

PUBLICAÇÃO

93

ISSN: 0101-9562

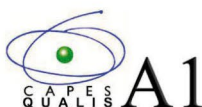
ISSN ELETRÔNICO: 2177-7055

SEQÜÊNCIA

Publicação do
Programa de Pós-Graduação
em Direito da UFSC

VOLUME 44 ■ ANO 2023

Estudos
jurídicos
e políticos



SEQUÊNCIA – ESTUDOS JURÍDICOS E POLÍTICOS é uma publicação temática e de periodicidade quadrimestral, editada pelo Programa de Pós-Graduação Stricto Sensu em Direito da Universidade Federal de Santa Catarina – UFSC.

SEQUÊNCIA – ESTUDOS JURÍDICOS E POLÍTICOS is a thematic publication, printed every four months, edited by the Program in law of the Federal University of Santa Catarina – UFSC.

Versão eletrônica: <http://www.periodicos.ufsc.br/index.php/sequencia>

Editora-Chefe: Norma Sueli Padilha

Editor Associado: José Sérgio da Silva Cristóvam

Editores Adjuntos: Priscilla Camargo Santos, Thanderson Pereira de Sousa

A publicação é indexada nas seguintes bases de dados e diretórios/
The Publication is indexed in the following databases and directories:

Base OJS	OJS
Base PKP	PKP
CCN (Catálogo Coletivo Nacional)	Portal de Periódicos UFSC
Dialnet	Portal do SEER
DOAJ (Directory of Open Access Journals)	ProQuest
EBSCOhost	SciELO
Genamics Journalseek	Sherpa/Romeo
ICAP (Indexação Compartilhada de Artigos de Periódicos)	Sumarios.org
Latindex	ULRICH'S
LivRe!	vLex

Ficha catalográfica

Seqüência: Estudos jurídicos e políticos. Universidade Federal de Santa Catarina. Programa de Pós-Graduação em Direito. n.1 (janeiro 1980)-.

Florianópolis: Fundação José Boiteux. 1980-.

Publicação contínua

Resumo em português e inglês


Versão impressa ISSN 0101-9562

Versão on-line ISSN 2177-7055

1. Ciência jurídica. 2. Teoria política. 3. Filosofia do direito. 4. Periódicos. I. Universidade Federal de Santa Catarina. Programa de Pós-graduação em Direito

CDU 34(05)

Catálogo na fonte por: João Oscar do Espírito Santo CRB 14/849

PUBLICAÇÃO		SEQÜÊNCIA	Estudos jurídicos e políticos

Aspectos gerais e trabalhistas sobre a proteção cooperada-integrada de dados pessoais

General and labor aspects on cooperated-integrated protection of personal data

Lucas Reckziegel Weschenfelder¹

Luiz Gonzaga Silva Adolfo¹

¹Universidade de Santa Cruz do Sul, Santa Cruz do Sul, Brasil.

RESUMO: Estuda-se a proteção de dados pessoais nas relações sociotrabalhistas, com uma abordagem jusfundamental. Segue-se, na primeira etapa, por uma perspectiva da filosofia da tecnologia. Adianta-se uma visão tradicional e contemporânea relativamente ao tema, traçando-se os aspectos jurídico-normativos de uma proteção cooperada-integrada de dados pessoais. Na segunda seção, apresenta-se uma análise normativa vinculada aos dados pessoais ordinários e sensíveis nas relações de trabalho, indicando padrões jurídico-semânticos atrelados às partes, empregado e empregador. Indica-se, ao fim, com a hipótese de que os dados pessoais reivindicam uma proteção cooperada-integrada, particularmente nas relações juslaborais, um necessário exercício coordenado pelos atores que se inserem nesse cenário, não apenas individual, ou como incumbência exclusiva do Estado. Metodologicamente, utiliza-se da hermenêutica, partindo-se de premissas que se consubstanciam no problema. Em procedimento, emprega-se o monográfico, e a técnica de pesquisa, a bibliográfica.

PALAVRAS-CHAVE: Dados pessoais. Direitos Fundamentais Trabalhistas. Proteção cooperada-integrada. Relações de trabalho.

ABSTRACT: The protection of personal data in socio-labor relations is studied, with a jusfundamental approach. In the first section, the topic is approached from a philosophy of technology perspective. A traditional and contemporary view on the subject is advanced, outlining the legal-normative aspects of a cooperative-integrated protection of personal data. The second section presents a normative



analysis linked to ordinary and sensitive personal data in labor relations, indicating legal-semantic standards linked to the parties, employee and employer. Finally, with the hypothesis that personal data claim a cooperative-integrated protection, particularly in work relations, it is indicated a necessary, coordinated exercise by the actors who are part in this scenario, not only individually, or as an exclusive responsibility of the State. Methodologically, it is based on hermeneutics, starting from premises that embody the problem. In procedure, the monographic, and the research technique, the bibliographic.

KEYWORDS: Personal Data. Fundamental Rights at Work. Cooperative-integrated protection. Labor Relations.

1 CONSIDERAÇÕES INICIAIS

Não é novidade que as sociedades contemporâneas estão expostas a riscos nunca antes tão aproximados ao hodierno da vida. Apesar de tal constatação, os riscos que se apresentam à sociedade e aos sujeitos individualmente considerados, que a compõem, como também aos entes coletivizados erigidos por eles, retiram de suas visões uma perspectiva com conteúdos de segurança e de certeza(s). A certeza e a segurança passaram a ser um ideal, uma ficção, um chão sólido para se pisar em meio a um terreno pantanoso, em que, parafraseando Carl Sagan, lembra-se uma vela acesa na escuridão.

Trata-se, em verdade, de um paradoxo ordenado pela neo-metafísica: a complexidade. Sabe-se que, a humanidade, está sendo impactada por “realidades” multifatoriais e perigosas, pois, em sua empiria, o ser humano tem sido atingido, de um modo, ou de outro. Tais realidades, contudo, não são visíveis em sua totalidade, nem nas tentativas mais sofisticadas de reflexividade ou prospecção: as certezas/verdades, e o afã pela segurança, exurgem nesse cenário de contínua parcialidade, de inexistência de causas e efeitos observáveis a olho “nu”, de incertezas regionais, nacionais e globais.

O Direito, que se insere nesse cenário como um sistema social, tende para segurança, previsibilidade e coerência. Isso acontece não

apenas em sua linguagem científica, na dogmática jurídica, mas, sim, enquanto instituto modelo-social humano, complexo, que trata das expectativas cognitivo-normativas, e coordena as ações humanas, caminhando e se encontrando com outros subsistemas, tais como o do Poder, o da Economia e, no caso a ser debatido, com o da Tecnologia.

O presente texto seguirá nesta toada, pois questiona-se se a tutela dos dados pessoais nas relações de trabalho é adequada, pensando-se este direito enquanto unicamente de personalidade dos trabalhadores. Divide-se a construção do conteúdo em duas etapas, as quais se interconectarão, iniciando-se, na primeira, com uma abordagem sobre a necessidade de uma proteção cooperada-integrada dos dados pessoais, elucidando propostas tradicionais, e os novos formatos, sem exaustão, sobre a temática. A segunda parte focalizará em aspectos trabalhistas da proteção de dados pessoais, uma vez entendido como pressuposto que, as relações juslaborais serão impactadas (já o são) intensamente pelos regulamentos nacionais e internacionais sobre a matéria, com a pretensão de apontar problemáticas intersubjetivas, interpessoais e institucionais, as quais, novamente, não possuirão ares de exaustividade, mas, tão somente, serão um acréscimo pontual à discussão tão rica e complexa que já está iniciada por tantos outros, e que continuará frutífera nos próximos anos.

Emprega-se a metodologia hermenêutica, organizando-se o texto a partir de premissas que se consubstanciam no problema, perseguindo-se a hipótese ao estudar o que se crê essencial para a delimitação do objeto do conhecimento. Como método de procedimento, emprega-se o monográfico, o qual servirá de critérios na e para a ação de construção do conteúdo estudado, estremando-se os conteúdos da pesquisa, e possibilitando um estudo agudizado sobre os aspectos necessários para a explanação do trabalho. A técnica de pesquisa utilizada é a bibliográfica, levantando-se pesquisas nacionais e internacionais que se tem como primordiais na área.

O presente trabalho foi realizado com apoio da PUCRS através do Programa de Excelência Acadêmica – PROEX – CAPES.

2 APONTAMENTOS SOBRE A NECESSÁRIA PROTEÇÃO COOPERADA-INTEGRADA DOS DADOS PESSOAIS

2.1 Filosofia da tecnologia e a digitalização

Nos estudos voltados à Filosofia da Tecnologia, especialmente aqueles derivados da escola Crítica, tem-se uma máxima que norteia, de forma implícita ou explícita, todas as especulações sobre a matéria que se pretendam lúcidas: o desenvolvimento tecnológico dos últimos duzentos anos é, em geral, unilateralmente imposto pelo sistema econômico, cujos conteúdos refletem decisões tomadas a par do sistema político e jurídico da sociedade. Há, portanto, um caráter extremamente antidemocrático no desenvolvimento tecnológico e, por causa disso, se tem que, as pessoas, nesse cenário, são impactadas em suas vidas, em seus “seres”, por decisões promovedoras de desenvolvimento de instrumentos tecnológicos (de toda sorte), cujo resultado, de um todo, é a moldura dos contextos sociais, econômicos, ambientais, políticos e jurídicos da sociedade, revelando-se, entretanto, como obscuras, não visualizadas comumente.

Não se adentrando em aspectos teóricos aprofundados, entende-se que, o desenvolvimento tecnológico é um processo coordenado de decisões. Há, contudo, dificuldades em se observar esse processo como condicionado socialmente por escolhas. Isso se dá, primordialmente, devido ao nível de sociabilidade tradicionalmente posto em relação à tecnologia. É verdade que, a tecnologia não possui características de sociabilidade tão abertas como o Direito e a Economia, por exemplo. Essa dificuldade, todavia, não deixa de mostrar, em muitas circunstâncias, como a tecnologia é condicionada e influenciada por projetos de mudanças com caráter democrático e progressivo, cujo forte é a manutenção de uma fenda de acessibilidade para o mundo social racionalizado. Basta observar os movimentos contra a poluição, de tecnologias assistivas para pessoas com deficiência e, no ponto, a proteção de dados pessoais.

Em resumo, a identificação da racionalidade social na tecnologia é muito complexa e dificultosa, devido, rigorosamente, à antecipação histórica colocada como um *a priori* legítimo do processo tecnocrático da modernidade. Feenberg (2017) defende que, a ideologia das primeiras versões do livre mercado até a presente legitimação das sociedades tecnocráticas avançadas, obstaculizam e fomentam a dificuldade de um desenvolvimento crítico da tecnologia. Nas palavras do autor (2017, p. 316), “é muito mais difícil identificar e criticar o enviesamento formal dos artefatos e instituições socialmente racionais do que legitimações míticas e tradicionais herdadas”.

Com isso em mente, segue-se ao tema notado nessa linha teórica, e retomando-se o discurso jurídico. Em um primeiro momento, questiona-se: o que são os dados pessoais nessa perspectiva tecnológica? Os dados pessoais “digitais” são tecnologias que se originaram com o desenvolvimento da ciência da computação e da Internet, as quais, também, são tecnologias, e chegaram a um patamar imprevisto, considerando-se o primeiro projeto de rede doméstica em grande escala, no início dos anos 1980, na França, intitulado de Plano Minitel.

O avanço de tais tecnologias é tanto que se formaram disciplinas interconectadas, denominadas em uma tríade – Internet Das Coisas, *Big Data* e Inteligência Artificial –, as quais já estão transformando a sociedade, e prometem, nos próximos anos, formatar inúmeras novas “realidades”. As questões, pois, que nos aproximam humanamente de tais tecnologias são variadas, embora o cerne esteja, justamente, nos dados pessoais “digitais”. Os dados pessoais são a fonte de inteligência e de operacionalização de todas essas tecnologias que já estão em funcionamento em muitas esferas, tais como da saúde, do mercado, profissionais, pessoais, políticas, consumeristas, educacionais e, por claro, trabalhistas.

O Direito é reivindicado para atuar, mas, antes do agir jurídico, impõe-se uma pergunta: “qual o papel do Direito e qual a sua capacidade de regular este mundo cada vez mais invisivelmente técnico” (BRANCO, 2019, p. 13)? O ponto de partida, nesse sentido, vem sendo

estabelecido da seguinte forma: o mote normativo protetivo dos dados pessoais deve sempre prevalecer como um *a priori* condicionador de toda atuação de guarda, processamento, e instrumentalização dos dados para os mais variados fins. Proteger os dados pessoais representa defender e proteger a pessoa, ou seja, deve-se adequar a um direito fundamental a proteção dos dados pessoais, com as suas dimensões objetiva e subjetiva, aplicando-se isso aos andares de processamento e ações de Inteligência Artificial automatizadas, ou não automatizadas, porque

A proteção de dados pessoais é uma maneira indireta de atingir um objetivo último, que é a proteção da pessoa. Ao estabelecer um regime de obrigações para os responsáveis pelo tratamento de dados, bem como de direitos para os titulares destes, não se está meramente regulando um objeto externo à pessoa, porém uma representação da própria pessoa. Os dados pessoais, por definição, representam algum atributo de uma pessoa identificada ou identificável e, portanto, mantém uma ligação concreta e viva com a pessoa titular destes dados. Os dados pessoais são a pessoa e, portanto, como tal devem ser tratados, justificando o recurso ao instrumental jurídico destinado à tutela da pessoa e afastando a utilização de um regime de livre apropriação e disposição contratual destes dados que não leve em conta seu caráter personalíssimo. Também destas suas características deriva a consideração que, hoje, diversos ordenamentos jurídicos realizam, de que a proteção de dados pessoais é um direito fundamental – uma verdadeira chave para efetivar a liberdade da pessoa nos meandros da Sociedade da Informação (BRASIL, 2010, p. 39).

Exatamente devido a esse caráter humano dos dados, e ao próprio formato obnubilado das tecnologias que se desenvolvem com base neles, é que se deve pensar em conjunturas normativas adequadas à tutela dos dados pessoais. A Constituição de 1988 passou a reconhecer, com a Emenda Constitucional nº 115, de 2022, a jusfundamentalidade do direito à proteção dos dados pessoais, “inclusive nos meios digitais”.

Dito reconhecimento, no capítulo I, Dos Direitos e Deveres Individuais e Coletivos, no Título II, Dos Direitos e Garantias Fundamentais, simboliza em muito o que já se fez, e condicionará, normativamente, o que se está por fazer.¹

2.2 Dados pessoais, informação e a sua tradicional-e-atual orientação normativa-protetiva

Antes de dispor, sucintamente, sobre a necessidade cooperada-integrada da proteção aos dados pessoais, é relevante explicitar que tais dados pessoais possuem algumas características conceituais que devem ser colocadas, de maneira preparatória, para adentrar na própria matéria dos dados pessoais e, em avanço, distingui-los do que se compreende sobre informação.

Os dados pessoais são todos aqueles que podem identificar uma pessoa, tais como números, características pessoais, qualificação pessoal, dados genéticos. Por outro lado, os dados pessoais sensíveis são informações que podem ser empregadas discriminatoriamente. Eles reclamam uma tutela especial, dirigida a dados sobre origem racial ou étnica, convicções religiosas, filiação a sindicatos ou outras associações de caráter político, religioso ou filosófico, sobre saúde ou vida sexual, dados genéticos e biométricos (MAGRANI, 2019). Essa diferença é importante devido ao “espaço e tempo” da normatização protetiva e ao que se compreende por informação.

O “dado” e a “informação” contêm conteúdos e tempos distintos, embora empregados, em vezes, indistintamente. Ambos se lançam

¹ Registra-se duas observações. Tramita o Projeto de Lei (PL) nº 21/2020 no Congresso Nacional, cuja ementa remete: “Estabelece fundamentos, princípios e diretrizes para o desenvolvimento e a aplicação da inteligência artificial no Brasil; e dá outras providências. Demais, já se encontra em andamento a Estratégia Brasileira de Inteligência Artificial – EBIA. Ambas as iniciativas merecem um olhar mais atento da sociedade, dadas as omissões existentes no PL e na EBIA. Impossível olvidar o tratamento constitucional sobre a matéria, nos arts. 218 a 219-B.

sobre o processo de origem, processamento e instrumentalização dos dados, porém, cada qual possui sua importância e característica próprias. O dado se apresenta como uma forma mais primitiva e fragmentada do que a informação; é, em realidade, uma informação em estado potencial, antes de ser transmitida, associado a uma espécie de “pré-informação”, que antecede a interpretação e um procedimento de estruturação. A informação, em seu turno, corresponde a algo além da representação percebível no dado, “chegando ao limiar da cognição [...] na informação já se pressupõe uma fase inicial de depuração de seu conteúdo – daí que a informação carrega um sentido instrumental, no sentido da redução de um estado de incerteza” (DONEDA, 2011, p. 94).

Nesses termos, fica claro que, o tratamento de “dados pessoais”, e de “informação pessoal”, remete, necessariamente, à proteção da privacidade. Isso não será explorado profundamente, contudo registra-se que, o âmbito normativo dos dados pessoais é muito mais complexo e amplo, e não se refere, obrigatoriamente, a uma congruência normativa voltada à privacidade individual-subjetiva, mas, sim, à proteção objetiva, enquanto espaço global de garantias das liberdades públicas e de atuação individual ou coletiva. Ademais, são com esses termos normativos, advindos das doutrinas constitucionais dos direitos fundamentais, que se superam, em locuções jurídicas, o “*nothing to hide argument*”, a falácia “*all-or-nothing*”, e “*why privacy isn’t merely an individual right*” (SOLOVE, 2011), uma vez que, o proposto é estabelecer uma colmatação de estruturas e instrumentalizações de prevenção e reforço mediante o Direito, às liberdades fundamentais e à igualdade dos e entre os cidadãos, em busca de uma sociedade livre, justa e solidária.

Snowden (2015), o analista de sistemas que tornou público os avanços com características de vigilância da agência dos Estados Unidos, a NSA, inclusive conduzindo acessos sobre autoridades públicas de outros Estados soberanos, como, a saber, em face da ex-presidente do Brasil, Dilma Rousseff, e da chanceler alemã, Angela Merkel, expõe:

people who say they don't care about privacy because they have got nothing to hide have not thought too deeply about these issues. What they are really saying is I do not care about this right. When you say I don't care about the right to privacy because I have nothing to hide, that is no different than saying I don't care about freedom of speech because I have nothing to say or freedom of press because I have nothing to write.²

Assentando-se as premissas sobre a relevância de se proteger os dados pessoais, estatuindo-se a fundamentalidade de se ter o direito à proteção de tais bens, mostra-se complexa a tarefa que se manifesta à sociedade. Os dados pessoais possuem formas e conteúdos distintos, os quais requerem, por conseguinte, tutelas consentâneas às suas especificidades e, ademais, moldadas a cada etapa procedimental que um dado pessoal possa atravessar, até chegar-se à instrumentalização via Inteligência Artificial/Big Data, por exemplo. Para se ter um satisfatório “organograma” normativo, faz-se necessário o estabelecimento de leis e/ou de políticas públicas abertas à cooperação-integrada entre Estado, Sociedade e Mercado, uma vez que

a proibição geral de processamento da informação relativa à pessoa se sustenta no pressuposto de que o processamento automático de dados traz em si um sério risco para a sociedade que se baseia nos direitos fundamentais do indivíduo. Como foi ressaltado pela Corte Constitucional alemã, indivíduos que não sabem quem processa seus dados, quais os dados processados, para que finalidade e em que condições, inevitavelmente, tenderão a renunciar a seu poder de livremente expressar

² Disponível em: <https://www.theguardian.com/us-news/2015/may/22/edward-snowden-nsa-reform>. Tradução livre: as pessoas que dizem que não se importam com a privacidade porque não possuem nada a esconder não se detiveram profundamente sobre esse tema. O que elas realmente estão falando é isto: “eu não me importo com esse direito”. Quando alguém diz que não se importa com o direito à privacidade/dados pessoais porque não tem nada a esconder, não é diferente de dizer que não se importa com o direito à liberdade de expressão porque não tem nada a dizer, ou à liberdade de imprensa porque não tem nada a escrever.

suas opiniões, de demonstrar simpatia ou se juntar a partido político, sindicato ou qualquer associação para se adaptar às potenciais expectativas da entidade processadora. A adaptação antecipatória irá, assim, substituir gradualmente, todas as tentativas de participação crítica e, com o tempo, erodir o próprio fundamento da sociedade democrática. Nessas condições, não só o exercício dos direitos fundamentais pela própria pessoa fica visivelmente prejudicado, como também a construção do espaço público na sociedade democrática. Existe, pois, uma interconexão entre a deliberada restrição ao acesso de dados pessoais e a liberdade individual que justifica o estabelecimento desse limite (SANDEN, 2014, p. 73-74).

É sabido que, no Brasil, não se tem uma tradição regulatória preocupada com a proteção de dados pessoais, no sentido que se afigura neste trabalho e nos diálogos acadêmicos atuais e regramentos legais. Somente em 2012, com o PL nº 4.060, é que aparece, no Congresso Nacional, uma proposta acuradamente voltada à proteção dos dados pessoais. Embora apenas em 2018 tenha-se vista de uma legislação específica sobre o tema, a saber, a Lei Geral de Proteção de Dados Pessoais (LGPD nº 13.709 de 2018, inclui-se o Decreto nº 10.046/2019), a legislação que inaugurou uma regulação sobre os dados pessoais e a Internet, é de 2014, denominada de Marco Civil da Internet, em que a proteção dos dados pessoais é estabelecida como princípio (art. 3º, III, da Lei 12.965/2014). Não se está dizendo, com isso, que, os dados pessoais e a privacidade *lato sensu*, enquanto direitos de personalidade, não estavam tutelados normativamente pela Constituição, Código Civil, Código de Defesa do Consumidor e C.L.T, entre outras legislações, mas, sim, que não havia, no arcabouço legislativo nacional, regras e princípios adequados à conjunção técnica necessária a tais assuntos, diferentemente da tradição europeia, por exemplo.

É na tradição legislativa de além-mar que se pode observar, historicamente, quatro tipos de leis que se preocupa(m)ram com a proteção dos dados pessoais. Em rápida síntese, é possível afirmar-se que, a primeira geração de leis cuidou de uma dinâmica meramente

computacional, centralizada, de aferição e gestão de dados com um controle *a posteriori* pelos órgãos públicos, mostrando, também, que, no seu horizonte normativo, estava, essencialmente, o Estado e a Administração Pública. Estão enquadradas nessa geração a lei do Land Alemão de Hessen (1970), a lei de dados da Suécia (1973), a Lei federal de proteção de dados da Alemanha (1977), o *fair credit reporting act* dos EUA (1974) e, sem exaurir a lista, em um escopo Constitucional, a Carta Portuguesa (1976), expressamente, em seu art. 35.

Já na segunda geração de leis, há um avanço na percepção do amplo leque de possibilidades existentes de obtenção e usos de dados pessoais, além de uma visão meramente preocupada com o Estado ou com os “desenvolvimentos computacionais”, dando-se ênfase à própria noção de privacidade e de liberdade a ser exercida pelo cidadão enquanto direito em uma esfera tecnológica altamente descentralizada. Vê-se essa noção na Lei Francesa de 1978, a *Informatique et Libertés*.

Na terceira onda de leis, observa-se uma normatização sofisticada dos dados pessoais, centrada no cidadão e, somando-se a isso, com o estabelecimento de garantias de efetividade para as liberdades enquanto direito de exercício de proteção dos dados pessoais. “A proteção de dados é vista, por tais leis, como um processo mais complexo, que envolve a própria participação do indivíduo na sociedade” e leva em consideração a sua circunstância social e pessoal, na qual lhe são solicitados os seus dados, proporcionando meios de atuação em ocasiões tais em que sua decisão poderia estar cerceada por motivos outros que retirariam, sem tais garantias protetivas, a sua liberdade de escolha (CUEVA, 2016).

Embora as leis de terceira geração possam ser enquadradas como leis “aperfeiçoadas”, havia uma diligência procedimental acarretadora de exclusão de grande parte dos cidadãos no acompanhamento do tratamento de seus dados, uma vez que, o processo era formatado no tempo, em inúmeras etapas, resultando, portanto, em fases complexas e custosas, prejudicando a denominada autodeterminação informativa.

Visando a uma ampliação da proteção de dados a todos, a quarta geração de leis caracteriza-se por superar uma perspectiva normativa

que traduz, no individual, a possibilidade de resguardo de direitos. Essas novas legislações possuem como intuito trazer à sociedade e aos cidadãos estruturas objetivas que lhes garantam a sua liberdade de atuação em moldes multifacetários, reconhecendo-se um desequilíbrio relacional entre as entidades, públicas e privadas, que coletam e processam dados, e as pessoas. Cria-se, pois, uma normatividade complexa que supera a mera individualidade autônoma do consentimento e da fiscalização individualizada, como, também, de uma locução restrita da privacidade. Ademais, constitui-se, em todos os corpos legais sérios, e intencionados em proteger as pessoas e o próprio sistema democrático, os modelos de autoridades públicas independentes, regulações temáticas e especiais a cada formato de dados pessoais, sensíveis ou não pessoais, de que se tem como origem normativa os textos e normas das Diretivas europeias 95/46/CE e 2000/58/CE (DONEDA, 2011).

A despeito da impossibilidade de se adentrar em outros aspectos históricos que exsurtem como relevantes para a caracterização do estado da arte da proteção de dados, observa-se que, a proteção integrada-cooperada é vislumbrada desde a década de 1960 e 1970 e, precisamente, os seus princípios normativos atuais são reconhecidos em um estudo de 1973, da *Secretary for health, education and welfare*, nos Estados Unidos. Os citados princípios formam um arcabouço procedimental e material de garantias, de indícios semânticos para a formatação normativa de resguardo dos dados pessoais, os quais, inclusive, podem ser visualizados na novel Lei Geral de Proteção de Dados Pessoais (vigência para 2021, art. 6º), no Regulamento Geral sobre Proteção de Dados na União Europeia (2018) e, remotamente, na Convenção de Strasbourg (1981), como, inclusive, em *Guidelines* da OCDE e da OIT, dentre outras normativas oriundas de organizações internacionais. Esses princípios, também denominados, enquanto conjunto de normas deontológicas, de *Fair Information Practice Principles*,³ podem ser qualificados da seguinte forma:

³ The International Association of Privacy Professional. Disponível em: <https://iapp.org/resources/article/fair-information-practices/>.

Princípio da publicidade (ou da transparência), pelo qual a existência de um banco de dados com dados pessoais deve ser de conhecimento público, seja por meio da exigência de autorização prévia para funcionar, da notificação a uma autoridade sobre sua existência, ou do envio de relatórios periódicos;

Princípio da exatidão: os dados armazenados devem ser fiéis à realidade, o que compreende a necessidade de que sua coleta e seu tratamento sejam feitos com cuidado e correção, e de que sejam realizadas atualizações periódicas conforme a necessidade;

Princípio da finalidade, pelo qual qualquer utilização dos dados pessoais deve obedecer à finalidade comunicada ao interessado antes da coleta de seus dados. Este princípio possui grande relevância prática: com base nele fundamenta-se a restrição da transferência de dados pessoais a terceiros, além do que se pode, a partir dele, estruturar-se um critério para valorar a razoabilidade da utilização de determinados dados para certa finalidade (fora da qual haveria abusividade);

Princípio do livre acesso, pelo qual o indivíduo tem acesso ao banco de dados no qual suas informações estão armazenadas, podendo obter cópias desses registros, com a consequente possibilidade de controle desses dados; após este acesso e de acordo com o princípio da exatidão, as informações incorretas poderão ser corrigidas e aquelas obsoletas ou impertinentes poderão ser suprimidas, ou mesmo pode-se proceder a eventuais acréscimos;

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 (DONEDA, 2011, p. 100-101).

São esses os princípios que fundam uma normatividade da “proteção adequada” dos dados pessoais enquanto Direito Fundamental. Quando se fala sobre a proteção cooperada-integrada de dados, tem-se uma ideia de formatação objetiva de sua tutela, além de uma mera condução subjetiva, muitas vezes, e, equivocadamente, interconectada à mera privacidade. Os Estados, a Sociedade, o Mercado, as Organizações Internacionais e os Sindicatos, o Terceiro Setor, em parceria,

possuem a incumbência de instruir modalidades persuasivas, preventivas e corretivas em suas estruturas, na Sociedade da Informação, interconectadas, descentralizadas e complexas, expondo aos cidadãos as suas possibilidades, e lhes informando os seus espaços de ação, garantidos materialmente e, com isso, promovendo um bem comum, um sentido de boa vida, no qual a pessoa humana é convocada para exercer seus direitos.

Essa defesa, por acaso, também é vista com Menezes Neto e Moraes (2018), no sentido de que a proteção de dados pessoais deve ser realizada por todos/outros os atores que se encontram inseridos em dinâmicas relacionais fundadas via operacionalização de tecnologias da informação e comunicação, justamente porque a atuação exclusivamente estatal, na regulação e instrumentalização de mecanismos de proteção, com o mundo globalizado, enfrenta muitos desafios de efetividade.

Esta tarefa, por claro, não desponta fácil. Há, inclusive, outros pontos normativos que exurgem como relevantes, os quais devem, assim, se amalgamar: i) privacidade adequada; ii) prestação de contas e responsabilidade; iii) segurança e proteção; iv) transparência e explicação/tradução dos termos; v) *fairness* e não discriminação; vi) controle humano sobre a tecnologia; vii) responsabilização profissional; viii) proteção de valores humanos; ix) proteção dos direitos humanos e fundamentais. Esses indicadores-princípios enumerados são a base mapeadora de uma aproximação ética e fundamentada em direitos no que diz respeito a Inteligência Artificial. Eis, em síntese, a necessidade de se formatar uma proteção cooperada-integrada: tais tecnologias são interconectadas e interconectáveis, seus códigos e possibilidades impactam determinantemente a vida, a humanidade e seu destino. O alerta e a atenção devem ser perenes e amplos, de acordo com o que se pode visualizar, todavia, especialmente devido ao que nos escapa sorrateiramente, com os riscos naturalmente advindos de nossas próprias criações e desejos consubstanciados em decisões.

3 A PROTEÇÃO DE DADOS PESSOAIS NAS RELAÇÕES DE TRABALHO

3.1 Da automação à proteção de dados pessoais em atmosfera trabalhista

O ponto central dos debates sobre a tecnologia nas relações de trabalho possui como berço o tema da automação (MILL, 1996). De um lado, existe a preocupação de que, se a tecnologia substituir os humanos, logo causará desemprego em massa que resultará em um colapso do mundo do trabalho. De outra paragem, dizem que, na verdade, exsurgirão novas funções no âmbito laboral, as quais salvarão a humanidade do colapso social e econômico de um sistema produtivo sem humanos inseridos em sua dinâmica. No meio de tais extremos, será preciso buscar soluções, considerando-se essas duas posições que, sem dúvida, devem ser equilibradas, de modo a enquadrar o desenvolvimento tecnológico no mundo laboral ao direito humano-fundamental à proteção em face da automação (art. 7º, XVIII, C.F/88) e dos princípios jurídico-políticos fundamentais do valor social do trabalho e da livre iniciativa (art. 1º, IV, C.F/88).

É certo que os dados pessoais, nas relações juslaborais, surgem como uma tecnologia para o aumento da i) eficiência e do ii) lucro, princípios norteadores do mercado. Há, portanto, uma verdadeira interconexão de temas, entre automação e dados pessoais, obviamente, muito mais complexa do que as preocupações com o desenvolvimento tecnológico, com o propósito de automação dos séculos XVIII, XIX e XX, uma vez que, o estado de desenvolvimento atual supera a mera noção de “máquinas produtivas” dessas eras.

Pode-se aprofundar que, a tecnologia, no universo laboral, de acordo com as discussões trabalhistas contemporâneas, deverá respeitar a regra da inserção auxiliar como formato subsidiário à produção. Isso quer dizer que, há um movimento multilateral de desenvolvimento tecnológico em inúmeras instâncias interconectadas, e o âmbito laboral não escapa, ou não escapará de tais efeitos. Tem-se a necessidade, por

consequência, de se conformar, por intermédio de políticas governamentais, uma imputação gradual e sempre com caráter subsidiário (em *prima facie*, mantém-se a pessoa humana) e de auxílio (o instrumento tecnológico vem para ajudar e aperfeiçoar a humanidade, não para substituí-la).

Os dados pessoais, como posto, firmam-se como uma nova matéria-prima, de forma que podem ser utilizados para aumentar a eficiência e, em decorrência disso, o lucro empresarial. Tais afirmações possuem locuções com razões meramente econômicas, ao largo do mundo da vida e da preocupação que o Direito possui, em proteger os direitos das pessoas por intermédio de coordenação e barreiras de intersecção. Com isto em mente, passa-se à reflexão da proteção aos dados pessoais em uma perspectiva relacional entre empregador – trabalhador/empregado.

3.2 Empregado e empregador e seus respectivos interesses frente à tutela de proteção de dados pessoais – a imperatividade de uma proteção cooperada-integrada com o Estado, Sindicato, agências e organizações internacionais.

O primeiro ponto a ser exposto é este: devem-se respeitar as regras e princípios legais e constitucionais de proteção de dados pessoais em qualquer processamento e suas etapas. Diz-se isso, tendo-se em vista duas situações iniciais pelo lado do empregador: 1) os dados auferidos por determinação/obrigação legal e 2) aqueles obtidos por mera iniciativa empresarial, a fim de elevar a produtividade da empresa, inclusive, de fontes terceiras (não cabe ao fôlego que o presente texto possui abordar de forma detida este imbróglio). Na perspectiva 1), tem-se um processo que causa ruídos na chamada gestão de consentimentos. A empresa, por cumprimento de disposições legais, deve realizar, processar, guardar e conservar dados pessoais dos trabalhadores/empregados. São três os pontos que devem reger essa dinâmica: i) será necessário o consentimento do trabalhador(?); ii) colhido o dado, deve-se pensar em definir

a sua espécie e indicar o tratamento proporcional, lícito, adequado e seguro que ele precisa receber; iii) deve-se atentar para a finalidade e a transparência atrelada ao dado colhido, conforme a determinação legal para a qual foi obtido e, por medida de clareza, às normas de proteção que incutem ao próprio empregador a diligência necessária no tratamento de tal dado, independentemente do consentimento (i) e da “espécie” do dado pessoal auferido (ii).⁴ Estão incluídos nesses procedimentos, a saber, os exames médicos (sensíveis), os dados pessoais dos empregados/trabalhadores a serem inseridos no e-Social ou livro de registros, os controles de jornada, se a opção da modalidade pelo empregador der-se por via biométrica (sensíveis), além de muitos outros. Tem-se, nesse sentido, que, mesmo que o dado seja colhido por motivo de cumprimento de uma obrigação legal, que vai além, desse modo, da iniciativa empresarial, com consentimento ou dispensada a manifestação, seja o dado pessoal ordinário ou sensível, não há uma isenção de responsabilidade pelo tratamento e proteção adequada aos dados pessoais coletados dos trabalhadores (a expectativa do titular dos dados, e o legítimo interesse do agente de tratamento, precisam estar conforme à base legal de tratamento, e à proteção normativa/objetiva, atrelada para essas relações sociojurídicas) .

Na segunda “vertente”, pelo lado do empregador 2), iniciativa empresarial para elevar a produtividade, inclusive, por fontes terceiras, encontra-se um mundo de possibilidades e, igualmente, um mundo normativo do Direito que deve ser resguardado, uma vez que, os dados pessoais representam as próprias pessoas, e não, insumos. O primeiro ponto, i), consiste em indagar se está na discricionariedade empresarial a iniciativa para estabelecer as formas e conteúdos do recolhimento, processamento, instrumentalização e conservação dos dados pessoais, com o fim de elevar a produtividade (logo, o lucro).

Como já exposto, para a iniciativa, a resposta é, sim; para as formas e conteúdos, não. A discricionariedade encontra-se domesticada

⁴ BRASIL. LGPD. art. 7º, I, II, § 6º Art. 11, II, “a”, § 2º, § 3º.

pela legislação infraconstitucional e pela Constituição (regras e princípios). Correto. Mas, ainda que pareça abstrata essa asserção, inferem-se normas específicas que ordenam essas “possibilidades normatizadas”.⁵

ii) O segundo ponto diz respeito à definição da espécie de dado que se pretende colher, à indicação da sua atividade e finalidade e, em conjunto, deve-se questionar a viabilidade de garantir a privacidade, a segurança, a transparência, e o acesso, por parte dos trabalhadores, aos protocolos voltados a tais garantias individuais (subjetivas) e coletivas. Essa parte, portanto, passa por uma avaliação de “opção gerencial (É necessária e oportuna a aferição dos dados? Quais os riscos?)” e jurídica (Será legal/adequado o recolhimento dos dados em um sentido protetivo? A forma, a atividade e a finalidade às quais serão processados os dados possuem validade? Se, sim, as garantias necessárias a esse processamento serão exequíveis?). Assim, o arquétipo normativo que deve nortear a atuação do empregador, no modelo de processamento de dados pessoais, a fim de elevar a produtividade empresarial, passa por uma formatação teórica de Administração (eficiência, organização, lucro, aspectos concorrenciais, etc.) e, por outro lado, do Direito, às balizas legais e constitucionais objetivas (os conteúdos que serão objeto de processamento, os aspectos estruturais e instrumentais necessários) e subjetivas (adequação e necessidade de acordo com uma perspectiva delimitada nos direitos “individuais” do trabalhador). À guisa de exemplos, citam-se o monitoramento de temperatura,⁶ a fiscalização

⁵ O Tribunal Superior do Trabalho (TST), em recente decisão (E-RR- 933-49.2012.5.10.0001), julgou procedente ação civil pública, condenando empresa a se abster de utilização de banco de dados, com finalidade de proteção ao crédito, para aferir “condições” pessoais/privadas de empregados e de candidatos, para fins de “empregabilidade”, em razão dos riscos de tratamento discriminatório em cadeia, e no subverter a finalidade para qual os dados foram inicialmente tratados (proteção ao crédito). A referida decisão encontra-se, por exemplo, de acordo com os 21 Destaques para o Futuro do Trabalho, do recente Livro Verde, de Portugal (2021).

⁶ A saber e para demonstrar em um contexto gravíssimo e real, e simplificando-se a questão, o tratamento de dados sensíveis em épocas pandêmicas, em que o recolhimento por intermédio de monitoramento de temperatura está autorizado legalmente,

sobre a produtividade individual (exemplo: estabelecimento de câmeras nos monitores de computadores, a fim de obter reconhecimento biométrico (íris), acopladas à ativação do sistema da empresa, tornando possível aferir o “real” “tempo à disposição” e a produtividade dos trabalhadores), o meio ambiente do trabalho em si, no estabelecimento empresarial, ou quando de regime de teletrabalho “domiciliar”, entre outras inúmeras possibilidades.

Com efeito, o lado do empregador não pode ser observado sem que se contemple o lado do empregado, apesar da divisão “estrutural” gestada. Afirmar-se que, o nexos relevante que perpassa a problemática pela perspectiva do empregado está subdividido, sinteticamente, em três olhares: 1) o imprescindível consentimento ou a sua dispensa; 2) o conteúdo dos dados (ordinários ou sensíveis) e as formas de acesso e 3) as garantias materiais (privadas, legais e institucionais) que possam favorecer e materializar, autenticamente, as disposições de vontade (1), quando essas forem respeitadas e necessárias, além da própria defesa legal e institucional de tais direitos, considerando-se que, essas relações e seus conteúdos independem, como posto, de uma simples manifestação de vontade para tornar algum processamento de dados lícito ou ilícito (2).

As normativas que estão sendo expostas não dão ao “consentimento” individual (ou coletivo, a propósito) do empregado/trabalhador/sindicato o caráter, a etiquetagem de “legítima” e “legal”, a eventual decisão, possivelmente, limitadora de direitos, e esta questão, por claro, concerne profundamente ao empregador, uma vez que, tornada nula ou ilícita determinada organização procedimental de dados, poderá

independentemente do consentimento do trabalhador (Brasil e Portugal, por exemplo), que não se trata de uma carta branca. Deve-se respeitar, contudo, a anonimização dos dados, a privacidade, o questionamento sobre qual profissional realizará o exame, se médico ou qualquer profissional (dadas as características da empresa, etc.), considerando, além de outros fatores, o aspecto estigmatizante da doença e as possíveis violações a direitos decorrentes de uma admissível identificação (além da própria violação do dever de proteção aos dados pessoais).

haver penalidades administrativas graves, além de reparações coletivas e individuais. Esses sentidos perpassam por toda a duração da relação contratual, desde as responsabilidades pré-contratuais (currículos em geral, processos de seleção, internos ou externos), as existentes no decurso da vida laboral (dados obtidos por obrigações legais ou mediante a idealização de procedimentos para o aumento da produtividade) e as pós-contratuais (todas as informações sobre a relação contratual: salários, contribuições sociais, faltas, razões (privadas) de dispensa, faltas graves, invenções, acidentes, conversas, etc.).

Pode-se enquadrar, como acréscimo ao horizonte de sentidos para a proteção dos dados e, logo, de “liberdade” e limites ao poder diretivo, inclusive, 1) o que se tem na doutrina “clássica”, e 2) o que a jurisprudência trabalhista já decidiu sobre o tema. (1) Da doutrina “clássica” advêm i) a limitação dos meios ou métodos utilizados para a obtenção dos dados; ii) a proteção especial de alguns tipos de dados-informação (sensíveis); iii) os limites ao direito de perguntar do empregador (visto, também, como o direito de omitir ou de mentir do empregado); e (2), da jurisprudência trabalhista, a adequação e a possibilidade proporcional ligadas à finalidade, na obtenção consoante a atividade econômica desenvolvida, e a função a ser cumprida pelo trabalhador na empresa (SANDEN, 2014).

Apesar do caráter resumido da descrição dos problemas que se está construindo, destaca-se uma máxima, que norteia toda a normatização de proteção de dados pessoais, não apenas no Brasil ou nas relações juslaborais: as normas se remetem a atuações persuasivas e preventivas, muito além de sancionatórias ou reparatórias, e isso precisará adentrar na cultura “empresarial” e, claro, na dos trabalhadores, sindicatos, Ministério Público do Trabalho, Auditorias Fiscais do Trabalho e Poder Judiciário, além da própria Autoridade Nacional. Veja-se a importância desta questão, uma vez considerada a doutrina do direito de acesso (*the subject access requests*) e as possibilidades de o empregado/trabalhador vislumbrar o que foi aferido sobre ele, quais as mensagens e comunicações, e o conteúdo vinculado a sua pessoa

enquanto empregado, antes, durante e após a vigência da relação contratual – os riscos e perigos são enormes e imprevisíveis *a priori*, como colocado na primeira parte deste texto.

Nesse sentido, ficam as seguintes provocações: i) para o tratamento de qualquer modalidade de dados pessoais em relações trabalhistas, que necessitem de anuência, há uma preocupação que precisará ser desenvolvida: bastará uma “negociação” individual ou haverá a necessidade de negociação coletiva para tanto, tendo-se em vista que os dados pessoais não são meros “direitos de personalidade”, interconectados com a privacidade, que reclamam uma proteção cooperada-integrada, especialmente devido ao caráter objetivo de tais direitos? ii) Os atores, sindicatos e trabalhadores, terão que se reinventar, de modo conjunto à empresa, de forma a corresponder a um tratamento adequado aos dados pessoais, por vias protocolares “extrajudiciais” e, se preciso, judiciais. iii) A Inspeção do Trabalho, operacionalizada pelos Auditores Fiscais do Trabalho, e o Ministério Público do Trabalho, deverão agir por intermédio de razões persuasivas e preventivas, além de coordenarem um *enforcement* sincronizado com a Autoridade Nacional – será preciso, tendo em vista isso, estabelecerem-se regras de atribuições claras e, dispondo-se, igualmente, canais de diálogo e compartilhamento de informações a cada instituição. iv) A Justiça do Trabalho, sem dúvidas, deverá estar pronta para conciliar, processar e julgar casos individuais e coletivos, acertadamente, destinados à sua competência, a qual, contudo, será estabelecida apenas com o desenvolvimento paulatino das regulações e normativas a serem impostas. Faz-se necessária, portanto, uma preparação objetiva e subjetiva dos juízes, e demais auxiliares da justiça, de modo a harmonizarem-se com essas novas realidades.

De modo a acrescer uma estrutura inicial para esse tratamento cooperado-integrado, deixa-se como sugestão, quatro etapas e questionamentos. Primeira, i) coleta de dados: qual tecnologia usada? Quais as fontes para a coleta dos dados? O sindicato possui conhecimento ou acesso a esse tratamento de dados? Os empregados

possuem conhecimento ou acesso a esse tratamento de dados? Se, sim, como está materializado o direito de oposição e de acesso? Segunda, ii) análise dos dados: quais direitos assegurados aos empregados, para acessar os dados tratados, e as informações/inferências construídas sobre eles, e a sua finalidade. Terceira, iii) depósito e conservação dos dados: em quais servidores? Em que região do planeta esses servidores estão instalados? Estão sob qual jurisdição? Quarta, iv) dados oriundos do desligamento do empregado/trabalhador (*data off-boarding*): os dados são transferidos, ou vendidos? Para quem? São deletados? Os trabalhadores possuem o direito de oposição a esse tratamento? Esses questionamentos aplicam-se a todos os dados pessoais produzidos, inclusive as inferências construídas com base neles, sobre o empregado (COLCLOUGH, 2020). Com a LGPD, se encontra uma camada normativa tripartite, onde, em cada uma dessas etapas, deve-se ponderar quais as condições de legitimidade para se realizar o tratamento de dados pessoais, estabelecendo-se os procedimentos para a garantia dos direitos relativos à matéria e, sucessivamente, delimitando-se as consequências administrativas e civis decorrentes da violação das fases anteriores (MENDES, 2019, p. 46).⁷

Deixa-se claro, ao fim, que, quando se declara um “deve”, ou a indicação de sentidos para a criação de normas adequadas para a proteção de dados nas relações laborais, dispostas sucintamente neste texto, não se está afirmando, categoricamente, a “verdade”, mas, sim, formando-se indicadores de sentidos jurídicos adequados às leis, às regras e aos princípios impostos, nacional e internacionalmente, atendendo-se para a necessidade de estabelecimento de uma construção

⁷ Há de se construir uma estrutura particular a cada tipo de tratamento, e os dados pessoais objetos, no contexto das relações sociotrabalhistas. No caso de dados sensíveis, médicos e biométricos, a normatividade há ser construída é ainda mais complexa. Sarlet e Caldeira (2019) mostram a complexidade normativa da experiência brasileira e portuguesa, relativa à proteção de dados pessoais sensíveis, de saúde, na internet, com o enfoque nos direitos fundamentais dos titulares, integrada à base legal para o tratamento adequado, de modo a proteger, integralmente, a pessoa humana, em âmbito nacional, e global.

normativa que se atenha a procedimentos racionais, logo, controláveis, oponíveis e de justificação, sem solipsismos ou arbitrariedades semânticas, em uma noção “rütheriana”, de “interpretações sem limites e constrangimentos” (*unbegrenzte Auslegung*) (RÜTHERS, 1997) e, sem dúvida, contempladas aos perigos democráticos que a esses temas se ligam. As relações juslaborais já estão sendo impactadas e o serão ainda mais: é preciso preparar-se.

4 CONCLUSÃO

De modo a concluir, percebe-se que, os dados pessoais precisam de uma proteção cooperada-integrada adequada aos seus pontos normativos, uma vez que o direito fundamental à proteção dos dados pessoais ultrapassa o sentido tradicional de proteção dos direitos de personalidade, tais como, por exemplo, a privacidade, a imagem e a honra, além de se inserir em um contexto globalizado, que ultrapassa a noção de proteção meramente estatal. Nas relações de trabalho, o tema se apresenta com extrema complexidade, considerando-se a dinâmica, “poder diretivo e subordinação”, além das próprias circunstâncias sociais que as regulam em seu pano de fundo. Essa preocupação está exposta no último *report* do Parlamento Europeu (2021), “*Data Subjects, digital surveillance, AI and the future of work*”.

Embora posta esta constatação, a proteção integrada-cooperada dos dados pessoais expõe, em texto, pela via constitucional e infraconstitucional, nacional e internacional, inúmeros indicadores semânticos, para que isso possa ser formatado apropriadamente, elencando duas máximas: i) a proteção à pessoa sempre deverá prevalecer; e ii) as regras e princípios devem ser observados e instrumentalizados, independentemente do escopo, do conteúdo e da forma em que o tratamento de dados vá se materializar, incluindo-se, pois, essas duas máximas nas relações juslaborais. Ademais e por consequência, define-se que, a proteção integrada-cooperadas dos dados pessoais, em especial nas

relações de trabalho, devem ser incumbência de todos os atores que atuam nesse cenário, superando-se a noção de um direito de personalidade individualmente “protegido”, ou, ainda, de uma proteção exclusivamente estatal. Os trabalhadores, os sindicatos, as empresas e demais agentes nacionais e internacionais possuem a incumbência de construir uma esfera normativa adequada.

REFERÊNCIAS

BRASIL. Decreto-Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. Brasília, DF: Presidência da República, 1943. Disponível em: http://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 01 ago. 2023.

BRASIL. Constituição da República Federativa do Brasil de 1988. Brasília, DF: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 01 ago. 2023.

BRASIL. Lei nº 8.078, de 11 de setembro de 1990. **Dispõe sobre a proteção do consumidor e dá outras providências.** Brasília, DF: Presidência da República, 1990. Disponível em: http://www.planalto.gov.br/ccivil_03/leis/18078compilado.htm.

BRASIL. Escola Nacional de Defesa do Consumidor. **A proteção de dados pessoais nas relações de consumo: para além da informação creditícia.** Elaboração Danilo Doneda. Brasília: SDE/DPDC, 2010.

BRASIL. Lei nº 13.709 de 14 de agosto de 2018. Lei Geral de Proteção de Dados Pessoais (LGPD). Brasília, DF: Presidência da República, 2018. Disponível em: http://www.planalto.gov.br/ccivil_03/_ato2015-2018/2018/lei/113709.htm.

BRASIL. Tribunal Superior do Trabalho (SDI-1). **Embargos em Recurso de Revista nº 933-49.2012.5.10.0001.** Relator: Alberto Luiz Bresciani de Fontan Pereira. Brasília, DF: TST, 16 de dezembro de 2021. Disponível em: <https://jurisprudencia.tst.jus.br/>. Acesso em: 30 fev. 2022.

BRANCO, Sergio. **Entre dados e robôs: ética e privacidade na era da hiperconectividade.** Prefácio. *In*: MAGRANI, Eduardo. *Entre dados*

e robôs: ética e privacidade na era da hiperconectividade. Porto Alegre: Arquipélago Editorial, 2019.

COLCLOUGH, Christina. Worker's rights: negotiating and co-governing digital systems at work. **Social Europe.eu**, 30 set. 2020. Disponível em: <https://socialeurope.eu/workers-rights-negotiating-and-co-governing-digital-systems-at-work>. Acesso em: 6 setembro 2020.

CUEVA, Ricardo Villas Bôas. Justiça e Cidadania. **Editorajc.com.br**, 5 dez. 2016. Disponível em: <https://www.editorajc.com.br/a-insuficiente-protecao-de-dados-pessoais-no-brasil/>. Acesso em: 8 maio 2020.

DONEDA, Daniel. A proteção dos dados pessoais como um direito fundamental. **Espaço Jurídico**, n. 2, p. 91-108, Joaçaba, jul./dez. 2011.

FEENBERG, Andrew. **Entre a razão e a experiência: ensaios sobre tecnologia e modernidade**. Lisboa: MITPortugal, 2017.

MAGRANI, Eduardo. **Entre dados e robôs: ética e privacidade na era da hiperconectividade**. Porto Alegre: Arquipélago Editorial, 2019.

MENDES, Laura Schertel. A lei geral de proteção de dados pessoais: um modelo de aplicação em três níveis. **Caderno Especial LGPD**, São Paulo: RT, nov. 2019, p. 35-56.

MENEZES NETO, E.J.; MORAIS, J.L.D. A fragilização do estado-nação na proteção dos direitos humanos violadores pelas tecnologias da informação e comunicação. **Revista de Direitos Fundamentais & Democracia**, Curitiba, v. 23, n. 3, p. 231-257, set/dez, 2018.

MILL, Stuart. O Capital Circulante e o Capital Fixo. In: MILL, Stuart. **Princípios de Economia Política**. São Paulo: Nova Cultural, 1996. p. 150-153.

PARLAMENTO EUROPEU. **Data subjects, digital surveillance, AI and the future of work**. Disponível em: [https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU\(2020\)656305_EN.pdf](https://www.europarl.europa.eu/RegData/etudes/STUD/2020/656305/EPRS_STU(2020)656305_EN.pdf). Acesso em: 5 abril 2022.

PORTUGAL. **Livro verde do futuro do trabalho 2021**. Disponível em: <https://cdn.pista73.com/media/2021/03/Livro-Verde-do-Futuro-do-Trabalho.pdf>. Acesso em: 14 abr. 2021.

RÜTHERS, Bernd. **Die unbegrenzte Auslegung: zum Wandel der Privatrechtsordnung im Nationalsozialismus**. 5te Aufl. Heidelberg: C. F. Müller, 1997.

SANDEN, Ana F.M.S. **A proteção de dados pessoais do empregado no direito brasileiro: um estudo sobre os limites na obtenção e no uso pelo empregador da informação relativa ao empregado.** São Paulo: LTr, 2014.

SARLET, Gabrielle Bezerra Sales.; CALDEIRA, Cristina. O consentimento informado e a proteção de dados pessoais de saúde na internet: uma análise das experiências legislativas de Portugal e do Brasil para a proteção integral da pessoa humana. *Civilistica.com*, v.8, n. 1, p. 1-27, abr. 2019.

SNOWDEN, Edward. NSA reform in the US is only the beginning. *TheGuardian.com*. Disponível em: <https://www.theguardian.com/us-news/2015/may/22/edward-snowden-nsa-reform>. Acesso em: 2 abr. 2020.

SOLOVE, Daniel J. **Nothing to hide: the false tradeoff between privacy and security.** Yale University Press: 2011.

LUCAS RECKZIEGEL WESCHENFELDER

Mestrado em Direito pela Universidade de Santa Cruz do Sul, Pós-Graduação em Direito pela Universidade Federal do Rio Grande do Sul, e graduação em Direito pela Universidade de Santa Cruz do Sul. Advogado.

Endereço profissional: Avenida Independência, 2293, Santa Cruz do Sul, RS, 96815-900, Brasil.

ORCID ID: <https://orcid.org/0000-0001-9297-7465>

E-MAIL: lucasweschen@yahoo.com.br

LUIZ GONZAGA SILVA ADOLFO

Possui mestrado em Direito pela Universidade do Vale do Rio dos Sinos (2000); doutorado em Direito pela Universidade do Vale do Rio dos Sinos (2006); e pós-doutorado em Direito pela Pontifícia Universidade Católica do Rio Grande do Sul (2018). Professor do Curso de Direito e do Programa de Pós-Graduação em Direito (Mestrado) da Universidade de Santa Cruz do Sul-UNISC. Professor

do Curso de Direito da Universidade Luterana do Brasil-ULBRA, Campus Gravataí. Membro da Associação Portuguesa de Direito Intelectual-APDI, da Associação Brasileira de Direito Autoral-ABDA, e desde 2001 ininterruptamente da Comissão Especial de Propriedade Intelectual da Ordem dos Advogados do Brasil (OAB/RS), que presidiu na gestão 2010/2012. Consultor jurídico nas áreas dos Direitos Autorais e da proteção de dados pessoais. É **perito** credenciado junto ao Tribunal de Justiça do Estado do Rio Grande do Sul para ações de Propriedade Intelectual. Tem experiência na área de Direito, com ênfase em Direito Privado, atuando principalmente nos seguintes temas: Direito da Propriedade Intelectual, Sociedade da Informação, Direitos Culturais, Direito Civil, Prática Jurídica Cível, e Teoria do Direito.

Endereço profissional: Avenida Independência, 2293, Santa Cruz do Sul, RS, 96815-900, Brasil.

ORCID ID: <https://orcid.org/0000-0003-3786-3590>

E-MAIL: adolfo@unisc.br

Recebido em: 06/07/2020

Aceito em: 07/04/2022



Este trabalho está licenciado sob uma licença Creative Commons Attribution 4.0 International License.

Autores e autoras cedem à Revista Sequência direitos exclusivos de primeira publicação, ficando o trabalho licenciado sob a Creative Commons Attribution 4.0 International License. A licença autoriza que terceiros remixem, adaptem e ou criem a partir do trabalho publicado, indicando o crédito ao trabalho original e sua publicação inicial. Os autores têm permissão para assumir contratos adicionais em separado, com distribuição não exclusiva da versão publicada na Revista Sequência, indicando, de todo modo, a autoria e publicação inicial neste periódico.