999).

Trata-se de direito que orienta até hoje a proteção de dados pessoais na Alemanha e exerce grande influência em países do sistema jurídico romano-germânico, encontrando acolhida também no Tribunal Constitucional Espanhol na sua sentença 254/93 (DONEDA, 2006, p. 196-197).

De acordo com Fortes (2015, p. 134), é preciso ressaltar "[...] a fundamental importância do conceito de autodeterminação informacional, instituído na vanguarda normativa alemã, e que constitui a gênese normativa da proteção de dados pessoais no continente europeu [...]".

5. AUTORIDADE INDEPENDENTE

Outro aspecto a ser delimitado é a importância de existir um órgão responsável pela proteção dos dados pessoais. Trata-se de órgão com diversas atribuições sociais, políticas e jurídicas, pois, como se observa em experiências europeias, além de fiscalizar, controlar e aplicar sanções à violação dos dados pessoais, cabe a promoção de ações educativas e de informação tanto para cidadãos quanto para órgãos públicos.

É preciso delimitar as atribuições, estrutura, composição e observar uma autonomia financeira e política a esse órgão. A vinculação a órgãos governamentais e ligados ao Poder

Executivo não é desejável. Ainda, a dependência ao Poder Legislativo, Judiciário ou outros da estrutura jurídico-administrativa (Ministério Público, por exemplo) também podem comprometer a segurança dos dados, notadamente pelo interesse em determinadas demandas.

O novo órgão deve ter autonomia e meios efetivos de executar sanções aos infratores, além de organizar as políticas para a conscientização quanto à utilização e guarda de dados pessoais.

Ademais, sua composição deverá ser híbrida e seus integrantes oriundos de diversos segmentos sociais. Ao mesmo tempo em que é importante que se tenha um órgão com conhecimentos técnicos acerca da criação e manutenção de banco de dados é importante que haja uma interdisciplinaridade em seu Conselho administrativo.

Nesse sentido, referidos integrantes poderão advir de diferentes áreas do conhecimento contribuindo para uma melhor regulamentação da legislação protetiva e adequação à realidade das relações sociais e institucionais.

Conforme destacada no trabalho, o Agência Espanhola de Proteção de Dados é dirigida por um presidente eleito entre os membros do Conselho Consultivo, o qual é formado por representantes de cada uma das casas do Poder Legislativo, um representante indicado pelo governo central, outro proposto pelas administrações locais concentradas na Federação Espanhola de Municípios e Províncias, um membro da Academia Real de História, um técnico no assunto selecionado pelo Conselho Superior de Universidades, um representante dos consumidores e usuários, além de um representante do setor de banco de dados privados.

A presença de membros dos Poderes Executivo, Legislativo, Judiciário tende a manter a ideia da sistema de controle e execução de cada uma das atividades a que se lhes atribui constitucionalmente. Os Estados federados, seja por meio de associações ou entidades representativas por regiões geográficas, podem igualmente indicar membro(s) no sentido de procurar trazer uma contribuição acerca das distintas realidades nas regiões brasileiras. Representantes oriundos de entes educacionais e setores de tecnologia e informação contribuem para uma visão diferenciada da regulação dos arquivos.

Referida inter-relação faz com que tanto questões política-econômico-sociais e técnicas sejam levadas em consideração tanto no momento de definições fundamentais na proteção dos dados por meio de instrumentos regulatórios quanto no julgamento dos casos concretos a ela submetidos.

Ao falar sobre a independência de uma autoridade independente de proteção de dados, Doneda (2006, p. 393) afirma que referida característica pressupõe a presença de "mecanismos de nomeação de seus membros, geralmente limitando a discricionariedade na

sua escolha (através, por exemplo, da exigência de determinada formação ou atuação profissional)", além "da incompatibilidade de sua atuação com outras atividades, atuais ou mesmo pregressas (e também futuras [...]), além da limitação temporal de seu cargo" (DONEDA, 2006, p. 393).

Ainda, a independência pressupõe "a ausência de ingerência governamental sobre seus atos, que se pode obter situando tais órgãos fora de uma posição hierárquica em relação ao governo" (DONEDA, 2006, 393-394).

Além da especificidade referente à matéria e da função de velar pela fiel cumprimento e respeito à lei, interpretando-a e aplicando-a, o ente independente deve ser dotado de poderes para inspecionar e aplicar sanções. É preciso que os responsáveis pelos arquivos mantenham referido órgão informado acerca das características de seu banco, além de, sendo o caso, quando requisitados, deem acesso aos dados que nele constam.

6. CONCLUSÃO

O tema da privacidade tem relação direta com o nível de desenvolvimento tecnológico da sociedade. Conforme se prolifera o uso das novas tecnologias no meio social, aumenta a necessidade de se pensar as relações de poder, transparência e autonomia individual na sociedade.

O uso de produtos tecnológicos tem crescido significativamente nos últimos anos e tem sido influenciado a rotina das pessoas. A cada acesso à rede mundial de computadores, pesquisas, buscas, compras realizadas em sítios virtuais, navegação e comportamentos em redes sociais um número exponencial de informações são capturadas e armazenadas em diversos locais do ciberespaço ou meio digital

O número de horas que as pessoas dedicam ao ambiente virtual, assim como a exposição relatada, deixam as pessoas vulneráveis diante da facilidade do acesso a dados e informações que são deixadas nas redes ou coletadas pelos sítios.

Especial atenção é necessária à captação, tratamento e utilização de informações pessoais por órgãos públicos. Conforme destacado no texto, a iniciativa de desburocratizar o sistema de identificação dos indivíduos é salutar. Não obstante, a efetivação do Documento Nacional de Identificação deve ser submetida ao crivo da segurança e de uma efetiva proteção dos dados pessoais.

A criação de um documento único de identificação, não alicerçado numa legislação especializada de proteção de dados, põe em risco o direito à privacidade do cidadão. A Lei nº 13.444/2017 legitima o compartilhamento de dados sensíveis entre diferentes órgãos estatais e, ao mesmo tempo, não estabelece os parâmetros acerca do controle, limite e responsabilidade no tratamento dessas informações.

Observa-se uma série de artigos no texto instituidor da ICN que garante a comunicabilidade das informações sem uma preocupação mais objetiva sobre o tema da privacidade e da proteção de dados.

Interoperabilidade, acesso a outras bases, integração do banco de dados com o de outros órgãos, cruzamento de informações são palavras e expressões recorrentes no texto. Contudo, a regulação é feita tão somente em uma legislação composta de treze artigos nos quais há uma relevante deficiência na proteção de dados pessoais, a qual se acentua diante da falta da lei específica.

O sistema jurídico de proteção dos dados pessoais deve ser constituído por estrutura sólida, a qual dê transparência estabeleça uma sistema de identificação e armazenamento de dados com salvaguardas. É necessária uma definição claro acerca de quem controla, quem fiscaliza, quem é responsável e a forma como os dados podem ser compartilhados.

No presente estudo foi verificado que o sistema jurídico brasileiro não apresenta as características citadas, confirmando a hipótese inicial. Especialmente por inexistir uma lei de proteção de dados pessoais. Referido instrumento legal permitiria que se estabelecem parâmetros à efetivação do direito fundamental à privacidade, auxiliando para impedir o uso e o tratamento ilegal de informações acerca da vida privada das pessoas.

O uso indiscriminado desses dados além de vulnerar direito fundamental facilita o controle e monitoramento dos cidadãos. Pois conforme afirmado, com o emprego de tecnologias de informação e comunicação fica mais fácil classificar aspectos que isoladamente não teriam relevância, mas que no seu conjunto ou quando comparados e processos em conjunto transparecem aspectos específicos das pessoas. E, ao final, podem não apenas individualizá-las como serem usados com finalidades diversas, como para oferta de produtos ou para negar a oferta deles ou diferenciar ou discriminar o acesso a bens e serviços.

É importante que se amplie o controle dos dados e informações pelo próprio indivíduo, o qual necessita ter acesso às informações armazenadas nos bancos de dados a seu respeito, podendo exigir a sua retirada ou alteração e atualização. Busca-se, em última análise, a correção dos dados, conhecimento pelo indivíduo acerca da existência de cadastro e do que consta a seu respeito.

Ademais, a criação de uma autoridade independente pode contribuir, a exemplo do direito europeu, para a efetivação proteção dos dados. Nos moldes apresentados trata-se de ente multidisciplinar, mas ao mesmo tempo especializado no tema, sem subordinação a órgãos estatais e privados.

Outra vantagem de referida autoridade é resolver as demandas ainda no âmbito administrativo, sem necessidade de se recorrer ao Poder Judiciário. Todavia, é preciso que tanto procedimento, funções, sanções e demais atribuições estejam previstas em legislação específica.

Portanto, é mister a implementação de uma legislação protetiva dos dados pessoais no sistema jurídico brasileiro para garantia da privacidade dos cidadãos. É a partir de parâmetros claros, transparentes, e com a especificação de princípios, direitos e deveres acerca do tema que o Documento Nacional de Identificação poderá ser utilizado com êxito e com cautelas para não tornar vulneráveis os dados pessoais.

7. REFERÊNCIAS

BRASIL. Lei nº 13.444 (2017). **Lei nº 13.444**. Estabelece normas para as eleições. Brasília, DF: Presidência da República, 2017. Disponível em: <http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2017/lei/L13444.htm>. Acesso em: 07 abr. 2018.

CELLA, José Renato Gaziero; ARNS DE OLIVEIRA, Marlus H. A unificação do registro de identidade civil e a proteção de dados pessoais no Brasil. In: **III Encontro de Internacionalização do CONPEDI**, 2015, Madrid.

COMISIÓN EUROPEA. **Estrategia de la ue para la protección de datos en internet**. 2010. <http://ec.europa.eu/spain/actualidad-y-prensa/noticias/internet-y-sociedad-de-la-informacion/proteccion-datos-internet-ue_es.htm>. Acesso em: 23 set. 2015.

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

FORTES, Vinícius Borges. **O direito fundamental à privacidade**: uma proposta conceitual para a regulamentação da proteção dos dados pessoais na internet no Brasil. 2015. 225p. Tese (Doutorado em Direito) - Universidade Estácio de Sá, Rio de Janeiro, 2015.

GALINDO AYUDA, Fernando. Seguridad y sociedad del conocimiento. In: GALINDO, Fernando (ed.). **El derecho de la sociedad en red**. Lefis Series, 14. Zaragoza: Prensas de la Universidad de Zaragoza, 2013. p. 129-154.

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

RODOTÀ, Stefano. **A vida na sociedade da vigilância**: a privacidade hoje. Tradução: Danilo Doneda e Luciana Cabral Doneda. Rio de Janeiro: Renovar, 2008.

RODOTÀ, Stefano. **Tecnologie e diritti**. Bologna: Il Mulino, 1995.

TRIBUNAL SUPERIOR ELEITORAL. **Biometria atual por UF**. 2018a. Disponível em: <http://www.tse.jus.br/eleitor-e-eleicoes/eleicoes/biometria/biometria-atual-uf>. Acesso em: 07 abr. 2018.

TRIBUNAL SUPERIOR ELEITORAL. **Pré-atendimento eleitoral - Título NET**. 2018b. Disponível em: < http://www.tse.jus.br/eleitor-e-eleicoes/servicos/titulo-de-eleitor/pre-atendimento-eleitoral-titulo-net/pre-atendimento-eleitoral-titulo-net >. Acesso em: 07 abr. 2018.