A CULTURA DE COMPLIANCE EM MATÉRIA DE PROTEÇÃO DE DADOS E SUA ADOÇÃO NO ÂMBITO LABORAL

The culture of compliance in relation to data protection and its adoption in the context of labor

Revista de Direito do Trabalho | vol. 214/2020 | p. 323 - 340 | Nov - Dez / 2020
DTR\2020\13289

Beatriz de Felippe Reis
Mestra em Direito pelo Programa de Pós-Graduação em Direito (UNESC). Especialista em Direito do Trabalho (UNISINOS). Graduada em Ciências Jurídicas e Sociais (UFRGS). Analista Judiciário do TRT4ª Região. Membro do CIELO LABORAL. bialippe@hotmail.com

Área do Direito: Trabalho
Resumo: O artigo abordou o compliance em matéria de proteção de dados e sua adoção no ambiente laboral. Baseado na doutrina e na legislação sobre a matéria, o objetivo foi demonstrar que os programas de compliance, também denominados de programas de governança em privacidade, funcionam como importante instrumento operacional e preventivo da ocorrência de violações aos direitos dos titulares de dados, na medida em que orientam os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD. Partindo disso, verificou-se que a implementação destes programas podem ocorrer tanto em pequenas como em grandes companhias, inclusive aquelas que operam nos meios digitais, sendo mais uma ferramenta à disposição das empresas, que devem proteger os dados pessoais dos seus trabalhadores.

Palavras-chave: Compliance – Governança em privacidade – LGPD – Proteção de dados – Relação laboral
Abstract: The article discussed the compliance in relation to data protection and its adoption in the work environment. Based on the doctrine and legislation on the matter, the objective was to demonstrate that compliance programs, also called privacy governance programs, function as an important operational and preventive instrument against the occurrence of violations of data subjects' rights, insofar as they guide treatment agents, translating LGPD's principles into its daily activities. Based on this, it was found that the implementation of these programs can occur in both small and large companies, including those that operate in digital media, being another tool available to companies, which must protect the personal data of their workers.

Keywords: Compliance – Governance in privacy – LGPD – Data protection – Labor relationship
Sumário:

Introdução

Com o advento da chamada sociedade da informação, o crescente uso da tecnologia favorece uma maior disponibilidade de informações, permitindo que o tratamento e a combinação de dados de caráter pessoal seja cada vez mais frequente. Tal prática permite revelar elementos sobre indivíduos específicos, podendo ensejar violação a direitos fundamentais dos seus titulares.

No tocante ao tema, nas relações de trabalho em especial, a necessidade de tutelar os dados pessoais e sensíveis é ainda mais premente, pois, ao adentrar nesses dados, o

empregador obtém informações que não revelam somente aptidões profissionais, mas também questões ligadas à privacidade e à intimidade do trabalhador.

Nesse contexto, dado o nível de desenvolvimento tecnológico, a urgência de se garantir maior segurança jurídica às relações, bem como o de se estabelecer uma legislação compatível com a de ouros países, o Congresso Nacional Brasileiro aprovou a Lei 13.709/2018 (LGL\2018\7222), de 14 de agosto de 2018, conhecida como a Lei Geral de Proteção de Dados – LGPD.

A referida lei dispõe sobre a proteção de dados pessoais. Trata-se de uma lei geral, mas que em conjunto com os seus princípios, bem como pela adoção de programas de compliance, reúne importantes instrumentos para garantir uma proteção efetiva no tratamento aos dados pessoais e sensíveis do trabalhador no ambiente laboral.

Partindo disso, o artigo fará uma breve abordagem sobre a cultura de compliance em matéria de proteção de dados, apontando os elementos mínimos que caracterizam um programa robusto. Posteriormente, examina-se a sua implementação, inclusive na chamada economia colaborativa, de forma a proteger os dados pessoais desses trabalhadores.

Por fim, com base na análise da bibliografia e legislação na matéria, o objetivo do artigo é fazer avançar a discussão sobre a criação de normas protetivas aos dados pessoais e sensíveis do trabalhador, ainda que a LGPD não estabeleça regras específicas sobre a proteção de dados no âmbito laboral, pois inegável que nestas relações há um campo fértil relacionado ao tratamento de dados.

1. Os dados pessoais dos trabalhadores e as boas práticas no seu tratamento

Na era digital, um dos grandes desafios que surge nas relações entre empregador e trabalhador consiste em como processar as informações de cunho pessoal sem comprometer o direito fundamental dos trabalhadores a uma eficaz e efetiva proteção de dados pessoais, na medida em que "a gestão da informação sobre si próprio tornou-se expressão fundamental do indivíduo" (FRAZÃO; OLIVA; ABILIO, 2019, p. 678).

Com efeito, frente à relevância do tema, a Organização Internacional do Trabalho – OIT, em 1997, ao aprovar o Repertório de Recomendações Práticas em matéria de proteção de dados pessoais dos trabalhadores, dispôs no item 5.11 que

"Os empregadores, os trabalhadores e seus representantes devem cooperar na proteção de dados pessoais e na elaboração de uma política de empresa que respeite a vida privada dos trabalhadores, de acordo com os princípios estabelecidos neste repertório[1] (OIT, 1997, p. 02, tradução nossa)."

Percebe-se, portanto, que uma das ações indicadas pela OIT para a tutela dos dados pessoais e sensíveis dos trabalhadores consiste, em outras palavras, na implementação dos chamados programas de compliance, os quais correspondem à noção de "conformidade com a legislação do Estado e com as demais normas de conduta que possam ser aplicáveis às pessoas de determinada organização" (ANDRADE, 2017, p. 76).

Assim, o termo corresponde

"à adesão da companhia a normas ou procedimentos de determinado setor. Seu objetivo primordial é o combate à corrupção. Diferentemente da ética, que é assumida com espontaneidade, o compliance está relacionado à responsabilidade legal [...]. Ser ético é agir voluntariamente com princípios morais para com a sociedade. Já compliance é cumprir com regras e regulamentos; é trabalhar ou agir dentro da lei. [...] Formado por leis, decretos, resoluções, normas, atos e portarias, o compliance é todo arcabouço regulatório aplicado pelas agências que controlam e regulam o setor no qual a empresa está inserida. As maiores e mais organizadas corporações também criam suas próprias normativas internas para direcionar o comportamento de seus diretores e executivos e,

assim, coibir comportamentos negativos, desvios de conduta e inconformidades (ANTONIK, 2016, p. 976 e 987)."

Ou seja, o compliance cuida

"da estruturação de políticas e procedimentos corporativos que se traduzam em ações sistemáticas com o objetivo de atender ao cumprimento aos preceitos normativos, a permitir a prevenção do ato ilícito ou, caso tal não seja possível, minorar seus efeitos e sancionar eventuais responsáveis (FRAZÃO; OLIVA; ABILIO, 2019, p. 683-684)."

No Brasil, o instituto ganhou relevo após os escândalos de corrupções políticas, tendo como marco principal a Lei Anticorrupção[2] ou Lei do Compliance, cujo instrumento normativo dispõe sobre a responsabilização administrativa e civil de pessoas jurídicas, de qualquer natureza ou formato societário, pela prática de atos contra a administração pública nacional ou estrangeira.

Assim, o compliance, também conhecido como programa de comprometimento ou programa de integridade[3], emergiu "como uma necessidade imposta pela sociedade em direção às empresas, de forma a exigir maior transparência e seriedade nas relações negociais" (LAZZARIN; CAVAGNOLI, 2018, p. 99).

Em um primeiro momento, prevaleceu o entendimento de que tais programas seriam apenas um mecanismo para minimizar a aplicação de sanções penais contra empresas e organizações privadas que praticassem atos de corrupção ao realizarem negócios com a Administração Pública.[4]

Apesar disso, a adoção do instituto não se ateve ao campo penal, pois o programa não se limita ao combate à corrupção, uma vez que há falhas que podem ser muito mais danosas para uma empresa, razão pela qual deve incluir áreas como a antitruste, tributária, ambiental, propriedade intelectual, trabalhista[5], assim como todos os campos suscetíveis a erros.

No caso específico do tratamento dos dados pessoais e sensíveis,

"diante da facilidade e imediatismo do compartilhamento de informações, pela exposição de conteúdos, privacidade e imagens, inegavelmente, há constante preocupação com a gestão dos riscos e danos decorrentes dessas atividades (BLUM; ZAMPERLIN, 2016)."

Dessa maneira, frente ao atual cenário marcado, por um lado, pelas alterações na lógica até então vigente quanto ao tratamento de dados e, por outro, pela necessidade de se conferir papel primordial na efetividade dos direitos e na prevenção de danos, a adoção de mecanismos de compliance consubstancia valioso instrumento desse viés operacional e preventivo, auxiliando na promoção de condutas compatíveis com a regulamentação legal.

Assim,

"seja por seu inerente dinamismo, seja por haver diversas lacunas para se viabilizar o cumprimento dos preceitos legais, o papel das ações dos agentes econômicos robustece-se ainda mais. A implementação de boas práticas no tratamento de dados pessoais possui estrondoso potencial para auxiliar no atendimento aos comandos gerais da lei de acordo com as particularidades de determinados agentes econômicos, bem como prevenir a ocorrência de violações aos direitos dos titulares, na medida em que permite orientar os agentes de tratamento, traduzindo para suas atividades cotidianas as premissas principiológicas da LGPD e concretizando vários dos seus standards e conceitos abertos (FRAZÃO; OLIVA; ABILIO, 2019, p. 682)."

Dessa forma, o caráter complementar das políticas de compliance tem grande serventia, isso porque

"a LGPD apresenta grande plasticidade, utilizando-se de diversos standards e conceitos abertos, que precisam ser necessariamente contextualizados diante da realidade de cada agente econômico, do contexto social e econômico e da evolução tecnológica do momento em que forem aplicados. Logo, é fundamental que, ao lado do papel regulamentador da autoridade nacional, os agentes econômicos possam também ter a iniciativa de dar concretude aos comandos legais, adaptando-os à sua realidade a partir dos incentivos e dos esclarecimentos que recebem do próprio Estado (FRAZÃO; OLIVA; ABILIO, 2019, p. 685)."

A propósito, o artigo 50 da LGPD, ao tratar das boas práticas e da governança, previu a implementação de programas de compliance, aos quais denominou de programas de governança em privacidade, nos seguintes termos:

"Art. 50. Os controladores e operadores, no âmbito de suas competências, pelo tratamento de dados pessoais, individualmente ou por meio de associações, poderão formular regras de boas práticas e de governança que estabeleçam as condições de organização, o regime de funcionamento, os procedimentos, incluindo reclamações e petições de titulares, as normas de segurança, os padrões técnicos, as obrigações específicas para os diversos envolvidos no tratamento, as ações educativas, os mecanismos internos de supervisão e de mitigação de riscos e outros aspectos relacionados ao tratamento de dados pessoais. § 1º Ao estabelecer regras de boas práticas, o controlador e o operador levarão em consideração, em relação ao tratamento e aos dados, a natureza, o escopo, a finalidade e a probabilidade e a gravidade dos riscos e dos benefícios decorrentes de tratamento de dados do titular. § 2º Na aplicação dos princípios indicados nos incisos VII e VIII do caput do art. 6º desta Lei, o controlador, observados a estrutura, a escala e o volume de suas operações, bem como a sensibilidade dos dados tratados e a probabilidade e a gravidade dos danos para os titulares dos dados, poderá: I – implementar programa de governança em privacidade que, no mínimo: a) demonstre o comprometimento do controlador em adotar processos e políticas internas que assegurem o cumprimento, de forma abrangente, de normas e boas práticas relativas à proteção de dados pessoais; b) seja aplicável a todo o conjunto de dados pessoais que estejam sob seu controle, independentemente do modo como se realizou sua coleta; c) seja adaptado à estrutura, à escala e ao volume de suas operações, bem como à sensibilidade dos dados tratados; d) estabeleça políticas e salvaguardas adequadas com base em processo de avaliação sistemática de impactos e riscos à privacidade; e) tenha o objetivo de estabelecer relação de confiança com o titular, por meio de atuação transparente e que assegure mecanismos de participação do titular; f) esteja integrado a sua estrutura geral de governança e estabeleça e aplique mecanismos de supervisão internos e externos; g) conte com planos de resposta a incidentes e remediação; e h) seja atualizado constantemente com base em informações obtidas a partir de monitoramento contínuo e avaliações periódicas; II – demonstrar a efetividade de seu programa de governança em privacidade quando apropriado e, em especial, a pedido da autoridade nacional ou de outra entidade responsável por promover o cumprimento de boas práticas ou códigos de conduta, os quais, de forma independente, promovam o cumprimento desta Lei (BRASIL, Lei 13.709, de 14 de agosto de 2018 (LGL\2018\7222))."[6]

Portanto, 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.

2. Elementos para um programa de compliance em matéria de proteção de dados

Embora o programa de compliance represente um passo importante para o tratamento de dados, para que as suas vantagens[7] sejam efetivamente materializadas, a doutrina elenca dez elementos mínimos que caracterizam a sua robustez, sendo estes aplicáveis ao compliance de dados no âmbito laboral.

O primeiro deles refere-se à avaliação contínua de riscos e atualização do programa. De acordo com este elemento, deve-se avaliar os riscos a que se submete a empresa (levando em consideração as suas peculiaridades, tais como a complexidade e a estrutura da organização). Com isso, será possível elaborar um programa personalizado que efetivamente se contraponha aos pontos mais sensíveis para a entidade.

Em se tratando de compliance de dados,

"a noção de tratamento de dados utilizada pela LGPD é ampla, de forma que é difícil se imaginar algum agente econômico que não esteja sujeito à atividade e aos riscos respectivos. Entretanto, o tipo e a intensidade do tratamento de dados, bem como os riscos a ele inerentes, podem variar consideravelmente entre os agentes econômicos, a exigirem uma atenta e individualizada análise. Não é sem razão que a própria LGPD já oferece uma importante referência desse tipo de avaliação, ao definir o relatório de impacto à proteção de dados como a 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 (art. 5º, XVII) (FRAZÃO; OLIVA; ABILIO, 2019, p. 687-688)."

Portanto, para garantir a efetividade do programa, torna-se fundamental avaliar os riscos envolvidos, bem como reavaliá-los constantemente, atualizando e adaptando as normas internas. Sobre o tema, Pinheiro (2019, p. 320) apresenta as seguintes reflexões:

"a conformidade à proteção de dados é o tipo de projeto contínuo, que exigirá uma revisitação da pauta periodicamente, visto que os negócios estão também em transformação, assim como a tecnologia, trazendo inovação e novas funcionalidades, logo o que é feito hoje sofrerá alterações em curto espaço de tempo e os procedimentos bem como a documentação sobre proteção de dados pessoais, precisará de atualização em intervalos não superiores a dois anos, especialmente no tocante às políticas de privacidade, termos de uso e contratos. Logo, ter a lei é apenas o começo de uma longa jornada que teremos que atravessar tanto no âmbito público como privado. Atender aos requisitos da nova lei exige investimento, atualização de ferramentas de segurança de dados, revisão documental, melhoria de processos e, acima de tudo, mudança de cultura."

O segundo elemento corresponde à elaboração de códigos de ética e conduta, os quais

"são acordos que estabelecem direitos e deveres de uma dada corporação e que devem ser respeitados e seguidos por seus colaboradores e demais envolvidos. [...] Recomenda-se que tais códigos estejam em conformidade, ou seja, que estejam em compliance com ideais democráticos, a dignidade da pessoa humana, leis trabalhistas, leis ambientais e demais normas pertinentes. No bojo dos códigos de ética torna-se interessante que estejam expressados princípios relacionados à proteção do patrimônio corporativo, à necessária transparência nas comunicações dentro e fora da corporação, ao assédio moral, assédio profissional, assédio sexual e outras formas de assédio, relacionamento interpessoal e parental entre colaboradores, bem como a ações relacionadas à denúncia em caso de práticas de suborno ou corrupção (CAMARGO; SANTOS, 2019, p. 221-231)."

A LGPD incentiva a criação de códigos de ética ou de conduta, de forma a tornar mais efetivo[8] o cumprimento das disposições por parte dos diferentes setores, tendo em consideração as suas especificidades, bem como a certificação[9] na área da proteção de dados e de selos de proteção.

O terceiro elemento diz respeito à organização compatível com o risco da atividade. Ou seja, o programa deve ser estruturado, aplicado e atualizado de acordo com as características e riscos das atividades de cada pessoa jurídica. Soma-se a isso, a

implementação de um setor independente e com recursos capazes de assegurar o respeito ao programa, além de representar padrão de conduta dos próprios administradores (FRAZÃO; OLIVA; ABILIO, 2019).

O comprometimento da alta administração corresponde ao quarto elemento. Isso requer o comprometimento dos gestores com a incorporação e a observância de uma cultura empresarial que aplique e valorize as melhores práticas de gestão para atingir a compliance, pois

"caso a gerência da pessoa jurídica manifeste-se de forma contraditória com os planos constantes no programa de compliance, a mensagem recebida pelos funcionários será de que esse não passa de simples instrumento de fachada (FRAZÃO; OLIVA; ABILIO, 2019, p. 690)."

Corroborando tal entendimento, Janoni e Gieremek (2013) advertem que

"se os colaboradores de uma empresa perceberem que não há coerência entre as disposições do Código e as práticas adotadas na organização (por exemplo, sonegação de impostos, pagamentos realizados 'por fora' do contrato de trabalho, condutas desrespeitosas aos direitos do trabalhador, maus-tratos), por mais bem feita que seja a norma, seguramente será tida como 'letra morta'."

O quinto elemento relaciona-se à autonomia e independência do setor de compliance, o qual poderá ser um setor específico dentro da empresa ou então um escritório especializado para este fim. Independentemente da situação, o setor deve ser dotado de poderes para implementar políticas, procedimentos e controles adequados, bem como ter capacidade para supervisionar e executar as normas previstas no programa, podendo tomar decisões sem a necessidade de recorrer a outras áreas.

O sexto elemento refere-se aos treinamentos periódicos, ou seja, as empresas devem promover treinamentos constantes e palestras explicativas tanto para os empregados quanto para os executivos, devendo ser consideradas as particularidades de cada setor e os riscos a que estão sujeitos, a fim de que todos compreendam o seu papel e contribuam para a minimização dos riscos. Para que isso aconteça

"O compliance deve ser ativo, explicativo e acessível a todos, permitindo que as regras a serem seguidas sejam de conhecimento geral, que a respectiva execução seja acompanhada e que eventuais atos infratores possam ser identificados e/ou denunciados (BLUM; ZAMPERLIN, 2016)."

O sétimo elemento corresponde à criação de uma cultura corporativa de respeito à ética e às leis. Está relacionada à instituição de medidas preventivas, podendo ser utilizadas para combater condutas antiéticas e ilegais. No caso da LGPD, Pinheiro (2019) aponta que tal lei representou uma primeira etapa, sendo agora necessário um prazo para o mercado amadurecer e se adaptar às novas exigências. Além disso, a efetiva implementação da lei geral de proteção de dados

"exige uma própria mudança de cultura, a fim de reconhecer que a titularidade e o controle dos dados pertencem aos respectivos titulares, de forma que as práticas empresariais deverão ser reestruturadas com esse propósito (FRAZÃO; OLIVA; ABILIO, 2019, p. 691)."

O monitoramento constante dos controles e processos, inclusive para fins de atualização do programa é enunciado como o oitavo elemento. A instituição do monitoramento permite identificar a existência de conflitos e possibilita a adoção de medidas corretivas (MATHIES, 2018). De modo mais específico, "outra peculiaridade do compliance de dados é que certamente precisará de atualizações conforme evolua o estado das tecnologias utilizadas para a proteção de dados" (FRAZÃO; OLIVA; ABILIO, 2019, p. 692).

O penúltimo elemento refere-se à implementação de canais seguros e abertos de comunicação de infrações e mecanismos de proteção dos informantes. Tais canais auxiliam no saneamento de dúvidas, difundem comportamentos de conformidade, facilitam o conhecimento de ilícitos pela empresa, permitem a adoção de medidas preventivas e impeditivas de novas condutas semelhantes, além de oportunizar a realização de denúncias (FRAZÃO; OLIVA; ABILIO, 2019).

Desse modo, o

"empregado deve saber que tem a quem recorrer e que será ouvido, sem riscos de retaliação. Daí a necessidade de canais de denúncias, que admitam o anonimato, a fim de preservar a identidade daquele que, corajosamente, decidiu dividir a sua dor ou mesmo expor uma fragilidade sistêmica, de controles, ou um fato concreto. [...] Com essa medida, tanto se divulgará que a empresa não tolera malfeitos, sejam de que natureza for, como ouve os seus colaboradores e apura com rigor os fatos que sejam trazidos ao seu conhecimento (JANONI; GIEREMEK, 2013)."

Contudo, além da implementação dos canais, é importante instruir os funcionários para que evitem o seu emprego malicioso, sendo "salutar também estabelecer procedimentos a serem adotados no caso de recebimento de denúncia para identificar aquelas que não possuem plausibilidade" (FRAZÃO; OLIVA; ABILIO, 2019, p. 693).

Por fim, a detecção, apuração e punição de condutas contrárias ao programa de compliance corresponde ao último elemento para identificar a sua robustez. Assim, "deve-se assegurar rápida e adequada punição às condutas a ele contrárias", sob pena de a credibilidade do programa ser abalada e todo o trabalho perdido (FRAZÃO; OLIVA; ABILIO, 2019, p. 693).

Destaca-se que, em se tratando de compliance de dados no âmbito laboral, não há um modelo único a ser seguido, porém, conforme exposto, a doutrina traça alguns elementos mínimos que, somado aos princípios previstos na LGPD, auxiliam na sua implementação. Ao lado destes, são apresentados três pilares, identificados como linhas mestras, responsáveis por dar a direção a ser adotada: prevenção, detecção e correção.

O pilar de prevenção é considerado o mais importante, cabendo à instituição empregadora investir a maior parte de seus recursos para garantir a segurança das informações dos trabalhadores, evitando acessos não autorizados, bem como situações acidentais ou ilícitas de destruição, perda, alteração, comunicação ou difusão.

Em outras palavras, é preciso lembrar que em matéria de proteção de dados, é muito mais difícil recuperar um dado ou uma informação violados do que defendê-los de uma primeira violação, especialmente se houver vazamento ou até mau uso dos dados sensíveis dos trabalhadores. (GOULART, 2014). Tal pilar se amolda ao poder diretivo de organização e direção do empregador (JOBIM, 2018). No sentido de se respeitar o princípio de prevenção, a doutrina fala no chamado

"Privacy Impact Assessment (PIA), algo semelhante a um Estudo de Impacto Ambiental, porém direcionado às atividades tecnológicas. Assim, qualquer atividade que envolvesse a possibilidade de violação de privacidade, deveria ser precedida do PIA, a fim de se verificar os possíveis impactos (GOULART, 2014, p. 80)."

O segundo pilar relaciona-se à detecção, assumindo papel fundamental a existência de canais de denúncia como forma de controle eficaz dentro do ambiente laboral (COMPLIANCE TOTAL, 2014). Este pilar pode ser desenvolvido por meio do poder diretivo fiscalizatório ou de controle do empregador (JOBIM, 2018).

Já o pilar da correção refere-se à tolerância zero para desvios em relação aos valores e princípios éticos da instituição. Ocorrendo uma falha, esta deve ser corrigida de imediato, seguida da medida disciplinar pertinente, sob pena da credibilidade do programa ser abalada e todo o trabalho perdido (COMPLIANCE TOTAL, 2014). Este pilar

fortalece o poder diretivo disciplinar do empregador (JOBIM, 2018).

Dessa forma, elencados os elementos mínimos caracterizadores de um programa de compliance robusto, bem como os pilares que podem auxiliar na sua execução no âmbito laboral, cabe examinar a sua adoção como ferramenta de proteção aos dados pessoais dos trabalhadores.

3. A implementação do compliance no ambiente laboral

Vale destacar que o compliance em matéria de proteção de dados não é uma realidade apenas para as grandes companhias. A Lei 13.709/2018 (LGL\2018\7222) aplica-se indistintamente a todas às pessoas natural ou jurídica de direito público ou privado, sem fazer distinção quanto ao porte[10]. Logo, implementar boas práticas para o tratamento dos dados pessoais dos trabalhadores e estar em conformidade com a legislação é uma exigência cada vez mais presente.

Nesse sentido, o próprio Conselho Administrativo de Defesa Econômica (CADE)

"entende que pequenas e médias entidades podem implementar programas de compliance, ainda que eles sejam mais modestos e contem com orçamentos muito reduzidos em face dos programas de grandes companhias (CADE, 2016)."

Portanto, ainda que estas empresas contem com quadro reduzido de trabalhadores, com menor fluxo de dados, guardadas as devidas proporções, elas podem implantar no âmbito laboral programas de compliance. Tal medida, se bem conduzida à luz dos elementos supramencionados, favorecerá o estabelecimento de uma cultura ética, pautada por normas e políticas internas que atendam às disposições da LGPD, evitando ou mitigando riscos reais e potenciais decorrentes do mau uso ou do uso abusivo dos dados aos direitos fundamentais do trabalhador.

Além dos elementos, dos princípios e dos pilares reportados, quando se fala em compliance de dados, surge outro aspecto de extrema importância: a regulação pela tecnologia. Embora a LGPD não se limite ao tratamento de dados no ciberespaço, é justamente neste cenário que ocorrem os maiores desafios.

Com efeito, como observa Bioni (2019, p. 05-06) a

"informação é o (novo) elemento estruturante que (re)organiza a sociedade, tal como o fizeram a terra, as máquinas a vapor e a eletricidade, bem como os serviços, respectivamente, nas sociedade agrícola, industrial e pós-industrial. Ainda que essa nova forma de organização social não se resuma apenas ao meio ambiente virtual, a computação eletrônica e a Internet são as ferramentas de destaque desse processo."

Disso decorre

"a necessidade de que os programas de compliance de dados não se limitem apenas à previsão de princípios ou regras de comportamento, mas visem também à adoção de tecnologias que possam ser compatíveis com a eficácia de tais regras (FRAZÃO; OLIVA; ABILIO, 2019, p. 710)."

Com relação ao ciberespaço e a circulação de dados, umas das grandes preocupações consiste em como proteger os dados dos trabalhadores na chamada economia colaborativa, isso, porque as relações de trabalho vêm passando por uma reconfiguração em âmbito mundial, sendo cada vez mais comum novas e emergentes formas de labor, especialmente aquelas por meio de aplicativos digitais.

Tamanha a relevância do tema que, na 108ª Conferência Internacional do Trabalho, em celebração ao Centenário da OIT, foi promulgada a Declaração do Centenário, a qual coloca o ser humano como o centro das políticas laborais e reconhece a necessidade de que se estabeleça um piso mínimo de direitos independente da natureza do vínculo de

emprego existente. O texto, além de reafirmar os princípios da Declaração da Filadélfia, assegura a todos os trabalhadores, independentemente do seu status, a garantia da proteção da privacidade e dos dados pessoais[11] (OIT, 2019).

A preocupação com os diretos fundamentais inespecíficos (em especial a privacidade, a proteção de dados e a reserva da intimidade) dos trabalhadores ganha ainda maior sentido frente ao atual contexto. Os gigantes dos aplicativos exercem um controle cada vez mais instrusivo e perigoso, feito à distância pelos algoritmos e pela inteligência artificial, que recolhem as pistas digitais deixadas (in)voluntariamente pela rede mundial de computadores. Em conjunto, tais "pistas" conferem um poder de controle da informação, permitindo aos seus detentores a realização de operações com os dados pessoais daqueles que lhe prestam serviço, bem como a criação de perfis. Disso decorre a necessidade de proteção dos dados pessoais e sensíveis destes trabalhadores digitais.

Sobre o tema, o Parlamento Europeu aprovou em 20 de junho de 2019 o Regulamento relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha. Trata-se um regulamento inédito, cujo objetivo é introduzir novas regras que proporcionem às empresas um enquadramento mais transparente, justo e previsível, e que tenha vias de recurso rápidas e eficientes.

No que tange aos dados, incluindo os dados pessoais, o mencionado Regulamento estabelece que cabe aos prestadores de serviços de intermediação em linha transmitir aos utilizadores profissionais uma descrição clara do âmbito de aplicação, da natureza e das condições de acesso e utilização de determinadas categorias de dados.[12]

Nesse sentido, importante destacar que a parte final do considerando 35 do Regulamento prevê expressamente que o

"tratamento dos dados pessoais deverá respeitar o regime jurídico da União relativo à proteção das pessoas singulares no que diz respeito ao tratamento de dados pessoais, ao respeito pela vida privada e à proteção dos dados pessoais nas comunicações eletrônicas, mais particularmente o Regulamento (UE) 2016/6791, a Diretiva (UE) 2016/6802 e a Diretiva 2002/58/CE3 do Parlamento Europeu e do Conselho (UNIÃO EUROPEIA, 2019)."

O Regulamento também estabelece obrigações de transparência para as plataformas digitais, obrigando estas a utilizarem termos e condições claros e inteligíveis para a prestação dos seus serviços de intermediação em linhas, fornecendo uma exposição de motivos quando decidirem suspender, restringir ou pôr termo à utilização dos seus serviços por um utilizador profissional. Somado a isso, prevê a necessidade de as plataformas divulgarem publicamente os principais parâmetros que determinam a classificação dos utilizadores nos resultados de pesquisa.

Embora a aprovação do Regulamento esteja restrita à União Europeia, trata-se de um primeiro passo para que as plataformas digitais divulguem os motivos porque estão suspendendo, por exemplo, um motorista de aplicativo, ou, ainda, os principais parâmetros utilizados nos hankings para a seleção de prestadores de serviços. Além disso, o Regulamento também obriga todas as plataformas (exceto as pequenas[13]) a criarem um sistema interno de tratamento de reclamações rápido e eficiente e a apresentarem anualmente um relatório sobre a sua eficácia.

Com efeito, revela-se de extrema importância a criação de um sistema que lide rapidamente com as queixas, isso, porque assim como os demais trabalhadores, os profissionais que prestam serviços por meio destas platafomas, também estão sujeitos a avaliações, a sanções disciplinares, a práticas de assédio, aos riscos à saúde (em razão do stress, das longas jornadas, dentre outros fatores), sem que houvesse até o presente momento a possiblidade de reclamação.

O Regulamento também exige que as plataformas incluam, nos seus termos e condições,

dois ou mais mediadores para os casos em que o sistema interno de tratamento de reclamações não permita resolver um litígio entre utilizadores empresariais. Ademais, estabelece o direito das organizações e associações representativas ou dos organismos públicos a iniciarem um processo judicial contra plataformas que não cumpram os requisitos do Regulamento, sendo autorizado os Estados-Membros definirem sanções conformes com os seus sistemas nacionais em caso de infração.

Logo, dada a peculiaridade das plataformas digitais, as quais contam com milhões de utilizadores profissionais e com atuação em âmbito mundial, tem-se que o regulamento da União Europeia, embora destinado às plataformas estabelecidas na UE e que ofereçam bens ou serviços a consumidores que também estejam localizados na UE, traça elementos característicos de um programa de compliance, inclusive com diretrizes que podem ser estendidas para a proteção aos dados pessoais dos trabalhadores que laboram utilizando-se de plataformas digitais.

Verifica-se, ainda, que o Regulamento prevê a elaboração de códigos de conduta por parte dos prestadores de serviços de intermediação em linha e das organizações e associações que os representem, juntamente com os utilizadores profissionais. Também estabelece que devem ser levadas em consideração as características específicas dos setores em causa. Além disso, os prestadores de serviços de intermediação devem disponibilizar facilmente as informações relativas ao funcionamento e à eficácia dos seus procedimentos internos de tratamento de reclamações, os quais são passíveis de atualização periódica. Ou seja, ainda que com outras palavras, o Regulamento traça elementos característicos de um programa de comprometimento para as empresas proprietárias de plataformas digitais.

No caso, quando estas empresas realizam o tratamento dos dados pessoais e sensíveis dos utilizadores profissionais, elas também se tornam responsáveis pela segurança destes dados, sendo a implementação do compliance uma forma eficaz de protegê-los. E, tendo em vista que estas empresas atuam, sobretudo em meio digital, a tecnologia também pode ser utilizada como um importante instrumento para a promoção dos programas de integridade de dados.

"Se por um lado, a tecnologia pode ser invasiva à privacidade informacional, [...] por outro lado, ela pode ser uma ferramenta para a proteção dos dados pessoais, tal como propõem as denominadas Privacy Enhancing Technologies/PETs[14] (BIONI, 2019, p. 176)."

Logo, as PETs apresentam-se como uma possível solução para a equalização das assimetrias do mercado informacional, a fim de que o cidadão-trabalhador, titular dos dados, diante da sua (hiper)vulnerabilidade, possa ser empoderado com um melhor controle sobre as suas informações.

Portanto, seja para as típicas relações de trabalho, seja para as novas configurações, a implementação dos programas de compliance contribuem para garantir o cumprimento das normas de proteção aos dados pessoais e sensíveis dos trabalhadores, promovendo uma ambiente de confiança entre os seus titulares, fundamental em uma sociedade marcada pelo grande fluxo de informações.

Conclusão

Com o uso intensivo das novas ferramentas tecnológicas e do cruzamento de dados no ambiente laboral, somada à recente aprovação do regime geral de proteção de dados no Brasil, questões envolvendo o tratamento dos dados pessoais e sensíveis do trabalhador ganham relevo e geram preocupações que transcendem o espaço acadêmico.

No Brasil, a recente aprovação da Lei Geral de Proteção de Dados em 2018, impôs às empresas que realizam o tratamento de dados, compreendido neste toda operação envolvendo a coleta, classificação, utilização, acesso, reprodução, transmissão,

distribuição, processamento, armazenamento, eliminação e transferência de dados pessoais, uma série de deveres e obrigações a serem observados de forma a proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade dos titulares de dados pessoais.

No campo das relações de trabalho, a situação fica ainda mais preocupante pois diante da falta de regulamentação, questões envolvendo a obtenção e o uso por parte do empregador de dados e informações relativas ao trabalhador acabam não recebendo o tratamento adequado por parte das empresas empregadoras no que tange ao resguardo do seu conteúdo.

Assim, diante da necessidade de se adotar medidas capazes de comprovar a observância e o cumprimento das normas de proteção de dados pessoais e, inclusive, da eficácia dessas medidas, o que abrange aquelas que se desenvolvem no ambiente laboral, verificou-se que a implementação dos programas de compliance em matéria de proteção de dados, também conhecidas como padrões de boas práticas e da governança, podem funcionar positivamente garantindo o direito fundamental dos trabalhadores quanto à proteção dos seus dados.

Por fim, como visto, tais programas, somados às denominadas Privacy Enhancing Technologies/PETs, contribuem para a prevenção da ocorrência de violações aos direitos dos titulares de dados, na medida em que traçam orientações aos agentes de tratamento, transpondo para suas atividades cotidianas as premissas principiológicas da Lei Geral de Proteção de Dados, independente do porte da empresa e da sua atuação, se em meio digital ou seguindo o modelo tradicional.

Referências

ANDRADE, Flávio Carvalho Monteiro de; FERREIRA, Isadora Costa. Compliance trabalhista: compreendendo a prevenção de risco trabalhista por meio de programa de integridade. Revista Síntese: trabalhista e previdenciária. São Paulo, v. 28, n. 331, p. 73-84, jan. 2017.

ANTONIK, Luis Roberto. Compliance, ética, responsabilidade social e empresarial: uma visão prática. Rio de Janeiro: Alta Books, 2016. Edição do Kindle.

BIONI, Bruno Ricardo. Proteção de dados pessoais: a função e os limites do consentimento. Rio de Janeiro: Forense, 2019.

BLUM, Renato Opice; ZAMPERLIN, Emelyn. Compliance, responsabilidade empresarial e segurança da informação. Lex Magister, Porto Alegre, 23 jun. 2016. Disponível em: [www.lex.com.br/doutrina_27159943_compliance_responsabilidade_empresarial_e_seguranca_da_infor
Acesso em: 26.10.2019.

CAMARGO, Coriolano Almeida; SANTOS, Cleorbete. Fundamentos do compliance. 2019. Edição do Kindle.

COMPLIANCE TOTAL. Pilares de um mecanismo de integridade e sistema de compliance. Texto baseado no conteúdo do livro "Compliance – A excelência na prática" de Wagner Giovanini. 2014. Disponível em: [www.compliancetotal.com.br/compliance/pilares]. Acesso em: 14.10.2019.

CONSELHO ADMINISTRATIVO DE DEFESA ECONÔMICA (CADE). Guia para programas de compliance. Brasília, 2016. Disponível em: [www.cade.gov.br/acesso-a-informacao/publicacoes-institucionais/guias_do_Cade/guia-compliance-vers
Acesso em: 11.01.2019.

FRAZÃO, Ana; OLIVA, Milena Donato; ABILIO, Vivianne da Silveira. Compliance de dados pessoais. In: FRAZÃO, Ana; TEPEDINO, Gustavo; OLIVA, Milena Donato (Coords.). A lei geral de proteção de dados pessoais e suas repercussões no direito brasileiro. São Paulo:

Thomson Reuters Revista dos Tribunais, 2019. p. 677-715.

GOULART, Guilherme Damasio. Limites do BYOD: entre o poder do empregador e a proteção dos direitos da personalidade do empregado. Revista de direito do trabalho, São Paulo, v. 40, n. 159, p. 71-86, set.-out. 2014.

JANONI, Daniella; GIEREMEK, Rogéria. Relações de trabalho e compliance: parceria necessária. São Paulo, 01 fev. 2013. Disponível em: [www.administradores.com.br/noticias/carreira/relacoes-de-trabalho-e-compliance-parceria-necessaria/ Acesso em: 26.10.2019.

JOBIM, Rosana Kim. Compliance e trabalho: entre o poder diretivo do empregador e os direitos inespecíficos do empregado. Florianópolis: Tirant Lo Blanch, 2018.

LAZZARIN, Sonilde Kugel; CAVAGNOLI, Fernanda Onzi. Compliance trabalhista. Revista Fórum Justiça do Trabalho. Belo Horizonte, v. 35, n. 417, p. 95-110, set. 2018.

MATHIES, Anaruez. Assédio moral e compliance na relação de emprego: dos danos e dos custos e instrumentos de prevenção. Curitiba: Juruá, 2018. p. 131-181.

MUNIZ, Mirella Karen de Carvalho Bifano; DIAS, Ronaldo Mayrink de Castro Garcia. Compliance e direito do trabalho: novas práticas para mitigar novos riscos. LTr Suplemento Trabalhista, São Paulo, v. 52, n. 094, p. 529-537, nov. 2016.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT). ILO Centenary Declaration. Geneva: International Labour Office, 2019. Disponível em: [www.ilo.org/wcmsp5/groups/public/---ed_norm/---relconf/documents/meetingdocument/wcms_70062 Acesso em: 03.11.2019.

ORGANIZACIÓN INTERNACIONAL DEL TRABAJO (OIT). Repertorio de recomendaciones prácticas de la OIT. Ginebra: Oficina Internacional del Trabajo, 1997. Disponível em: [www.ilo.org/wcmsp5/groups/public/---ed_protect/---protrav/---safework/documents/normativeinstrum Acesso em: 23.08.2018.

PINHEIRO, Patrícia Peck Garrido. Nova lei brasileira de proteção de dados pessoais (LGPD) e o impacto nas instituições públicas e privadas. Sociedade da informação: inquietudes e desafios. Revista dos Tribunais, São Paulo, v. 1000, ano 108, p. 309-323, fev. 2019.

UNIÃO EUROPEIA. Regulamento do Parlamento Europeu e do Conselho. Relativo à promoção da equidade e da transparência para os utilizadores profissionais de serviços de intermediação em linha. Disponível em: [https://data.consilium.europa.eu/doc/document/PE-56-2019-INIT/pt/pdf]. Acesso em: 04.11.2019.

---

1 .“Los empleadores, los trabajadores y sus representantes deberían cooperar en la protección de los datos personales y en la elaboración de una política de empresa que respete la vida privada de los trabajadores, con arreglo a los principios enunciados en el presente repertorio”.

2 .Lei 12.846, de 1º de agosto de 2013.

3 .O Decreto 8.420/2015, de 18 de março de 2015, que regulamenta a Lei 12.846/2013, disciplinou em seu artigo 41 os programas de integridade para designar os programas de compliance. Cabe, ainda, destacar a recente publicação do Decreto 9.751, de 21 de novembro de 2018, que estabelece as diretrizes nacionais sobre empresas e direitos

humanos, o qual também prevê em seu artigo 10 a criação e manutenção de programas integridade.

4 .Tal noção se explica, na medida em que a origem dos programas de compliance remonta ao ano de 1977, quando o Governo dos Estados Unidos da América promulgou o Foreign Corrupt Practices Act (FCPA), momento em que o pano de fundo era o escândalo de corrupção conhecido como Watergate (MUNIZ; DIAS, 2016, p. 530).

5 .Na seara laboral, embora inexista uma lei específica sobre compliance, a sua implementação deve nortear-se pela legislação trabalhista, pela observância dos direitos de personalidade do trabalhador, pela adesão às práticas de governança corporativa, pela criação de um código de ética ou código de conduta, pelo oferecimento de treinamento aos trabalhadores para melhor desempenho de suas funções, pela implementação de canais de denúncia, dentre outras (LAZZARIN; CAVAGNOLI, 2018).

6 .Com relação ao dispositivo, o legislador segmenta as regras corporativas em "'regras de boas práticas e de governança' – previstas no caput do art. 50 – e o 'programa de governança em privacidade' – previsto exclusivamente para os controladores no § 2º. Enquanto o primeiro parece preocupar-se mais com os aspectos operacionais do processo de tratamento dos dados, de modo a servir como instrumento de definição dos padrões técnicos e dos mecanismos em que se estruturarão o sistema a ser empregado; ao segundo foi conferido escopo mais amplo (como sói acontecer na elaboração das normas de governança corporativa), cogitando-se também das garantias aos titulares dos dados. Em qualquer dos casos, ressalta-se no caput, no § 1º e no § 2º o fator risco é primordial" (FRAZÃO; OLIVA; ABILIO, 2019, p. 701).

7 .São "vantagens tradicionalmente atribuídas aos programas de compliance – (i) permitir a adequada gestão do risco da atividade – na medida em que identifica os pontos sensíveis em que há exposição ao descumprimento – e, por consequência, auxiliar na prevenção de ilícitos; (ii) viabilizar a pronta identificação de eventual descumprimento, bem como a remediação de danos daí decorrentes, auxiliando, assim, na minoração dos prejuízos; (iii) fomentar a criação de uma cultura corporativa de observância às normas legais; e (iv) servir potencialmente como atenuante no caso de punições administrativas –, na tutela de dados soma-se à vantagem adicional de adaptar e operacionalizar diversos dos comandos gerais e conceitos abertos da LGPD. Podem-se enumerar, ainda, benefícios, ainda que indiretos, concernentes ao desenvolvimento em qualidade e inovação, além de incrementos reputacionais (FRAZÃO; OLIVA; ABILIO, 2019, p. 686).

8 ."Para garantir sua efetividade, tais instrumentos devem fixar deveres expressos e concretos, bem como ser de simples leitura, valendo-se de linguagem clara e direta. Afinal, destinam-se a todos os setores da pessoa jurídica e, sem que seus funcionários sejam capazes de compreender os preceitos ali contidos, não será viável sua observância. Recomenda-se, ainda, que os documentos sejam de fácil e constante acesso, sem prejuízo de sua disponibilização periódica, ainda que não haja mudanças, e que se estruturem canais para dúvidas e esclarecimentos" (FRAZÃO; OLIVA; ABILIO, 2019, p. 689).

9 .Soma-se a isso, a edição da ISO 19600:2014, pela Organização Internacional de Normatização (International Organization of Standardization – ISO), a qual estabelece diretrizes para desenvolvimento, implantação, manutenção e avaliação do sistema de gestão de compliance. Trata-se de uma padronização, cuja adesão é voluntária, porém importante para a disseminação do compliance, "pois a tendência é que as empresas

passem a exigir de seus fornecedores a certificação de implantação de normas estabelecidas na referida regra" (MATHIES, 2018, p. 141-142).

10 .Nesse sentido, verifica-se que o legislador esteve atento a tal questão, tanto que, ao tratar das "boas práticas e da governança", estabeleceu, no artigo 50, § 2º, que a estrutura, a escala e o volume das operações deverão ser levados em conta, o que viabiliza a implementação de programa de compliance em matéria de dados independentemente do tamanho da empresa.

11 .Item III, "B", "v", da Declaração do Centenário da OIT.

12 .De acordo com o considerando 34 do Regulamento, "é importante que os utilizadores profissionais tenham conhecimento se o prestador de serviços partilha com terceiros alguns dados que tenham sido gerados pela utilização do serviço de intermediação por parte do utilizador profissional. Em especial, os utilizadores profissionais deverão ser informados de toda a partilha de dados com terceiros que ocorra para fins não necessários ao bom funcionamento dos serviços de intermediação em linha; por exemplo, caso o fornecedor utilize esses dados para fins lucrativos. Para que os utilizadores profissionais possam exercer plenamente os seus direitos de influenciar esta partilha de dados, os prestadores de serviços de intermediação em linha deverão também ser explícitos relativamente a eventuais faculdades de autoexclusão da partilha de dados previstas na sua relação contratual com o utilizador profissional" (UNIÃO EUROPERIA, 2019).

13 .De acordo com o considerando 38 do Regulamento, tendo em conta os custos, os prestadores de serviços de intermediação em linha que sejam pequenas empresas (em conformidade com as disposições da Recomendação 2003/361/CE da Comissão, de 6 de maio de 2003, relativa à definição de micro, pequenas e médias empresas), estão isentos da obrigação de implementar procedimentos internos de tratamento de reclamações. Contudo, nada impede que estas empresas venham a estabelecer de forma voluntária tais procedimentos, devendo, no caso, observar os critérios definidos no regulamento (UNIÃO EUROPEIA, 2019).

14 .Segundo a tradução literal – PETs correspondem a "tecnologias que reforçam-melhoram a privacidade – denota abrangência do termo que, como um guarda-chuva, é capaz de abarcar toda e qualquer tecnologia que seja amigável e facilitadora à privacidade." Como exemplo dessas tecnologias, menciona-se "a criptografia que assegura a confidencialidade das comunicações. Ou, ainda, a anonimização dos dados pessoais que quebra ou pelo menos dificulta o vínculo de identificação entre um dado e o sujeito ao qual ele está atrelado [...], bem como mecanismos de navegação anônima que impedem o rastreamento do usuário" (BIONI, 2019, p. 176-177).