REVISTA DE DIREITOS HUMANOS
E DESENVOLVIMENTO SOCIAL

DOSSIÊ

Inteligência artificial, proteção de dados e direitos humanos

Editores
Fernanda Carolina Araújo Ifanger e Lucas Catib De Laurentiis

Conflito de interesses
O autor declara não haver conflito de interesses.

Recebido
12 jul. 2024

Versão final
22 ago. 2024

Aprovado
26 ago. 2024

Proposta de solução para a efetivação da salvaguarda do direito fundamental à proteção dos dados pessoais dos empregados

Proposed solution for safeguarding the fundamental right to the protection of employees' personal data

Daniel de Almeida Alves[1]

[1] Pontifícia Universidade Católica de Campinas (PUC-Campinas), Escola de Ciências Humanas, Jurídicas e Sociais, Faculdade de Direito. Campinas, SP, Brasil. *E-mail*: <dalves2004@hotmail.com>.

Artigo elaborado a partir da dissertação de D. A. ALVES, intitulada "O direito à privacidade, intimidade e proteção de dados dos trabalhadores perante o avanço tecnológico". Pontifícia Universidade Católica de Campinas (PUC-Campinas), 2023.

Como citar este artigo: Alves, D. A. Proposta de solução para a efetivação da salvaguarda do direito fundamental à proteção dos dados pessoais dos empregados. *Revista de Direitos Humanos e Desenvolvimento Social*, v. 5, e2413759, 2024. https://doi.org/10.24220/2675-9160v5a2024e13759

Resumo

O objetivo do presente estudo, por intermédio do método hipotético-dedutivo, consiste em propor soluções práticas para que as empresas possam e devam adotar para que o direito fundamental da proteção de dados do trabalhador seja cumprido e para que as empresas não sejam sancionadas administrativa e judicialmente. O problema central está atrelado em como as empresas podem proteger os dados pessoais dos trabalhadores diante do avanço tecnológico e da aplicação de inteligência artificial, evitando práticas discriminatórias e garantindo a privacidade no ambiente de trabalho. Em que pese no Brasil a proteção de dados e seu reconhecimento ter sido tardia (apesar de já existentes algumas normativas do setor de saúde e do próprio Código de Defesa do Consumidor), foi somente com a Lei nº 12.965/2014 e Lei nº 13.709/2018, que trata da Proteção de Dados Pessoais, que foram estabelecidos regramentos e princípios próprios acerca do uso da Internet, do tratamento e proteção de dados, respectivamente. Nesse cenário, a utilização desmedida e irresponsável da tecnologia pode acarretar violação da privacidade e intimidade do trabalhador, o que pode ocasionar julgamentos discriminatórios, que muitas vezes não correspondem ao padrão ou preferência social do empregador que pode prejudicar a admissão ou até mesmo a manutenção do trabalho.

Palavras-chave: Compliance. Inteligência artificial. Privacidade do trabalhador. Proteção de dados pessoais.

Abstract

The main goal of the present study, through the hypothetico-deductive method, consists in proposing practical solutions for companies to adopt so that the fundamental right from its employees to have their data protected is achieved and fulfilled, avoiding sanctions, wether they

are administrative or judicial. The main purpose of this study is to examine how companies can protect the sensitive and personal data of its employees, taking advantage of the technological breakthroughs and by applying artificial intelligence, avoiding discriminatory practices while assuring privacy in a working and corporate environment. Even though Brazil has a fairly recent focus in data protection (although there were already norms in that sense on the health field and in consumer law), it was only through the editing of Laws 12.965/2014 and 13.709/2018, which regulate personal data protection, that rulings and legal principles were properly established regarding internet use and the protection of data, respectively. In this context, the careless and irresponsible usage of technology can result in breachings in privacy and intimacy of the employees, leading to potentially discriminatory treatment, which often will not correspond to his or her social orientations, resulting in potential harm during admission processes or even during the length of a laboral contract.

Keywords: *Compliance. Artificial intelligence. Employment privacy. Personal data protection.*

Introdução

México: O avanço tecnológico possibilitou que cada vez mais as pessoas disponibilizem informações pessoais na internet[2], principalmente os trabalhadores, incluindo quando são admitidos, sendo necessário disponibilizar diversas informações pessoais e muitas vezes sensíveis nos quais são organizados e estruturados com logicidade em banco de dados[3] proporcionando ao empregador a maximização de aproveitamento deste conjunto de informações coletadas, desta maneira se potencializa as formas e variedades pelas quais essas informações podem ser utilizadas ou apropriadas uma vez que o banco de dados permite o aumento da comunicação de informações e da capacidade de armazenamento.

Cita-se, como exemplo, os próprios dados biométricos, nos quais, conforme o Art. 5º, da Lei Geral de Proteção de Dados (LGPD) (Brasil, 2018), são considerados dados sensíveis[4] e, mesmo que não haja menção expressa acerca de sua proteção na relação laboral, é evidente que merece colhida a tutela pretendida aos dados biométricos na relação de trabalho, mormente pelo fato de se saber que o uso da biometria no pacto laboral é muito comum para se ter acesso ao sistema de informática nas empresas, principalmente para o registro de controle de ponto (ou para o acesso às dependências do empregador), consideradas práticas comumente utilizadas por décadas no Brasil, incluindo como outro exemplo a própria videovigilância, que tem impactos significativos no direito à privacidade dos trabalhadores, podendo ter abusos nestas áreas que o comprometem.

No que se refere aos dados biométricos, conforme mencionado, trata-se de dados sensíveis conforme Art. 5º, inc. II, da LGPD, portanto, nessas situações é necessário coletar o consentimento do trabalhador de forma mais esclarecida e devidamente justificada, principalmente nas hipóteses do Art. 11, da LGPD, devendo informar ao trabalhador os métodos da coleta, as finalidades e os meios de segurança utilizados para o tratamento, pois os dados biométricos somente podem ser tratados em "empresas sujeitas à restrição de tráfego, bem como para controle de acesso a

[2] A disponibilização dos dados pessoais se encontra na Internet superficial, nos quais são acessadas comumente pela população em geral, o que representa 0,18% da Internet existente. A Internet profunda é de acesso somente para pessoas que possuem conhecimentos mais avançados no local denominado "internet invisível" que possibilita a anonimização de quem o usa. Por fim, a internet escura é o local utilizada principalmente por "crackers" e está atrelada ao mundo do crime também, onde realmente ocorrem os mais diversos crimes na Internet, tais como pedofilia, compra e venda de armamento, tráfico humano, venda de órgãos etc., sendo que a internet profunda representa 99,82% de todo o conteúdo virtual existente (Bergman, 2001).

[3] Os dados são considerados hodiernamente como um elemento central na sociedade contemporânea em decorrência do múltiplo uso de vastos aparelhos eletrônicos. De origem etimologicamente latina (*datum*), o termo dado é referido comumente a algo que é concedido a alguém. Dentre diversos conceitos denotativos existentes, pode-se definir dado como um registro representativo de um conceito, uma instrução, um fato, um elemento e, até mesmo, a um atributo de uma pessoa, coisa ou entidade (Estavillo, 1997; Gouvêa, 1997). Estes dados podem ser agrupados e reunidos de forma sistematizada, nascendo daí o banco de dados, que é o "conjunto de dados relacionados ou relacionáveis com determinado assunto" (Marques; Martins, 2000, p. 290).

[4] Dado sensível relaciona-se à "origem racial ou étnica, convicção religiosa, opinião política, filiação a sindicato ou a organização de caráter religioso, filosófico ou político, dado referente à saúde ou à vida sexual, dado genético ou biométrico, quando vinculado a uma pessoa natural" (Brasil, 2018, Art. 5º, inc. II).

dispositivos e aplicativos de computação também considerados de acesso restrito pela empresa" (Sankievicz; Pinheiro, 2021, p. 513).

Entretanto, não se pode atribuir, aprioristicamente, incompatibilidade dos direitos trabalhistas com o avanço tecnológico em si, sendo necessário buscar equilíbrio entre interesses antagônicos (trabalho e capital) que se traduzem na necessidade do empregador em obter informações sobre as atividades desenvolvidas e dos trabalhadores com o direito à privacidade e proteção de dados, considerando principalmente a potencialidade lesiva que as novas tecnologias podem oferecer quanto à violação da proteção de dados, sendo necessário nesse viés traçar diretrizes e princípios a serem seguidos e observados (Guerra, 2004).

Portanto, o problema central está atrelado em como as empresas podem proteger os dados pessoais dos trabalhadores diante do avanço tecnológico e da aplicação de inteligência artificial, evitando práticas discriminatórias e garantindo a privacidade no ambiente de trabalho. Além disso, o objetivo principal[5] deste artigo, por intermédio do método hipotético-dedutivo (Popper, 1975), consiste em propor soluções práticas para que as empresas possam e devam adotar para que o direito fundamental da proteção de dados do trabalhador seja cumprido e para que as empresas não sejam sancionadas administrativa e judicialmente.

Para isso, realizou-se uma abordagem acerca da necessidade da proteção de dados pessoais dos empregados em um contexto de crescente uso de tecnologias e inteligência artificial[6], além de sugestionar soluções práticas para mitigação de riscos em conformidade legal, garantindo-se maior efetividade à privacidade e intimidade dos empregados, colaborando para que não ocorram ilícitos discriminatórios e nem situações sancionatórias às empresas, seja em âmbito administrativo, seja em âmbito judicial.

Nesta toada, conjectura-se, hipoteticamente, de que a aplicação de medidas rigorosas de compliance e a utilização responsável da inteligência artificial nas empresas podem assegurar a proteção dos dados pessoais dos trabalhadores, evitando práticas discriminatórias e garantindo a privacidade no ambiente de trabalho, pois aborda-se, no presente estudo, a importância de proteger os dados pessoais dos empregados, especialmente em um contexto no qual a utilização de inteligência artificial encontra-se em crescente expansão.

Deduzir-se-á consequentemente, com base na conjectura previamente abordada, que se as empresas implementarem medidas rigorosas de compliance e utilizarem a inteligência artificial com parcimônia e com responsabilidade, poderá acarretar consequências positivas. Dentre as consequências possíveis, (a) deverá haver a redução de práticas discriminatórias no ambiente de trabalho com o uso ético da inteligência artificial, evitando-se decisões enviesadas; (b) deverá haver um aumento na proteção dos dados pessoais com a consequente melhoria na segurança e proteção dos dados pessoais dos trabalhadores, com menor incidência de vazamentos ou usos indevidos dos dados; (c) deverá haver maior conformidade com a LGPD, evitando-se sanções legais, administrativas e melhorando a confiança dos trabalhadores; por fim, (d) deverá haver maior

[5] Trata-se, na verdade, do problema central, uma vez "que a ciência parte de problemas; que esses problemas aparecem nas tentativas que fazemos para compreender o mundo da nossa 'experiência' ('experiência' que consiste em grande parte de expectativas ou teorias, e também em parte em conhecimento derivado da observação – embora ache que não existe conhecimento derivado da observação pura, sem mescla de teorias e expectativas)" (Popper, 1975, p. 181).

[6] Interessante os conceitos de Inteligência Artificial definidos pela Comissão Europeia e pela OCDE no qual "a IA é um conjunto de tecnologias que combinam dados, algoritmos e capacidade computacional" sendo um "sistema baseado em máquina que pode, para um determinado conjunto de objetivos, fazer previsões, recomendações ou decisões que influenciam ambientes reais ou virtuais. Usa entradas de máquina e/ou humanos para perceber ambientes reais ou virtuais; para extrair tais percepções em modelos (de forma automatizada, por exemplo com aprendizado de máquina ou manualmente); e para usar o modelo de inferência para formular opções de informação ou ação. Os sistemas de IA são projetados para operar com vários níveis de autonomia" (Organisation for Economic Cooperation and Development, 2019a, *online*).

satisfação e credibilidade dos empregados em relação à forma como seus dados são gerenciados pelo empregador.

Apesar da ausência de dados formais governamentais e oficiais, bem como dados estatísticos e fiscalizatórios, é prescindível, para o escopo do presente estudo, a realização de teste empírico com coleta de dados qualitativos e quantitativos, bem como estudos de casos e métodos comparativos com empresas que não se utilizam de medidas de compliance, pois é evidente, como corolário lógico, que nestas situações haverá maior incidência de discriminação, violação de dados, desconformidade com a LGPD e insatisfação dos empregados, corroborando-se com as hipóteses aventadas.

Entretanto, é de suma importância enaltecer de que conforme a metodologia utilizada, as medidas e procedimentos sugestionados encontram-se em constantes alterações conforme transmudações culturais, históricas, tecnológicas e legais, até porque "na medida em que um enunciado científico se refere à realidade, ele tem que ser falseável; na medida em que não é falseável, não se refere à realidade" (Popper, 1975, p. 346).

Superada essas menções introdutórias, na primeira parte do presente estudo será abordada a crescente adoção de tecnologias contemporâneas pelo empregador, tais como a biometria, *big data*[7], internet das coisas[8], inteligência artificial e demais situações no afã de contextualizar a problemática e demonstrando a potencialidade lesiva que o uso indiscriminado e irresponsável dessas tecnologias podem acarretar em relação à privacidade e intimidade dos trabalhadores, enfatizando-se a necessidade constante de uma fiscalização rigorosa e adoção de práticas éticas, considerando-se principalmente a transparência e assimetria de poder existente entre o trabalhador e empregador, sem olvidar de diretrizes internacionais e a LGPD como marcos regulatórios essenciais.

Na segunda parte será abordada as recomendações de boas práticas para a proteção de dados dos empregados, destacando-se a importância da transparência e da adoção de medidas de segurança por parte dos empregadores em conformidade com as orientações de regulamentações europeias e da própria LGPD, relacionando-se com programas de compliance para que seja garantida a proteção de dados, prevenção de riscos e garantia de que os trabalhadores tenham conhecimento claro sobre a utilização e destinação de seus dados pessoais, priorizando uma cultura organizacional voltada para a privacidade com atualizações constantes e treinamentos, para que seja garantida a devida proteção de dados e que quaisquer violações que possam ocorrer, sejam corrigidas com a maior brevidade possível.

Nas considerações finais corroborou-se os riscos associados ao avanço tecnológico e à aplicação da inteligência artificial no ambiente de trabalho, no qual destaca-se a possibilidade de invasão da privacidade dos trabalhadores e a necessidade de proteção de seus dados pessoais. Nesse contexto de crescente utilização de métodos automatizados, os empregadores podem monitorar constantemente os trabalhadores, tanto em suas atividades profissionais quanto pessoais, criando perfis que influenciam decisões de contratação e manutenção do emprego. Como soluções passíveis de implementação, enfatiza-se a importância de garantir a confiança no

[7] Em sua conceituação mais ampla, *big data* é uma consequência da própria confluência da tecnologia, tais como computação em nuvem, comunicações de banda larga e internet das coisas, possibilitando uma reunião de dados em escalas gigantescas, sendo que, no contexto do presente artigo, refere-se pela possibilidade de criação de perfis dos trabalhadores que poderão influenciar na escolha da admissão a um emprego bem como a constante avaliação, tanto para produtividade quanto até para eventual promoção ou demissão do trabalhador, entrecruzando diversas informações e dados pessoais (Kojirovski, 2015).

[8] A internet das coisas possibilita a aproximação do mundo físico das coisas com o mundo digital, realizando interações contínuas por intermédio da interligação das informações geradas pelas pessoas com as informações geradas pelas coisas.

tratamento dos dados, inclusive que seja permitido que os trabalhadores possam acessar e retificar seus dados conforme boas práticas internacionais e programas de compliance para prevenção de abusos e promoção de maior transparência e fiscalização no uso das tecnologias pelo empregador.

Contextualização da problemática tecnológica empregatícia

As tecnologias contemporâneas podem ser um vetor negativo quando utilizado de forma desmensurada e irresponsável, sendo que as tecnologias que mais podem ser potenciais violadoras da privacidade e intimidade do trabalhador são a biometria, análise de big data, internet das coisas e inteligência artificial, principalmente nas fases pré-contratual e durante a vigência do contrato de trabalho.

De acordo com as informações da União Europeia, a título estatístico e exemplificativo, ocorreram mais de 89 mil violações de dados registrados entre 2018 e 2019 (European Data Protection Board, 2019), sendo que os dados produzidos ao redor do mundo no interstício de 2018 e 2025 aumentará de 33 para 175 *zettabytes*[9] com taxa de crescimento anual da produção de dados entre 2018 e 2025 de 61% (European Commission, 2020).

Muitas práticas ocorrem de forma escondida dos empregados ou candidatos ao emprego, tais como a mineração de dados[10], buscas online, perfis em redes sociais etc., com total ausência de transparência e sem indicações de critérios precisos, que acabam sendo utilizados no processo de admissão, não sendo raro, no mais das vezes, o empregador se blindar destas práticas alegando parametrização baseada em segredo empresarial aliada às estratégias comerciais ou processo produtivo, tornando eventual reprimenda de difícil detecção e aferição.

Neste sentido, não basta, por si só, a vedação ou proibição da coleta de dados nos moldes apresentados como um ilícito, é necessário que haja procedimento mais incisivo e imediato, mas cuja solução acaba sendo, no mais das vezes, socorrer-se do judiciário. Conforme a ampliação da competência material da Justiça do Trabalho por intermédio da Emenda Constitucional nº 45/2004 (Brasil, 2004), é de bom alvitre salientar que a apreciação da violação da privacidade e intimidade do empregado oriunda de uma relação de trabalho (ou empregatícia) pela violação de seus dados é da competência da Justiça do Trabalho, nos exatos termos dos incisos I, IV e VI, do Art. 114, da Constituição Federal de 1988 (CF/88)[11], sendo a competência territorial resolvida nos termos do Art. 651, da Consolidação das Leis do Trabalho (CLT) (Brasil, 1943).

Entretanto, apesar da complexidade envolvida, em algumas situações é possível identificar os ilícitos acometidos. Cita-se, como exemplo, o próprio hackeamento[12], no qual caso ocorra a violação dos dados do empregado, por intermédio da URL[13] (*home page*) é possível identificar o site

[9] *Zettabyte* é uma unidade de informação ou memória que corresponde a 10^{21} bytes.

[10] Mineração de dados, também denominada de Data mining, é uma técnica com objetivo de angariar "novas informações, que podem estar ocultas, a partir de banco de dados" (Marçula; Benini Filho, 2008, p. 198) com objetivo de realizar perfilamento do indivíduo, por intermédio da técnica denominada *profiling*, que "pode ser aplicada a indivíduos bem como estendidas a grupos. Nela os dados pessoais são tratados, com auxílio de métodos estatísticos, técnicas de inteligência artificial e outros mais, com o fim de obter uma 'metainformação', que consistiria numa síntese de hábitos, preferências pessoais e outros registros da vida dessa pessoa. O resultado pode ser utilizado para traçar um quadro de tendências de futuras decisões, comportamentos e destinos de uma pessoa ou grupo" (Doneda 2006, p. 173).

[11] Esta competência permanece inclusive entre os filiados e os sindicatos (relativos aos dados pessoais dos sindicalizados) bem como entre empresas que realizam o tratamento de dados dos empregados em face do empregador, conforme Art. 114, inc. III, da CF/88, inclusive, sendo cabível, na espécie, Habeas Data (Brasil, 1988).

[12] Hacker se refere a toda possibilidade que um indivíduo se utiliza para invasão do sistema informático de outrem, inclusive para uso lícito, como se dá quando se faz para aperfeiçoar e testar um sistema e sua segurança para detecção de falhas e vulnerabilidades. Os que o fazem com intuito ilícito para angariar vantagens indevidas, denomina-se de crackers, nos quais comumente realizam pirataria digital.

[13] URL é uma sigla que se traduz em *Uniform Resource Locator*, que é um termo técnico que se refere ao endereço de rede no qual se encontra o endereço de algum site na internet conforme o que for digitado na barra do navegador para que se tenha acesso a um determinado serviço ou página.

pelo endereço de IP ou pelo domínio que se encontra, uma vez que o IP[14] (Protocolo da Internet) é o que traz a identificação da origem da ilicitude perpetrada. Existem outros *softwares* que colaboram também para esta identificação, incluindo mensagens eletrônicas, país de origem, IP, e-mails etc. (Fiorillo; Conte, 2013).

Além do mais, é necessário conceder ao trabalhador maior controle sobre seus dados, independentemente de ter havido ou não alguma violação, uma vez que ao empregador, ao coletar seus dados, não se sabe ao certo qual será sua finalidade e utilização, inclusive em momento futuro devido ao seu armazenamento.

Normalmente, o empregador acredita que para conceder ao empregado maior controle sobre seus dados, basta que haja o consentimento, mas são dotados de informações abstratas e com vagueza sobre seu alcance, não sabendo ao certo as informações sobre o destino da utilização dos dados do trabalhador ou para quem serão transferidos após a coleta e para quais finalidades; não é por outro motivo que o próprio Regulamento Geral de Proteção de Dados da União Europeia qualificou este consentimento de forma mais restrita e rígida, exigindo não só o consentimento expresso, mas também a manifestação consentida livre, inequívoca, explícita, específica e informada.

Diante deste armazenamento pelo empregador, é imprescindível que haja uma fiscalização rígida de como as empresas armazenam os dados pessoais e sensíveis dos trabalhadores, principalmente àqueles relacionados à saúde, mapeando e identificando atos discriminatórios e coletando dados para fins estatísticos acerca da empregabilidade dos trabalhadores nestas circunstâncias.

Ademais, o armazenamento e coleta de dados com a utilização de inteligência artificial e algoritmos devem necessariamente passar por uma análise interseccional, uma vez que, de acordo com a legislação vigente, apenas o termo de consentimento assinado pelo trabalhador não é suficiente para justificar a coleta e armazenamento indiscriminado de dados. A discriminação algorítmica que pode surgir desse processo é preocupante, pois o consentimento exigido nessas circunstâncias é realizado de forma unilateral pelo empregador, refletindo a falta de paridade decorrente da assimetria de poder entre as partes.

Além do consentimento expresso do trabalhador, é necessário que haja uma garantia contra a discriminação e a melhoria de processamento de dados para fins estatísticos de maneira que impeça a individualização e identificação do trabalhador. Isso é crucial para evitar que os dados sejam utilizados de forma injusta ou discriminatória, preservando os direitos dos trabalhadores e garantindo que o uso de inteligência artificial e algoritmos seja conduzido de forma ética e justa.

Em relação ao uso da inteligência artificial[15], a própria OCDE estabeleceu alguns princípios a serem seguidos, nos quais a inteligência artificial deve ser "inovadora, de confiança e que respeita os direitos humanos e os valores democráticos" (Organisation for Economic Cooperation and Development, 2019b). A União Europeia, por intermédio de seu documento denominado *Orientações Éticas para uma Inteligência Artificial de Confiança*, estabeleceu diretrizes com foco

[14] IP é uma sigla que significa *Internet Protocol*, que é um endereço específico e exclusivo que possibilita a identificação na Internet contendo informações de localização, sendo parte essencial do funcionamento da internet. É uma sequência de conjunto de números matematicamente gerados de forma não aleatória e submetido a uma organização sem fins lucrativos estadunidense denominada ICANN (*Internet Corporation for Assigned Names and Numbers*) podendo ser privado ou público (O que é..., c2024).

[15] Diversos países (cita-se somente como exemplo os EUA, Canadá, China, Alemanha, França etc.) estão criando estratégias de nível nacional para lidar com a inteligência artificial em decorrência da concorrência desleal que seu uso acarreta em relação às pequenas e médias empresas, uma vez que somente 20% das empresas consideradas de nível mundial (tais como IBM, Facebook, Microsoft, Google, Amazon, Apple etc.) adotam a utilização da inteligência artificial em sua produção ou fornecimento de serviços (Servoz, 2019).

na proteção de pessoas por intermédio da necessidade de se haver transparência, respeito a autonomia humana, proteção dos dados pessoais, direito à privacidade com vedação da discriminação. Em âmbito trabalhista, a própria Organização Internacional do Trabalho (OIT) ao alegar de que "o trabalho não é uma mercadoria; nem é um robô", estabelece premissas de uso da inteligência artificial, nos quais se privilegia a tomada de decisões pela autonomia humana em decorrência da inteligência emocional, pois as decisões que afetem o ambiente de trabalho precisa perpassar pelo crivo humano, pois "a gestão de algoritmos, a vigilância e o controle através de sensores e de outras formas de monitoramento, precisa ser regulado para proteger a dignidade dos trabalhadores" (Organização Internacional do Trabalho, 2019, pp. 13, 45).

Em relação à desnecessidade de consentimento expresso, a própria LGPD já excepciona as circunstâncias no qual o consentimento expresso é prescindido, conforme Art. 11, inc. II, alínea "b", que se relaciona à execução, pela administração pública, de políticas públicas previstas em leis ou regulamentos ou outras hipóteses de interesse público, sendo realizada uma ponderação apriorística legal que considera mais relevante os interesses públicos em detrimento do titular dos dados. Assim, depreende-se de que as críticas a esse dispositivo são no sentido de que a proteção dos dados pessoais e sensíveis devem ser considerados um direito fundamental merecedor de tutela ampla e plena, apesar de que este dispositivo não se aplica na presente pesquisa, uma vez que se aborda sob a ótica do empregador em âmbito privado.

Recomendações de boas práticas como proposta de solução à proteção de dados dos empregados

Interessante notar as recomendações como propostas de solução oriundas do Regulamento (EU) nº 2016/679 do Parlamento Europeu (Bruxelas, 2016) por intermédio da Recomendação do Comitê de Ministros sobre Tratamento de Dados Pessoais no contexto do emprego, no qual há orientação aos empregadores para que seja evitada intromissão abusiva e injustificada na privacidade dos trabalhadores, sendo estendida esta proteção para todos os mecanismos tecnológicos utilizados pelo empregador, nos quais ao serem utilizados pelos trabalhadores devem ser informados *in totum* acerca da política de privacidade utilizada pelo empregador, sempre de forma periódica e adequada, incluindo na política a finalidade do processamento dos dados e a forma de coleta e armazenamento.

Orienta-se neste sentido para que o acesso das páginas de internet pelo trabalhador sejam adotadas medidas preventivas, tais como utilização de filtros que impeçam o acesso e monitoramento de dados pessoais do trabalhador; os trabalhadores devem ser informados que as comunicações eletrônicas profissionais podem ser acessadas pelo empregador quando necessário, por motivos legítimos ou por segurança; vedação completa de acesso e monitoramento de comunicação privada do trabalhador; orienta-se também para que o empregador adote medidas transparentes quando do desligamento do trabalhador, nos quais os conteúdos podem ser acessados para uso exclusivo da organização da empresa antes da saída do trabalhador, preferencialmente que seja realizado em sua presença.

Deste modo, há diversas obrigações e responsabilidades que o empregador deve seguir como o responsável pelo tratamento de dados recolhidos e acessados, com adoção de medidas técnicas de segurança e controle suficientemente adequadas para que os dados sejam confidenciais, permitindo o acesso, autorização e recolhimento desses dados do trabalhador somente para pessoas devidamente legitimadas.

Além disso, o seu desrespeito, seja proposital ou acidental, deverá acarretar de imediato a notificação e o aviso ao trabalhador detentor dos dados acerca da ocorrência, devendo o empregador com maior brevidade possível sanar a questão e envidar esforços para mitigar os eventuais prejuízos ocasionados, nos quais, havendo quaisquer falhas na proteção de dados do trabalhador, deve-se atuar com a maior celeridade possível e aplicar a medida disciplinar correspondente à gravidade ocasionada e detectada.

Essas responsabilidades e obrigações dirigidas ao empregador no que tange à proteção de dados, podem ser implementadas, empiricamente, no modelo organizacional da empresa, por diversas formas, sendo uma das mais comuns por intermédio de programas denominados de *compliance* (Reis, 2019).

Sem adentrar nas pormenoridades e acerca da amplidão denotativa que o termo *compliance* abrange, o que interessa para esta pesquisa é sobre programas que tenham como objetivo a governança em privacidade, conforme se observa pelas boas práticas insculpidas no Art. 50, da LGPD (Reis, 2019).

Logo, programas desta estirpe colaboram para a própria adaptação gerencial da empresa e para a operacionalização das diretrizes, comandos e conceituações da LGPD no âmbito laborativo, pois

> o *compliance* na LGPD, além de permitir a prevenção, funciona como um instrumento de contenção de riscos, na medida em que a empresa que o adota se compromete a cumprir o ordenamento jurídico e as imposições dos órgãos de regulamentação, dentro dos padrões exigidos para o seu segmento de atuação (Reis, 2019, p. 124).

Evidentemente que não se trata de um programa estanque de aplicabilidade unívoca e uniforme, pois as alterações legislativas e, principalmente, as inovações e avanços tecnológicos demandam da própria empresa reiteradas atualizações desses programas em constante sintonia e vigilância, devendo com certa periodicidade, revisar seus documentos (tais como códigos de ética e conduta, políticas de privacidade, entre outros) e investir nas melhorias procedimentais, de segurança e proteção de dados como método de prevenção, evitando-se acessos não autorizados, perda, alteração, destruição e demais situações correlatas em relação aos dados dos trabalhadores[16].

Para que haja e que surta maior efetividade para os programas de *compliance*[17] no âmbito laboral e de proteção de dados, é necessário que sejam simples, com linguagem acessível e de fácil compreensão, permitindo fácil acessibilidade e transparência ao empregado, uma vez que para sua efetividade, é necessário que todos os setores da empresa compreendam o teor de tais documentos, devendo ainda a empresa[18], para devida otimização do programa, fornecer canais para saneamento de dúvidas, esclarecimentos além da possibilidade de denúncias caso haja descumprimento, como modo eficaz de detecção.

Para que isso seja possível dentro do âmbito da empresa, é necessário incutir a cultura da proteção de dados e criar, preferencialmente, um setor específico e autônomo dentro da empresa que cuide da proteção de dados, com o devido comprometimento dos gestores e dos empregadores

[16] Até mesmo porque não cabe ao empregador em optar em não proteger ou proteger de forma deficitária e descuidada os dados dos trabalhadores, pois o empregador tem o dever legal de prestação de contas e demonstrar quais são as medidas que estão sendo tomadas, conforme se extrai, explicitamente, do Art. 6º, inc. X, da LGPD (Brasil, 2018).

[17] Uma das formas e possibilidades de se auferir se os programas de compliance em proteção de dados estão sendo atingidos, são por intermédio de selos e certificações que estabelecem diretrizes próprias e específicas para a gestão do compliance, citando-se como exemplo a própria ISO (*International Organization of Standardization*), conforme Arts. 33, inc. II, alínea "d" e 35, ambos da LGPD, que inclusive servem como atenuantes nas sanções administrativas caso as empresas o possuem, conforme se extrai do Art. 52, §1º, inc. VIII, da LGPD (Brasil, 2018).

[18] Cada programa deve ser moldado e adaptado para cada tipo de empresa e pelas atividades e riscos que nelas se encontram presentes.

de forma geral, com implementação de medidas programáticas, tais como palestras e constantes treinamentos, por exemplo.

Importante mencionar também de que, apesar do programa de compliance em si mesmo ser uma medida facultativa ao empregador de implementação, as demais diretrizes são comandos e imperativos legais de seguimento obrigatório, pois

> embora a LGPD não seja uma normativa específica em matéria de proteção de dados dos trabalhadores, as medidas nela estabelecidas, como as relativas à *avaliação de impacto sobre proteção de dados* (AIPD), ao *registro das operações de tratamento*, à obrigação de indicar um encarregado da proteção de dados (EPD), bem como aos *selos, certificados e códigos de conduta regularmente emitidos*, são aplicáveis no âmbito laboral, por força do parágrafo primeiro do artigo 8º da CLT, que admite a aplicação subsidiária e supletiva do direito comum (Reis, 2019, p. 146).

Assim, entende-se que o empregador precisa deixar claro quais são os riscos existentes aos trabalhadores em relação aos dados, a) quais as medidas utilizadas para a proteção dos dados; b) quais as finalidades e operações usadas; c) qual a necessidade e proporcionalidade, conforme estatuído no Art. 5º, inc. XVII, da LGPD, por exemplo, que aborda o relatório de impacto à proteção de dados pessoais (Brasil, 2018).

Em relação ao trabalhador titular dos dados, deve-lhe ser concedido diversos direitos, como o direito ao esquecimento, acesso, alteração, retificação, portabilidade e demais direitos correlacionados aos seus dados, garantindo ainda ao trabalhador a ciência acerca da utilização de seus dados e a sua destinação, mesmo nas situações previstas em leis (como o fornecimento dos dados do trabalhador para o governo), devendo haver na empresa um responsável[19] direto a quem o trabalhador pode acionar caso queira obter essas informações, bem como alguma instituição governamental onde possa se socorrer caso esses direitos não sejam respeitados.

Além do mais, no aspecto contratual, seja para novos contratos ou que estão em vigência, deverá o empregador promover a devida alteração, adequação e atualização dos contratos conforme as diretrizes da LGPD, com cláusulas expressas, simples e claras acerca do tratamento dos dados, permitindo ao trabalhador ter a ciência completa acerca da coleta dos dados e dos seus direitos, proibindo-se dubiedades interpretativas.

Nesse sentido, é necessário que haja medidas de proteção da privacidade dos dados pessoais do empregado por intermédio de diversos direitos de defesa que serão abordados no transcorrer deste tópico. Primeiramente, para que seja possível um direito de defesa eficaz, o empregado tem o direito de acesso, conforme se observa nos Arts. 5º, inc. LXXII, alínea "a", da CF/88 (Brasil, 1988), Art. 43, *caput*, do Código de Defesa do Consumidor (Brasil, 1990) e Art. 7º, inc. I, da Lei nº 9.507/1997 (Brasil, 1997) e Art. 5º, inc. II, da Lei nº 12.414/2011 (Brasil, 2011), exemplificativamente.

O princípio do livre acesso do empregado de seus dados pessoais, antes de sua abordagem pela LGPD, teve influência direta do Art. 12, alínea "a", da Diretiva nº 95/46/CE bem como já havia sido abordada pela Oficina da OIT com o seguinte teor:

> 11.1. os trabalhadores deveriam ter o direito a ser informados com regularidade sobre os dados pessoais que lhes digam respeito e sobre o tratamento deles. 11.2. os trabalhadores deveriam ter acesso a todos os seus dados pessoais, independentemente de que sejam objeto de um tratamento automático ou de que sejam conservados em um expediente manual ou em qualquer outro arquivo que compreenda dados pessoais seus (Organização Internacional do Trabalho, 1997, p. 12).

[19] O responsável deve ser, preferencialmente, o encarregado da proteção de dados com plena autonomia na sua função, conforme se observa no Art. 5º, inc. VIII, da LGPD, cujas atribuições e acessibilidade, encontram-se no Art. 41, §1º e 2º, da LGPD (Brasil, 2018).

A clareza e objetividade dos dados pessoais do empregado e sua manutenção, confere-lhe o direito à retificação caso o empregado perceba inexatidão, inveracidade ou necessidade de complementação de seus dados que se encontram em um banco de dados (De La Cueva, 1993). Engloba-se neste direito também o cancelamento, seja por necessidade de supressão, seja pelo fato de que tais dados não deveriam ter sido colhidos (cita-se como exemplo o Art. 5º, inc. I, da Lei nº 12.414/2011 que prevê o direito do consumidor em ter cancelado registro desabonador com a quitação do débito pretérito) (Brasil, 2011; De La Cueva, 1993).

O empregado tem o direito também de compelir o empregador, por intermédio da obrigação de fazer, para que seus dados pessoais coletados sejam tratados e mantidos conforme a finalidade em que o fora autorizado, podendo o empregado restringir seu uso pelo empregador ou até mesmo vedar o seu uso para fins diferentes daqueles originalmente colhidos (Valdés, 1996). Compreende-se também neste direito, o resguardo da confidencialidade do empregado e sigilo de seus dados que não estejam em conformidade com o fim que se destina.

Considerando que com o desvio de finalidade dos dados coletados pelo empregador pode ser caracterizado uma fraude trabalhista, nos termos do Art. 9º, da CLT (Brasil, 2017), é passível de nulidade judicial quaisquer dispensas ou não contratação com base no uso indevido destes dados quando utilizado para criar perfil do empregado e discriminá-lo em decorrência disso, podendo ser readmitido ou indenizado se dispensado ou somente indenizado, caso não contratado (uma vez que não há contratação forçada por causa da livre-iniciativa do empregador).

Importante mencionar de que a proteção que se faz alusão é dos dados pessoais do trabalhador, uma vez que os dados sensíveis, em regra, nem devem ser tratados e armazenados pelo empregador, seja antes, durante ou após o pacto laboral, podendo ser caracterizado, inclusive, como tratamento com rigor excessivo pelo empregador, sendo lícito ao empregado invocar a rescisão indireta de seu contrato, nos termos do art. 483, alínea "b", da CLT (Brasil, 2017).

Infere-se, portanto, que é fundamental as empresas adotarem medidas rigorosas para proteger os dados pessoais dos trabalhadores, conforme estabelecido pela LGPD e outras normativas aplicáveis. O uso de programas de compliance eficazes, aliados à transparência e à acessibilidade das políticas de privacidade, são essenciais para garantir que os direitos dos trabalhadores sejam respeitados e que a coleta e o tratamento de dados sejam realizados de maneira ética e legal. Além disso, é imperativo que os empregadores se comprometam a atualizar continuamente essas políticas e práticas, assegurando que as inovações tecnológicas e as mudanças legislativas sejam incorporadas de maneira a proteger os trabalhadores de possíveis abusos e discriminações.

Considerações Finais

Em sede de considerações finais, corroborou-se a hipótese de que as medidas de compliance e o uso responsável da inteligência artificial nas empresas resultam na proteção efetiva dos dados pessoais dos trabalhadores, na redução de práticas discriminatórias, na conformidade com a LGPD e na satisfação dos empregados.

Neste contexto de avanço tecnológico e aplicação da inteligência artificial cada vez mais presente na sociedade contemporânea com a consequente disseminação do uso desses meios tecnológicos, possibilita que haja uma potencial invasão da privacidade dos trabalhadores por diversos mecanismos diferentes, trazendo riscos aos dados pessoais, sendo muitas das vezes sem a ciência dos trabalhadores.

O tratamento de dados pessoais que são processados cada vez mais de formas automatizadas, permitem que haja um maior controle de forma unificada das diversas atividades do trabalhador em suas pormenoridades, possibilitando maior acessibilidade pelo empregador do comportamento do trabalhador em âmbito privado e público em uma verdadeira vigilância constante e em tempo real.

As novas tecnologias permitem ao empregador aglomerar dados dos trabalhadores por intermédio de métodos observacionais, englobando tanto o tempo dispendido no local de trabalho, quanto à descoberta das preferências e interesses dos trabalhadores, como por exemplo, analisando os sites mais navegados, possibilitando que sejam criados perfis dos trabalhadores e servindo para tomada de decisões, tanto para contratação quanto para a manutenção do contrato de trabalho.

Neste sentido, a necessidade da criação do direito à proteção de dados pessoais dos empregados se deu para que houvesse garantia e confiança no tratamento de dados, com objetivo em se saber qual seria a finalidade e destinação dos dados coletados, principalmente para que não haja desvirtuamento sem o consentimento do trabalhador, bem como da necessidade de se conferir acessibilidade do titular aos bancos de dados, para que este possa retificar as informações a seu respeito.

Conclui-se, portanto, conforme abordado neste artigo, quais são as situações que indicam como se deve tratar da questão do avanço da tecnologia no ambiente do trabalho, considerando principalmente o latente desafio de repreender as práticas discriminatórias advindas do uso imoderado da tecnologia pelo empregador. Diante disso, este artigo buscou indicar possíveis soluções além do acesso ao Judiciário, indicando modelos de referência internacional sobre boas práticas acerca dos tratamentos de dados e medidas que reforcem a autodeterminação informativa e maior transparência e fiscalização do empregador, sem olvidar das implementações de programas, como o compliance, que colabora no efeito preventivo em prol da empresa.

Referências

Bergman, M. K. White Paper: The Deep Web: Surfacing Hidden Value. *Taking License*, v. 7, n. 1., 2001. Disponível em: https://quod.lib.umich.edu/j/jep/3336451.0007.104?view=text;rgn=main. Acesso em: 9 nov. 2024.

Brasil. [Constituição (1988)]. *Constituição da República Federativa do Brasil de 1988*. Brasília: Presidência da República, 1988. Disponível em: http://www.planalto.gov.br/ccivil_03/constituicao/constituicao.htm. Acesso em: 12 maio 2023.

Brasil. Presidência da República. Decreto-Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. *Diário Oficial da União*: seção 1, n. 157, Brasília, p. 11937, 9 ago. 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 12 maio 2023.

Brasil. Presidência da República. Decreto-Lei nº 5.452, de 1º de maio de 1943. Aprova a Consolidação das Leis do Trabalho. *Diário Oficial da União*: Brasília, p. 11.937, 9 ago. 1943. Disponível em: https://www.planalto.gov.br/ccivil_03/decreto-lei/del5452.htm. Acesso em: 8 nov. 2024.

Brasil. Presidência da República. Emenda Constitucional nº 45, de 30 de dezembro de 2004. Altera dispositivos dos arts. 5º, 36, 52, 92, 93, 95, 98, 99, 102, 103, 104, 105, 107, 109, 111, 112, 114, 115, 125, 126, 127, 128, 129, 134 e 168 da Constituição Federal, e acrescenta os arts. 103-A, 103B, 111-A e 130-A, e dá outras providências. *Diário Oficial da União*: seção 1, n. 157, Brasília, p. 9, 31 dez. 2004. Disponível em: https://www.planalto.gov.br/ccivil_03/constituicao/emendas/emc/emc45.htm. Acesso em 12 maio 2023.

Brasil. Presidência da República. Lei nº 12.414, de 9 de junho de 2011. Disciplina a formação e consulta a bancos de dados com informações de adimplemento, de pessoas naturais ou de pessoas jurídicas, para formação de histórico de crédito. *Diário Oficial da União*: seção 1, n. 111, Brasília, p. 2, 10 jun. 2011. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=2&data=10/06/2011. Acesso em: 14 maio 2023.

Brasil. Presidência da República. Lei nº 13.467, de 13 de julho de 2017. Altera a Consolidação das Leis do Trabalho (CLT), aprovada pelo Decreto-Lei nº 5.452, de 1º de maio de 1943, e as Leis n º 6.019, de 3 de janeiro de 1974, 8.036, de 11 de maio de 1990, e 8.212, de 24 de julho de 1991, a fim de adequar a legislação às novas relações de trabalho. *Diário Oficial da União*: seção 1, ano 154, n. 134, Brasília, 14 jul. 2017. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=14/07/2017. Acesso em: 12 maio 2023.

Brasil. Presidência da República. Lei nº 13.709, de 14 de agosto de 2018. Dispõe sobre a proteção de dados pessoais e altera a Lei nº 12.965, de 23 de abril de 2014 (Marco Civil da Internet). Lei Geral de Proteção de Dados Pessoais (LGPD). *Diário Oficial da União*: seção 1, n. 157, Brasília, p. 59, 15 ago. 2018. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?data=15/08/2018&jornal=515&pagina=59&totalArquivos=215. Acesso em: 12 maio 2023.

Brasil. Presidência da República. Lei nº 8.078, de 11 de setembro de 1990. Dispõe sobre a proteção do consumidor e dá outras providências. *Diário Oficial da União*: seção 1, n. 176, Brasília, p. 1, 12 set. 1990. Disponível em: https://www.planalto.gov.br/ccivil_03/leis/l8078compilado.htm. Acesso em: 12 maio 2023.

Brasil. Presidência da República. Lei nº 9.507, de 12 de novembro de 1997. Regula o direito de acesso a informações e disciplina o rito processual do habeas data. *Diário Oficial da União*: seção 1, ano 134, n. 220, Brasília, p. 1, 13 nov. 1997. Disponível em: https://pesquisa.in.gov.br/imprensa/jsp/visualiza/index.jsp?jornal=1&pagina=1&data=13/11/1997. Acesso em: 14 maio 2023.

Bruxelas (UE). Regulamento (UE) 2016/679 do parlamento europeu e do conselho de 27 de abril de 2016. Relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais e à livre circulação desses dados e que revoga a Diretiva 95/46/CE (Regulamento Geral sobre a Proteção de Dados). *Jornal Oficial da União Europeia*, 2016. Disponível em: https://eur-lex.europa.eu/legal-content/PT/TXT/PDF/?uri=CELEX:32016R0679. Acesso em: 12 maio 2023.

De la Cueva, P. L. M. *Informatica y proteccion de datos personales*. Madrid: Centro de Estudios Constitucionales, 1993.

Doneda, D. *Da privacidade à proteção de dados pessoais*. Rio de Janeiro: Renovar, 2006.

Estavillo, J. J. R. *Derecho e informática en México*: informática jurídica y derecho de la información. México: Universidaded Nacional Autónoma de México, 1997.

European Commission. *A European Strategy for Data*. Brussels: European Commission, 2020. Disponível em: https://digital-strategy.ec.europa.eu/en/policies/strategy-data. Acesso em: 30 out. 2023.

European Data Protection Board. 1 year GDPR - taking stock. *EDPB, Brussels*, 22 may 2019. News. Disponível em: https://edpb.europa.eu/news/news/2019/1-year-gdpr-taking-stock_en. Acesso em: 30 out. 2023.

Fiorillo, C. A. P.; Conte, C. P. *Crimes no meio ambiente digital*. São Paulo: Saraiva, 2013.

Gouvêa, S. *O direito na era digital*: crimes praticados por meio da informática. Rio de Janeiro: Mauad, 1997.

Guerra, A. *A privacidade no local de trabalho*. As novas tecnologias e o controlo dos trabalhadores através de sistemas automatizados-uma abordagem ao Código do Trabalho. São Paulo: Almedina, 2004.

Kojirovski, G. O Big Data vai decidir quem será promovido. *Revista Exame*, [*s. l.*]: 6 maio 2015. Disponível em: https://exame.com/revista-exame/o-big-data-vai-decidir-quem-sera-promovido/. Acesso em: 20 ago. 2024.

Marçula, M.; Benini Filho, P. A. *Informática*: conceitos e aplicações. 3. ed. São Paulo: Érica, 2008.

Marques, G.; Martins, L. *Direito da Informática*. Coimbra: Almedina, 2000.

O que é endereço IP e como proteger o seu? *Kaspersky, c2024*. Disponível em: https://www.kaspersky.com.br/resource-center/definitions/what-is-an-ip-address. Acesso em: 21 ago. 2024.

Organisation for Economic Cooperation and Development. *Recommendation of the Council on Artificial Intelligence*. [*s. l.*]: OECD Legal Instruments, 2019b. Disponível em: https://legalinstruments.oecd.org/api/print?ids=648&lang=en. Acesso em 30 out. 2023.

Organisation for Economic Cooperation and Development. *Scoping the OECD AI Principles*: Deliberations of the Expert Group on Artificial Intelligence at the OECD (AIGO). OECD Publishing, Paris, 2019a. Disponível em: https://www.oecd-ilibrary.org/science-and-technology/scoping-the-oecd-ai-principles_d62f618a-en. Acesso em 30 out. 2023.

Organização Internacional do Trabalho. Protección de los datos personales de los trabajadores: repertorio de recomendaciones prácticas de la OIT. *Oficina Internacional del Trabajo*, Genebra, 1997. Disponível em: https://www.ilo.org/global/publications/ilo-bookstore/order-online/books/WCMS_PUBL_9223103290_ES/lang--es/index.htm. Acesso em: 30 out. 2023.

Organização Internacional do Trabalho. Trabalhar para um Futuro Melhor. *Comissão Mundial sobre o Futuro do Trabalho*. Genebra: OIT, 2019. Disponível em: https://www.ilo.org/wcmsp5/groups/public/---europe/---ro-geneva/---ilo-lisbon/documents/publication/wcms_677383.pdf. Acesso em: 30 out. 2023.

Popper, K. S. *A lógica da pesquisa científica*. 2 ed. São Paulo: Cultrix, 1975.

Reis, B. F. *O direito fundamental à proteção de dados pessoais e sensíveis do trabalhador frente às novas tecnologias da informação e comunicação*. 2019. 176 f. Dissertação (Mestrado em Direito) – Universidade do Extremo Sul Catarinense, Criciúma, 2019. Disponível em: http://repositorio.unesc.net/handle/1/7469. Acesso em: 5 jul. 2024.

Sankievicz, A.; Pinheiro, G. P. Aspectos da proteção de dados nas relações de trabalho. *In*: Mendes, L. S. *et al. Tratado de Proteção de Dados Pessoais*. Rio de Janeiro: Forense, 2021.

Servoz, M. AI, the future of work? Work of the future! on how artificial intelligence, robotics and automation are transforming jobs and the economy in Europe. *European Political Strategy Centre*, 3 may 2019. Disponível em: https://digital-strategy.ec.europa.eu/en/library/future-work-work-future. Acesso em: 30 out. 2023.

Valdés, J. T. *Derecho informático*. 2. ed. McGraw-Hill, 1996.