A RESPONSABILIDADE DO EMPREGADOR PELA PROTEÇÃO DE DADOS NO MEIO AMBIENTE DE TRABALHO: CONSEQUÊNCIAS JURÍDICAS

THE EMPLOYER RESPONSIBILITY FOR DATA PROTECTION IN THE WORK ENVIRONMENT: LEGAL CONSEQUENCES

JOÃO GABRIEL YAEGASHI[1]
CLEBER SANFELICI OTERO[2]

RESUMO

Neste artigo, objetiva-se estudar a maneira como ocorre o tratamento de dados no meio ambiente de trabalho, com enfoque na responsabilidade do empregador frente à nova concepção do direito à proteção de dados pessoais. Procede-se a uma pesquisa bibliográfica e documental, com o emprego do método de abordagem dedutivo, com o estudo, primeiramente, acerca de como ocorreu o desenvolvimento da informática até o atual modelo de capitalismo de vigilância, acabando por demandar um novo direito fundamental à proteção de dados pessoais. Depois, discorre-se acerca da responsabilidade sob uma perspectiva moderna, aplicável a este contexto tecnológico e, por fim, aborda-se especificamente as dificuldades e peculiaridades que envolvem o tratamento de dados nas relações de trabalho ao longo de todas as fases do contrato. Conclui-se que a tecnologia e o tratamento de dados configuram elementos intrínsecos da contemporaneidade e de particular incidência nas relações de trabalho, de forma que o devido reconhecimento e respeito a um direito de proteção de dados pessoais se mostra imprescindível para a proteção da pessoa humana em sua dignidade e personalidade.

Palavras-chave: proteção de dados pessoais; direitos da personalidade; relação de trabalho; responsabilidade civil; LGPD.

ABSTRACT

This article intends to study how data is processed in the work environment, with a focus on the employer's responsibilities, in view of the new conception of the right to the protection of personal data. A bibliographical and documentary research is carried out, using the deductive approach method, with the study of how the devel-

1 Mestrando em Ciências Jurídicas pela Universidade Cesumar (UNICESUMAR). Bolsista CAPES. Graduado em Direito pela Universidade Estadual de Maringá (UEM). ORCID iD: https://orcid.org/0000-0002-6341-0942.

2 Doutor em Sistema Constitucional de Garantia de Direitos pela Instituição Toledo de Ensino (ITE). Graduado em Direito pela Faculdade de Direito da Universidade de São Paulo (USP). Juiz Federal. Docente no Programa de Pós-Graduação em Ciências Jurídicas da Universidade Cesumar (UNICESUMAR). ORCID iD: https://orcid.org/0000-0001-6035-7835.

Como citar esse artigo:/*How to cite this article*:
YAEGASHI, João Gabriel; OTERO, Cleber Sanfelici. A reponsabilidade do empregador pela proteção de dados no meio ambiente de trabalho: consequências jurídicas. **Revista Meritum**, Belo Horizonte, v. 17, n. 3, p. 284-299, 2022. DOI: https://doi.org/10.46560/meritum.v17i3.8807.

opment of computing up to the current model of surveillance capitalism occurred, ending up demanding a new fundamental right to the protection of personal data. Then, responsibility is discussed from a modern perspective, applicable to this technological context and, finally, it specifically addresses the difficulties and peculiarities that involve the processing of data in labor relations throughout all phases of the contract. It is concluded that technology and data processing are intrinsic elements of contemporaneity and of particular impact on labor relations, so that due recognition and respect for a right to protection of personal data is essential for the protection of the human person in its dignity and personality.

Keywords: *protection of personal data; personality rights; work relationship; civil responsability; GDPL.*

1. INTRODUÇÃO

A difusão da tecnologia para os diversos campos da vida é irremissível, de forma que o direito, estrutura organizacional da sociedade, é instado a reestruturar antigas bases normativas de forma a salvaguardar a pessoa humana em sua dignidade e personalidade. Nesse ponto, reconhece-se a existência de um novo modelo de mercado que ataca essa personalidade humana, monetizando-a com a apropriação unilateral dos dados pessoais e influência de comportamentos futuros para a aquisição de produtos e serviços.

Nas relações de trabalho, igual salvaguarda é necessária, uma vez que a ampliação dos mecanismos tecnológicos, paralelamente, acarreta maior monitoramento e apropriação de dados do empregado-titular, algo que, com a devida vênia, não pode continuar a ser feito de forma leviana em detrimento da dignidade da pessoa humana.

Por esse motivo, releva-se o estudo da tutela jurídica dos direitos da personalidade do empregado na sociedade de informação pelo reconhecimento de um direito à proteção de dados pessoais, o qual, no território nacional, possui por principal expoente a Lei Geral de Proteção de Dados (LGPD).

O problema a ser investigado diz respeito à forma pela qual o ordenamento brasileiro influencia as diversas fases da relação laboral para a proteção da dignidade do trabalhador em um contexto de sociedade de informação e processamento massivo de dados.

Partindo-se dessa indagação, busca-se investigar a maneira como ocorre o tratamento de dados no meio ambiente de trabalho, com enfoque nas responsabilidades do empregador, frente à nova concepção do direito à proteção de dados pessoais.

A pesquisa se justifica na medida em que a proteção de dados, cuja essencialidade já é rediscutida no cenário mundial, passou a ser abordada apenas recentemente no Brasil. Somente em setembro do ano de 2020, entrou em vigor a Lei Geral de Proteção de Dados (LGPD) (BRASIL, 2018), legislação específica que tutela tão importante segmento social, de forma que estudos sobre seus efeitos, em momento tão tenro, mostram-se pertinentes para a sociedade como um todo.

A fim de atender ao objetivo do estudo, emprega-se o método dedutivo, com vista a revelar que o direito à proteção de dados pessoais influencia a relação empregatícia para a proteção do trabalhador ao longo das diversas fases da relação laboral, por intermédio de uma pesquisa documental, tendo como fonte a legislação brasileira, e bibliográfica, com a intenção de com-

preender o desenvolvimento da abordagem jurídica da matéria até o estágio atual. Para tanto, recorre-se a artigos disponibilizados em periódicos, livros e demais produções sobre a temática.

Para fins didáticos, o artigo está dividido em três seções. Na primeira, encontra-se o estudo do desenvolvimento e da difusão das tecnologias pelo globo, com a constatação de um movimento de despersonalização da personalidade e necessidade de um reconhecimento de um direito à proteção de dados pessoais para o combate a este quadro nocivo. Na segunda, discute-se acerca do fundamento e formas de responsabilidade pela proteção de dados decorrentes do aspecto objetivo deste direito à proteção de dados pessoais, com um especial enfoque na responsabilidade civil encarada em um viés de sociedade tecnológica. Na terceira, por fim, aborda-se a relação de trabalho em suas diversas fases e quais as necessárias cautelas que o empregador deve observar acerca do tratamento de dados nessas respectivas etapas, as quais são dispostas, de forma protagonizada, pela LGPD.

2. DIREITO À PROTEÇÃO DOS DADOS PESSOAIS

A contemporaneidade é marcada por uma revolução das maneiras de interação humana e de gerenciamento de informação, algo que se concretizou em razão do sistema de rede global mantido pelas tecnologias de comunicação.

A onipresença da tecnologia constitui característica marcante de nossa época, já que a vida no século XXI é monitorada e condicionada nos mais diversos campos por eletrônicos e algoritmos (WIMMER, 2019). Sarlet (2021), na mesma toada, ressalta a significante influência da tecnologia nos campos social, econômico, político e cultural da vida contemporânea, ao que se comumente denomina *ubiquitous computing.* A chamada computação pervasiva, segundo a qual o ser humano se conecta com computadores distribuídos em tantos locais que acaba por interagir sem perceber, ganha ainda maior mobilidade e invisibilidade na medida em que a computação ubíqua permite a integração da informática com as ações naturais das pessoas em função do uso da tecnologia móvel em celulares, automóveis e outros aparelhos em diversos ambientes, de forma a conectá-los com uma virtualidade encorpada, muitas vezes de maneira imperceptível (WEISER, 1991).

A criação de uma rede global de comunicação ocorreu a partir da difusão das tecnologias da informação, a qual retroage à Segunda Guerra Mundial e ao período seguinte, especialmente a década de 1970 (CASTELLS, 2020), com os primeiros computadores e a sua rede de compartilhamento desenvolvida para propósitos militares (ROSSINI, 2004). Precedente ao desenvolvimento dos computadores, houve o desenvolvimento da telefonia, o qual permitiu uma interligação e comunicação em nível global (HARVEY, 1993). Com a junção desses instrumentos, a partir da década de 80, houve uma acentuada difusão da informática pelo mundo, com a interligação em redes de conexão e interação, o que possibilitou uma nova base material para o desempenho de atividades em toda a estrutura social (CASTELLS, 2020).

Essa difusão acelerada das Tecnologias de Informação e Comunicação (TICs) e o estabelecimento da rede mundial de computadores alterou as bases do modelo social vigente, o qual se sustenta por um grande fluxo de informações (LEHFELD *et al.,* 2021). Esse fluxo de informações utilizadas para a manutenção do modelo social é o que caracteriza a denominada

"sociedade da informação" (LISBOA, 2006; PEREZ-ZUNIGA *et al.*, 2018), algo que seria impossível sem a conexão e pulverização de dados em escala global.

Nessa sociedade de informação, de abrangência global pela rede, a tecnologia condiciona a vida e os mais diversos segmentos da economia. Assim como sustenta Castells (2020, p. 555), "a nova economia está organizada em torno de redes globais de capital, gerenciamento e informação cujo acesso a *know-how* tecnológico é importantíssimo para a produtividade e competitividade".

Anteriormente a esse cenário tecnológico, sabe-se que os diversos ordenamentos jurídicos buscaram se readaptar a uma necessidade de maior proteção da pessoa humana frente ao esvaziamento de sua "dignidade", fenômeno que se nominou de *repersonalização do direito civil* (SZANIAWSKI, 2005), algo que se acompanhou pelos últimos 30 (trinta) anos no Brasil com a chamada teoria da *constitucionalização do direito civil*, que nada mais é que a personalização do direito privado. O Direito Civil Constitucional parte da premissa da funcionalização das situações patrimoniais às existenciais, uma repressão às situações econômicas que desconsiderem a pessoa humana como fundamento e fonte do ordenamento jurídico.

Tal premissa se consagrou na Constituição brasileira pela cláusula geral de tutela da dignidade da pessoa humana como princípio fundamental estruturante de todo o sistema jurídico no Estado Democrático de Direito (BRASIL, 1988), de forma que se reconhece a pessoa humana como o ente com qualidade intrínseca, universal, indissociável, irrenunciável e inalienável, que a torna merecedora de respeito e sujeito de direitos perante a sociedade e o Estado, que deverá, ao seu turno, assumir e cumprir o ônus de proteger o ser humano contra abusos e degradações, bem como lhe garantir o mínimo existencial para uma vida digna em comunidade (SARLET, 2015).

Conquanto fosse esse o pano de fundo, as influências da tecnologia parecem ter impulsionado a carruagem para um caminho inverso, ao que Rosenvald denomina, ao tratar sobre a responsabilidade civil em um contexto tecnológico, de *despersonalização da personalidade* (PALESTRA..., 2021; ROSENVALD, 2021, p. 178), um fenômeno que ataca as bases do precitado Direito Civil Constitucional.

Nessa sociedade tecnológica, há três movimentos que subvertem as premissas humanísticas do Direito Civil Constitucional. São estes: a) expropriação da personalidade; b) ameaça da autonomia humana, com o ataque à consciência; e c) conversão do ser humano em projeto de personalização (PALESTRA..., 2021), decorrente de uma nova forma de mercado chamada por Zulboff (2020) de *capitalismo de vigilância*.

Quanto ao primeiro, *expropriação da personalidade* em prol de finalidades alheias, tem-se que estamos em um capitalismo de vigilância, uma nova forma de mercado, que tem por premissa reivindicar, unilateralmente, a experiência humana como uma matéria prima para a tradução de dados comportamentais, que são disponibilizados como produtos de predição, com antecipação e modelação de comportamentos futuros, de tal forma que, enquanto capitalismo industrial reivindicava a natureza, agora o capitalismo de vigilância reivindica a natureza humana (ZUBOFF, 2020, p. 562 e 578). Morreu a premissa kantiana do ser humano como fundamento em si, pois o que há agora é uma instrumentalização, uma usurpação da personalidade para finalidades alheias, porquanto, na era digital, situações existenciais são uma nova propriedade, baseada na "despossessão" da essência do que nos define (ZUBOFF,

apud ROSENVALD, 2021, p. 177). Assim, "não basta mais automatizar o fluxo de informação sobre nós; a meta agora é nos *automatizar*" (ZUBOFF, 2020, p. 19).

Quanto ao segundo movimento, da "ameaça da autonomia humana com o ataque à consciência", verificam-se efeitos ainda mais nefastos à personalidade humana. A autonomia privada é a pedra angular do Direito Privado, e consiste na possibilidade e consciência de viver de acordo com as próprias normas (CANTALI, 2009), uma *regulação pelo eu* não apenas na esfera econômica, mas no livre arbítrio de gerir seus pensamentos.

(PALESTRA..., 2021) afirma que a ciência desmente a falácia do livre arbítrio, pois este seria apenas uma distração criada pela narrativa liberal. A bem da verdade, somos um conjunto de sinapses, somos química e, na era digital, um conjunto de algoritmos passíveis de comercialização. A consequência desse processo ocorre em dois níveis, no consentimento e na consciência humana.

Quando da navegação em *sites* de provedores, encontra-se a pessoa em um contrato de adesão, mas em um grau muito maior de ausência de consentimento, já que as atividades dos provedores, em seus termos de uso, são alteradas a qualquer momento sem consentimento do usuário. Com a apropriação unilateral dos dados pelos provedores, para não dizer uma apropriação unilateral de direitos, ainda se nota uma gradual perda da própria consciência, já que a tecnologia emprega técnicas que induzem a uma modificação comportamental.

O ser autônomo é aquele que tem a possibilidade de premeditar, projetar escolhas e realizar julgamentos morais. Perdemos essa autonomia quando as ferramentas de predição assaltam a nossa mente e inconsciente para nos induzir a contratar bens e serviços, uma economia pautada em emoções e impulsos, que podem ser previstos e traduzidos pelos dados pessoais apropriados de forma não consentida. Muitas vezes, aliás, se a pessoa precisa de acesso a um determinado serviço, não há alternativa senão concordar com cláusulas contratuais que permitem a apropriação de uma série de dados do usuário, com múltiplos propósitos.

Por fim, o terceiro movimento, *conversão do ser humano em um projeto de personalização*. Personalizar é colocar a pessoa humana no ápice do ordenamento. Hoje, isso virou um *slogan*, um eufemismo para a coisificação da pessoa, para a monetização da vida em troca de segurança, serviços e conveniências. Pessoas não buscam mais um mínimo existencial, mas um máximo existencial, o supérfluo se torna necessário.

Quando do aceite dos termos de uso e da compra de produtos inteligentes, abre-se mão, por consequência, da privacidade. O fornecimento de informações é uma alternativa obrigatória ao consentimento de uso. E não apenas o fornecedor "contratado" possui acesso a essas informações, uma vez que elas são, automaticamente e sem consentimento, compartilhadas com terceiros (analistas, publicistas, etc), os quais não declaram qualquer responsabilidade pela gerência dos dados recebidos.

Em produtos inteligentes, há uma coligação contratual. O produto contratado é apenas a ponta do *iceberg*, que remete a outros demais produtos e serviços diretamente relacionados, como a aquisição de *softwares*. Trata-se de uma forma de renderizar a pessoa, por intermédio da extração de serviços adicionais que não se relacionam com a transação que se pensa ter feito, como a respiração, os batimentos cardíacos, os dados biométricos, dentre outras tantas informações sensíveis. Esse é o mercado de comportamento futuro, formas contratuais em que a base é a monitoração e customização de produtos amoldados às suas experiências.

Conclui-se, nesse cenário, que se sacrificou a liberdade em troca de um conhecimento que não é do titular, mas, na verdade, apropriado pelos fornecedores (PALESTRA..., 2021).

A realidade criada pelo desenvolvimento dos meios tecnológicos é capaz de infligir medo no coração de qualquer um que reflita sobre o assunto, sobremaneira pela incapacidade das instituições em acompanhar e se adaptar na mesma proporção à influência dessas tecnologias. A angústia em relação ao futuro, contudo, não implica a sua recusa.

No mesmo sentido, ao discorrer acerca do significado do quadro *Angelus Novus* e a sua associação com a invencível e inevitável força, Benjamin nos impele a refletir a respeito do futuro e do progresso:

> Há um quadro de Klee que se chama Angelus Novus. Representa um anjo que parece querer afastar-se de algo que ele encara fixamente. Seus olhos estão escancarados, sua boca dilatada, suas asas abertas. O anjo da história deve ter esse aspecto. Seu rosto está dirigido para o passado. Onde nós vemos uma cadeia de acontecimentos, ele vê uma catástrofe única, que acumula incansavelmente ruína sobre ruína e as dispersa a nossos pés. Ele gostaria de deter-se para acordar os mortos e juntar os fragmentos. Mas uma tempestade sopra do paraíso e prende-se em suas asas com tanta força que ele não pode mais fechá-las. Essa tempestade o impele irresistivelmente para o futuro, ao qual ele vira as costas, enquanto o amontoado de ruínas cresce até o céu. Essa tempestade é o que chamamos progresso. (BENJAMIN, 1987, p. 226)

Conquanto os riscos inerentes ao progresso tecnológico, sabe-se da impossibilidade de detê-lo, mesmo que acompanhado de algumas qualidades negativas (RODOTÀ, 2008). Logo, não há como se conceber e sustentar as bases dos complexos e atuais sistemas de governo e de mercado sem o emprego em rede de recursos tecnológicos.

Não à toa, na sociedade de informação, o acesso à internet já é reconhecido como um direito fundamental e necessário para o desenvolvimento (UNITED NATIONS, 2011), de forma que é necessário estabelecer diretrizes, princípios e regras para atenuar eventuais efeitos negativos do desenfreado desenvolvimento tecnológico (WIMMER, 2019). De outro lado, uma vez vivendo na inevitável sociedade de informação, é necessário se adaptar para coexistir com a tecnologia que sustenta as atuais bases sociais, o que ocorre, atualmente, pelo desenvolvimento de um direito à proteção de dados pessoais.

Tendo em vista os precitados ataques à privacidade e à autodeterminação da pessoa humana pelo dinamismo dos recursos tecnológicos, coloca-se em xeque a própria capacidade do Estado como ente protetor do indivíduo, de forma que há muito se discute a necessidade de um processo de *digitalização dos direitos fundamentais*, algo que demanda o reconhecimento, na esfera internacional e constitucional, de um direito fundamental à proteção de dados e uma releitura de outros direitos fundamentais clássicos (SARLET, 2021).

A primeira legislação em todo o mundo a tratar desse aspecto foi a Lei de Proteção de Dados do *Bundesland* de Hesse, Alemanha, em 1970 (DONEDA, 2021), ao passo que a primeira legislação a tratar da matéria em âmbito federal no mesmo país foi editada em 1977 (SARLET, 2021).

No âmbito internacional, a despeito da possibilidade de interpretação do direito à proteção de dados em outras declarações e tratados, foi somente no ano 2000, na Carta de Direitos Fundamentais da União Europeia, que tal direito foi tratado de forma autônoma. Dentro da

REVISTA MERITUM • v.17 • n.3 • p. 284-299 • Set. - Dez. 2022

soberania dos Estados, seguiu-se igual rumo, positivando-se esse direito nas Constituições, embora alguns países, como atualmente é o caso do Brasil, permaneçam reconhecendo tal direito apenas de forma implícita, por uma hermenêutica acerca do ordenamento jurídico (SARLET, 2021).

Esse novo direito humano e fundamental, reconhecido por critérios de historicidade (FACHIN; FACHIN, 2020), ancora-se na dignidade da pessoa humana para justificar sua fundamentabilidade, determinar seu conteúdo e estabelecer certos pontos de contato com outros direitos fundamentais, de forma que se interrelaciona, não obstante seu caráter autônomo, com o livre desenvolvimento da personalidade (em sua natureza geral), com a autodeterminação informativa (em sua natureza específica) e com a privacidade.

É importante frisar que o direito à proteção de dados vai além da autodeterminação informativa, conquanto encontre nesta o seu eixo estruturante, uma vez que possui viés mais amplo, indo além da mera proteção a dados ou conjuntos de forma individual, mas se preocupando com a integralidade dos sistemas técnicos-informacionais como um todo (SARLET, 2021). Da mesma forma, não se confunde com o direito à vida privada e à intimidade, já que estes se limitam a um viés negativo e estático de proteção, restrito a impossibilitar a interferência injustificada de terceiros nessa esfera (informação e sigilo). A proteção de dados, ao seu turno, vai além, conferindo ao seu titular poderes positivos e dinâmicos sobre o controle e coleta de dados que lhe digam respeito (informação, circulação e controle) (RODOTÀ, 2008).

No Brasil, baseada nas mesmas premissas alhures expostas, reconhece-se o direito autônomo à proteção de dados, com clara a influência recíproca entre a ordem jurídica interna e a ordem jurídica internacional quando tratada a matéria, mormente pela simetria de nossa recente Lei Geral de Proteção de Dados (LGPD) com o Regulamento Geral de Proteção de Dados Europeu (RGPDE) (SARLET, 2021).

Internamente, compreende-se, de forma pacífica, a natureza jurídica tríplice do direito à proteção de dados pessoais como um direito humano, fundamental e da personalidade, algo decorrente de toda a interpretação de seu sentido material e formal, o que lhe confere, dentro da ordem constitucional doméstica, idênticos efeitos jurídicos devidos a estes chamados direitos fundamentais, como a autoaplicabilidade e vinculação (art. 5º, § 1º, CF/88), imposição de limites materiais ao poder de reforma constitucional (art. 60, § 4º, CF/88) e a possibilidade de aplicação de mecanismos constitucionais de controle de legitimidade dos atos, tais como a proporcionalidade, segurança jurídica, dentre outros (SARLET, 2021).

Quanto ao seu objeto, sem prejuízo da possibilidade de diferenciação técnica entre os conceitos de "dado" e "informação", verifica-se que a própria LGPD cuidou de englobar ambas quando da especificação do conceito de "dado pessoal", enunciando, em seu art. 5º, I, como aquele consistente em "informação relacionada a pessoa natural identificada ou identificável" (BRASIL, 2018), o que torna irrelevante tal diferenciação para fins de proteção legal, de forma que a legislação trata de tutelar os dados propriamente ditos e a informação processada em dados.

Tais constatações podem ser ratificadas em *leading case* recentemente patrocinado pelo Supremo Tribunal Federal (STF) nos dias 06 e 07 de maio de 2020, no julgamento de várias Ações Diretas de Inconstitucionalidade (ADIs nº 6.387, 6.388, 6.389, 6.390 e 6.393), que julgaram, com largura de um placar de 10 votos favoráveis, pela inconstitucionalidade da MP nº 954/2020. Na citada decisão, entendeu a Corte Constitucional brasileira que a medida em si,

genérica e sem a previsão de procedimentos de segurança da informação, vilipendiava um direito autônomo aos dados pessoais, implicitamente consagrado na Constituição e dotado de uma dupla dimensão (subjetiva e objetiva). A dimensão subjetiva se desdobra em uma liberdade negativa do titular, a qual pode opor sua legítima esfera pessoal ao Estado e particulares. A dimensão objetiva, ao seu turno, é o que demanda um dever de atuação positivo do Estado na proteção de um direito fundamental à proteção de dados, legitimando, pois, a intervenção do Poder Judiciário para a sua concretização (MENDES; RODRIGUES JÚNIOR; FONSECA, 2021).

Não obstante a atenção do mundo para essa necessidade, a normatização específica tardou a ser formulada no Brasil, que tratava da questão, até então, de forma dissolvida em diversos instrumentos normativos, consoante se pode observar na Política Nacional de Informática, no *habeas data*, no Código de Defesa do Consumidor, na Lei de Acesso à Informação, na Lei do Cadastro Positivo, no Marco Civil da Internet e na Política Nacional de Segurança da Informação da Administração Pública Federal (BARRETO, 2019), o que foi taxativamente fulminado com a sanção da Lei nº 13.709, de 14 de agosto de 2018, ementada como "Lei Geral de Proteção de Dados Pessoais (LGPD)" (BRASIL, 2018), alterada pela Lei nº 13.853/2019, a qual tem por escopo proteger, de forma ampla, os dados pessoais, criar direitos ao titular, indicar as hipóteses e princípios de orientação ao tratamento, bem como prever responsabilidades pela via administrativa e civil em caso de danos provocados aos titulares.

E mesmo que já implicitamente extraível da Constituição Federal, releva mencionar a existência do Projeto de Emenda à Constituição (PEC) nº 17/2019, o qual busca alterar o texto constitucional de forma a inserir "a proteção de dados pessoais" no rol dos direitos e garantias fundamentais, bem como limitar tal matéria à competência legislativa privativa da União (MENDES; RODRIGUES JÚNIOR; FONSECA, 2021), cenário que se vislumbra no horizonte, seja pela urgência emprestada pela decisão do STF, seja pelo reconhecido impacto já causado pelo tenro tempo de vigência da LGPD. A positivação, embora desnecessária para os efeitos fundamentais do direito, é bem-vinda pela agregação de valor substancial a esse direito fundamental, trazendo segurança jurídica e certeza de sua natureza fundamental autônoma, bem como uma agregação de força hierárquica, em razão da integração formal na Constituição (SARLET, 2021).

3. A RESPONSABILIDADE EM UMA PERSPECTIVA MODERNA

O Direito, como estrutura organizacional e normativa regulatória de todas as searas da sociedade, deve dar uma resposta quando tratado do direito à proteção de dados pessoais. Como já dito, o direito fundamental à proteção de dados acaba por ter um aspecto subjetivo e outro objetivo. O primeiro é servível para uma postura negativa do titular, o segundo, por sua vez, demanda uma atuação positiva do Estado na proteção desse direito. É na dimensão objetiva que reside a legitimidade das múltiplas intervenções estatais, as quais podem ocorrer por intermédio de normas penais, pelo estabelecimento da responsabilidade civil (art. 42 e seguintes da LGPD) e de atuações concretas de órgãos fiscalizadores do poder público (art. 52 e seguintes da LGPD), como atualmente o faz por intermédio da Autoridade Nacional de Proteção de Dados (art. 55-A e seguintes da LGPD).

Sem desprezar as demais esferas de atuação do poder público, dar-se-á maior enfoque à responsabilidade civil em razão de seu protagonismo na resposta a este estado de coisas trazido à baila pela sociedade tecnológica.

Rosenvald (2021, p. 176) destaca que a responsabilidade civil é o repositório das disfuncionalidades nas atividades econômicas e sociais, contudo, ao menos no Brasil, deixa de atender adequadamente às várias situações da vida em razão da cultura de litígio e compensação vigorante no país, que a enxerga de forma míope, apenas no aspecto que tange à indenização de danos em um aspecto litigioso. Esta modalidade da responsabilidade civil, no Direito estadunidense pautado no *common law*, chama-se *Liability*, a qual representa, nas palavras do autor (ROSENVALD, 2021, p. 181), apenas "a parte visível do *iceberg*", um reflexo de cultura de compensação de danos (*full compensation*), e não de prevenção de ilícitos. Não obstante, a responsabilidade civil, para uma tratativa adequada das questões envolvendo a responsabilidade numa sociedade tecnológica, deve ser vista por outros vieses igualmente importantes, mais de caráter preventivo, os quais, ainda na tradição do *common law*, resultam nas chamadas *Responsibility*, *Accountability* e *Answerability*, cada uma trabalhando em uma camada do gênero "responsabilidade" de forma a transcender o conflito individual.

Responsibility é uma responsabilidade moral compartilhada socialmente, aceita voluntariamente sem imposição normativa e centrada no indivíduo. É a ideia de, com base na própria autonomia, escolher a ética como instrumento de modelação da vida para o passado, presente e futuro (ao contrário da *liability,* que permanece estanque no passado), direcionar o seu agir para o bem comum (ROSENVALD, 2021, p. 185). O provedor, dessa forma, deve inserir ética na utilização algorítmica, e o usuário, por sua vez, deve ter educação digital, de forma a fazer um uso responsável da internet para o exercício da cidadania.

Os princípios que sustentam esta ideia de *responsibility* na LGPD estão insculpidos no art. 2º, especificamente nos incisos I e II, consistentes na privacidade (em sua dimensão decisória para controle de seus atos) e a autodeterminação informativa (controlar a utilização e divulgação dos próprios dados). Trata-se de princípios inseridos para resguardar a pessoa, não enquanto proprietária dos dados, mas como tomadores de decisão num contexto informacional, em razão da prevalência do interesse existencial ao meramente patrimonial sobre esses dados.

Accountability, por sua vez, consoante explica Rosenvald, são deveres impostos perante outras pessoas, parâmetros regulatórios preventivos para a boa gestão e mitigação de danos. Num contexto de proteção de dados, torna-se essencial para impor obrigações aos desenvolvedores sobre a atuação do algoritmo e o seu impacto social. Atua em conjunto com a *liability*, regulando-a por uma governança de dados *ex ante* e *ex post* ao dano, conforme consta no art. 6º, inciso X, da LGPD. Na primeira, é um guia para o desenvolvedor, controlador e protagonistas de tratamento de dados atuarem de forma a mitigar os riscos, uma conformidade a parâmetros regulatórios preventivos, e se encontra na LGPD a partir do art. 50, quando da deliberação de normas de *compliance*, critérios preventivos e mitigadores de danos. A atuação *ex post*, por sua vez, servirá para trazer segurança jurídica às decisões judiciais, concedendo parâmetros aos magistrados para identificar os responsáveis e estabelecer remédios mais adequados ao caso concreto, uma vez que nem todo dano causado no âmbito do tratamento de dados configura uma responsabilidade objetiva (ROSENVALD, 2021, p. 188-189).

A *accountability* é importante para o estabelecimento de uma cultura de boas práticas. Ainda que condenados em razão de danos ocorridos em sua atividade, os juízes e a própria ANPD, percebendo a existência de normas de *compliance*, deverão realizar uma sanção premial, uma função promocional da responsabilidade civil, um estímulo a virtudes (SANKIEVICZ; PINHEIRO, 2021).

Por derradeiro, a *answerability* (explicabilidade), trata-se de um procedimento de justificação de escolhas, que vai muito além do "direito à informação", para que se possa aferir a expectativa depositada sobre cada participante da atividade, especialmente quanto à previsibilidade de eventuais consequências (BARBOSA, apud ROSENVALD, 2021, p. 197). Mais além, se houver risco elevado para direitos e liberdades das pessoas, o responsável pelo tratamento de dados deve realizar uma avaliação prévia dos impactos, de maneira que apenas devem ser chanceladas as inovações algorítmicas proporcionadoras de benefícios e em conformidade com um desenvolvimento sustentável (FREITAS; FREITAS, 2020, p. 66). Assim, por exemplo, a inteligência artificial, por praticar atos jurídicos na contemporaneidade, deve ser explicável, transparente, inteligível e motivada para que não se desvirtue a ética.

Fora a transparência, a *answerability* possibilita ao usuário o que se chama "*´ability to appeal',* ou seja, o titular dos dados tem direito a solicitar a revisão de decisões tomadas unicamente com base em tratamento automatizado de dados pessoais que afetem seus interesses, incluídas as decisões destinadas a definir o seu perfil" (ROSENVALD, 2021, p. 197). Na LGPD, verifica-se este aspecto da explicabilidade no art. 20, o qual faculta ao titular, prejudicado pela inteligência artificial, requerer uma revisão do ato por um humano (BRASIL, 2018). Na ausência de explicação, torna-se cabível a indenização, ou seja, a *liability* aparece em momento posterior. Trata-se de um meio de defesa do titular, que poderá ser utilizado de forma individual ou, preferencialmente, de forma coletiva. Caixas pretas não existem mais, e isso decorre da *answerability*, que impõe a transparência e a colocação da inteligência artificial em seu devido lugar de mera apoiadora, e não substitutiva do ser humano quando da tomada de decisões (PALESTRA..., 2021; ROSENVALD 2021, p. 199).

4. O TRATAMENTO DE DADOS E AS CONSEQUÊNCIAS DE SUA IRREGULARIDADE NAS VÁRIAS FASES DA RELAÇÃO DE TRABALHO

Chega-se ao ponto nodal da pesquisa, qual seja, "até que ponto a discricionariedade contemplada pelo poder diretivo confere liberdade ao empregador para recorrer a instrumentos de controle e monitoramento que não configuram violação da privacidade e da proteção de dados pessoais dos trabalhadores" (SANKIEVICZ; PINHEIRO, 2021, p. 509) e como isso deve ocorrer ao longo das diversas fases da relação de trabalho.

Desde antes da LGPD, a jurisprudência do Tribunal Superior do Trabalho (TST) já se inclinava para admitir o monitoramento como um apêndice do poder diretivo do empregador, desde que realizado de forma ponderada, necessária e, sobretudo, informada ao empregado, pres-

supondo-se tacitamente o seu aceite em razão do vínculo empregatício. Com a LGPD, essa jurisprudência há de ser revista, sobretudo no concernente ao consentimento esclarecido.

Primeiramente, é importante ressaltar, de forma pacífica, que a LGPD é aplicável às relações de trabalho, uma vez que se trata de norma protetiva e garantista de direito fundamental, de forma que sua incidência deve ser interpretada de maneira expansiva (art. 5º, § 2º, CF/88), e suas exceções, *a contrario sensu*, de forma taxativa, ao que se enterra com pá de cal por mera leitura do art. 4º da LGPD, que não prevê hipótese de não aplicação nas relações laborais.

Quando da aplicação da LGPD, é imperioso que se dê preferência à interpretação dos princípios contidos em seu art. 6º ao caso concreto, uma vez que a proteção de dados possui, por pano de fundo, a necessidade de regulamentação adequada acerca da convivência do titular com os recursos tecnológicos difundidos nos incontáveis setores sociais. Essa regulamentação deverá ocorrer, sobremaneira, no âmbito principiológico, associando-se esses princípios a tendências de longo prazo, uma vez que, para as instituições jurídicas, é impossível acompanhar a evolução tecnológica em mesma proporção e velocidade (RODOTÀ, 2008). *In verbis*:

> Art. 6º As atividades de tratamento de dados pessoais deverão observar a boa-fé e os seguintes princípios:
>
> I - finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular, sem possibilidade de tratamento posterior de forma incompatível com essas finalidades;
>
> II - adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento;
>
> III - necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados;
>
> IV - livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais;
>
> V - qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento;
>
> VI - transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial;
>
> VII - segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão;
>
> VIII - prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais;
>
> IX - não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos;
>
> X - responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas (BRASIL, 2018).

A primeira dificuldade para o tratamento de dados pessoais nas relações de trabalho reside na confusão entre os aparatos utilizados pelo empregado e disponibilizados pelo empregador para a execução dos serviços. As relações de trabalho foram impactadas pela tecnologia, a qual possibilita, dentre outros efeitos, a ampliação das técnicas de monitoração do empregador, algo que demanda cautela no proceder da atividade.

A monitoração encontrou justificativa no fato de que trabalhadores faziam uso abusivo de computadores, internet e *e-mail* funcionais, muitas vezes para fins pessoais em tempo excessivo e até mesmo para divulgação de pornografia infantil, de caráter racista, além de outros crimes, a ponto de causarem o comprometimento da imagem e/ou a responsabilização do empregador (RUARO, 2007, p. 230-233). Com sistemas de monitoramento, de outro lado, houve empregadores que abusaram na vigilância.

Um dos efeitos da modernização, destacado por Jimene (2019), foi o fenômeno do *bring your own device* (BYOD), no qual o empregado, conectado à nuvem e em posse de recursos tecnológicos próprios, exerce suas funções com os mesmos dispositivos utilizados para fins particulares ou pessoais. O desafio reside em como garantir a segurança da informação quando os equipamentos sequer estão em posse ou propriedade do empregador.

Para essa questão, utiliza-se da conteinerização, que consiste na criação de um "contêiner" dentro do equipamento particular do empregado, para armazenamento e gestão exclusiva das informações da empresa. A instalação desse *software* dependerá de consentimento do trabalhador e de uso restrito da aplicação às afirmações da empresa.

Quanto aos procedimentos específicos que deverão ser adotados ao longo do contrato de trabalho, destacam-se de início (no momento da contratação) até o fim (no momento da rescisão) e, consequentemente, do término do tratamento.

Os processos seletivos e tratamento de bancos de dados curriculares são a primeira preocupação do empregador quando do tratamento de dados na atividade laboral, porquanto envolve a coleta e processamento de dados de candidatos para eventual preenchimento de vagas na empresa.

Quando do tratamento de dados nessa etapa, embora autorizado por expressa hipótese carreada no art. 7º, V, da LGPD, deverá o empregador buscar o consentimento informado do empregado, esclarecendo-o e justificando qual a razão e necessidade dos dados requeridos no momento do processo de seleção, bem como dos exatos limites de sua finalidade para a vaga de emprego pretendida e como será feito o seu tratamento (SANKIEVICZ; PINHEIRO, 2021).

Tudo isso com vistas a atender aos princípios insculpidos no art. 6º da LGPD, devendo o empregador evitar, sempre que possível, a coleta de dados sensíveis ou desnecessários à ocasião, sendo-lhe, ainda, defesa a utilização dos dados para fins diversos daqueles informados quando da contratação, bem como vedadas quaisquer práticas discriminatórias com base nas informações coletadas, algo que, mesmo antes da LGPD, já vinha positivado pela Lei nº 9.029/1995.

Quando o tratamento dos dados coletados for realizado por intermédio de algoritmos, deverá ser o candidato igualmente informado de tal situação, cabendo-lhe, nesse caso, o direito de revisão por uma pessoa natural acaso se sinta prejudicado por eventual erro do sistema, conforme dispõe o art. 20 da LGPD.

REVISTA MERITUM • v.17 • n.3 • p. 284-299 • Set. - Dez. 2022

Quanto aos contratos de trabalho novos ou já vigentes, deverá o empregador promover uma devida alteração para a sistemática da LGPD. No tocante às cláusulas que disponham sobre o tratamento de dados, deverão ser dispostas de forma clara e destacada no contrato, permitindo ao empregado/titular o devido conhecimento de seu teor e dos seus direitos, de forma que não haja margem para dúvidas acerca do consentimento em sua disponibilização. Igualmente, justificativas acerca da necessidade dos dados solicitados, assim como as formas e limites de seu tratamento são pertinentes, de forma a sempre amparar o tratamento em mais de uma hipótese autorizante do art. 7º da LGPD (SANKIEVICZ; PINHEIRO, 2021).

No que se refere ao tratamento dos dados biométricos, é necessária especial ressalva nos contratos de trabalho, uma vez que se cuidam de dados considerados sensíveis pela legislação vigente (art. 5º, II, LGPD), impondo um consentimento ainda mais esclarecido e justificado de forma imprescindível em alguma das hipóteses do art. 11 da LGPD. A coleta de tais dados demanda, igualmente, o esclarecimento de suas finalidades e métodos de segurança empregados para o seu tratamento, os quais, dada a importância dos dados em si, envolverão maiores custos ao empregador.

É importante destacar que o tratamento de dados sensíveis é tutelado de forma geral pela LGPD, contudo, diante das simetrias entre essa lei e a GDPR (General Data Protection Regulation ou Regulamento Geral de Proteção de Dados, em português), nada impede que, por analogia, adote a empresa parâmetros indicados naquela legislação para a sua atividade (art. 9º, GDPR), os quais, dada a concreta preocupação daquela norma com os princípios da finalidade, necessidade e adequação, servem de norte para a devida e segura atuação da empresa. Assim, apenas se justifica o tratamento de dados biométricos em "empresas sujeitas à restrição de tráfego, bem como para controle de acesso a dispositivos e aplicativos de computação também considerados de acesso restrito pela empresa"; veda-se, por fim, que a autenticação biométrica seja fundada em amostragem biológica, limitando-se o tratamento apenas a um justificado método biométrico (SANKIEVICZ; PINHEIRO, 2021, p. 513).

No tocante à transferência para terceiros, deverá, necessariamente, ser comunicada ao titular e, quando não amparada nas demais hipóteses do art. 7º da LGPD, imprescinde de seu consentimento, uma vez que, em regra, os dados devem ser eliminados findo o tratamento (art. 15, LGPD). Permite-se, contudo, sua conservação para o cumprimento de obrigação legal ou regulatória, bem como a transferência a terceiros, desde que respeitadas as premissas da LGPD, dentre elas, em algumas hipóteses, a anonimização (art. 16, LGPD). Releva destacar que, a despeito da transferência independer de consentimento, ainda possui o trabalhador o direito de demandar informações sobre os seus dados pessoais, com espeque nos princípios do livre acesso e da transparência (SANKIEVICZ; PINHEIRO, 2021).

As relações de trabalho, complexas *per si*, devem ser reinterpretadas e reestruturadas com base no novo reconhecimento de um direito à proteção de dados pessoais, de forma a garantir o devido respeito à personalidade do trabalhador-titular num contexto de sociedade de informação, salvaguardando sua privacidade, sua autodeterminação informativa e demais direitos que desaguam em sua dignidade como pessoa humana.

Nessa senda, uma mudança na cultura de responsabilidade é necessária, para uma alternância da cultura de compensação de danos para uma cultura de prevenção e responsabilidade, algo que já se vê inserido nos dispositivos regulatórios da Lei Geral de Proteção de Dados. Cuida-se de norma de viés principiológico e de indispensável necessidade para a garantia da

personalidade, empoderando o titular para o exercício de seus direitos de forma consciente, elevando-o a protagonista e não mero anuente na tomada das decisões pertinentes aos seus dados pessoais.

Cabe, portanto, ao empregado se empoderar, e ao empregador observar os devidos princípios protetivos da atividade de tratamento de dados ao longo do contrato de trabalho, sob pena de, em não o fazendo, responder, na medida de sua culpabilidade, em todas as esferas de responsabilidade cabíveis ao caso.

5. CONSIDERAÇÕES FINAIS

Da análise procedida neste artigo, conclui-se que a tecnologia e o tratamento de dados configuram elementos intrínsecos da contemporaneidade e de particular incidência nas relações de trabalho, de forma que o devido reconhecimento e respeito a um direito de proteção de dados pessoais se mostra imprescindível para a proteção da pessoa humana em sua dignidade e personalidade. O estudo da tutela jurídica da proteção dos dados pessoais do trabalhador na sociedade de informação permitiu desvendar como o ordenamento jurídico responde às especiais necessidades imprescindíveis na contemporaneidade.

Após revisão bibliográfica e documental, chegou-se à conclusão de que o desenvolvimento das tecnologias de informação e comunicação na modernidade interligou o globo e ampliou as relações de monitoramento e controle incidentes sobre a pessoa humana. A onipresença tecnológica, nos vários ramos da vida, é algo inevitável, restando, então, a necessidade da previsão de mecanismos de salvaguarda da pessoa humana em sua dignidade e personalidade, algo que se faz, necessariamente, pelo reconhecimento de um direito à proteção de dados pessoais.

O reconhecimento desse direito, de natureza humana, fundamental e da personalidade, influencia a ordem mundial e, em âmbito interno, as direções do Estado brasileiro para a salvaguarda da dignidade da pessoa humana, com seus desdobramentos na privacidade e autodeterminação informativa, algo que, pelo que se observa dos dispositivos da LGPD, caminha em um sentido de mudança da atual cultura de responsabilidade, principalmente no que toca à responsabilidade civil, que deve se adaptar a um contexto tecnológico.

Quanto às várias fases da relação de trabalho em si, verificou-se como a LGPD, por meio de preceitos principiológicos, cuidou de reestruturar todos os pontos da relação jurídica de maneira a assegurar também o empoderamento do empregado-titular no tocante ao seu protagonismo quanto às decisões existenciais sobre os seus dados pessoais, de forma que resta ao empregador a reformulação de antigos modelos despreocupados com o empregado para práticas benéficas e pautadas em uma proteção da dignidade do trabalhador, sob pena de, em não o fazendo, responder nas diversas formas de responsabilidade decorrentes da irregularidade no tratamento de dados pessoais.

REVISTA MERITUM • v.17 • n.3 • p. 284-299 • Set. - Dez. 2022

REFERÊNCIAS

BARRETO, Ana Amelia Menna. A proteção de dados pessoais no Brasil. *In:* LIMA, Ana Paula M. Canto de; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes (Org.). **Direito digital:** debates contemporâneos. São Paulo: Revista dos Tribunais, 2019.

BRASIL [Constituição (1988)]. **Constituição da República Federativa do Brasil de 1988.** Brasília, DF: Presidência da República, [2020]. Disponível em: http://www.planalto.gov.br/ccivil_03/Constituicao/Constituicao.htm. Acesso em: 20 out. 2021.

BRASIL. **Lei nº 13.709, de 14 de agosto de 2018.** Lei Geral de Proteção de Dados (LGPD). Brasília, DF: Presidência da República, [2019]. Disponível em:

http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/L13709.htm. Acesso em: 20 out. 2021.

CANTALI, Fernanda Borghetti. **Direitos da Personalidade:** disponibilidade relativa, autonomia privada e dignidade humana. Porto Alegre: Livraria do Advogado, 2009.

CASTELLS, Manuel. **A sociedade em rede**. Tradução: Roneide Venancio Majer. 22. ed. São Paulo: Paz e Terra, 2020.

DONEDA, Danilo. Panorama histórico da proteção de dados pessoais. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang. RODRIGUES JÚNIOR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021. p. 03-20.

FACHIN, Zulmar; FACHIN, Jéssica. Direitos Humanos em Norberto Bobbio: a trajetória de uma utopia em busca de concretização. **Revista Jurídica Unicuritiba.** Curitiba, v. 03, n. 60, p. 107-125, jul./set. 2020. Disponível em: http://revista.unicuritiba.edu.br/index.php/RevJur/article/view/4174. Acesso em: 30 nov. 2021.

FREITAS, Juarez; FREITAS, Thomas Bellini. **Direito e inteligência artificial:** em defesa do humano. Belo Horizonte: Fórum, 2020.

HARVEY, David. **A condição pós-moderna.** São Paulo: Loyola, 1993.

JIMENE, Camilla do Vale. Impactos da tecnologia nas relações de trabalho. *In:* LIMA, Ana Paula M. Canto de; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes (Org.). **Direito digital:** debates contemporâneos. São Paulo: Revista dos Tribunais, 2019. p. 107-116.

LEHFELD, Lucas de Souza *et al*. A (hiper)vulnerabilidade do consumidor no ciberespaço e as perspectivas da LGPD. **Revista Eletrônica Pesquiseduca**, Santos, v. 13, n. 29, p. 236-255, jan./abr. 2021. Disponível em: https://periodicos.unisantos.br/pesquiseduca/article/view/1029/902. Acesso em: 20 out. 2021.

LISBOA, Roberto Senise. Direito na sociedade da informação. **Revista dos Tribunais**, São Paulo, v. 95, n. 847, p. 7 8-95, 2006.

MENDES, Laura Schertel; RODRIGUES JÚNIOR, Otavio Luiz; FONSECA, Gabriel Campos Soares da. O Supremo Tribunal Federal e a Proteção Constitucional dos Dados Pessoais: rumo a um direito fundamental autônomo. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz.

Tratado de Proteção de Dados Pessoais, Rio de Janeiro: Forense, 2021. p. 61-71.

PEREZ-ZUNIGA, Ricardo *et al*. La sociedad del conocimiento y la sociedad de la información como la piedra angular en la innovación tecnológica educativa. **RIDE – Revista Iberoamericana para la Investigación y el Desarrollo Educativo**, Zapopan, v. 8, n. 16, p. 847-870, ene./jun. 2018. Disponível em:

https://www.ride.org.mx/index.php/RIDE/article/view/371/1683. Acesso em: 20 out. 2021.

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

PALESTRA Prof Rosenvald 2021 09 23 at 04 08 GMT 7. *[S.l: s.n.],* 23 set. 2021. 1 vídeo (65 min). Publicado pelo canal Cleber OT. Disponível em: https://www.youtube.com/watch?v=7WclcyT_nIk. Acesso em: 20 out. 2021.

ROSENVALD, Nelson. Conceitos de responsabilidade civil para a 4ª Revolução Industrial e o capitalismo de vigilância. *In:* EHRHARDT JÚNIOR, Marcos (coord.). **Direito Civil:** Futuros Possíveis. Belo Horizonte: Fórum, 2021. p. 175-205.

ROSSINI, Augusto. **Informática, Telemática e Direito Penal.** São Paulo: Memória Jurídica, 2004.

RUARO, Regina Linden. O conteúdo essencial dos direitos fundamentais à intimidade e à vida privada na relação de emprego: o monitoramento do correio eletrônico pelo empregador. *In:* SARLET, Ingo Wolfgang (Org.). **Direitos fundamentais, informática e comunicação:** algumas aproximações. Porto Alegre: Livraria do Advogado, 2007. p. 227-252.

SANKIEVICZ, Alexandre; PINHEIRO, Guilherme Pereira. Aspectos da proteção de dados nas relações de trabalho. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, p. 507-522.

SARLET, Ingo Wolfgang. **Dignidade (da Pessoa) Humana e Direitos Fundamentais na Constituição Federal de 1988.** 10. ed. Porto Alegre: Livraria do Advogado, 2015.

SARLET, Ingo Wolfgang. Fundamentos Constitucionais: o direito fundamental à proteção de dados. *In:* MENDES, Laura Schertel; DONEDA, Danilo; SARLET, Ingo Wolfgang; RODRIGUES JÚNIOR, Otavio Luiz. **Tratado de Proteção de Dados Pessoais.** Rio de Janeiro: Forense, 2021, p. 21-59.

SZANIAWSKI, Elimar. **Direitos de personalidade e sua tutela.** 2. ed. São Paulo: Revista dos Tribunais, 2005.

UNITED NATIONS. **Report of the Special Rapport eur on the promotion and protection of the right to freedom of opinion and expression, Frank La Rue.** 2011. Disponível em:

https://www2.ohchr.org/english/bodies/hrcouncil/docs/17session/A.HRC.17.27_en.pdf. Acesso em: 20 out. 2021.

WEISER, Mark. The computer for the 21st Century. **Scientific American**, New York, v. 265, n. 3, p. 94-104, sept. 1991. Disponível em: https://www.lri.fr/~mbl/Stanford/CS477/papers/Weiser-SciAm.pdf. Acesso em: 30 nov. 2021.

WIMMER, Miriam. Inteligência artificial, algoritmos e o direito: um panorama dos principais desafios. *In:* LIMA, Ana Paula M. Canto de; HISSA, Carmina Bezerra; SALDANHA, Paloma Mendes (Org.). **Direito digital:** debates contemporâneos. São Paulo: Revista dos Tribunais, 2019. p. 15-30.

ZUBOFF, Shoshana. **A era do capitalismo de vigilância:** a luta por um futuro humano na nova fronteira do poder. Tradução: George Schlesinger. Rio de Janeiro: Intrínseca, 2020.

Dados do processo editorial

• Recebido em: 02/12/2021

• Controle preliminar e verificação de plágio: 04/12/2021

• Avaliação 1: 05/01/2022

• Avaliação 2: 23/10/2022

• Decisão editorial preliminar: 23/10/2022

• Retorno rodada de correções: 31/10/2022

• Decisão editorial/aprovado: 28/11/2022

Equipe editorial envolvida

• Editor-chefe: 1 (SHZF)

• Editor-assistente: 1 (ASR)

• Revisores: 2