COMPLIANCE DIGITAL LABORAL

SUMÁRIO

1. Introdução
2. *Compliance* digital laboral - Brazil
3. Principais normas e instrumentos
4. *Privacy by Design* e *by Default*
5. Contratos de trabalho
6. *Compliance* digital laboral – Portugal
7. Estratégia anticorrupção Portuguesa
8. Futuro do trabalho
9. Conclusão

CONTACTOS

GUILHERME DRAY
GDRAY@MACEDOVITORINO.COM

DENISE FINCATO
DENISE@DENISEFINCATO.COM.BR

1. INTRODUÇÃO

O *Compliance* laboral obriga não só ao cumprimento das normas legais aplicáveis (*hard law*), mas também à adoção de boas práticas empresariais (*soft law*) que não decorrem da lei estrita e que, em contexto laboral, podem incidir sobre questões como a igualdade e não discriminação, assédio moral e sexual, cidadania no trabalho, entre outros aspetos. Em regra, estas boas práticas decorrem de códigos de conduta, regulamentos internos e convenções coletivas de trabalho.

As empresas têm, naturalmente, maior resistência em adotar regras que não lhes são impostas por lei. No entanto, esta complementaridade entre o que decorre da lei e aquilo que resulta da chamada *soft law* é essencial para o cumprimento da legislação laboral, para colmatar eventuais lacunas existentes na relação entre trabalhador e empregador e para promover bons ambientes de trabalho e o bem-estar dos trabalhadores.

Nas últimas décadas, assistimos a uma grande consciencialização das empresas na sua responsabilidade social, moral e ambiental, à luz do conceito de "**ESG** – Environment, Social, and Governance", o que melhorou a aplicação da igualdade no local de trabalho e a defesa de outros temas ligados aos direitos de cidadania, como sejam a prevenção do assédio e a implementação de políticas de privacidade e de proteção de dados pessoais.

Com o estabelecimento de políticas de *compliance* e, consequentemente, com a preocupação das empresas em assegurar o "bem comum", os efeitos reputacionais são imediatos, na medida em que as empresas se tornam mais apelativas no mercado laboral, construindo um bom ambiente de trabalho que, indiscutivelmente, levará à atração de talento e a um aumento de produtividade.

O *Compliance* laboral tem passado, nomeadamente, pela implementação de códigos de conduta contra o assédio, de políticas de igualdade de género, nomeadamente salarial, pela criação de canais de denúncia para proteger os denunciantes de infrações conhecidas em ambiente de

trabalho, bem como pela criação de códigos de ética e conduta e de programas de cumprimento normativo para prevenir o branqueamento de capitais e práticas de corrupção.

A obrigação de implementação destes instrumentos de *soft law*, em certos casos, decorre da legislação laboral ou de alguns diplomas legais avulsos. Noutros casos, estas políticas decorrem das convenções coletivas de trabalho negociadas entre as empresas e os sindicatos.

2. *COMPLIANCE* DIGITAL LABORAL NO BRASIL

No Brasil, a Lei nº 12.846/13, denominada Lei Anticorrupção, regulamentada pelo Decreto nº 8.420/15, evidencia a importância da adoção de um adequado programa de *Compliance* para as empresas brasileiras e da prática de um sistema efetivo de governança corporativa capaz de implementar uma cultura de prevenção e de fortalecimento da transparência e da ética, ao dispor sobre a responsabilidade das pessoas jurídicas pela prática de actos (lesivos) contra a administração pública.

O Programa de Integridade, instituído pelo Decreto nº 8.420/15 no seu capítulo IV, artigo 41, ao prever um conjunto de procedimentos e ferramentas de integridade a serem aplicados internamente nas empresas com o objetivo de combater a corrupção, trouxe ao ordenamento jurídico brasileiro os primeiros indícios da necessidade de adoção de um autêntico programa de *Compliance*.

Nesse sentido, a Lei nº 12.846/13 impulsionou, ainda mais, a adoção de mecanismos inerentes ao *Compliance* pelas organizações, estabelecendo a redução das sanções previstas para as empresas que comprovarem a sua cooperação no apuramento e análise de infrações, incluindo a aplicação de procedimentos internos de integridade e auditoria. A Lei também estimulou a implementação de canais de denúncia e códigos de ética, consoante incisos VII e VIII, do art 7º, ferramentas estas comuns ao programa de *Compliance*.

3. PRINCIPAIS NORMAS E INSTRUMENTOS DOS PROGRAMAS DE *COMPLIANCE* DIGITAL LABORAL, COM DESTAQUE PARA A LGPD

A fim de garantir a permanência dos dados e atividades dentro dos ditames legais, o *Compliance* acentuou-se no meio digital a partir da entrada em vigor da Lei Geral de Proteção de Dados (**LGPD**), Lei nº 13.709/2018, que evidenciou ser imprescindível a adoção de mecanismos específicos (e eficazes) nos programas de integridade.

Observa-se que a abrangência da incidência da **LGPD** enseja a adaptação não somente dos setores relativos à coleta de informações, mas também das demais operações que demandem a utilização de dados relacionados ou relacionáveis a pessoais singulares, repercutindo-se, também e, portanto, nas relações de trabalho.

No Brasil, a privacidade e a intimidade são direitos fundamentais (art. 5º, LXXIX, da CF/88), mas, diferentemente do **RGPD** (Regulamento Geral de Proteção de Dados), a **LGPD** não contempla expressa disposição sobre sua aplicação às relações de trabalho, o que, todavia, é indiscutível. A relação de trabalho sequer teria como se iniciar e desenvolver sem o tratamento dos dados pessoais coletados nas diversas fases do contrato individual de trabalho dos trabalhadores ou de candidatos a emprego. A lacuna legal apontada, entretanto, permite que o sistema normativo brasileiro se abra ao direito comparado (art. 8º da **CLT**) e, com isto, ao revés da aparente desproteção, os padrões internacionais passam a ser de possível utilização nas relações laborais brasileiras.

Nesse sentido, verifica-se que o *Compliance* digital laboral assume um papel fundamental, tornando-se necessário rever os padrões de conduta estabelecidos para o cumprimento de outras normas, de modo a evitar, por exemplo, a recolha de dados dispensáveis ou cujo tratamento possa ser considerado discriminatório.

4. MÉTODOS *PRIVACY BY DESIGN* E *PRIVACY BY DEFAULT*

O **RGPD** foi pioneiro ao introduzir dois novos conceitos chamados de *Privacy by Design* e *Privacy by Default*. A **LGPD** não adotou tais princípios expressamente, mas traz alguns conceitos similares ao descrever as medidas que as empresas devem tomar para proteção dos dados, especialmente no artigo 46.º, n.º 2, da **LGPD**.

Privacy by Design significa garantir a proteção dos dados desde a concepção do projeto e pode ser melhor compreendido analisando-se os seus sete princípios informadores. São eles: (i) atuação proativa e não reativa, preventivas e não corretivas; (ii) privacidade incorporada ao design; (iii) funcionalidade completa; (iv) segurança de ponta a ponta; (v) visibilidade e transparência; (vi) respeito pela privacidade do utilizador o e (vii) privacidade como configuração padrão (*Privacy by Default*).

Pode-se dizer que o *Privacy by Default* é uma decorrência do *Privacy by Design*. A ideia de *Privacy by Default* é de que a privacidade deve ser sempre a configuração padrão em qualquer sistema ou mesmo prática de negócio, e que o usuário deve liberar o acesso à coleta de mais informações se preferir, de modo a que os aplicativos coletariam somente o necessário. Em outras palavras, deve ser sempre respeitada a decisão do usuário (direito à autodeterminação informativa), já que os dados são propriedade dele.

As metodologias citadas permitem começar um projeto já de forma aderente à **LGPD**, reduzindo custos com adequação posterior à lei.

5. POSSIBILIDADES DE INSERÇÃO DE CLÁUSULAS DE *COMPLIANCE* LABORAL DIGITAL APLICÁVEIS AOS CONTRATOS DE TRABALHO

A **LGPD** introduziu a função de "encarregado de dados" (também conhecido como *Data Protection Officer* - **DPO**) no Brasil, sendo este a pessoa que actua como canal de comunicação entre a instituição, os titulares dos dados e a Autoridade Nacional de Proteção de Dados (**ANPD**). Porém, o legislador preferiu ser mais flexível quanto à função do encarregado, se comparado com outras legislações como, por exemplo, o **RGPD**.

Em se tratando de *Compliance* de dados no âmbito laboral, não há um modelo único de implementação a ser seguido, porém, há três pilares que o auxiliam: a prevenção, a detecção e a correcção.

O pilar de prevenção é considerado o mais importante, cabendo ao empregador investir a maior parte de seus recursos para garantir a segurança das informações dos trabalhadores. O segundo pilar, da detecção, relaciona-se com a existência de canais de denúncia como forma de controlo no local de trabalho. Já o pilar da correcção estabelece que, ocorrendo uma falha, deve esta ser corrigida de imediato.

Sabe-se da presunção de assimetria na relação empregador-trabalhador, o que torna improvável que o consentimento possa ser única e exclusiva considerado fundamento jurídico para o tratamento de dados no local de trabalho, a menos que os trabalhadores possam retirá-lo a qualquer momento e sem consequências adversas, conforme o Parecer nº 2/2017 sobre o tratamento de dados no local de trabalho, do Grupo de trabalho do artigo 29º para a proteção de dados. A execução de um contrato e o interesse legítimo podem, por vezes, ser invocados como suporte para o tratamento de dados nas relações de emprego, desde que o tratamento seja estritamente necessário para uma finalidade legítima e respeite os princípios da proporcionalidade e da subsidiariedade.

Ressalta-se que as empresas de pequeno porte possuem um tratamento diferenciado, mas não estão isentas do cumprimento de dispositivos da legislação em questão. A flexibilização da legislação para os pequenos negócios, em resumo, refere-se à simplificação quanto ao tratamento de dados e à comunicação de incidentes de segurança (comunicação que poderá ser feita a partir

de modelo disponibilizado pela própria Autoridade Nacional de Proteção de Dados - conforme a Resolução CD/ANPD no 2, de 27 e janeiro de 2022, a qual regula a aplicação da **LGPD** para agentes de tratamento de pequeno porte).

6. PORTUGAL - *COMPLIANCE* DIGITAL E PROTEÇÃO DE DADOS

A palavra *compliance* tem origem no verbo inglês "*to comply* (*with*)", que significa "agir de acordo (com)", "em conformidade (com)". Podemos, assim, dizer (de forma simples) que o "*Compliance*" é o mecanismo utilizado para se atingir a conformidade e se estar conforme, pelo que pode ser simultaneamente um meio (para atingir a conformidade) e um fim em si mesmo (o estar conforme).

A conformidade pode ser jurídica, tecnológica, de gestão, entre outras, e é transversal a qualquer organização, independentemente da sua natureza pública ou privada, área de atividade e até dimensão.

O processo de conformidade, quando seja direcionado ao ambiente ciberespacial e digital, não é mais nem menos do que aquilo a podemos designar por *Compliance* digital. Ou seja, a adoção de um conjunto de regras, processos e procedimentos pelas empresas para proteger os seus dados e que constituem um dos seus activos mais valiosos ou se se quiser um dos seus activos estratégicos.

Por essa razão, é essencial integrar o *Compliance* digital na estratégia de negócio das organizações. Qualquer atividade empresarial pressupõe necessariamente operações de tratamento de dados pessoais e não pessoais, o que deve ser feito em cumprimento da legislação europeia e nacional.

No âmbito da proteção de dados não pessoais, o Parlamento Europeu adotou o Regulamento n.º 2018/1807, de 14 de novembro de 2018, que visa promover a livre circulação dos dados eletrónicos não pessoais na União Europeia. Por contraposição a "dados pessoais", os dados não pessoais são informações que não se reportam diretamente a uma pessoa singular (indivíduo) identificada ou identificável. Exemplos de dados não pessoais são conjuntos de dados agregados e anonimizados utilizados para a análise de grandes volumes de dados, no atual contexto de forte expansão da internet das coisas, da inteligência artificial, dos sistemas autónomos e do 5G.

No âmbito da proteção de dados pessoais, é aplicável em Portugal o Regulamento (UE) n.º 2016/679, de 27 de abril de 2016, que aprovou o Regulamento Geral de Proteção de Dados (**RGPD**), e a Lei n.º 58/2019, de 8 de agosto, que assegura a execução do **RGPD** em Portugal.

A lei portuguesa, de resto, contém disposições sobre a proteção de dados pessoais especificamente aplicáveis ao contexto laboral, incluindo regras sobre a utilização de dados biométricos e sobre os meios de vigilância à distância, os quais estão regulamentados.

Para possibilitar a implementação destes diplomas são criadas e modificadas normas de padrões internacionais, criando uma correspondência entre as normas técnicas e jurídicas.

A norma ISO 27001 é um dos exemplos.

A norma visa permitir que ambientes organizacionais públicos e privados se encontrem adequados à proteção de dados exigida pelo **RGPD**, procurando sintetizar a união entre o diploma, a segurança da informação e gestão e a tecnologia de informação, o que representa uma evidência de *Compliance* digital.

Em Portugal, com o cenário recente de pandemia vivido recentemente, os ataques cibernéticos tornaram-se mais frequentes, motivados pelo crescimento exponencial do aumento do tráfego na Internet e pela adoção do regime de teletrabalho.

Perante isto, e em acréscimo à preocupação de cumprimento da legislação sobre proteção de dados, o *Compliance* digital tem sido uma preocupação cada vez maior das empresas, que se procuram proteger a si, aos seus colaboradores, clientes, fornecedores e a todos aqueles que com a empresa interajem.

7. ESTRATÉGIA PORTUGUESA ANTICORRUPÇÃO 2020-2024 (MENAC)

Em Portugal, muitas foram as medidas adotadas para prevenir e reprimir a corrupção e a fraude nos últimos anos.

Contudo, a constatação de que apenas uma visão de longo prazo, congregadora de esforços e geradora de dinâmicas ao nível dos diferentes poderes do Estado, das distintas áreas de governação e dos setores privados e social, teria capacidade para enfrentar o fenómeno da corrupção, determinou a necessidade de conceção de uma Estratégia Nacional Anticorrupção 2024 ("Estratégia"), a qual consagrou como prioridade a prevenção e detecção dos "riscos de corrupção no setor público, através, entre outras medidas, da adoção de Programas de Cumprimento Normativo no Setor Público, com base na experiência do setor privado" (Prioridade 2), bem como a necessidade de "Comprometer o setor privado na prevenção, detecção e repressão da corrupção" (Prioridade 3).

Tendo por base essas prioridades, foram criados alguns diplomas legislativos, nomeadamente, o Decreto-Lei n.º 109-E/2021, de 9 de dezembro, que criou o Mecanismo Nacional Anticorrupção (**MENAC**) e o Regime Geral da Prevenção da Corrupção (**RGPC**).

O **MENAC** assume a natureza de entidade administrativa independente, cuja missão é a promoção da transparência e da integridade na ação pública e a garantia da efetividade de políticas de prevenção da corrupção e de infrações conexas.

O **MENAC** detém poderes de iniciativa, de controle e de sanção, competindo-lhe, nomeadamente: (i) desenvolver, em conjunto com o Governo, programas e iniciativas com o objetivo de criar uma cultura de integridade e transparência, abrangendo todas as áreas da gestão pública e todos os níveis de ensino; (ii) desenvolver campanhas de prevenção da corrupção; (iii) recolher e organizar informação relativa à prevenção e repressão da corrupção e crimes conexos; (iv) emitir orientações e diretivas a que deve obedecer a conceção e termos de execução dos programas de cumprimento normativo; (v) avaliar a aplicação do **RGPC**; (vi) fiscalizar o cumprimento das normas previstas no **RGPC**.

Em suma: a criação do **MENAC**, decorrente da Estratégia, visa prevenir e detectar os riscos de corrupção no setor público, bem como comprometer o setor privado na prevenção, detecção e repressão da corrupção.

8. O FUTURO DO TRABALHO E O DIREITO À PRIVACIDADE

Face à utilização crescente de novas tecnologias, como a inteligência artificial, a chamada "internet das coisas" (*Internet of Things - IoT*) e a análise de *big data*, as preocupações com a privacidade, proteção de dados e riscos digitais têm aumentado de forma significativa.

A revolução digital e os impactos no mercado de trabalho são suscetíveis de gerar riscos ao nível da privacidade e da proteção de dados pessoais, particularmente no teletrabalho e no trabalho à distância, bem como nas plataformas digitais.

Com efeito, as novas tecnologias de informação e comunicação colocam à disposição do empregador novos meios de vigilância da atividade laboral, permitindo um controle mais intrusivo e permanente, bem como o tratamento quase ilimitado de dados pessoais.

Em face desta realidade, importa proteger a tutela do direito à privacidade e os dados pessoais.

Em Portugal, a Constituição da República Portuguesa prevê o direito à reserva da intimidade da vida privada (artigo 26.º) e o direito à proteção de dados pessoais (artigo 35.º).

A nível europeu, a tutela da vida privada resulta da Convenção Europeia dos Direitos Humanos (artigo 7.º) e da Carta dos Direitos Fundamentais da União Europeia (artigo 8.º).

A proteção de dados pessoais, por sua vez, resulta do **RGPD**, que contém uma regra específica no que diz respeito ao tratamento de dados em contexto laboral (artigo 88.º), assim como da Lei n.º 58/2019, que prevê situações específicas de tratamento de dados pessoais, em particular, no âmbito das relações laborais (artigo 28.º).

A nível estritamente laboral, importa ainda ter em conta os artigos 14.º a 22.º do Código do Trabalho, que incluem o direito à reserva da intimidade da vida privada (artigo 16.º) e a proteção de dados pessoais (artigo 17.º).

Tendo em conta, em qualquer caso, os riscos acrescidos decorrentes do incremento e massificação das novas tecnologias, o *Livro Verde Sobre o Futuro do Trabalho*, aprovado pelo Governo português em 2021, estabeleceu novas recomendações, relativas à privacidade no contexto laboral, nomeadamente as seguintes:

- Prevenir e regulamentar de modo restritivo a prática do employment background check, evitando que a avaliação do perfil e curriculum profissional do candidato a emprego seja feita com recurso a dados pessoais do próprio que não têm ligação direta com o tipo de actividade para a qual o mesmo se está a candidatar e que interferem com a sua esfera pessoal ou íntima;
- Prevenir o recurso a ferramentas que permitem monitorar e-mails, sites visitados, a quantidade de mensagens enviadas e de chamadas/reuniões realizadas, originando um significativo risco de vigilância remota dos trabalhadores em tempo real, assim como possibilitando a criação de perfis de comportamentos.

O Futuro do Trabalho passa, em suma, pela proteção da privacidade e dos dados pessoais de todas as partes envolvidas, em particular dos trabalhadores.

9. CONCLUSÃO

Conclui-se que, para garantir a efetividade de um programa de *Compliance*, torna-se fundamental avaliar os riscos envolvidos, bem como reavaliá-los de forma contínua, porquanto os negócios também estão em constante transformação, assim como a tecnologia, no fito de evitar ou mitigar danos decorrentes do mau uso ou do uso abusivo dos dados dos trabalhadores.

No Brazil, no âmbito do *Compliance* digital laboral, depreende-se que, muito embora a **LGPD** não estabeleça, expressamente, previsões aplicáveis às relações de trabalho, o tratamento de dados pesoais é fundamental nas diversas fases do contrato de trabalho, revelando-se, portanto, uma área delicada para a sua implantação e efetivo cumprimento. Pode, inclusive, ser vista como uma oportunidade para o sistema normativo brasileiro se abrir ao direito comparado, nomeadamente, ao **RGPD**.

Em Portugal, o **RGPD** e a lei nacional que assegura a sua execução (a Lei n.º 58/2019) têm disposições específicas para o contexto laboral, que se aplicam a par do Código de Trabalho, e cujo cumprimento é indispensável à implementação de um programa de *Compliance*.

Para além disso, os *stakeholders* têm exigido paridade de cuidado no tratamento de dados, uma vez que a responsabilidade por danos decorrentes de incidentes é solidária e, mais, a

conformidade no tocante aos dados dos titulares constitui-se em um valor corporativo e activo estratégico das organizações.

É importante que os profissionais da área aboral tenham especial atenção às obrigações impostas pela legislação e se prepararem para adequar as rotinas /práticas laborais às exigências de proteção de dados, principalmente através de um sistema de gestão de riscos a integrar em um eficiente programa de *Compliance* digital no contexto laboral.

© 2022 MACEDO VITORINO

This information is provided for general purposes only and does not constitute professional advice.