A PROTEÇÃO DE DADOS NO CONTRATO DE TRABALHO

Antônio Carlos Aguiar

RESUMO

As mudanças sociais que impactaram em grande medida o Mundo do Trabalho são inevitáveis e já se consolidaram. Os novos desafios envolvem, nesse cenário, também, os dados pessoais, petróleo do século XXI, antes mesmo de se formar qualquer vínculo de trabalho e após o encerramento da relação. Essa nova dinâmica e os fundamentos legais que se formaram exige a transição do direito social restrito para a aplicação prático-estrutural atual, se fazendo necessária a compreensão dos novos atores nessa nova realidade que nos desafia com novos desdobramentos jurídicos e factuais que devem ser avaliados sob as perspectivas jurídico-protetivas.

Palavras chave: direito do trabalho; impactos tecnológicos; proteção de dados; privacidade; autodeterminação informativa.

1. Introdução: Purgatório de Dante

"Só para lembrar, Henry Ford aplicou os princípios da administração científica de Taylor e Fayol em sua empresa e revolucionou o mundo. Temos produtos em nossas casas graças à implementação de três paradigmas fundamentais dessa escola: 1. Linha de produção com a micro divisão de atividades; 2. Adestramento da mão de obra para a execução de tarefas simples; 3. Controle dos 'tempos e movimentos' em busca de maior produtividade. Em outras palavras, uma estrutura organizacional hierárquica na qual há uma turma que mantenha e pensa, outra que obedece e vigia uma terceira com juízo suficiente para executar tudo isto".

E ainda hoje as empresas e, portanto, os efeitos reflexivos desta padronização organizacional se espraiam perante os contratos de trabalho, adotam essas regras. Isso, em um ambiente de trabalho onde a um simples clique, é possível, via internet, ter acesso a tudo, desde manuais, dicas, questionários, chegando a impressoras digitais que replicam (muito) mais barato o produto que o empregado "adestrado pelo modelo tradicional de linha de produção" trabalha diuturnamente.

Aqui está um dos pontos principais de destaque a ser enxergado e visitado: o limbo

Antônio Carlos Aguiar

Doutor em Direito do Trabalho pela Pontifícia Universidade Católica de São Paulo – PUC/SP. Mestre em Direito do Trabalho pela Pontifícia Universidade Católica de São Paulo – PUC/SP. Especialista em Direito do Trabalho pela Universidade de São Paulo – USP

estrutural que cerca as relações de trabalho neste momento de transição (em velocidade exponencial) do recém passado ao presente (novo e pouco conhecido), com a precária utilização, na grande maioria das vezes, de instrumentos que não já não mais se encaixam neste status quo pós-moderno.

Vivenciamos o Purgatório de Dante, utilizando-se de licença poética, o meio do caminho – entre esse passado e o futuro (já presente) –, ou seja: "Saídos do Inferno, e da Terra, por um longo e tortuoso caminho subterrâneo, atravessado por um arroio que eles acompanham contra sua corrente, e chegados ao ar livre da praia do Purgatório, Dante e Virgílio se encantam com a visão da noite estrelada, especialmente com as quatro estrelas que correspondem, no céu austral, à constelação da Ursa Menor no céu setentrional. Encontram, logo mais, o guardião do Purgatório, que é Catão de Útica, o famosos legista da república de Roma antiga, o qual interpela, maravilhado e suspeitoso pela maneira insólita de sua chegada ao Purgatório, vindo necessariamente do Inferno, mas acaba aceitando as explicações de Virgílio e fornecendo-lhes todos os ensinamentos para seu novo cometimento" .

Precisamos conversar com o Guardião. Por favor, Catão de Útica do Purgatório Digital nos atenda.

Necessitamos de uma espécie de guia que se materialize por meio de um observatório digital das relações de trabalho, em especial, que nos faça compreender e trabalhar com todas as miudezas, desdobramentos e efeitos (positivos e negativos) que fazem parte do chamado petróleo do século XXI, segundo a revista britânica The Economist, vale dizer, os dados pessoais: por quem, como e por que. Caminhemos por entre os estágios dessa montanha .

2. Primeiro estágio: fase pré-contratual

Atualmente até a busca por uma ocupação ou recolocação profissional está diferenciada. Quem ainda manda pelo correio ou entrega pessoalmente um currículo expresso? Aliás, cabe outra pergunta: o que mesmo deve conter neste currículo (digital)?

Hoje por meio do espaço cibernético encontra-se tudo. Ele é tutorial. Um grande "supermercado digital" demonstrando as praticidades do como fazer. Vídeos explicativos, aulas, manuais, pórticos exemplificativos, etc. Uma interessante vitrine de mecanismos de atuação variados. A pergunta (outra) que fica é: mecanismo de ajuda/apoio ou de padronização/stantardlização? Estaríamos impedindo que Óblio possa manifestar e ser auto-criativo?

Comporte-se bem e adequadamente. Entrevistas de candidatos a emprego. Quantas "dicas" são dadas/oferecidas aos candidatos, a fim de que "se comportem bem" numa entrevista. Que impressionem. Apresentem o "seu melhor". Que apresentem suas "qualificações e qualificativos" que retratem quem ele é (ou quer/deva ser). E todas essas informações serão "guardadas numa 'caixinha'".

Essa abordagem é identificada para destacar que a base de informações obtidas, antes mesmo do início de uma relação de trabalho, por parte do empregador (pelo mercado e/ou mídias sociais), é indutiva e, por via reflexiva, invasiva na vida da (na) vida privada do entrevistado; da nossa vida...

Passam por esse estágio perguntas pessoais, personalíssimas, que, por vezes,

vão bem além daquilo que necessária e obrigatoriamente deveria o empregador ter acesso informativo para a prestação de um serviço que poderá (ou não) num futuro ser-lhe fornecido.

Vão desde com quem mora: filhos, cônjuge, pais, amigos, etc., até para que time torce; religião que professa; opinião política, redes sociais que está presente, gostos, cultura, prática esportiva, hobby, rituais, amigos (network), e daí por diante, passando, é claro, pelo básico, ou seja, escolaridade e experiência profissional anterior, tudo por meio de mecanismos "científicos" de avaliação e "constatação" direta, como: capacidade profissional, experiência, formação direta e indireta (nível de empatia, comportamento em equipe, resiliência e empregabilidade), por exemplo.

Aliás, no que se refere à experiência anterior, juntamente com o grau técnico de sua avaliação, são acompanhados questionamentos outros, como a razão da sua saída, procedidos do porquê da escolha de um novo e eventual empregador, acrescidos, de modo sútil e aparentemente inocente, de outras perguntas, que têm o fito de saber se o candidato tem algum tipo de vício, se apresenta algum problema de saúde pessoal e/ou familiar, se tem espírito questionador, tudo devidamente atrelado aos seus hábitos nos empregos anteriores, como qual frequência/necessidade de uso de smartphone, como entende as ordens e orientações recebidas, faltas ao serviço e assim por diante.

Questiona-se, ainda, onde mora e a distância de sua casa até a empresa, bem como quantas conduções são necessárias ao deslocamento, não somente para fins de cálculos relacionados a custos, como com vale transporte, mas, também, como um meio de monitoramento relacionado a futuros e possíveis atrasos.

Ao final, a entrevista é encerrada e dela advém um resumo, um fechamento opinativo quanto à avaliação (subjetiva ou por meio de algum programa – ou algoritmo) da personalidade do candidato: pessoa calma, paciente, "resiliente", "promissora", agitada, ansiosa, dinâmica, criativa, com iniciativa, identificando – segundo os critérios de quem o avaliou – os seus pontos positivos e negativos.

Esse relatório conclusivo serve à contratação ou não da pessoa.

As perguntas que ficam a partir desse complexo processo, são: qual o destino dessa profícua e detalhada fonte de informações dessa pessoa? Qual o compromisso de sigilo daqueles que as obtiveram, que estiveram envolvidos neste procedimento? Qual a garantia do entrevistado de que seus dados pessoais não serão abertos (ou conhecidos) por terceiros? Qual a proteção jurídica desses dados pessoais? Qual a diferenciação de tratamento (se existente) dessas informações, entre os contratados e os não-contratados (e o critério de acesso)? Se existente, qual ou quais os motivos jurídicos para isso?

3. Segundo estágio: vigência do contrato de trabalho.

Parabéns: você foi aprovado na entrevista, de candidato torna-se um colaborador efetivo. Passa, muitas vezes, a ter convênio médico e a empresa, prestadora desses serviços, ilimitado acesso a toda a sua condição físico-mental (por vezes, da sua família também). Internamente,

tem direito ao uso de ferramentas digitais (e espaço para arquivamento de fotos, vídeos e outros documentos pessoais), tudo e por óbvio, armazenado e guardado por constantes backups efetuados pelo empregador em suas máquinas (os computadores, smarthphones, tablets, etc. continuam sendo de propriedade do empregador) – pelo menos, essa é a regra (que, claro, comporta exceções).

Se o empregado prestar serviços externos ou em home office poderá (se não houver explícita ordem em sentido contrário) se utilizar de rede wi-fi pública e/ou gratuita. Estará (o risco é grande e efetivo), contudo, trabalhando e possivelmente disponibilizando informações confidenciais para quem não deveria nesta hipótese. Será que ninguém lhe disse que isso não era seguro? Não há alguma política interna ou disposição contratual alertando-o para esse fato de risco? A necessidade dessas prévias comunicativas é importantíssima, diante dos reflexos negativos que podem desdobrar-se da sua (má) utilização.

Por falar em política interna será que há alguma disciplinando como ele deve usar (ou não usar) os aparelhos que lhe são ofertados para o trabalho, como computadores, smarthphones, tablets, etc.? E mais: que eles serão considerados como ferramenta de trabalho e, portanto, sujeitos à fiscalização e controle? Condição que implica análise e verificação de (por) terceiros de fatos, fotos e comportamentos íntimos?

Ou mais ainda: que o empregador poderá, ao longo do contrato, obter informações estritamente pessoais relacionadas ao comportamento geral do empregado, geradoras de fórmulas que lhe permitem avaliar e assegurar a sua produtividade, influenciando diretamente na sua carreira profissional, sem que tenha possibilidade de um "contraditório" quanto ao subjetivo entendimento daquele que detém acesso a essas informações?

Ainda com relação ao uso do wi-fi aberto para clientes apenas com senha sem identificação, a empregadora teria explicitado sobre os riscos de a sua utilização poder ser tratada em determinadas situações como crime virtual – além do acesso indevido por terceiros das informações contidas no aparelho? – como, por exemplo, um roubo de identidade e de senha, com a utilização das informações pessoais para realizar compras online ou efetuar transações financeiras de forma indevida. Ou, então: a) falsa identidade; b) calúnia, injúria ou difamação na internet; c) estelionato; d) pirataria; e) discriminação (comentários preconceituosos de cunho racista, sexista, homofóbico, transfóbico, etc.); e) pedofilia.

A lista é grande.

4. Terceiro estágio. "Fim do casamento": depois da rescisão contratual

Terminada a relação teria o empregado um salvo conduto relativo a uma espécie de direito ao esquecimento? Seus dados pessoais são seus e de mais ninguém. Logo, tudo que estiver (se previamente autorizado para tanto) guardado em seu maquinário deverá ser-lhe entregue por meio de pendrive ou mídia equivalente, com garantia de não armazenamento por parte do empregador.

Há de se observar, ainda, outros aspectos periféricos e reflexivos supervenientes ao fim do contrato, não diretamente ligados ao arquivo/guarda de "coisas" pessoais. A

relação profissional que foi mantida entre empregado e empregador é originária de um contrato sinalagmático, limitado tão somente àqueles que o constituíram, à vista do seu caráter de direitos e obrigações exclusivas aos envolvidos. Salvo informações de índole estatal, que obrigatoriamente devem ser guardadas e eventual ou periodicamente repassadas à fiscalização do Estado, a fidúcia contratual obriga as partes que respeitem a individualidade personalíssima do contrato. Não é juridicamente admissível e possível repassar a terceiros dados e/ou informações sem a anuência do seu titular.

O que fica, para estudo e avaliação jurídica, é o como, ou seja, a instrumentalização de mecanismos eficazes de controle, para efetividade deste comando ético, à vista da ruptura contratual havida no relacionamento entre as partes. Único, diga-se de passagem, elo jurídico e factual que as ligava.

Sem dúvida alguma, é importantíssima a celebração de mecanismos jurídicos de vazão eficaz para essa garantia. Eles podem perpassar por aditivos contratuais; compromissos expressos pós-contratuais, com cláusulas restritivas de liberdade; acordos coletivos de trabalho; políticas internas de compliance; e tudo mais que tenha o condão de limitar (pelo menos mitigar) o conteúdo comunicativo dessas informações/dados pessoais e profissionais dos envolvidos ausentes, diante da ruptura do laço contratual.

Não há aqui que se esperar bom senso ou outra medida moral subjetiva. Deve-se, ao contrário, exteriorizar e expressar categoricamente os entendimentos e seus limites. Somente assim, se terá o respeito jurídico necessário e a possibilidade de reparo, diante de uma eventual e futura infração.

5. Proteção de dados: uma garantia jurídica

Quando se fala em proteção, dentro de um contexto social permeado por questões tecnológicas, o que está em jogo não é a construção de meios e formas que garantam ao indivíduo (a pessoa humana) uma proibição plena quanto ao acesso à sua vida privada; à sua intimidade (algo como: me deixe em paz).

O que é possível e deve ser respeitado é outro modo garantidor, qual seja o controle. Dispositivos legais que delimitem o acesso e uso dos seus dados pessoais, formadores da sua identidade e personalidade, que protejam o segredo (se assim a pessoa o quiser) sobre esses dados; sobre o fluxo dessas informações.

Muito embora no Brasil não exista uma regulamentação específica acerca da proteção de dados, a tutela privada de direitos da personalidade do trabalhador tem sua garantia, com vistas à proteção da dignidade da pessoa humana. Para tanto, observam-se as disposições principiológicas da Constituição Federal, Consolidação das Leis do Trabalho e Marco Civil da Internet.

Por sua vez, a União Europeia, em 27 de abril de 2016, editou normas que compõem o agora chamado General Data Protection Regulation (GDPR). De acordo com o estabelecido, as organizações que manipulam e tratam dados pessoais da Comunidade Europeia tiveram até maio de 2018 para se adequar às novas regras, dois anos após a edição . O GDPR é composto por:

a) Regulamento (UE) 2016/679 do Parlamento Europeu e do Conselho – 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) ;

b) Diretiva (UE) 2016/680 do Parlamento Europeu e do Conselho – relativa à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais pelas autoridades competentes para efeitos de prevenção, investigação, deteção ou repressão de infrações penais ou execução de sanções penais, e à livre circulação desses dados, e que revoga a Decisão-Quadro 2008/977/JAI do Conselho ;

c) Diretiva (UE) 2016/681 do Parlamento Europeu e do Conselho de 27 de abril de 2016 – relativa à utilização dos dados dos registos de identificação dos passageiros (PNR) para efeitos de prevenção, deteção, investigação e repressão das infrações terroristas e da criminalidade grave .

Em relação ao âmbito de aplicação, devemos ter em mente que o GDPR aplica-se a empresas brasileiras que tratam dados de cidadãos europeus, como, por exemplo, empresas que tenham matriz ou filial europeia, com sistema integrado para tratamento de dados .

Numa relação de emprego, como bem alerta e destaca Tatiana de Almeida Granja , estão presentes princípios próprios do Direito do Trabalho, que impõem limites aos poderes do empregador (direção, hierárquico e de fiscalização), garantidores, portanto, da proteção de dados. Neste sentido, ao destacar, primeiramente, o princípio da irrenunciabilidade de Direitos, ela o faz citando outros dois autores:

Primeiro, a jurista Maria Belén Cardona Rubert , que identifica as possibilidades de tratamento de dados sensíveis:

> "O empresário unicamente poderá proceder ao tratamento automatizado destes dados sensíveis quando, pela natureza do posto, o trabalhador deva realizar tarefas carregadas de um indubitável conteúdo ideológico, devendo ser excluída esta possibilidade no caso de se tratar de tarefas neutras, já que a aptidão para executar ditas prestações não depende da participação do trabalhador na tendência ou linha ideológica da empresa e, portanto, são ilícitas todas as indagações realizadas pelo empresário dirigidas a obter informação relativa a ideologia, crenças religiosas, afinidade política ou sindical do candidato ao emprego ou do trabalhador do quadro que tenha que desenvolver ou desenvolva atividades ideologicamente neutras".

Depois, traz à tona o entendimento de Daniel Martínez Fons :

> "[...]. no que se refere aos dados especialmente protegidos, deve-se ter em conta que a exigência do consentimento na coleta e no tratamento de dados sensíveis não substitui nem neutraliza os direitos fundamentais à intimidade, liberdade religiosa, ideológica e sindical na relação de trabalho. Efetivamente, o requerimento empresarial ao trabalhador de qualquer informação relativa a algum dos aspectos agora citados se sujeita ao princípio da proporcionalidade. Isto significa que deve ser comprovado um interesse relevante no conhecimento da

informação".

A seguir, trata do princípio da qualidade dos dados, evidenciando que por esse princípio "os dados coletados devem ser adequados, necessários e proporcionais (não excessivos) e adequados à finalidade de tratamento a que se destinam. Além disso, eles devem ser, de fato, necessários, indispensáveis e não excessivos ao propósito do tratamento. [...] deve haver proporcionalidade entre as naturezas dos dados levantados e o objetivo do tratamento de dados. Insta registrar que as três exigências relacionadas à qualidade dos dados – adequação, pertinência ou necessidade e proporcionalidade em sentido estrito – correspondem aos três elementos do Princípio da Proporcionalidade".

Depois, completa com o Princípio da Informação, onde "é obrigação do empregador informar a existência e a finalidade do tratamento. É também necessário informar os meios e as fontes que serão utilizadas na obtenção dos dados, bem como as consequências da negativa de consentimento e/ou fornecimento das informações. [...] é mister demonstrar a idoneidade e garantir a transparência do tratamento de dados de caráter pessoal".

Outro princípio por ela relacionado refere-se ao Princípio do Consentimento, onde "em qualquer espécie de tratamento de dados, o consentimento do indivíduo tem importância capital. Trata-se do princípio que legitima todo o tratamento. Ele permite que o afetado controle a utilização de seus dados pessoais, o que se denomina direito à autodeterminação informativa".

Especificamente com relação a esse princípio, uma vez mais, ela se vale das assertivas e preciosas lições de Daniel Martínez Fons , para quem:

> […] o consentimento da pessoa afetada é princípio essencial da relação de tratamento de dados […]. A aplicação de tecnologias que permitam coletar, armazenar e tratar dados de caráter pessoal exige, com caráter geral, o consentimento do afetado […]. Trata-se, portanto, de acordo com a doutrina, do "informed consent", isto é, um consentimento informado e plenamente consciente sobre a relação jurídico-privada que se constrói entre o responsável do ficheiro e o afetado (tradução e grifos nossos).

E completa a relação com os princípios: (i) Princípio da Dignidade da Pessoa Humana; (ii) Princípio da Não-Discriminação; e (iii) Princípio da Boa-Fé.

Para um real e efetivo efeito garantidor, hão de ser habilitados e reconhecidos alguns direitos suplementares: (a) direito de acesso; (b) direitos de retificação e de cancelamento; e (c) direito de oposição.

O empregado tem de ter acesso às informações que lhe dizem respeito. Deve-lhe ser facilitado o conhecimento, com simplicidade de caminhos para obtenção de todas as informações que concernem à sua vida (pessoal e profissional).

Neste sentido, Daniel Martínez Fons assegura que:

> […] não cabe impor restrições indiretas que desestimulem o exercício do direito de acessar; de maneira que se deve rejeitar qualquer prática neste sentido, tais como circunscrever o exercício do direito fora da jornada de trabalho ou que o tempo investido não seja considerado tempo de trabalho, submeter a questionários

> os trabalhadores que querem acessar, nem, enfim, estabelecer um registro autônomo dos trabalhadores que fazem uso de sua faculdade.

Quanto à periodicidade, Tatiana de Almeida Granja, entende que deve ser fixado "um intervalo mínimo entre os acessos dos trabalhadores aos seus próprios dados, evitando transtornos para a organização decorrentes de sucessivos e despropositados acessos [...] com o estabelecimento de exigências mínimas que demonstrem a legitimidade de interesse".

Por óbvio, quando houver necessidades excepcionais e justificáveis, esse período pode sofrer alterações para atender essas legitimas urgências.

Embora não haja regulamentação específica na legislação brasileira (fora da relação de trabalho) há de se interpretar que a tutela dos direitos privados abarca a proteção do trabalhador, com base nas garantias constitucionais, Código Civil e Consolidação das Leis do Trabalho.

Os dados poderão ser objeto de correção (Direitos de retificação e de cancelamento), por meio de cancelamento (exclusão física do dado) ou, em alguns casos, pelo simples bloqueio ao acesso.

Há, ainda, a possibilidade do exercício do Direito de oposição, facultado ao empregado apresentar justificativas legítimas para exposição e/ou manutenção de seus dados pessoais, uma espécie de jus resistentiae no contrato de trabalho.

Note-se que esse procedimento de controle é indispensável dentro do seio da sociedade eminentemente digital que vivemos. Como alerta, Fernanda Bruno, professora e pesquisadora da UFRJ, "os contornos modernos que conhecemos e herdamos – a separação público/privado e a definição de papéis em cada uma dessas esferas, a valorização da família, os direitos do indivíduo, a inviolabilidade do domínio privado, o direito ao segredo, à solidão, a proteção ao anonimato etc – foram resultado de embates na definição das relações entre o estado e a sociedade civil, o indivíduo e o coletivo. Logo, a privacidade, não sendo uma condição "natural", está sujeita a variações, mas estas não seguem um princípio "evolutivo" que levaria a sua extinção (como quer Zuckerberg, presidente do Facebook), mas são (e foram sempre) o efeito de embates sociais, políticos, econômicos. A história da privacidade é uma história política do cotidiano, onde a micro e a macro-política não cessam de se misturar. É nesse sentido que se deve compreender as recentes transformações nos seus limites. A privacidade hoje está em disputa. Não se trata de afirmar que ela existe ou deixou se existir, mas de compreender os discursos, forças e práticas que hoje disputam pelo sentido, valor e experiência da privacidade. Essa disputa é especialmente sensível no campo das redes distribuídas de comunicação. Assim, é preciso entrecruzar a disputa em torno da privacidade e as disputas políticas, econômicas, sociais, cognitivas e estéticas que se travam no âmbito dessas redes, de seus "bens" materiais e imateriais, de seus modelos de comunicação, circulação e produção de informação, conhecimento, cultura etc. Não raro (embora não necessariamente) os que clamam pelo fim da privacidade também clamam pelo controle da liberdade e do anonimato, ou pelo controle das práticas de compartilhamento e colaboração na rede ".

O importante, sem dúvida alguma, é o cuidado e a forma como são tratadas, divulgadas e destinadas às informações provenientes de dados pessoais do trabalhador (antes, durante e após a relação de emprego), na medida em que esses dados pessoais (e sua publicidade) estão sob um invólucro digital de duas ordens:

a) Uma primeira que pode ser chamada de mais superficial e visível, "onde as pessoas geram e disponibilizam voluntariamente e sobre os quais usualmente têm o controle do seu grau de visibilidade e publicidade (conforme as ferramentas disponibilizadas aos usuários, e nas quais inscrevem-se as nuances éticas da política de privacidade desses serviços e ambientes)"; e

b) uma segunda camada, que chamaremos de profunda, de dados que podem ou não conter meios de identificação dos indivíduos que os geraram. "Agregados em bancos de dados e submetidos a técnicas de mineração e profiling, tais dados geram mapas e perfis de consumo, interesse, comportamento, sociabilidade, preferências políticas que podem ser usados para os mais diversos fins, do marketing à administração pública ou privada, da indústria do entretenimento à indústria da segurança, entre outros. Neste caso, o controle do indivíduo sobre os seus próprios dados é bem menos evidente e a noção de privacidade (nos seus termos jurídicos) não dá conta da complexidade de questões sociais, políticas e cognitivas envolvidas" .

Logo, a proteção e guarda dos dados deve ser feita de maneira própria e complexa e não de modo amador e subjetivo, até porque o Marco Civil da Internet exige a proteção da privacidade do usuário, mas pede a manutenção, por um ano, de registros que possam identificar os autores dos acessos.

6. LGPD: Legislação Brasileira

A lei 13.709 de 14 de agosto de 2018 disciplinou a proteção de dados, dispondo sobre o tratamento de dados pessoais, inclusive nos meios digitais, por pessoa natural ou por pessoa jurídica de direito público ou privado, com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural.

Sendo assim, pode-se considerar como fundamentos legais (a) o respeito à privacidade; (b) a autodeterminação informativa; (c) a liberdade de expressão, de informação e de opinião; (d) a inviolabilidade da intimidade, da honra e da imagem; (e) o desenvolvimento econômico e tecnológico e a inovação; (f) a livre-iniciativa, a livre concorrência e a defesa do consumidor; (g) os diretos humanos, o livre desenvolvimento da personalidade, a dignidade e o exercício da cidadania pelas pessoas naturais.

Estão excluídos da aplicação da lei alguns meios de tratamento de dados realizados exclusivamente para fins artísticos, jornalísticos e acadêmicos. As informações relativas exclusivamente à segurança pública, defesa nacional e atividades de investigação, repressão de infrações penais.

Dentre os princípios que regem a legislação têm-se a (a) finalidade: realização do tratamento para propósitos legítimos, específicos, explícitos e informados ao titular,

sem possibilidade de tratamento posterior de forma incompatível com essas finalidades, (b) adequação: compatibilidade do tratamento com as finalidades informadas ao titular, de acordo com o contexto do tratamento, (c) necessidade: limitação do tratamento ao mínimo necessário para a realização de suas finalidades, com abrangência dos dados pertinentes, proporcionais e não excessivos em relação às finalidades do tratamento de dados, (d) livre acesso: garantia, aos titulares, de consulta facilitada e gratuita sobre a forma e a duração do tratamento, bem como sobre a integralidade de seus dados pessoais, (e) qualidade dos dados: garantia, aos titulares, de exatidão, clareza, relevância e atualização dos dados, de acordo com a necessidade e para o cumprimento da finalidade de seu tratamento, (f) transparência: garantia, aos titulares, de informações claras, precisas e facilmente acessíveis sobre a realização do tratamento e os respectivos agentes de tratamento, observados os segredos comercial e industrial, (g) segurança: utilização de medidas técnicas e administrativas aptas a proteger os dados pessoais de acessos não autorizados e de situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão, (h) prevenção: adoção de medidas para prevenir a ocorrência de danos em virtude do tratamento de dados pessoais, (i) não discriminação: impossibilidade de realização do tratamento para fins discriminatórios ilícitos ou abusivos, (j) responsabilização e prestação de contas: demonstração, pelo agente, da adoção de medidas eficazes e capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas.

Foi explícita ao disciplinar conceitos, partícipes e elementos integrativos de toda a cadeia relacionada à proteção de dados, considerando: I - dado pessoal: informação relacionada a pessoa natural identificada ou identificável; II - dado pessoal sensível: dado pessoal sobre 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; III - dado anonimizado: dado relativo a titular que não possa ser identificado, considerando a utilização de meios técnicos razoáveis e disponíveis na ocasião de seu tratamento; IV - banco de dados: conjunto estruturado de dados pessoais, estabelecido em um ou em vários locais, em suporte eletrônico ou físico; V - titular: pessoa natural a quem se referem os dados pessoais que são objeto de tratamento; VI - controlador: pessoa natural ou jurídica, de direito público ou privado, a quem competem as decisões referentes ao tratamento de dados pessoais; VII - operador: pessoa natural ou jurídica, de direito público ou privado, que realiza o tratamento de dados pessoais em nome do controlador; VIII - encarregado: pessoa indicada pelo controlador e operador para atuar como canal de comunicação entre o controlador, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (ANPD); IX - agentes de tratamento: o controlador e o operador; X - tratamento: toda operação realizada com dados pessoais, como as que se referem a coleta, produção, recepção, classificação, utilização, acesso, reprodução, transmissão, distribuição, processamento, arquivamento,

armazenamento, eliminação, avaliação ou controle da informação, modificação, comunicação, transferência, difusão ou extração; XI - anonimização: utilização de meios técnicos razoáveis e disponíveis no momento do tratamento, por meio dos quais um dado perde a possibilidade de associação, direta ou indireta, a um indivíduo; XII - consentimento: manifestação livre, informada e inequívoca pela qual o titular concorda com o tratamento de seus dados pessoais para uma finalidade determinada; XIII - bloqueio: suspensão temporária de qualquer operação de tratamento, mediante guarda do dado pessoal ou do banco de dados; XIV - eliminação: exclusão de dado ou de conjunto de dados armazenados em banco de dados, independentemente do procedimento empregado; XV - transferência internacional de dados: transferência de dados pessoais para país estrangeiro ou organismo internacional do qual o país seja membro; XVI - uso compartilhado de dados: comunicação, difusão, transferência internacional, interconexão de dados pessoais ou tratamento compartilhado de bancos de dados pessoais por órgãos e entidades públicos no cumprimento de suas competências legais, ou entre esses e entes privados, reciprocamente, com autorização específica, para uma ou mais modalidades de tratamento permitidas por esses entes públicos, ou entre entes privados; XVII - relatório de impacto à proteção de dados pessoais: documentação do controlador que contém a descrição dos processos de tratamento de dados pessoais que podem gerar riscos às liberdades civis e aos direitos fundamentais, bem como medidas, salvaguardas e mecanismos de mitigação de risco; XVIII - órgão de pesquisa: órgão ou entidade da administração pública direta ou indireta ou pessoa jurídica de direito privado sem fins lucrativos legalmente constituída sob as leis brasileiras, com sede e foro no País, que inclua em sua missão institucional ou em seu objetivo social ou estatutário a pesquisa básica ou aplicada de caráter histórico, científico, tecnológico ou estatístico; e XIX - autoridade nacional: órgão da administração pública responsável por zelar, implementar e fiscalizar o cumprimento desta Lei em todo o território nacional.

A LGPD prevê que o tratamento de dados só pode ser realizado nas seguintes hipóteses:

a) mediante o fornecimento de consentimento pelo titular;

b) para o cumprimento de obrigação legal ou regulatória pelo controlador;

c) pela administração pública, para o tratamento e uso compartilhado de dados necessários à execução de políticas públicas previstas em leis e regulamentos ou respaldadas em contratos, convênios ou instrumentos congêneres, observadas as disposições do Capítulo IV desta Lei;

d) para a realização de estudos por órgão de pesquisa, garantida, sempre que possível, a anonimização dos dados pessoais;

e) quando necessário para a execução de contrato ou de procedimentos preliminares relacionados a contrato do qual seja parte o titular, a pedido do titular dos dados;

f)para o exercício regular de direitos em processo judicial, administrativo ou arbitral;

g) para a proteção da vida ou da incolumidade física do titular ou de terceiros;

h) para a tutela da saúde, exclusivamente, em procedimento realizado

por profissionais de saúde, serviços de saúde ou autoridade sanitária;

i) quando necessário para atender aos interesses legítimos do controlador ou de terceiros, exceto no caso de prevalecerem direitos e liberdades fundamentais do titular que exijam a proteção dos dados pessoais; ou

j) para a proteção do crédito, inclusive quanto ao disposto na legislação pertinente.

A lei ainda determina que o titular tem direito ao acesso facilitado às informações sobre o tratamento de seus dados. Referidas informações devem ser disponibilizadas de forma clara, adequada e ostensiva acerca de, entre outras características previstas em regulamentação para o atendimento do princípio do livre acesso à finalidade específica do tratamento, sua forma e duração, observados os segredos comercial e industrial, com identificação e informações de contato do controlador, bem como sobre as informações acerca do uso compartilhado e responsabilidades dos agentes que realizarão o tratamento.

O controlador (pessoa física ou jurídica, de direito público ou privado), a quem compete as decisões referentes ao tratamento de dados pessoais, tem de obrigatoriamente indicar o encarregado pelo tratamento de dados pessoais. Esse encarregado será o responsável por aceitaras reclamações e comunicações dos titulares, prestar esclarecimentos e adotar providencias, receber comunicações da autoridade nacional de proteção de dados, bem como orientar os funcionários da entidade sobre as praticas que devem ser tomadas em relação à proteção de dados pessoais.

7. Conclusão: Proteção de Dados de mármore, não de murta.

A importância deste viés contratual quanto à proteção de dados, tem relevância estrutural e transversal, tanto que gerou até a criação de uma profissição nova e moldada à sua gerência e aplicabilidade, como é o caso do "diretor de proteção de dados". Em matéria específica sobre o tema, publicada no jornal O Estado de S. Paulo, destacou-se que "bancos, seguradoras, agências de publicidade e marketing e veículos de comunicação, todos procuram o mesmo profissional [..,] Data Protection Officer (diretor de proteção de dados, em tradução livre) ou DPO. Trata-se de responsável por elaborar estratégias sobre como coletar e proteger dados pessoais contra ciberataques, uma das novas exigências do Regulamento Geral Sobre Proteção de Dados Pessoais (GDPR). [...]. Com a entrada em vigor da GDPR, a União Europeia espera que o DPO seja capaz de dizer "não" a um presidente executivo que esteja a infringir as regras impostas pela legislação" .

O equilíbrio entre as inovações digitais, comércio eletrônico e vida privada tem de existir e ser regulado. Todo esse processo de publicidade direcionada, assistentes pessoais, redes sociais e serviços de geolocalização estão imbricados nos estágios acima relacionados e próprios da relação de emprego (melhor: de trabalho, em sentido lato), o que exige, portanto, precaução e definição de regras comportamentais contratuais com o fito de mitigar abusos e excessos, preservando-se a dignidade da pessoa humana.

O Regulamento Geral Sobre Proteção de Dados (GDPR) é um grande balizador do "como"

tratar o tema, uma vez que regulamenta direitos que incluem o acesso aos dados, retificação, direito ao esquecimento, direito à informação em caso de sinistro – como vazamento de dados –, direito à limitação de tratamento e, finalmente, direito à portabilidade de dados. Esse último muito inovador. O usuário vai poder transferir seus dados de um banco para outro, por exemplo, sem burocracia .

O momento, assim, valendo-se, aqui, da metáfora trazida por Leandro Karnal (lembrando Padre Vieira) é transformador: deve-se dar plena segurança jurídica à proteção de dados, lapidando-a em mármore e não de murta.

Destaca Karnal: "O padre Vieira criou uma ideia em seu Sermão do Espírito Santo, em 1657. Alguns povos, pensava o inaciano, são de difícil mudança e resistem à pregação do Evangelho. Diz o português que: 'Há umas nações naturalmente duras e constantes, as quais dificultosamente recebem a fé e deixam os erros de seus antepassados; resistem com armas, duvidam com o entendimento, repugnam com a vontade, cerram-se, teimam, argumentam, replicam, dão grande trabalho até se renderem; mas, uma vez rendidos, uma vez que receberam a fé, ficam nelas firmes, como estátuas de mármore; Não é necessário trabalhar mais nelas'. No caso desses povos, a conquista espiritual seria muito complexa e demorada. Uma vez realizada a tarefa hercúlea, a nova imagem seria dura como pedra e os convertidos ficariam apegados de forma definitiva à Boa-Nova. Haveria outros povos, como os indígenas do Brasil, que teriam comportamento oposto. Seria dóceis e receptivos ao novo modelo religioso. A facilidade da adesão seria acompanhada pela pouca constância no caminho de Jesus. Imediatamente cristianizados e com rapidez voltando às crenças antepassadas. No caso em questão, em vez de mármore, seria como esculpir em um arbusto, a murta, planta sobre a qual o jardineiro hábil pode produzir formas inventivas. Passadas algumas semanas (Vieira fala em 4 dias), o arbusto perde o modelo e retorna ao estado natural. No mundo clássico, a murta era dedicada à deusa Vênus/Afrodite, reforçando sua mutabilidade. Os 'gentios' do Novo Mundo eram alunos ambíguos: aceitariam tudo que lhes ensinavam e, teimosos, permanecem apegados ao seu universo de valores" .

Mais do que fundamental, imprescindível, se torna, assim, o respeito à garantia do controle de dados pessoais, por meio de políticas específicas e adequadas.

Referências bibliográficas

AGUIAR, Antonio Carlos. Direito do Trabalho 2.0: digital e disruptivo. São Paulo, LTr. 2018

ALIGHIERE, Dante, A Divina Comédia, Purgatório, Tradução e notas Italo Eugenio Mauro, Editora 34, São Paulo, 1998, 4ª reimpressão 2000.

ALMEIDA, Tatiana de. O Desafio da Proteção aos Dados pessoais do Trabalhador: a relação de trabalho. Disponível em: <http://direitoeti.com.br/artigos/o-desafio-da-protecao-aos-dados-pessoais-do-trabalhador-a-relacao-de-trabalho/> Acesso em 27 mai. 2018.

ALVES, Rubem. Concerto para corpo e alma. Papirus Editora. São Paulo, 2002.

BRUNO, Fernanda. O fim da privacidade

em disputa. Disponível em: <http://revistapontocom.org.br/edicoes-anteriores-artigos/o-fim-da-privacidade-em-disputa> Acessado em 27 mai.2018.

CARDONA RUBERT, Maria Belén. Informática y contrato de trabajo. Valencia: Tirant lo Blanch, 1999 apud GRANJA, Tatiana de Almeida. O desafio da proteção aos dados pessoais do trabalhador: a relação de trabalho. Disponível em: <http://direitoeti.com.br/artigos/o-desafio-da-protecao-aos-dados-pessoais-do-trabalhador-a-relacao-de-trabalho/> Acesso em 27 mai. 2018.

COLL, C; MONEREO, C (Org). Psicologia da educação virtual: aprender e ensinar com as tecnologias da informação e da comunicação. Tradução Naila Freitas. Porto Alegre: Armed

DUARTE, Roberto Dias, in Quem mexeu no meu currículo? Jornal O Estado de S. Paulo, 23 de outubro de 2011, p. 2, Caderno Empregos.

MARTÍNEZ FONS, Daniel. Tratamiento y protección de datos de los trabajadores en la relación de trabajo. Derecho social y nuevas tecnologías. Madrid: Consejo General del Poder Judicial, 2005 apud GRANJA, Tatiana de Almeida. O desafio da proteção aos dados pessoais do trabalhador: a relação de trabalho. Disponível em: <http://direitoeti.com.br/artigos/o-desafio-da-protecao-aos-dados-pessoais-do-trabalhador-a-relacao-de-trabalho/> Acesso em 27 mai. 2018.

Publicado originalmente na Revista Ltr : legislação do trabalho : Vol. 82, n. 6 (jun. 2018)