

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

LIBERDADE INFORMÁTICA E A AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS DO BRASIL

COMPUTER FREEDOM AND THE NATIONAL DATA PROTECTION AUTHORITY IN BRAZIL

William Costodio Lima¹

Wedner Costodio Lima²

RESUMO

Este artigo destaca a criação pela Lei 13.853/19 da Autoridade Nacional de Proteção de Dados do Brasil, como reflexo da necessidade do surgimento de tutelas inovadoras de direitos fundamentais. Sendo este o papel das autoridades independentes de proteção de dados, neste contexto, visa-se discutir as condições normativas no Brasil em relação a países da União Europeia que já vem legislando a mais tempo sobre a matéria e possuem um nível maior de proteção. Partindo da necessidade de assegurar uma liberdade informática como um direito humano de terceira geração, desde suas primeiras concepções com o surgimento das primeiras leis de proteção de dados até os dias atuais de intensificação de utilização das tecnologias da informação e comunicação e novas formas de tratamento de dados pessoais, se analisa o modelo brasileiro adotado em comparação com o modelo europeu, verificando sua efetiva independência para fiscalizar o cumprimento das normas protetivas pelo Estado e pelo mercado de modo a tutelar uma ampla gama de direitos fundamentais vitais para o exercício da cidadania nos tempos atuais.

Palavras-chave: Autoridade Nacional de Proteção de Dados. Direitos Fundamentais. Tutelas inovadoras.

ABSTRACT

This article highlights the creation by Law 13.853/19 of the National Data Protection Authority of Brazil, reflecting the need for the emergence of innovative tutelages of fundamental rights. This being the role of independent data protection authorities, in this context, the aim is to discuss the normative conditions in Brazil in relation to European Union countries that have been legislating on the matter for a longer time and have a higher level of protection. Starting from the need to ensure computer freedom as a third generation human right, from its first conceptions with the emergence of the first data protection laws to the current days of intensified use of information and communication technologies and new forms of data

¹ Mestre em Direito pela Universidade Federal de Santa Maria - UFSM (2020). Especialista em Ciências Penais e Criminologia (2016). Graduado em Direito pela Universidade Luterana do Brasil (2010). Pesquisador do Núcleo de Direito Informacional (NUDI) da Universidade Federal de Santa Maria (UFSM). Advogado.

² Mestre em Direito, UNISC. (2017) Pós-graduado em Direito Penal e Processo Penal pela Faculdade de Direito Damásio de Jesus (2014). Graduado em Direito pela Universidade Luterana do Brasil (2011). Advogado Criminalista. Professor universitário. Membro da Comissão da Advocacia Criminal da OAB/RS Subseção de Santa Maria - RS.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

processing. personal data, the Brazilian model adopted in comparison with the European model is analyzed, verifying its effective independence to monitor compliance with protective rules by the State and the market in order to protect a wide range of fundamental rights vital to the exercise of citizenship in the times current.

Keywords: National Data Protection Authority. Fundamental rights. Innovative tutelage.

INTRODUÇÃO

O presente artigo analisa o papel da Autoridade Nacional de Proteção de Dados do Brasil e se no plano normativo ela possui condições de atuar como forma inovadora de tutela de direitos fundamentais, discutindo em perspectiva comparada sua independência e seus potenciais de proteção. A discussão é atual diante da recente criação do órgão pelo Brasil pela Lei 13.853/19 (que altera a Lei 13.709/18, a Lei Geral de Proteção de Dados - LGPD). Ademais, a LGPD brasileira entrou em vigência há pouco tempo, em 18 de setembro de 2020, tendo sido intensificada as relações virtuais neste período, em razão das necessidades de distanciamento social ocasionadas pela pandemia da Covid-19 que surgiu no mesmo ano.

A LGPD dispõe sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural. A Autoridade Nacional de Proteção de Dados do Brasil possui competência para zelar pela proteção dos dados pessoais nos termos da legislação.

Atualmente, o órgão foi criado como vinculado ao Ministério da Justiça, o que deixa dúvidas quanto a sua necessária independência diante de sua finalidade de fiscalizar o mercado como o próprio Estado. Tendo já sido escolhido seu Conselho diretivo, e estando em vias de constituir o Conselho Nacional de Proteção de Dados, as demandas pela sua atuação de fiscalização tanto do setor público como o privado somente aumentam. A agência reguladora é indispensável para que o país seja reconhecido pela União Europeia como de nível adequado para o tratamento de dados e assim avançar em uma economia de mercado global e de capitalismo informacional.

Neste contexto, empregando-se o método de abordagem dedutivo, com as técnicas de pesquisa documental e bibliográfica, procura-se com este artigo responder ao seguinte problema de pesquisa: é possível afirmar que a Autoridade Nacional de Proteção de Dados criada no

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

Brasil possui no plano normativo as mesmas condições legais de tutela e independência que as que atuam nos países da União Europeia?

Para o desenvolvimento deste estudo, parte-se de um panorama geral sobre novos direitos e novas formas de tutela de direitos fundamentais, discutindo-se a liberdade informática e o papel da autoridade nacional de proteção de dados em contraste com a evolução conceitual e legislativa sobre o tema. Em seguida, analisa-se a autoridade de proteção criada no Brasil no plano normativo, em perspectiva comparada com as de países da União Europeia, a fim de averiguar as suas condições legais de tutela de direitos fundamentais através de autonomia técnica e financeira e sua indispensável independência.

1 A LIBERDADE INFORMÁTICA: O SURGIMENTO DE TUTELAS INOVADORAS DE DIREITOS FUNDAMENTAIS

O atual debate sobre a Autoridade Nacional de Proteção de Dados criada no Brasil decorre da aprovação de sua primeira lei geral sobre o tema. Estas, podem ser vistas em quatro gerações, desde o seu surgimento em países mais desenvolvidos nos anos 1970 às atuais legislações como o Regulamento Geral de Proteção de dados da União Europeia – RGPD (Regulamento EU nº 2016/679) e a Lei Geral de Proteção de Dados do Brasil – LGPD (Lei 13.709/2018). O papel das autoridades de proteção independentes vai ganhando relevância na medida do avanço tecnológico e novas formas de tratamento dos dados pessoais e o legislativo com a aprovação de novas leis em vários países como no Brasil e em países da União Europeia.

Por isso, uma visão global e didática do assunto implica em entender a importância das autoridades de proteção independentes para a tutela de direitos fundamentais, para, posteriormente, então, analisar o modelo adotado no Brasil. Neste sentido, utiliza-se de algumas considerações sobre o conceito de liberdade informática através da ótica das gerações de direitos humanos e os direitos de terceira geração, que implicam na adoção de tutelas inovadoras como a criação de autoridades independentes de proteção. Em seguida, procura-se então contrastar e fazer um paralelo com a evolução do conceito de proteção de dados e os riscos aos direitos fundamentais decorrentes do tratamento de dados desde o surgimento da informática aos dias atuais.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

O século XXI é caracterizado pela intensificação da utilização das tecnologias da informação e comunicação³. A pandemia da Covid-19 somente fez aumentar estes impactos⁴. Deste modo, ganha ainda mais relevância o direito humano à liberdade informática nos dias atuais, ainda que sua concepção tenha ocorrido em um período anterior, de seu surgimento e desenvolvimento inicial da Internet.

Como ressalta Pérez-Luño (2013, p. 173), este direito foi resultado de um movimento da doutrina jurídica e da jurisprudência, principalmente naqueles países considerados mais desenvolvidos, para regulamentar a capacidade técnica de armazenar informações e organizá-las diante da informática. Pode-se destacar, por conseguinte, as primeiras leis de proteção de dados e o conceito de “autodeterminação informativa” decorrente do julgamento da lei do censo em 1983 pela Suprema Corte Alemã.

O direito humano à liberdade informática seria de terceira geração. Abordando quase a totalidade das necessidades e interesses das pessoas atualmente em um mundo globalizado, este direito se realiza com os demais de primeira e segunda geração, no atual contexto histórico de surgimento da informática aos dias atuais de intensificação de sua utilização e novas e sofisticadas formas de tratamento e disseminação das relações virtuais através da Internet.

Os direitos humanos discutidos perante a sistemática das suas “gerações” não significam, porém, uma superação de direitos por outros, mas sim a evidência do surgimento de “novos direitos” em complemento às gerações anteriores (SARLET, 2015, p. 322). Assim foram os direitos de primeira geração, concebidos como direitos e garantias individuais como o direito à vida, à liberdade e os direitos civis e políticos. Em seguida, os direitos de segunda geração, que surgem diante dos conflitos de classes e os movimentos operários de reivindicação, caracterizando-se como complemento e condição de exercício para os direitos de primeira geração, conhecidos como direito econômicos, sociais e culturais⁵.

³ Neste viés é possível apontar o autor Manuel Castells (2003) como referência nas análises das transformações econômicas, culturais, políticas e sociais decorrentes da utilização das tecnologias da informação e comunicação.

⁴ É interessante citar aqui, a título de contextualização, a pesquisa desenvolvida pelo Comitê Gestor da Internet denominada “PAINEL TIC: Pesquisa *web* sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus” (2021) que aprofunda e detalha aspectos sobre o uso da Internet durante a pandemia e seus efeitos na sociedade.

⁵ Resume Pérez Luño (2013, p. 167, tradução nossa.): “Este contexto genético confere aos direitos humanos uns perfis ideológicos definidos. Os direitos humanos nascem, como é notório, com traço individualista, como liberdades individuais que configuram a primeira fase da geração de direitos humanos. Dita matriz ideológica individualista sofrerá um amplo processo de erosão e impugnação nas lutas sociais do século XIX. Estes

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

Os direitos de terceira geração, seriam consequências de reflexões no pós-segunda guerra mundial, por volta dos anos 1945. Dentre eles, pode-se perfeitamente entender o direito à paz entre os povos, o direito a usufruir de um meio ambiente saudável e o direito à liberdade informática (PÉREZ LUÑO, 2013, p. 168). Pérez Luño (2013, p. 168) ressalta que estas três gerações correspondem a evolução das três formas de Estado de direito e suas correlativas gerações de direitos, com as liberdades individuais representando o Estado liberal, os direitos econômicos, sociais e culturais constituindo o Estado social, e a terceira geração representando o modelo político atual do Estado Constitucional de direito.

Um dos desdobramentos sócio-políticos do desenvolvimento tecnológico é o reconhecimento da necessidade de uma liberdade informática, o que na visão de Pérez Luño (2000, p. 64), originam as primeiras leis de proteção de dados. Estas seriam novas estratégias reivindicativas dos direitos humanos de terceira geração, devido à contaminação das liberdades diante do uso das novas tecnologias.

Anteriormente, os direitos individuais estavam fundamentados na liberdade, e os direitos sociais, econômicos e culturais na igualdade. A terceira geração de direitos humanos é pautada pela solidariedade e necessitam de esforços em escala planetária. Por isso, a convergência internacional sobre as leis de proteção de dados se destaca, mas também, a criação de autoridades de proteção independentes tem sido um procedimento protagonista na defesa dos direitos e liberdades de terceira geração (PÉREZ LUÑO, 2013, p. 179-180).

Seu sistema oferece a vantagem de proteção efetiva dos direitos humanos, sendo difundida em vários países. As principais funções das autoridades de proteção independentes, além das típicas de Estado, são de informar o parlamento das dinâmicas e adaptações do desenvolvimento tecnológico, orientar os cidadãos sobre os procedimentos de tutela das liberdade e proteção de dados pessoais e prevenir ameaças aos direitos humanos evitando danos e agressões de difícil reparação e fiscalizar o cumprimento da lei.

Estas autoridades independentes de proteção foram criadas desde a primeira geração de leis de proteção de dados. Seu surgimento e necessidade decorre da evolução conceitual do

movimentos reivindicativos evidenciaram a necessidade de completar o catálogo dos direitos e liberdades da primeira geração com a segunda geração de direitos: os direitos econômicos, sociais e culturais. Estes direitos alcançam sua palatina consagração jurídica e política e a substituição do Estado liberal pelo Estado social de Direito.”.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

direito à privacidade e das inovações tecnológicas sobre o tratamento de dados pessoais e podem ser apontadas também como novas e inovadoras formas de tutela de direitos fundamentais.

Em uma breve síntese, pode-se dizer que o surgimento do direito à privacidade decorre do famoso artigo “The right to privacy” de Samuel Warren e Louis Brandeis, de 1890, nos EUA, quando se consolidavam os meios de comunicação de massa, como os jornais e revistas, e iniciava-se uma preocupação com a inviolabilidade da personalidade na publicação de escritos pessoais. A preocupação, portanto, não era proteger a propriedade, mas sim a personalidade da pessoa. Nas palavras de Leonardi (2011, p. 51), “[...] seu valor não está no direito de receber indenização em decorrência da publicação, mas sim na paz de espírito ou no alívio assegurado pela capacidade de impedir a própria publicação.”

O direito à privacidade passa a ser reconhecido internacionalmente em diversos textos como a Declaração Universal dos Direitos do homem (1948), Convenção Europeia dos Direitos do Homem (1950) e Convenção Americana dos Direitos do Homem (1969). No entanto, a partir do surgimento da informática e a possibilidade de tratamento informatizado dos dados pessoais, com sua rapidez e eficiência, novos desafios ao ordenamento jurídico surgiram, ensejando o nascimento da disciplina de proteção de dados pessoais, associando a proteção à privacidade e informações pessoais. Como afirma Mendes (2008, p. 10):

A partir da evolução da tecnologia da informação e das transformações do ordenamento jurídico, a privacidade deixa de ser concebida como o direito do indivíduo a ser deixado só, adquirindo progressivamente um caráter mais positivo, como sendo o direito de se construir uma esfera privada própria, a partir da ideia de livre desenvolvimento da personalidade.

Com estas transformações tecnológicas surge o direito à proteção de dados pessoais, compreendido como um fenômeno coletivo, diante dos potenciais danos causados pelo processamento de dados pessoais e sua natureza difusa. Leonardi (2011, p. 67), lembra que “Para essa corrente, a privacidade é a reivindicação de indivíduos, grupos ou instituições, de determinar por si próprios quando, como e em que extensão informações a seu respeito são comunicadas a terceiros na conhecida definição de Alan Westin.”

Portanto, a LGPD brasileira, ao ser concebida para proteger, diante o tratamento de dados pelo setor público e privado, o direito à liberdade, à privacidade e o livre

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

desenvolvimento da personalidade, reflete este desenvolvimento do conceito de proteção de dados pessoais. As respostas jurídicas que vieram através da criação de instrumentos nacionais e internacionais, passaram a tratar a proteção de dados pessoais como um direito autônomo. A Convenção de Estrasburgo, de 1981, garante o respeito aos direitos e liberdades fundamentais, e especialmente ao direito à vida privada, face o tratamento automatizado de dados pessoais. O Parlamento Europeu proclamou a Carta dos Direitos Fundamentais da União Europeia, no ano de 2000, tratando, no art. 7º, do respeito à vida privada, e, no art. 8º, da proteção de dados pessoais, reconhecendo a autonomia deste novo direito.

Artigo 7.º Respeito pela vida privada e familiar. Todas as pessoas têm direito ao respeito pela sua vida privada e familiar, pelo seu domicílio e pelas suas comunicações.

Artigo 8.º Proteção de dados pessoais. Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”. (UNIÃO EUROPEIA, 2000).

Mas, a primeira lei de proteção de dados do Brasil (LGPD) vem em momento histórico ainda mais urgente da necessidade de proteção da liberdade informática de quando da elaboração das primeiras leis de proteção de dados em países desenvolvidos. Os escândalos Snowden⁶, em 2013, e Cambridge Analytica⁷, 2016, revelaram ao mundo as inúmeras violações de direitos fundamentais através do desrespeito às regras de proteção de dados e privacidade que culminam inclusive no enfraquecimento da democracia.

A utilização dos dados pessoais por parte do Estado no seu objetivo de controle social, muitas vezes obrigam as empresas a fornecer seus bancos de dados, distorcendo a finalidade da sua utilização, um dos princípios basilares para o tratamento lícito de dados pessoais⁸. As

⁶ Nas palavras de Bauman *et al* (2015, p. 23) “Graças à documentação distribuída por Snowden e outros, sabemos agora mais do que sabíamos sobre o caráter e a extensão das práticas de coleta de informações de várias agências encarregadas de aumentar nossa segurança.”.

⁷ Em relatório da Unesco sobre as o papel das TIC para o desenvolvimento sustentável, a proteção e promoção de direitos humanos e a consolidação da democracia, o documento admite que elas podem gerar efeito contrário, realçando os riscos associados à segurança dos dados pessoais, trazendo como exemplo o escândalo Cambridge Analytica nas eleições americanas em 2016, fato que se revelou o poder desses dados. (UNESCO, 2019, p. 18).

⁸ Uma das condicionantes para que o indivíduo possa exercer o seu poder de autodeterminação informativa é a existência de princípios que devem nortear o tratamento de dados pessoais. Doneda (2006, p. 216-217), elabora

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

empresas, por sua vez, pelo simples fato de possuírem bancos de dados com grande capacidade de armazenamento, os coloca em uma situação privilegiada de informação e controle⁹, com potencial para infringir a dignidade, a liberdade e a autonomia das pessoas por suas práticas agressivas de marketing e publicidade direcionada.

Lyon (2014) adverte que uma das tendências atuais do *Big Data*, que consiste em uma nova técnica de tratamento de dados, é a crescente integração de governos e vigilância comercial. Desse modo, o uso comercial e para fins de segurança estimulam a integração desta atividade, tendo neste contexto a utilização de dados para diferentes finalidades, e esta mudança pode alterar como os titulares dos dados podem interpretar sua privacidade ou o estabelecimento de limites legais para o uso secundário destes (LYON, 2014, p. 05-06).

Neste sentido que Pérez Luño (2003, p. 170) já refletia sobre os riscos aos direitos humanos e fundamentais decorrentes do desenvolvimento tecnológico como fundamento para a necessidade de tutela da liberdade informática. Considerando ser a Internet a principal ferramenta para promover uma participação política mais autêntica, plena e efetiva nas democracias do século XXI, o que denomina como *cibercidadania*, ela pode ser um fenômeno de controle da vida cívica, uma *cidadania.com*, como ilustra a literatura do lado perverso das novas tecnologias.

As leis de proteção de dados vêm no sentido reequilibrar as relações entre o cidadão, o Estado e o mercado. E as autoridades de proteção independente são um órgão destinado a

uma síntese destes princípios: 1 – *Princípio da publicidade* (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja através da exigência de autorização prévia para seu funcionamento, pela notificação de sua criação a uma autoridade; ou pela divulgação de relatórios periódicos. 2 – *Princípio da exatidão*: Os dados armazenados deve ser fieis à realidade, o que compreende a necessidade que sua coleta e seu tratamento sejam feitos com cuidado e correção, e que sejam realizadas atualizações periódicas destes dados conforme a necessidade. 3 – *Princípio da finalidade*, pelo qual toda utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes de sua coleta. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que é possível a utilização de determinados dados para uma certa finalidade (fora da qual haveria abusividade). 4 - *Princípio do livre acesso*, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias destes registros com a consequente possibilidade de controle destes dados, após este acesso de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou ainda pode-se proceder a eventuais acréscimos. 5 – *Princípio da segurança física e lógica*, pelo qual os dados devem ser protegidos contra os riscos de seu extravio, destruição, modificação, transmissão ou acesso não autorizado.

⁹ Como afirma Masseno (2019, p. 08), os modelos de negócio baseados no *Big data* possibilitam um controle “[...] permanente sobre os consumidores, com dados obtidos e tratados em tempo real, conservados por tempo indeterminado, com vista a obter informações ainda não evidentes, muitas delas nem sequer previstas no momento de recolha e tratamento inicial dos dados.”

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

promover de forma inovadora a tutela de direitos fundamentais diante o fluxo informacional¹⁰. Se o exercício da cidadania atualmente implica na utilização das tecnologias da informação e comunicação, tal reflexão é vital¹¹, pois, como afirma Rodotà (2008, p. 233), “Apesar de acreditarmos estar apenas tratando do tema da proteção de dados, na verdade, estamos nos ocupando do destino das nossas sociedades, do seu presente e sobretudo do seu futuro.” .

Neste contexto, a liberdade informática no Brasil ganha força, sobretudo, porque estas novas gerações de leis de proteção de dados do século XXI apostam na regulação de uma autoridade independente de proteção. Todo esse preocupante quadro evidencia a imperiosa necessidade não só da edição de Lei de Proteção de Dados Pessoais, passo já dado pelo Brasil em 2018, mas que sua vigência venha acompanhada da necessária estrutura para a sua fiscalização, ressaltando-se o papel fundamental da Autoridade Nacional de Proteção de Dados e a necessidade de sua independência, conforme se verá na sequência, em comparação, no plano normativo, com autoridades de proteção pelo mundo e em países da União Europeia.

2 AUTORIDADE NACIONAL DE PROTEÇÃO DE DADOS: COMPARATIVO ENTRE O MODELO ADOTADO NO BRASIL E O ADOTADO EM ALGUNS PAÍSES DA UNIÃO EUROPEIA

Como visto, as Autoridades Nacionais de proteção de dados são um exemplo de tutela inovadora de proteção de direitos de terceira geração, que pela sua complexidade, envolvem uma ampla gama de direitos. Assim, a maioria dos países aprovou uma lei de proteção de dados, e, em consequência, criou uma autoridade independente de proteção. O Brasil, ao adotar o mesmo modelo, deve observar as suas condições de existência e efetividade, especialmente pelo critério da independência.

¹⁰ Prevê o Considerando número 117 do Regulamento Geral de Proteção de Dados da União Europeia, a criação de autoridade de controle nos Estados-membros, habilitados a desempenhar as suas funções e a exercer os seus poderes com total independência constitui um elemento essencial da proteção das pessoas singulares no que diz respeito ao tratamento dos seus dados pessoais.

¹¹ Conforme o art. 2º da LGPD: “[...] a disciplina da proteção de dados pessoais tem como fundamentos: I - o respeito à privacidade; II - a autodeterminação informativa; III - a liberdade de expressão, de informação, de comunicação e de opinião; IV - a inviolabilidade da intimidade, da honra e da imagem; V - o desenvolvimento econômico e tecnológico e a inovação; VI - a livre iniciativa, a livre concorrência e a defesa do consumidor; e VII - os direitos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

Em termos de estudos sobre autoridades de proteção de dados no mundo, Greenleaf (2017) aponta que 120 (cento e vinte) países possuem leis de proteção de dados e que destes mais de 80 % (oitenta por cento) estão com suas autoridades independentes e especializadas em funcionamento. É de se destacar a expressão de países no “Hall of Shame” (Calçada da vergonha), aqueles que legislando sobre a proteção de dados e nomeação de uma autoridade de proteção, o deixam de fazer por mais de um ano.

A Conferência Internacional dos Comissários de Proteção de Dados e Privacidade - ICDPPC (2017) indicou que das 87 (oitenta e sete) autoridades existentes, mais da metade se estabeleceu depois da década de 2000. E também que 98% (noventa e oito por cento) das autoridades estão presentes digitalmente e publicam relatórios anuais *on line*. Por fim, asseverou que cerca de 85 % (oitenta e cinco por cento) dos países possuem referências constitucionais sobre a proteção de dados, suas autoridades de proteção supervisionam os setores públicos e privados, e na maioria dos países conta-se com subsídios para o financiamento da autoridade, sendo uma pequena parte utiliza de multas e sanções.

Em relação aos países da União Europeia, todos possuem uma autoridade de proteção de dados (GREENLEAF, 2017, p. 03). Através de seus sítios eletrônicos é possível encontrar decisões sobre processos administrativos, normas setoriais e orientações sobre a proteção de dados e relatórios de suas atividades. O sistema de proteção de dados pessoais da Europa é bastante avançado, considerando seus países serem pioneiros em legislação sobre o tema, além de suas autoridades independentes de proteção de dados serem bastante atuantes, o que justifica que essas diretrizes sejam contrastadas com o tratamento normativo do tema no Brasil, que recentemente criou sua autoridade nacional de proteção de dados pessoais pela Lei 13.853/19.

Estas autoridades vêm sendo adotadas pelos primeiros países que legislaram sobre a matéria, criadas para atuarem como órgãos em que os cidadãos poderiam se reportar para registrar suas reclamações sobre o tratamento de dados pessoais. Ao longo dos anos, o modelo europeu de proteção de dados pessoais, baseado, até então, na Diretiva 95/46/CE, aprovou o Regulamento Geral de Proteção de Dados (Regulamento EU nº 2016/679), que dentre suas inovações, passou “[...] a prever novos mecanismos como relatórios de impacto, códigos de boas condutas, certificações e programas de governança, [...] normas que incentivam a implementação do conceito de *Privacy by Design* [...].”(MENDES, 2018, p. 2).

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

Este caminho do sistema europeu de proteção de dados tem como destaque as autoridades administrativas encarregadas da proteção de dados, pois são elas “[...] tanto mais necessárias com a diminuição do poder do indivíduo para a autorização ao processamento de seus dados [...]” (DONEDA, 2015, p. 373-374). O princípio do consentimento para o tratamento dos dados pessoais, nos termos de uma autodeterminação informativa, foi sendo questionado ao longo do tempo, como ressalta Mendes (2008, p. 36):

Por um lado, no âmbito do Estado Social, é muito difícil assegurar-se a liberdade informacional sem comprometer as funções dessa complexa burocracia que necessita de dados dos cidadãos para planificar. Por outro lado, também na relação entre privados é difícil se verificar o exercício do direito à privacidade informacional, na medida em que tal exercício poderá impedir o acesso do indivíduo a determinadas facilidades do mercado de consumo, que o fornecedor está disposto a conceder somente em troca do cadastro de suas informações pessoais.

Há, assim, a necessidade de se privilegiar um modelo jurídico de reconhecimento de fontes de legitimidade exteriores ao sistema político do Estado, com modalidades de tutela da proteção de dados que exigem a utilização de mecanismos de auto-regulamentação e de meios técnicos (DONEDA, 2006, p. 362). O modelo teórico regulatório da proteção de dados vem recebendo uma nova abordagem.

Centrada na regulação do risco, tem provocado “[...] uma mudança de rota para a prevenção de danos *antes que eles ocorram* e instrumentos regulatórios que incrementem o nível de informação e cognição de riscos por autoridades especializadas, bem como um conjunto de obrigações às empresas de tecnologia [...]”. (ZANATA, 2017, p. 188-189, grifo do autor.). Trata-se de um novo paradigma, cujo objetivo é “[...] encarar estas medidas de proteção de dados desde a concepção e por pré-definição, como pressupostos do desenho do sistema a implementar. O sentido [...] é o de revelar uma visão preventiva e não uma visão com recurso a medidas avulsas, reativas ou improvisadas.”. (FERREIRA, 2018, p. 62-63).

O Regulamento Geral de Proteção de Dados inovou no que tange a forma de regulação de fiscalização das empresas que fazem o tratamento de dados, determinando que estas devem ser sempre capazes de comprovar a licitude do tratamento, nos termos de uma auto-regulação.

Do ponto de vista operacional, a exigência de ter de comprovar a conformidade com o regulamento muda a forma de encarar a problemática da proteção de dados dentro das organizações. Até maio de 2018, a proteção de dados foi regulada numa

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

perspectiva de hetero-regulação, em que a necessidade de garantir a licitude do tratamento, através dos princípios e condições de legitimidade, ocorria essencialmente na fase inicial, pelos meios definidos pela autoridade de controle (notificação, uma licença ou autorização, por exemplo). Após a entrada em aplicação do RGPD, estamos perante uma nova realidade. O responsável pelo tratamento tem que conseguir, em qualquer momento do processo de tratamento de dados pessoais, a sua licitude e cumprimento com o RGPD, criando evidências para que o possa comprovar, ficando assim sujeito à fiscalização e supervisão da autoridade de controle [...]. (FERREIRA, 2018, p. 62-63).

As autoridades de controle, como nomeado pelo RGDP, são o ponto central deste regime de regulação. O regulamento estabelece que os Estados-Membros devem constituir uma ou mais autoridades públicas independentes a responsabilidade pela fiscalização de sua aplicação, a fim de defender os direitos e liberdades fundamentais das pessoas singulares relativamente ao tratamento e facilitar a livre circulação desses dados na União (artigo 51). São-lhe assegurados independência e autonomia técnica e financeira para exercer suas funções.

Prevê o seu art. 52 que as autoridades de controlo agem com total independência na prossecução das suas atribuições e no exercício dos poderes que-lhe são atribuídos nos termos do presente regulamento. Os membros das autoridades de controlo não estão sujeitos a influências externas, diretas ou indiretas no desempenho das suas funções e no exercício dos seus poderes nos termos do presente regulamento, e não solicitam nem recebem instruções de outrem.

No ano de 2010, a Agência de Direitos Fundamentais da União Europeia apresentou um relatório com uma visão comparativa sobre as autoridades nacionais de proteção de dados, em que em um dos pontos ressaltava a preocupação quanto a independência destas. Foram apontados alguns critérios para auferir a sua independência, como ser garantida por um procedimento de nomeação e de destituição de seus diretores, e que em autoridades que são anexadas ao Ministério da Justiça geram preocupações (EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS, 2010, p. 12).

Após a aprovação do RGDP há uma maior harmonização no que se refere aos critérios normativos de independências das autoridades de proteção independente dos países da União Europeia, já que o regulamento possui caráter vinculativo aos países, ao contrário da

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

anterior Diretiva 95/46/CE¹². Como há pouca pesquisa sobre autoridade de proteção de dados, os fundamentos das agências regulatórias independentes fornecem uma estrutura para a análise de seu conceito de independência (SCHUTZ, 2012).

Em suma, com a tendência de privatização dos serviços públicos durante as décadas de 1970 e 1980 na Europa, sob forte influência do modelo americano, as agências reguladoras passam a serem essenciais ao Estado regulador (SCHUTZ, 2012, p. 03-04). E uma das razões pela aposta nas agências reguladoras é a crença na aptidão técnica como sua fonte legitimadora, sendo, no entanto, difícil conceituar sua independência, podendo ser apenas no plano formal, na visão de Schutz (2012, p. 04).

O Brasil, adotou um modelo transitório de Autoridade Nacional de Proteção de Dados, nos seguintes termos:

Art. 55-A. Fica criada, sem aumento de despesa, a Autoridade Nacional de Proteção de Dados (ANPD), órgão da administração pública federal, integrante da Presidência da República. § 1º A natureza jurídica da ANPD é transitória e poderá ser transformada pelo Poder Executivo em entidade da administração pública federal indireta, submetida a regime autárquico especial e vinculada à Presidência da República. § 2º A avaliação quanto à transformação de que dispõe o § 1º deste artigo deverá ocorrer em até 2 (dois) anos da data da entrada em vigor da estrutura regimental da ANPD. § 3º O provimento dos cargos e das funções necessários à criação e à atuação da ANPD está condicionado à expressa autorização física e financeira na lei orçamentária anual e à permissão na lei de diretrizes orçamentárias.”. (BRASIL, 2019a).

Por isso, o problema básico em relação a criação da implementação da Autoridade Nacional de Proteção de Dados no Brasil é em relação à desconfiança quanto à sua independência. O órgão, sendo vinculado a Presidência da República, gera dúvidas em relação a possibilidade do cumprimento do seu dever de fiscalização do tratamento de dados pessoais tanto pelas empresas como pelo setor público.

Conforme modelo adotado pela maioria dos países, o órgão deve ser criado como autarquia, com mandatos de seus diretores que não coincidam com os de eleições do poder

¹² Sobre a diferença entre diretiva e regulamento: “Um «Regulamento» é um ato legislativo vinculativo, aplicável em todos os seus elementos em todos os países da UE, não carecendo de transposição para a ordem jurídica nacional. Tem um caráter geral e é obrigatório em todos os seus elementos e diretamente aplicável em todos os Estados-Membros (art. 288.º do Tratado sobre o Funcionamento da União Europeia). Uma directiva é um ato legislativo que fixa um objetivo geral que todos os países da EU devem alcançar. Contudo, cabe a cada país elaborar a sua própria legislação para dar cumprimento a esse objetivo (art. 288.º do Tratado sobre o Funcionamento da União Europeia).” (FERREIRA, 2018, p. 23-24).

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

legislativo e executivo, garantindo independência técnica e administrativa. Finalmente, os países da América Latina¹³ que foram reconhecidos pela União Europeia como detentores de mesmo nível de proteção de dados da União Europeia, tiveram como destaque possuírem uma autoridade independente de proteção.

A Comissão Europeia tem o poder de determinar se um país de fora da União Europeia oferece um nível adequado de proteção de dados, podendo os dados pessoais fluir nestes, sem necessidade de mais nenhuma salvaguarda. Obter essa aprovação é positivo para a segurança jurídica do país no comércio e cooperação internacional (INSTITUTO DE DEFESA DO CONSUMIDOR, 2019). Portanto, fundamental para o país se consolidar no capitalismo informacional.

Cabe ressaltar, ainda, que o Brasil não considera legalmente a proteção de dados como um direito fundamental, embora em recente julgamento da Adin nº 6.378 do Distrito Federal, o Supremo Tribunal Federal reconheça o direito à proteção de dados como implícito no rol de direitos fundamentais. Há um projeto de emenda à Constituição Federal, nº 17/2019¹⁴, para incluir no rol de direitos e garantias individuais previsto no art. 5º, o direito à proteção de dados, e a competência da União Federal para legislar sobre o assunto.

A iniciativa é louvável, mas considerando a Carta de Direitos Fundamentais da União Europeia de 2000¹⁵ em comparação com o texto da proposta de emenda à Constituição

¹³ Veja-se que na decisão da Comissão Europeia, ao entender ser o nível de proteção de dados do Uruguai adequado ao estabelecido na União Europeia, anotou que: “[...] (5) A Constituição da República Oriental do Uruguai, aprovada em 1967, não reconhece expressamente o direito ao respeito pela vida privada e à proteção dos dados pessoais. Contudo, a enumeração dos direitos fundamentais não constitui uma lista fechada, dado que o artigo 72.o da Constituição determina que a lista de direitos, obrigações e garantias previstos na Constituição não exclui outros que sejam inerentes à personalidade humana ou que derivem da forma republicana de governo. O artigo 1.o da Lei n.o 18.331 de proteção de dados pessoais e ação de habeas data, de 11 de agosto de 2008 (Ley n.o 18.331 de protección de datos personales y acción de habeas data) prevê expressamente que «o direito à proteção dos dados pessoais é inerente ao ser humano, pelo que se encontra abrangido pelo artigo 72.o da Constituição da República». [...] (10) A aplicação das normas de proteção de dados é garantida pela existência de vias de recurso administrativas e judiciais, em especial pela ação de habeas data, que permite à pessoa a quem se referem os dados intentar uma ação judicial contra o responsável pelo tratamento dos dados, a fim de exercer o direito de acesso, retificação e supressão, e por um controlo independente efetuado pela Unidade Reguladora e de Controlo de Dados Pessoais (Unidad Reguladora y de Control de Datos Personales – URCDP), que tem poderes de investigação, intervenção e sanção, seguindo o disposto no artigo 28.o da Diretiva 95/46/CE, e que atua de forma totalmente independente.”. (2012).

¹⁴ Acrescenta o inciso XII-A, ao art. 5º e o inciso XXX, ao art. 22, da Constituição Federal para incluir a proteção de dados pessoais entre os direitos fundamentais do cidadão e fixar a competência privativa da União para legislar sobre a matéria.

¹⁵ **Artigo 8.º Proteção de dados pessoais.** Todas as pessoas têm direito à proteção dos dados de carácter pessoal que lhes digam respeito. 2. Esses dados devem ser objeto de um tratamento leal, para fins específicos e com o

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

brasileira, é possível perceber a ausência de que este direito fica garantido com a existência de uma autoridade nacional de proteção independente. Com a previsão explícita, além do importante reconhecimento do direito à proteção de dados como um direito autônomo, seria não menos vital também prever a existência de uma autoridade independente para a garantia deste direito, podendo ser inclusive uma forma de pressão para que o órgão criado pelo Brasil vire de fato uma agência reguladora como previsto legalmente.

Com a garantia de independência da Autoridade Nacional de Proteção de Dados do Brasil é possível assegurar uma liberdade informática nos dias atuais. O exercício pleno da cidadania nos dias atuais depende desta forma inovadora de tutela. Ademais, cria as condições necessárias para que o país seja incluído em uma economia global e no capitalismo informacional, possibilitando desenvolvimento econômico. E como afirma a LGPD, um dos fundamentos proteção de dados tem como o desenvolvimento econômico e tecnológico, o fluxo informacional lícito e o exercício da cidadania.

CONCLUSÃO

O presente artigo procurou discorrer sobre a criação da Autoridade Nacional de Proteção de Dados no Brasil demonstrando sua relação com a necessidade de adoção de tutelas inovadoras de direitos fundamentais através da ótica dos direitos humanos, para ressaltar a importância da independência destas em relação ao poder público e setor privado. Estabelecido do que se trata uma autoridade independente de proteção e sua importância, em um segundo momento, procurou-se investigar comparativamente os requisitos normativos da independência no modelo adotado no Brasil com os atuantes em países da União Europeia.

Portanto, resgatando este problema de pesquisa, pode-se observar dois pontos fundamentais acerca da autoridade de proteção independente adotada no Brasil. Primeiramente, cabe anotar que o Brasil adotou o sistema europeu de proteção de dados, que pressupõe a existência de uma autoridade para fiscalizar o cumprimento da lei. No entanto, este mesmo sistema tem cada vez mais se consolidado pela necessidade de atuação das autoridades para a

consentimento da pessoa interessada ou com outro fundamento legítimo previsto por lei. Todas as pessoas têm o direito de aceder aos dados coligidos que lhes digam respeito e de obter a respectiva retificação. 3. O cumprimento destas regras fica sujeito a fiscalização por parte de uma autoridade independente.”. grifo nosso. (UNIÃO EUROPEIA, 2000).

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

regulação da proteção de dados, ao invés de crer apenas no consentimento para a utilização dos dados pessoais, também aposta na prevenção de riscos, pareceres consultivos em projetos de lei sobre o tema e campanhas de conscientização da população.

O segundo ponto, é que embora se entenda plausível a adoção de um regime de transição da autoridade de proteção de dados brasileira, criada inicialmente em vinculação com a Presidência da República, mas com previsão legal de discussão de mudança de sua estrutura para uma agência reguladora no prazo de 02 (dois) anos, se observa fundamental esta alteração. Adquirindo a estrutura de uma agência reguladora, a autoridade pode desenvolver uma melhor aptidão técnica e autonomia financeira, perfectibilizando, em tese, considerando apenas no plano normativo, sua independência para a fiscalização do setor público e privado.

O julgamento da Adin nº. 6.378 que reconheceu o direito à proteção de dados como um novo direito autônomo implícito na Constituição Federal através de um julgamento de uma lei que determinava o compartilhamento de dados pessoais de empresas de telefonia com o governo federal sinalizou a importância de se ter uma agência reguladora atuante que poderia, até mesmo, dar um parecer técnico sobre o projeto de lei. Por isso, além da importante discussão acerca da necessidade de explicitamente reconhecer-se o direito à proteção de dados na Constituição Federal, reservando a competência legislativa para a União Federal, cabe afirmar que na União Europeia, o texto legal equivalente prevê a existência de uma autoridade administrativa para a fiscalização do cumprimento da lei, o que seria o caso de acrescer a proposta brasileira.

REFERÊNCIAS

BAUMAN, Zygmunt et al. Após Snowden: Repensando o Impacto da Vigilância. **Revista Eco Pós**, Rio de Janeiro, v. 18, n. 2, p.8-35, 2015. Disponível em: https://revistaecopos.eco.ufrj.br/eco_pos/article/view/2660. Acesso em: 21 mai. 2021.

BRASIL. Lei nº 13853, de 08 de julho de 2019. **Altera a Lei nº 13.709, de 14 de agosto de 2018, para dispor sobre a proteção de dados pessoais e para criar a Autoridade Nacional de Proteção de Dados; e dá outras providências**. Brasília, 09 jul. 2019a. Disponível em: http://www.planalto.gov.br/ccivil_03/_Ato2019-2022/2019/Lei/L13853.htm#art2. Acesso em: 21 mai. 2021.

BRASIL. Lei nº 13.709, de 14 de agosto de 2018. **Lei Geral de Proteção de Dados Pessoais (LGPD)**. Brasília, 15 ago. 2018. Disponível em:

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 21 mai. 2021.

BRASIL. Senado Federal. **Proposta de Emenda à Constituição nº 17/2019b**. Disponível em: <https://www25.senado.leg.br/web/atividade/materias/-/materia/135594>. Acesso em: 21 mai. 2021.

CASTELLS, Manuel. **A galáxia da internet**: reflexões sobre a internet, os negócios e a sociedade. Tradução de Maria Luiza Borges. Rio de Janeiro: Zahar, 2003.

COMISSÃO EUROPEIA. **C (2012) 5704**: DECISÃO DE EXECUÇÃO DA COMISSÃO de 21 de agosto de 2012 nos termos da Diretiva 95/46/CE do Parlamento Europeu e do Conselho relativa à adequação do nível de proteção de dados pessoais pela República Oriental do Uruguai no que se refere ao tratamento automatizado de dados. Bruxelas, 2012. Disponível em: <https://op.europa.eu/et/publication-detail/-/publication/d3dd96fc-ee04-11e1-8e28-01aa75ed71a1/language-pt>. Acesso em: 21 mai. 2021.

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

DONEDA, Danilo. Princípios de Proteção de Dados Pessoais. *In*: LUCCA, Newton de; SIMÃO FILHO, Adalberto; LIMA, Cíntia Rosa Pereira de. **Direito & Internet III - Tomo I**: Marco Civil da internet (Lei n. 12.965/2014). São Paulo: Quartier Latin, 2015. p. 369-384.

EUROPEAN UNION AGENCY FOR FUNDAMENTAL RIGHTS. **Data protection in the European Union**: the role of National Data Protection Authorities. Luxemburgo: Publications Office of the European Union, 2010. 56 p. Disponível em: https://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf. Acesso em: 16 mai. 2021.

FERREIRA, Manuel. **O Regulamento Geral Sobre a Protecção de Dados**: aspectos legais e organizativos de governança nas organizações. 2018. 103 f. Dissertação (Mestrado) - Curso de Direito e Segurança, Direito, Universidade Nova de Lisboa, Lisboa, 2018. Disponível em: https://run.unl.pt/bitstream/10362/54953/1/ManuelFerreira_2018.pdf. Acesso em: 16 mai. 2021.

GREENLEAF, Graham. Data Privacy Authorities (DPAS) 2017: Growing Significance of Global Networks. **Privacy Laws & Business International Report**, Sydney, p.1-7, 2017. Disponível em: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2993186##. Acesso em: 16 mai. 2021.

INSTITUTO BRASILEIRO DE DEFESA DO CONSUMIDOR. **Autoridades de proteção de dados para a américa latina**: Um estudo dos modelos institucionais da Argentina, Colômbia e Uruguai. São Paulo, 2019. 59 p. Disponível em: <https://idec.org.br/publicacao/autoridade-de-protecao-de-dados-na-america-latina>. Acesso em: 21 mai. 2021.

INTERNACIONAL CONFERENCE OF DATA PROTECTION & PRIVACY COMMISSIONERS. **Counting on Commissioners**: High level results of the ICDPPC Census 2017. Hong Kong, 2017. 53 p. Disponível em: <https://globalprivacyassembly.org/wp-content/uploads/2017/09/ICDPPC-Census-Report-1.pdf>. Acesso em: 16 mai. 2021.

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

LEONARDI, Marcel. **Tutela e privacidade na internet**. São Paulo: Saraiva, 2011.

LYON, David. Surveillance, Snowden, and Big Data: Capacities, consequences, critique. **Big Data & Society**, [s.l.], v. 1, n. 2, p.205395171454186-13, 9 jul. 2014. SAGE Publications. <http://dx.doi.org/10.1177/2053951714541861>. Disponível em: <https://journals.sagepub.com/doi/full/10.1177/2053951714541861>. Acesso em: 16 mai. 2021.

MASSENO, Manuel David. Como a União Europeia procura proteger os cidadãos-consumidores em tempos de *Big Data*. **Revista Eletrônica do Curso de Direito**, Santa Maria, v. 14, n. 3, p.1-27, 2019. Disponível em: <https://periodicos.ufsm.br/revistadireito/article/view/41708>. Acesso em: 21 mai. 2021.

MENDES, Laura Schertel. Privacidade e dados pessoais. Proteção de dados pessoais: fundamento, conceitos e modelo de aplicação. **Revista Panorama Setorial da Internet**, São Paulo, p.1-6, jul. 2019. Disponível em: https://www.cetic.br/media/docs/publicacoes/6/15122520190717-panorama_setorial_ano_xi_n_2_privacidade_e_dados_pessoais.pdf. Acesso em: 16 mai. 2021.

MENDES, Laura Schertel. **Transparência e privacidade: violação e proteção da informação pessoal na Sociedade de Consumo**. 2008. 158 f. Dissertação (Mestrado) - Curso de Direito, Universidade de Brasília, Brasília, 2008. Disponível em: <https://repositorio.unb.br/bitstream/10482/4782/1/DISSERTACAO%20LAURA.pdf>. Acesso em: 16 mai. 2021.

NÚCLEO DE INFORMAÇÃO E COORDENAÇÃO DO PONTO BR. **Pesquisa web sobre o uso da Internet no Brasil durante a pandemia do novo coronavírus: Painel TIC COVID-19**. São Paulo: Comitê Gestor da Internet no Brasil, 2021. Disponível em: https://cetic.br/media/docs/publicacoes/2/20210426095323/painel_tic_covid19_livro_eletronico.pdf. Acesso em: 16 mai. 2021.

PÉREZ LUÑO, Antonio-Enrique. **? Ciberciudadani@ o ciudadani@.com?** Barcelona: Gedisa, 2003.

PÉREZ LUÑO, Antonio-Enrique. Las generaciones de derechos humanos. **Revista Direitos Emergentes na Sociedade Global**, Santa Maria, v. 2, n. 1, p.136-196, 2013. Disponível em: https://periodicos.ufsm.br/REDESG/article/view/10183/pdf_1#.XUpquuhKjiU. Acesso em: 16 mai. 2021.

PÉREZ LUÑO, Antonio-Enrique. La tutela de la libertad informática en la sociedad globalizada. **Isegoría**, [s.l.], n. 22, p.59-68, 30 set. 2000. Editorial CSIC. Disponível em: <http://isegoria.revistas.csic.es/index.php/isegoria/article/view/521/521>. Acesso em: 16 mai. 2021.

RODOTÀ, Stefano. **A vida na sociedade da vigilância – a privacidade hoje**. Rio de Janeiro: Renovar, 2008.

SARLET, Ingo. **Curso de direito constitucional**. São Paulo: Saraiva, 2015.

SCHUTZ, Philip. **Assessing Formal Independence of Data Protection Authorities in a Comparative Perspective**. 2012. Disponível em:

Volume 10 – Número 2 (2021) - Porto Alegre – Rio Grande do Sul – Brasil

https://link.springer.com/content/pdf/10.1007%2F978-3-642-31668-5_4.pdf. Acesso em: 16 mai. 2021.

UNESCO. **TIC para o desenvolvimento sustentável**: Recomendações de políticas públicas que garantem direitos. Montevideu: Cetic.br/nic.br, 2019. 80 p. Disponível em: <https://cetic.br/media/docs/publicacoes/8/14582020190716-tic-para-o-desenvolvimento-sustentavel.pdf>. Acesso em: 16 mai. 2021.

UNIÃO EUROPEIA. Carta nº (2000/C 364/01), de 18 de dezembro de 2000. **CARTA DOS DIREITOS FUNDAMENTAIS DA UNIÃO EUROPEIA**. Disponível em: https://www.europarl.europa.eu/charter/pdf/text_pt.pdf. Acesso em: 16 mai. 2021.

UNIÃO EUROPEIA. **Regulamento nº 2016/679, de 27 de abril de 2016**. Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho, de 27 de abril de 2016, relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). Disponível em: <https://eur-lex.europa.eu/eli/reg/2016/679/oj?locale=pt>. Acesso em: 16 mai. 2021.

ZANATTA, Rafael A. F. Proteção de dados pessoais como regulação do risco: uma nova moldura teórica? **I Encontro da rede de Pesquisa em Governança da Internet – REDE 2017**. São Paulo, 2018. p. 175. Disponível em: http://redegovernanca.net.br/public/conferences/1/anais/Anais_REDE_2017-1.pdf. Acesso em: 16 mai. 2021.